Performance analysis of safety instrumented systems against cascading failures during prolonged demands

Lin Xie, Mary Ann Lundteigen, Yiliu Liu

Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:
Cascading failure
Safety instrumented system
Demand
Reliability block diagram
System reliability

ABSTRACT

Cascading failures may occur in many technical systems where the failure of one component triggers successive events. Safety barriers like safety instrumented systems are installed in many industries to prevent failures and failure propagations. However, little attention has been paid to the impacts of safety instrumented systems employed to prevent cascading failures in the literature. This paper proposes a novel method for analyzing how the performance of safety instrumented systems influences the protection against and mitigation of cascading failures. It considers SIS reliability and SIS durability in the mitigation of cascading failures. The method uses recursive aggregations based on the reliability block diagram and is verified with Monte Carlo simulations. The application is illustrated with a practical case study, where the proposed method is found beneficial to identify the criticality of safety instrumented systems in consideration of their locations and performance.

1. Introduction

Cascading failures (CAFs) are multiple failures in which the failure of one component leads to high stress and a consequently high failure probability in other components [1]. CAFs are a concern for many technical systems, such as railway signaling systems, power distribution networks, process systems, industrial communication networks, and internet systems [2,3]. Functional dependencies and interactions exist commonly among components, and thus a single failure can negatively influence other parts in the same system. As a result, CAFs may cause catastrophes in technical systems without proper preventions and mitigations [4,5].

The awareness of CAFs is not new. In the past decade, much research has aimed at developing models to evaluate the effects of CAFs and associated preventive measures. These models can be categorized as topological, probabilistic, state-transition, and simulations. In the context of topological models, some efforts have been devoted to assessing mitigation measures of CAFs based on complex network theory [6–9] and graph theory [10–12]. Probabilistic models have been applied to quantify the ability of preventions against CAFs in risk propagations [13–16]. State-transition models, such as Markov processes, Petri nets, and Bayesian networks, have effectively analyzed CAFs [17–21]. Besides, simulations like the Monte Carlo simulation (MCS) have been used in analyzing the systems associated with CAFs in many application areas, including power and gas networks, traffic-power, and infrastructure systems [22–24].

To prevent CAFs, Safety instrumented systems (SISs) can install as a type of safety barrier. SISs are widely employed to reduce accidents in the process industries and other sectors [25]. An SIS applies electrical/electronic/programmable electronic (E/E/PE) technologies to detect and act upon hazardous situations arising in the assets [26]. The assets can be humans, equipment, or process sections. They are called equipment under control (EUC) in the generic standard IEC 61508 [26]. An SIS generally consists of three main subsystems: sensors (e.g., level transmitters, gas detectors, and push buttons), logic solvers (e.g., programmable logic controllers and industrial computers), and final elements (e.g., shutdown valves and circuit breakers). As illustrated in Fig. 1, the sensors detect possible abnormal situations (e.g., CAFs), and the logic solvers activate, then the final elements act according to the sensor inputs. The event upon which an SIS is activated is considered a demand [1]. A typical example of SISs to prevent CAFs is an automatic fire extinguishing system (AFES) [3]. An AFES activates when a fire or gas leakage at a tank is detected. If the SIS fails to extinguish or control the fire at a specific time, the fire can propagate and affect several facilities [27].

SIS performance is of great significance to ensure the safety of EUC systems [28]. Several indicators can reflect SIS performance, such as...
The SIS reliability is related to the ability to respond on-demand as expected. For example, when a fire occurs, an AFES is expected to start to splash water. If an SIS works on-demand, it is reliable. However, many SIS failures cannot be detected immediately after their occurrences. Instead, those failures can be revealed upon actual demands or period test intervals are fixed, the average PFD within one interval as 

\[ \text{PFD}_{\text{avg}} = \frac{1}{\lambda} \] 

is widely applied for FODs of SISs [26]. If the proof test intervals are fixed, the average PFD within one interval as \( \text{PFD}_{\text{avg}} \) is a commonly used reliability measure [22]. \( \text{PFD}_{\text{avg}} \) can be obtained by simplified formulas [1], IEC 61508 formulas [26], the PDS method [31], and Markov models [19,32].

In recent years, \( \text{PFD}_{\text{avg}} \) and SIS reliability have been intensively studied. For example, Cai et al. [28] have proposed a method for evaluating SISs with heterogeneous components based on Bayesian networks. Liu and Rausand have considered different demand modes for the SIS reliability analysis [19,33]. Alizadeh and Srimanula [34] have developed an unreliability model for redundant SISs using Markov chains. Meng et al. [35] have modeled the SIS reliability measures in AltaRica 3.0. Xie et al. [36] have considered the reliability of redundant SISs where dependent failures may occur. An analytical approach for simplification of complex Markov model has been proposed in SIS reliability analysis [37]. In addition, Ding et al. [38] have derived a diverse redundancy method based on system degradation using a reliability block diagram to evaluate the SIS reliability. Yu et al. [39] have proposed a fuzzy reliability assessment for SIS taking account of common cause failures.

However, little attention has been paid to the impacts of SISs employed to protect against CAFs. In addition, the currently defined SIS reliability is insufficient to evaluate the overall SIS performance in preventing and mitigating CAFs. That is because the demands on SISs for preventing or mitigating CAFs may not be instantaneous [3]. As a result, even though an SIS can respond to demands, it may fail afterward. For example, fires can last few seconds or several days, and AFESs must operate for a specified period to suppress fires. Such a period is defined as a prolonged demand duration. During this period, SISs are often exposed to high stress and thereby have more chances to fail.

Therefore, it is of interest to examine whether an SIS is reliable while responding and how an SIS performs after activation. The former is related to SIS reliability, whereas the latter is related to SIS durability. Durability represents how long an SIS can perform its safety instrumented function, and withstand stress. The failures related to durability are called failures \( \text{during demand (FDDs)} \) in this study. In other words, SISs that are employed against CAFs may suffer from intensive degradations and failure before demands are complete.

Considering both FODs and FDDs, it is thus challenging to use straightforward traditional methods to evaluate the SISs against CAFs. For example, fault tree analysis is often used for the specific analysis of the accident, and it is difficult to cope with dependent issues such as CAFs [40]. In addition, Markov models have a problem in dealing with a large-scale system where CAFs occur [37,41]. Furthermore, the formulas listed in IEC 61508 do not consider CAFs [42]. Therefore, a new method to assess the performance of SISs against CAFs is required.

This paper proposes a method for analyzing how SIS performance...
influences the protection against and mitigation of CAFs. This paper’s novelty and main contributions are two folds: 1) developing a new method to model SISs against CAFs and evaluate their effectiveness; 2) revealing the influences of reliability and durability of SISs on the mitigation of CAFs.

The benefits of the proposed method include the following: 1) providing precise and holistic performance analysis considering SIS reliability and durability; 2) considering time-dependent failures on SISs while responding and after activation, and there is no limitation on failure distributions; 3) offering guidelines for the SIS design and deployment to improve the reliability of EUC systems.

The rest of the paper is organized as follows. Section 2 illustrates the models of CAFs and SISs. Section 3 suggests the method for evaluating the impacts of SISs associated with their failures. In Section 4, an illustrative example is provided and is verified by Monte Carlo simulations. A practical case study in the oil and gas industry is presented in Section 5. Finally, in Section 6, we conclude and discuss future works.

2. Modeling SISs against cascading failures

2.1. Modeling cascading failures

CAFs are identified in the literature by many names, such as induced failures, domino failures, propagated failures, and interaction failures [43-45]. This paper deals with CAFs between EUC components. The case that CAFs within SISs have been studied in work [36]. CAFs are assumed to originate from a fault in an EUC component, triggering successive failures of other parts of EUC systems. For example, when an external leakage of flammable gases from a valve is detected, a failure in a control system can cause a valve miscarriage and sudden pressure increases.

In previous research [36,46-48], cascading probability γ_{ij} \in [0,1] has been introduced as a measure of propagation easiness. This measure is also employed in this paper. Given that EUC_i fails, the probability that the failure cascades to other components is γ_{ij}. The failure propagation is shown as a dotted curved arrow in Fig. 2 (a). Cascading probability influences the extent of CAFs damages. It can be estimated based on test data or historic failure records [48]. The probability that there are no CAFs is denoted by γ_i (γ_i = 1 - γ_{ij}).

2.2. Modeling SISs against CAFs

Fig. 2(b) illustrates that SIS_{ij} is installed to prevent failure propagation from EUC_j. This paper focuses on the situations that demands on SISs are prolonged (e.g., 2 hours or more). An SIS may fail due to failures in any of its three main subsystems (i.e., the sensors, logic solvers, and final elements). The failures can be classified into two groups:

- FOD refers to an event when an SIS cannot act on demands (e.g., the inability to activate an AFES). An FOD is always a dangerous undetected failure, as defined in IEC 61508 [26]. It is hidden until upon demand or in a proof test. An SIS is often considered as-good-as-new after a proof test [1]. If the proof test interval is not changed, PFD_{avg} is the same in the whole life. PFD_{avg} is also used to determine if an SIS satisfies a specified safety integrity level (SIL) [26]. IEC 61508 defines four SILs: SIL 1 (the lowest level) through SIL 4 (the highest level) [26].
- FDD refers to an event when an SIS fails during a prolonged demand (e.g., an AFES stops operating even though the fire has not been suppressed). Since an FDD is revealed immediately, it is similar to those dangerous detected failures defined in IEC 61508 [26]. The difference is that FDD is also undetectable by continuous monitoring. It is natural to assume an FDD can be found upon a demand or test. Time to FDD reflects the capability of SISs to resist stress during demands. It is reasonable to use known distributions with probability density functions f_{FDD}(t) for FDD, such as a Weibull distribution.

Fig. 3 depicts the sequence of failure events associated with Fig. 2(b). An initiating event is a hazardous event like overheating or a short circuit in the EUC system. EUC_j may fail due to hazardous events, which causes a fire. The fire can propagate to the other components with cascading probability γ_{ij}. An FOD may occur when the demand on SIS_{ij} presents. SIS_{ij} may also fail due to FDD even if it is activated. The failures in SIS_{ij}, including FOD and FDD, determine the outcomes of EUC_j.

This paper focuses on the performance of SISs starting from hazardous events, meaning that the moment t = 0 in this context is the occurrence of a hazardous event. In other words, the EUC system is assumed-as-new until t = 0. The EUC system is still functioning in a degraded mode under hazardous events. Let τ denote time that EUC_j fails, and a fire propagates from EUC_j. Then, a demand on SIS_{ij} occurs. The condition of the SIS is unknown when it needs to be activated, and it may be working or failed due to a hidden failure. An FOD may thus be observed at time τ. Let μ represent time when an FDD occurs. T_{DD} denotes a demand duration of SIS_{ij}. Fig. 4 describes failure time in EUC_i and SIS_{ij}.

Let P_{ij}(t) denote the probability that SIS_{ij} fails by time t, considering FOD and FDD. The probability P_{ij}(t) can be obtained as:

\[
P_{ij}(t) = P_r(SIS_{ij} \text{ fails by time } t)
\]

\[
= PFD(\tau) + [1 - PFD(\tau)][P(T_{DD} \leq (t - \tau))]
\]

\[
= PFD(\tau) + [1 - PFD(\tau)] \int_{0}^{\mu} f_{FDD}(t) \left[ \int_{0}^{t} f_{FDD}(\mu - t) dt \right] dt
\]

(1)

where T_{DD} denotes the operating time of SIS_{ij} from activation to the failed state. T_{DD} is assumed to be less than T_{DD}, because the demand is prolonged.

Accordingly, let P_{ij}(t) denote the probability that the SIS_{ij} functions by time t. The probability P_{ij}(t) can be obtained as:

\[
P_{ij}(t) = P_r(SIS_{ij} \text{ is functioning by time } t)
\]

\[
= [1 - PFD(\tau)][P(T_{DD} \geq (t - \tau))]
\]

\[
= [1 - PFD(\tau)] \int_{0}^{\mu} f_{FDD}(t) \left[ 1 - \int_{0}^{t} f_{FDD}(\mu - t) dt \right] dt
\]

(2)
3. Performance analysis considering CAFs and SISs

A recursive aggregation method based on reliability block diagrams (RBDs) is proposed in this section. The method builds on the previous studies of multi-state systems with failure propagation time [47]. The method in this paper is applied to EUC systems in which SISs are employed to intervene in CAF propagation. We take EUC system reliability into account in the analysis of SIS performance in the context of CAFs. The term of system reliability in the following sections refers to the reliability of EUC systems. EUC systems are constructed as typical series-parallel structures.

3.1. Reliability analysis with conditional failures

System reliability can usually be calculated with reliability functions derived from RBDs as long as there are two states of components (functioning and failed) [49]. However, when the system is subject to CAFs, the components are not independent. Consequently, the general rules for structure functions cannot be applied. Reliabilities with conditions are therefore introduced to complement the RBD method. Here, three scenarios may arise considering the states of EUC and CAFs: 1) EUC functions; 2) EUC fails, and the failure is not cascaded; 3) EUC fails, and the failure is cascaded, as shown in Fig. 5.
The conditional reliability of EUCi, denoted by $\tilde{R}_i(t)$, is defined as the probability that EUCi is functioning at time $t$ given no CAF from EUCi. No CAF phenomena include the two scenarios: 1) EUCi functions; 2) EUCi fails, and the failure is not cascaded. Hence, the probability of no CAF, denoted by $P_i(\text{No CAFs})$, is equal to $R_i(t) + \gamma_i \tilde{R}_i(t)$ or $1 - \gamma_i \tilde{R}_i(t)$. Accordingly, the probability that a CAF occurs $P_i(\text{CAF occurs})$ is equal to $\gamma_i \tilde{R}_i(t)$. The conditional reliability $\tilde{R}_i(t)$ can be described as:

$$
\tilde{R}_i(t) = \frac{P_i(\text{EUC functions})}{P_i(\text{No CAFs})} = \frac{R_i(t)}{R_i(t) + \gamma_i \tilde{R}_i(t)} = \frac{R_i(t)}{1 - \gamma_i \tilde{R}_i(t)} \quad (3)
$$

If the failure in EUCi will never be cascaded out, the conditional reliability $\tilde{R}_i(t)$ is defined to be equal to the reliability $R_i(t)$.

Consider a system $\Omega_n$ with $n$ components EUCi ($i = 1, 2, \ldots, n$) organized in a series structure. One can obtain the conditional system reliabilities by time $t$ as:

$$
\tilde{R}_{\text{series}}(t) = \prod_{i=1}^{n} \tilde{R}_i(t) \quad (4)
$$

Similarly, the conditional reliability of a parallel system with $n$ components EUCi can be obtained as:

$$
\tilde{R}_{\text{parallel}}(t) = 1 - \prod_{i=1}^{n} (1 - \tilde{R}_i(t)) \quad (5)
$$

The conditional system reliability for an arbitrary series-parallel system can be obtained based on Eqs. (4) and (5). The method is similar to the traditional RBD method [49], replacing component reliabilities by corresponding conditional reliabilities.

### 3.2. Reliability of an EUC system

This section presents the method for analyzing the reliability of an EUC system. The following assumptions are made:

- The two states are considered for EUCi functioning or failed.
- The time to failure in EUC follows a known distribution with probability density functions, denoted by $f_i(t)$.
- There are no repairs and inspections during demand durations.

First, consider a system $\Omega_n$ with $n$ components structured as a series-parallel system, and only one CAF may occur from EUCi to EUCj. If the CAF occurs and an SIS is functioning with the probability of $P_j(t)$, EUCj is protected from the CAF by the safety of the SIS. It implies that only EUCi is in a failed state at time $t$ for this system. On the contrary, when the CAF occurs and an SIS fails with the probability of $P_j(t)$, EUCj is impacted by the CAF. Both EUCi and EUCj are in failed states at time $t$. $P_j(t)$ corresponds to the conditional reliability $\tilde{R}_{\Omega_{n-1}}(t)$ in case that the SIS is functioning. Similarly, $P_i(t)$ corresponds to the conditional reliability $\tilde{R}_{\Omega_{n-1}}(t)$ in case that the SIS is in a failed state. Hence, the reliability of the system $\Omega_n$ by time $t$ is listed as follows:

$$
R_i(t) = P_i(\text{No CAFs}) \tilde{R}_{\Omega_n}(t) + P_i(\text{CAF occurs}) \left[ P_j(t) \tilde{R}_{\Omega_{n-1}}(t) + \gamma_j P_i(t) \tilde{R}_{\Omega_{n-1}}(t) \right]
$$

$$
= \left[ 1 - \gamma_i \tilde{R}_i(t) \right] \tilde{R}_{\Omega_n}(t) + \gamma_i \tilde{R}_i(t) \left[ P_j(t) \tilde{R}_{\Omega_{n-1}}(t) + P_j(t) \tilde{R}_{\Omega_{n-1}}(t) \right] \quad (6)
$$

where $\Omega_{n-1}(j)$ and $\Omega_{n-1}(\theta)$ are the subsystems with functioning components. $\tilde{R}_{\Omega_{n-1}}$ and $\tilde{R}_{\Omega_{n-1}}$ denote the corresponding conditional reliabilities of $\Omega_{n-1}(j)$ and $\Omega_{n-1}(\theta)$. The failed components can be removed when calculating system reliability, meaning that their reliabilities are replaced by zero. One can obtain $\tilde{R}_{\Omega_{n-1}}$ and $\tilde{R}_{\Omega_{n-1}}$ based on Eqs. (4) and (5).

Second, consider a system $\Omega_n$ with multiple CAFs. Subsystem $\Omega_m(\Omega_n \in \Omega_m)$ has $m$ EUC components with CAFs, denoted by CAF1, CAF2, CAF3, ... and CAFm. Cascading probabilities are $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_m$. All possible combinations of CAF occurrence are considered. The event $\theta_1$ describes no CAF in subsystem $\Omega_m$ ($\theta_1 = \text{CAF}_1 \cap \text{CAF}_2 \cap \ldots \cap \text{CAF}_m$). The event $\theta_2$ is a situation when CAFs generate from the first CAF ($\theta_2 = \text{CAF}_1 \cap \text{CAF}_2 \cap \ldots \cap \text{CAF}_m$). The event when all CAFs occur in $m$ components is denoted by $\theta_2$, ($\theta_2 = \text{CAF}_1 \cap \text{CAF}_2 \cap \ldots \cap \text{CAF}_m$). The probability $\theta_i(t)$ describes that the CAF event $\theta_i$ occurs by time $t$, and it is given as follows:

$$
\theta_i(t) = \prod_{j=1}^{m} \left[ \tilde{R}_j(t) \right]^{\text{mod}} \left( \left( \frac{1}{1 - \gamma_j} \right) \left( 1 - \tilde{R}_j(t) \right) \right) \quad (7)
$$

Assume the CAF event $\theta_i$ is connected to a specific subsystem $\Omega_i(\Omega_n \in \Omega_i)$ where CAFs are triggered from the components. Assume EUCi ($\text{EUC}_{i} \in \Omega_i$) is linked to $\Omega_i$ SISs denoted by SIS_{i1}, SIS_{i2}, SIS_{i3}, ... and SIS_{ik}. All possible combinations of the SISs’ states (i.e., functioning or failed) are considered SIS events. The event $\delta_1$ involves no SIS failure ($\delta_1 = \text{SIS}_{i1} \cap \text{SIS}_{i2} \cap \ldots \cap \text{SIS}_{ik}$). The event $\delta_1$ involves one failure in SIS_{i1} ($\delta_2 = \text{SIS}_{i1} \cap \text{SIS}_{i2} \cap \ldots \cap \text{SIS}_{ik}$). The event when all SIS fail is denoted by $\delta_2$ ($\delta_2 = \text{SIS}_{i1} \cap \text{SIS}_{i2} \cap \ldots \cap \text{SIS}_{ik}$). The probability $\delta_i(t)$ describes that EUCn fails and the SIS event $\delta_i$ occurs by time $t$, and it is given as follows:

$$
\delta_i(t) = \frac{\int_{t_0}^{t} f_i(t) \prod_{j=1}^{m} \left[ P_j(t) \right] \left( 1 - \text{mod} \left( \frac{1}{1 - \gamma_j} \right) \left( 1 - \tilde{R}_j(t) \right) \right) dt}{\int_{t_0}^{t} f_i(t) dt} \quad (8)
$$

where

$$
P_i(t) = \text{PFD}_{i \cap \theta_0} + \left( 1 - \text{PFD}_{i \cap \theta_0} \right) \int_{t_0}^{t} f_{i \cap \theta_0}(\mu - t) dt
$$
\[ Pr_h(t) = \left(1 - PF_{avg,h}\right) \left[1 - \int_{t_h}^{t} Pr_S(t - \tau) d\tau\right] \]

\( P_{hj}(t) \) is the probability that SIS\(_hj\) has failed by time \( t \), while \( Pr_h(t) \) is the probability that SIS\(_h\) is functioning at time \( t \). EUC\(_h\) fails at time \( t_h \). PF\(_{avg,h}\) denotes the steady-state probability for FOD in SIS\(_h\). SISs are critical safety barriers so that they are often designed to be highly reliable under normal conditions [50]. PF\(_D\) is relatively small and varies slightly. It is unnecessary to determine the probability as a function of time, and an average value is sufficient for FOD [1]. Furthermore, IEC 61508 distinguishes four SILs relating to PF\(_D\) rather than PF\(_D(t)\) [26]. Therefore, in Eq. (8), we use PF\(_D\)\(_{avg}\) to represent PF\(_D(t)\) approximately.

Combining all SIS events, conditional probability for the CAF event \( \theta \) by time \( t \) is obtained as:

\[ Q_{\theta}(t) = \prod_{h=1}^{m} \sum_{v=1}^{2} \delta_{h,v}(t) \tilde{R}_{h,v}(t) \tag{9} \]

where \( \Omega_{h,v} \) denotes a subsystem with the functioning EUC components, and \( \tilde{R}_{h,v}(t) \) denotes the conditional reliability by time \( t \) for the subsystem \( \Omega_{h,v} \). Eventually, system reliability can be obtained as:

\[ R_s(t) = \sum_{v=1}^{2} \theta_{\theta}(t) Q_{\theta}(t) \tag{10} \]

In short, system reliability can be obtained by applying the following steps:

1. Define a subsystem comprising \( m \) EUC components that may trigger CAFs and calculate their conditional reliabilities.
2. Generate all combinations of CAFs and compute probabilities of CAF events.
3. For each CAF event, generate all SIS states’ combinations and compute probabilities of SIS events.
4. Based on RBDs, compute conditional reliabilities for all SIS events.
5. Obtain system reliability by combining conditional reliabilities for all CAF events.

The following section introduces an example. Then, a practical case is used to present the method’s effectiveness.

### 4. Example and verifications

#### 4.1. An illustrative example

Consider a system \( \Omega_m \) with three EUC components (the RBD of this system is shown in Fig. 6). Subsystem \( \Omega_n \) represents a subsystem with \( m \) EUC components that may trigger multiple CAFs. The subsystem \( \Omega_m \) includes the components EUC\(_1\) and EUC\(_2\). The cascading possibilities are \( \gamma_1 \) and \( \gamma_2 \). SIS\(_{12}\), SIS\(_{13}\), SIS\(_{21}\), and SIS\(_{23}\) are installed to prevent and mitigate CAFs propagation. The probability of FODs is PF\(_{avg,12}\), PF\(_{avg,13}\), PF\(_{avg,21}\), and PF\(_{avg,23}\).

The reliability of the EUC system is calculated using the following five steps:

**Step 1:** According to Eq. (3), the conditional reliabilities of EUC\(_1\), EUC\(_2\), and EUC\(_3\) considering CAFs are obtained as:

\[ \tilde{R}_{1}(t) = \frac{R_{1}(t)}{1 - \gamma_{1} \tilde{R}_{1}(t)} \]

\[ \tilde{R}_{2}(t) = \frac{R_{2}(t)}{1 - \gamma_{2} \tilde{R}_{2}(t)} \]

\[ \tilde{R}_{3}(t) = \tilde{R}_{3}(t) \]

**Step 2:** By using Eq. (7), the probabilities of the CAF events are obtained as:

\[ \theta_{1}(t) = \left[1 - \gamma_{1} R_{1}(t)\right] \left[1 - \gamma_{2} R_{2}(t)\right] \]

\[ \theta_{2}(t) = \left[\gamma_{1} R_{1}(t)\right] \left[1 - \gamma_{2} R_{2}(t)\right] \]

\[ \theta_{3}(t) = \left[1 - \gamma_{1} R_{1}(t)\right] \left[\gamma_{2} R_{2}(t)\right] \]

\[ \theta_{4}(t) = \left[\gamma_{1} R_{1}(t)\right] \left[\gamma_{2} R_{2}(t)\right] \]

**Step 3:** By using Eq. (8), the probabilities of the SIS events are obtained as:

\[ \delta_{1,1}(t) = 1 \]

![Fig. 6. RBD of an EUC system with CAFs and SISs.](image)
Fig. 7. The MCS flowchart for failure propagations.
\[ \delta_{1.1}(t) = \int_{0}^{t} \left( (1 - PFD_{avg.12}) \left( 1 - f_{t_{01}}(\mu - t_1) \right) \right) \left( 1 - PFD_{avg.13} \left( 1 - f_{t_{01}}(\mu - t_1) \right) \right) \ dt_1 \]

\[ \delta_{1.2}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( PFD_{avg.12} + (1 - PFD_{avg.12}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_1) \ dt_1 \right) \left( 1 - PFD_{avg.13} \left( 1 - f_{t_{01}}(\mu - t_1) \right) \right) \ dt_1 \]

\[ \delta_{1.3}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( PFD_{avg.12} + (1 - PFD_{avg.12}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_1) \ dt_1 \right) \left( PFD_{avg.13} + (1 - PFD_{avg.13}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_1) \ dt_1 \right) \ dt_1 \]

\[ \delta_{1.4}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( PFD_{avg.12} + (1 - PFD_{avg.12}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_1) \ dt_1 \right) \left( PFD_{avg.13} + (1 - PFD_{avg.13}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_1) \ dt_1 \right) \ dt_1 \]

\[ \delta_{2.1}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( (1 - PFD_{avg.21}) \left( 1 - f_{t_{01}}(\mu - t_2) \right) \right) \left( 1 - PFD_{avg.23} \left( 1 - f_{t_{02}}(\mu - t_2) \right) \right) \ dt_2 \]

\[ \delta_{2.2}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( PFD_{avg.21} + (1 - PFD_{avg.21}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_2) \ dt_1 \right) \left( 1 - PFD_{avg.23} \left( 1 - f_{t_{02}}(\mu - t_2) \right) \right) \ dt_2 \]

\[ \delta_{2.3}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( PFD_{avg.21} + (1 - PFD_{avg.21}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_2) \ dt_1 \right) \left( PFD_{avg.23} + (1 - PFD_{avg.23}) \int_{0}^{t_1} f_{t_{02}}(\mu - t_2) \ dt_2 \right) \ dt_2 \]

\[ \delta_{2.4}(t) = \int_{0}^{t} f_{t_{01}}(t_1) \left( PFD_{avg.21} + (1 - PFD_{avg.21}) \int_{0}^{t_1} f_{t_{01}}(\mu - t_2) \ dt_1 \right) \left( PFD_{avg.23} + (1 - PFD_{avg.23}) \int_{0}^{t_1} f_{t_{02}}(\mu - t_2) \ dt_2 \right) \ dt_2 \]
Step 4: According to Eqs. (4) and (5), the conditional reliabilities of the subsystems considering CAFs can be obtained as:

\[
\begin{align*}
R_{\Omega_i}(t) &= \left[ R_i(t) + R_{\Omega_i}(t) R_i(t) \right] R_i(t) \\
R_{\Omega_{i\delta}}(t) &= R_i(t) R_{\Omega_i}(t) \\
R_{\Omega_{i\beta}}(t) &= R_i(t) R_{\Omega_i}(t) \\
R_{\Omega_{i\gamma}}(t) &= R_i(t) R_{\Omega_i}(t) = \hat{R}_{\Omega_{i\gamma}}(t) + \hat{R}_{\Omega_{i\beta}}(t) = 0
\end{align*}
\]

Step 5: The system reliability \( R_S(\cdot) \) can be calculated using Eq. (10):

\[
R_S(\cdot) = \theta_i(t) \delta_{\Omega_i}(t) \hat{R}_{\Omega_i}(t) + \theta_i(t) \delta_{\Omega_{i\delta}}(t) R_{\Omega_{i\delta}}(t) + \theta_i(t) \delta_{\Omega_{i\beta}}(t) R_{\Omega_{i\beta}}(t) + \theta_i(t) \delta_{\Omega_{i\gamma}}(t) R_{\Omega_{i\gamma}}(t)
\]

By removing the subsystems whose reliabilities with conditions are equal to zero, the system reliability can be obtained as:

\[
R_S(\cdot) = \theta_i(t) \delta_{\Omega_i}(t) \hat{R}_{\Omega_i}(t) + \theta_i(t) \delta_{\Omega_{i\delta}}(t) R_{\Omega_{i\delta}}(t) + \theta_i(t) \delta_{\Omega_{i\beta}}(t) R_{\Omega_{i\beta}}(t)
\]

Notice that the calculations regarding \( \theta_i(t) \) are excluded since the system is down when EUC1 and EUC2 fail simultaneously.

4.2. Verifications of the proposed formulas

Monte Carlo simulations (MCSs) were conducted to check the validity of the proposed method and Eq. (11) in the previous sections. Fig. 7 is a flowchart of MCSs constructed in MATLAB. The flowchart illustrates the simulation process of the example in section 4.1. The principals should be the same for different examples, but details may be modified according to the algorithm and configurations. The proposed method can be applied to any arbitrary type of failure distribution. In this case, the time to failures in EUC components is assumed to follow an exponential random variable, denoted by the time to failures in EUC components. An exponential random variable, denoted by the time to failures in EUC components, is assumed to follow an exponential random variable, denoted by \( T_i(\lambda_i) \), expresses the time to failure in EUC. A variable \( \eta \) is a random variable generated from a uniform \([0, 1]\). If \( \eta \) is smaller than cascading probability \( \gamma_\theta \), CAFs occur in the simulations. Similarly, \( \eta_1 \) is another random variable generated from a uniform \([0, 1]\). An FOD occurs when \( \eta_1 \) is smaller than FOD probability (i.e., \( PFD_{\text{avg}} \) of SISs). Time \( T_i(\Delta_{\text{FOD}}) \) denotes the simulated time to FDD of SISs, which is reflected by time \( (\mu - t_i) \) in Fig. 4. Time \( T_i \) denotes simulated time to system failure.

| Table 1 | The parameters of the illustrative example. |
|---------|----------------------------------------------|
| SIS    | EUC                                           |
|        | Failures | Parameter | Value | Parameter | Value |
| Case 1 | No SIS   | \( \lambda_1 \) | 0.2/hour | \( \gamma_1 \) | 0.5 |
| Case 2 | FOD     | \( PFD_{\text{avg}} \) | 0.1 | \( \lambda_2 \) | 0.2/hour |
|        | FDD     | \( \lambda_1 \) | 0.08/hour | \( \lambda_1 \) | 0.2/hour |
|        |         | \( \eta_1 \) | 1 | \( \eta_1 \) | 1 |
| Case 3 | FOD     | \( PFD_{\text{avg}} \) | 0.2 | \( \lambda_2 \) | 0.2/hour |
|        | FDD     | \( \lambda_1 \) | 0.16/hour | \( \lambda_1 \) | 0.1/hour |
|        |         | \( \eta_1 \) | 2 | \( \eta_1 \) | 1 |

The EUC components and SISs are assumed to be identical. Without losing generality, \( \gamma_1 \) and \( \gamma_2 \) are assigned to 0.2 and 0.3, respectively. The other parameters are presented in Table 1. Fig. 8 shows the system reliability profiles in 2 hours. Here, we run the simulations with 10^6 MC iterations. System reliability calculation using the proposed method in this paper gives the same results as the simulations for all three cases. Thus, it is demonstrated that the method in this paper is suitable for evaluating system reliability considering CAFs and SISs.

5. Case study

This section conducts a practical case study in the oil and gas industry to illustrate deploying SISs based on the proposed method. A EUC system consists of three separators (EUC1, EUC2, and EUC3), one scrubber (EUC4), and three compressors (EUC5, EUC6, and EUC7), as shown in Fig. 9. The separators separate production fluids into oil, gas, and water, and the scrubber is used to wash unwanted pollutants from the gas stream. Finally, the compressors are applied to increase gas pressure and temperature.

In this case, hazardous events like overheating or short circuits can result in failures of the EUC system. We assume that the failures in EUC2 and EUC6 can initiate fires. The fires can propagate to the components located in the same facility, as shown in Fig. 9. They cannot cause fires in the rest of the components because of separation systems like firewalls. Time to failure in an EUC component is assumed to follow a Weibull distribution with a scale parameter \( \alpha_{\text{EUC}} \) and a shape parameter \( \beta_{\text{EUC}} \). Cascading probabilities are denoted by \( \gamma_2 \) and \( \gamma_6 \). The parameters used in this case study are presented in Table 2. In general, such parameters can be obtained from historical statistics, vendor data, and equipment certifications. The failure probability of EUC components and SISs is much higher in regular operations. That is because they are supposed to be exposed to high stress in hazardous events in this case.

AFEAS are installed to suppress and extinguish fires. Each AFEAS is for the analysis generalized as SIS. As shown in Fig. 9, SIS24 and SIS25 can prevent failure propagation from EUC2, while SIS4 and SIS7 can prevent failure propagation from EUC6. For all SISs, \( PFD_{\text{avg}} \) is assigned to be 10^\(-3\) for FODs to achieve the required SIL 3 requirements, i.e., the maximum allowed value of a SIL 3 function. Time to FDD is assumed to follow a Weibull distribution with scale parameter \( \lambda_{\text{SIS}} \) and shape parameter \( \beta_{\text{SIS}} \). The parameters of SISs are summarized in Table 3.

5.1. System reliability calculation

The reliability of the EUC system can be calculated using Eq. (10). The EUC system is evaluated by considering the following states of the SISs: (1) perfect SISs, (2) SISs with FOD, and (3) SISs with FOD and FDD. Here, \( \gamma_2 \) and \( \gamma_6 \) are set at 0.5. The calculation results are shown in Fig. 10. Since we focus on the situations when demands on SISs are prolonged (e.g., 2 hours or more), it is reasonable to observe the reliability in the first two hours as an example. As seen, the reliability profiles of the EUC systems with (1) perfect SISs and (2) SISs with FOD are almost the same. That means the effects of FOD are relatively low. The reliability gap between the EUC systems with (1) perfect SISs and (3) SISs with FOD and FDD is noticeable. The effects of FDD can explain such a gap. The reason is that we focus on what happens after a hazardous event, and the probability of FOD is extremely low. The
reliability gaps can be changed when $\lambda_{SIS}$ and PFD$_{avg}$ are set differently. It implies that it is reasonable to pay more attention to the effects of FDD when considering the high stress from CAFs.

5.2. Sensitivity analysis

Given that SISs are installed, the reliability of the EUC system is impacted by the strength of CAFs (i.e., cascading probability $\gamma$) and the capacity of SISs (i.e., PFD$_{avg}$ in terms of FOD and scale parameters $\lambda_{SIS}$ for FDD). This section will carry out sensitivity analyses to understand the influences of these parameters.

5.2.1 Effects of origins of CAFs

To evaluate the impacts of CAFs, we observe the situations when cascading probabilities $\gamma_2$ and $\gamma_6$ are changed, keeping the other parameters as constants. For example, cascading probability $\gamma_2$ is increased, meaning that the failure is more likely to affect the others due to geographical location (e.g., closing to the center of an industrial area).
γ_2 and γ_6 are assigned from 0 to 0.5. The other parameters are presented in Table 2 and Table 3. The result at time t = 2 hours is provided in Figure 11. The 3D plot indicates that the system reliability is more sensitive to γ_6 than γ_2, which means that CAFs generated from EUC_6 are more critical to system reliability in this case. In other words, if EUC_6 is physically closer to other parts of the production system, the system is more vulnerable in case of fires.

5.2.2 Mitigating effects of SISs

The mitigating effects of SISs are considered in this section. Now, the cascading probabilities γ_2 and γ_6 are kept constant and set equal to 0.5, while the values of PFD_{avg} for FOD and scale parameters for FDD are changed. We assume that the same values are applied for all SISs since the SISs are identical and perform similar safety functions. The system reliabilities with increasing Log_{10}(PFD_{avg}) at the different observing times (e.g., t = 0.5, 1, 1.5, 2 hours) are presented in Fig. 12. For clarity, the ranges of SILs are SIL 1 to SIL 4. As seen, when changing Log_{10}(PFD_{avg}), the trend of the system reliability in the four subplots are approximately similar. The system reliabilities remain almost unchanged when SISs are at SIL 2 or higher. If the SIL of the SISs drops to SIL 1, the system reliabilities decrease dramatically. In other words, SISs mitigate CAFs almost as well at SIL 2 as at SIL 4. This analysis provides information on improving system reliabilities with increasing SILs regarding safety integrity. In practice, it is beneficial to determine proof test intervals of SISs to satisfy the SIL safety requirements and the EUC reliability requirements.

Fig. 13 illustrates how the system reliability is impacted when the scale parameters λ_{SIS} varies. For example, by t = 2 hours, the system reliabilities with λ_{SIS}, 1.5λ_{SIS}, 2λ_{SIS}, 2.5λ_{SIS}, 3λ_{SIS} of SISs are 0.74, 0.70, 0.66, 0.64 and 0.63, respectively. The system reliabilities do not decrease linearly with higher values of the scale parameters. Thus, it is necessary to analyze how specific SISs mitigate CAFs and deploy suitable SISs, and it will be discussed in the following sections.

5.3 Criticality analysis of SISs

Based on the method in Section 3, criticality analysis is carried out to identify optimal solutions of SISs in protecting against CAFs. We consider three variables related to optimal solutions: location, number, and cost of SISs. Specifically, risk achievement worth (RAW), denoted by I_{RAW}(SIS|t), is employed as the critical analysis. It is defined as the ratio of the system unreliability if an SIS is not present (or in the failed state) with the system unreliability if an SIS is functioning at time t [49]:

\[
I_{RAW}(SIS|t) = \frac{1 - h(0_{SIS}, R_S(t))}{1 - h(1_{SIS}, R_S(t))}
\]

Table 2
The parameters of EUC components in the case study.

| EUC_i | Components  | λ_{EUC} (/hour) | α_{EUC}  |
|-------|-------------|-----------------|----------|
| 1     | Separator 1 | 0.21            | 1.4      |
| 2     | Separator 2 | 0.12            | 1.3      |
| 3     | Separator 3 | 0.24            | 1.2      |
| 4     | Scrubber    | 0.17            | 1.5      |
| 5     | Compressor 1| 0.32            | 2.1      |
| 6     | Compressor 2| 0.32            | 2.1      |
| 7     | Compressor 3| 0.32            | 2.1      |

Table 3
The parameters of SISs in the case study.

| SIS_{ij} | λ_{SIS} (/hour) | FOD | α_{SIS} | PFD_{avg} |
|----------|-----------------|-----|---------|-----------|
| SIS_{24} | 0.42            | 2.0 | 10^{-3} |           |
| SIS_{25} | 0.33            | 2.0 | 10^{-3} |           |
| SIS_{64} | 0.41            | 2.0 | 10^{-3} |           |
| SIS_{67} | 0.18            | 2.0 | 10^{-3} |           |

Fig. 10. System reliability profiles for different states of SISs.
Fig. 11. System reliability considering $\gamma_2$ and $\gamma_6$ at $t = 2$ hours.

Fig. 12. System reliability considering $PFD_{avg}$ of SISs for FOD.
where $h(0, R_s(t))$ denotes system reliability without an SIS, while $h(1, R_s(t))$ denotes system reliability with an SIS. When $\text{plraw}(\text{SIS}|t)$ is large, the status of SIS can result in a comparatively significant change in the system reliability significantly at time $t$.

By combining Eqs. (10) and (12), $\text{plraw}(\text{SIS}|t)$ is obtained in Table 4. The parameters are shown in Table 2 and Table 3. Solution No.16 with the four SISs has the most significant effects in achieving system reliability against CAFs. On the other hand, No. 7 (SIS24, SIS64) effects are found approximately the same as ones of three SISs in solution No.12 (SIS24, SIS25, and SIS64). The reason is that the effects on preventing CAFs of solutions No.3 (SIS25), No.5 (SIS67), and their combination No.10 (SIS25, SIS67) are restricted. That implies that those SISs have less influence on the system reliability in comparison with the others.

The cost of SIS deployment can also be considered in the analysis. We assume that the installation cost is roughly the same for all SISs and equal to $\alpha$. Then, $\text{plraw}(\text{SIS}|t)/\alpha$ reflects the improvement of system reliability by installing an SIS. The analysis results are summarized in Table 4. Solution No.4 (SIS64) is the most efficient solution if only one SIS is considered. If two SISs are considered, the most efficient solutions are No.7 (SIS24, SIS64) and No.11 (SIS64, SIS67). This analysis can help the designers compare the effectiveness of solutions with a limited budget for installing SISs.

In addition to $\text{plraw}(\text{SIS}|t)$, we can also obtain the system reliability profiles to compare different solutions. For example, consider two potential solutions: No.6 (SIS24, SIS25) and No.11(SIS64 and SIS67). Fig. 14 indicates that the two solutions effectively improve system reliability, but solution No. 11 always has more significant effects in protecting against CAFs than solution No.6. It implies that SIS64 and SIS67 are more critical for the system reliability than SIS24 and SIS25. In other words, SIS64 and SIS67 can more effectively protect the 1003 subsystem (i.e., EUC5p, EUC6, EUC7) from CAFs than the others.

6. Conclusions and future research

This paper has proposed a novel method to evaluate the performance of SISs that are employed to protect the EUC system against CAFs. The method considers failures of SISs in responding and after activation and so analyzes SIS reliability and durability in performance analysis. The proposed method can provide designers and operators with information for the SIS design and deployment, thereby improving the safety and reliability of the EUC system. This paper applies the proposed method to SISs and EUC systems, but it can also be adopted in other safety barriers in industrial series-parallel systems.

The method is verified through simple applications, but it efficiently manages large systems with a limited number of CAFs. If the number increases, the combinations of CAFs grow exponentially. In that case, the
calculation efficiency of the method is expected to be further improved. However, the method is applicable for systems incorporating a moderate number of CAFs in most cases.

This paper has focused on SIS reliability and durability, but the other indicators, such as response time, capacity, and robustness, can also be important. Hence, they can be the research in the future. In addition, the assumption of constant cascading probability is somewhat restrictive; statistical dependency (e.g., time-dependent cascading probability) can be considered. Another direction of future work is extending the method to more complex systems (e.g., network systems and hierarchical systems) to investigate more interdependent relationships between SISs and CAFs.

**Authorship contributions**

The specific contributions made by each author (Lin Xie, Mary Ann Lundteigen, Yiliu Liu) is listed as below.

- Conception and design of study: Lin Xie, Mary Ann Lundteigen, Yiliu Liu;
- Acquisition analysis and interpretation of data: Lin Xie, Yiliu Liu;
- Drafting the manuscript: Lin Xie;
- Revising the manuscript critically: Mary Ann Lundteigen, Yiliu Liu.

**Declaration of Competing Interest**

All the authors of this paper certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers’ bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

**Acknowledgments**

The authors appreciate Dr. Gregory Levitin’s inspiration at the beginning of this work and valuable suggestions afterward. We also acknowledge the anonymous reviewers for their comments.

**References**

[1] Rausand M. Reliability of safety-critical systems: theory and applications. Hoboken, New Jersey, USA: John Wiley & Sons; 2014.
[2] Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 2014;121:43–60.
[3] Xing L. Cascading failures in internet of things: review and perspectives on reliability and resilience. IEEE Internet Thing J 2020;8:44–64.
[4] Cozzani V, Spadoni G, Reniers G. Approach to domino effect prevention and mitigation. Domino Effects in the process industries. MA, USA: Elsevier; 2013. p. 176–88.
[5] Abdolhamidzadeh B, Abassia T, Rashchian D, Abassia SA. Domino effect in process-industry accidents—an inventory of past events and identification of some patterns. J Loss Prev Process Ind 2011;24:575–93.
[6] Zhou J, Coit DW, Felder FA, Wang D. Resiliency-based restoration optimization for dependent network systems against cascading failures. Reliab Eng Syst Saf 2021;207:107383.
[7] Ash J, Newth D. Optimizing complex networks for resilience against cascading failure. Physica A 2007;380:673–83.
[8] Motter AE. Cascade control and defense in complex networks. Phys Rev Lett 2004;93:098701.
[9] Wang J. Mitigation strategies on scale-free networks against cascading failures. Physica A 2013;392:2257–64.
[10] Janssens J, Talarico L, Reniers G, Sørensen K. A decision model to allocate protective safety barriers and mitigate domino effects. Reliab Eng Syst Saf 2015;143:44–52.
[11] Khakzad N, Reniers G. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliab Eng Syst Saf 2015;143:63–73.
[12] Yang S, Chen W, Zhang X, Yang W. A Graph-based method for vulnerability analysis of renewable energy integrated power systems to cascading failures. Reliab Eng Syst Saf 2021;207:107354.
[13] Wu Y, Chen Z, Zhao X, Gong H, Su X, Chen Y. Propagation model of cascading failure based on discrete dynamical system. Reliab Eng Syst Saf 2021;209:107423.
[14] Landucci G, Argenti F, Tognoli A, Cozzani V. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab Eng Syst Saf 2015;143:30–43.

![Fig. 14. System reliability of the two solutions.](image-url)
[15] Bucelli M, Landucci G, Haugen S, Paltrinieri N, Cozzani V. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. Ocean Eng 2018;158:171–85.

[16] Korczak E, Levitin G. Survivability of systems under multiple factor impact. Reliab Eng Syst Saf 2007;92:269–74.

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

[18] Khakzad N, Khan F, Amyotte P, Cozzani V. Domino effect analysis using Bayesian networks. Risk Anal 2013;33:292–306.

[19] Liu Y, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prev Process Ind 2011;24:49–56.

[20] Dholepal SL, Flint MM. Series of semi-Markov processes to model infrastructure resilience under multihazards. Reliab Eng Syst Saf 2020;192:106659.

[21] Rahnamay-Naeini M, Hayat MM. Cascading failures in interdependent infrastructures: An independent Markov-chain approach. IEEE Trans Smart Grid 2016;7:1997–2006.

[22] Zou Q, Chen S. Enhancing resilience of interdependent traffic-electric power system. Reliab Eng Syst Saf 2019;191:106557.

[23] Bao M, Ding Y, Shao C, Yang Y, Wang P. Nodal reliability evaluation of interdependent gas and power systems considering cascading effects. IEEE Trans Smart Grid 2020;11:4090–104.

[24] Kong J, Simonovic SP. A model of interdependent infrastructure system resilience. Int J Safety and Secur Eng 2018;8:377–89.

[25] Liu Y. Safety barriers: Research advances and new thoughts on theory, engineering and management. J Loss Prev Process Ind 2020;104260.

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

[27] Xie L, Lundteigen MA, Liu Y. Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies. In: 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM); 2018. p. 122–7.

[28] Cai B, Li W, Liu Y, Shao X, Zhang Y, Zhao Y, et al. Modeling for evaluation of safety instrumented systems with heterogeneous components. Reliab Eng Syst Saf 2021;107823. vol. pp.

[29] Johansen IL, Rausand M. Barrier management in the offshore oil and gas industry. J Loss Prev Process Ind 2015;34:49–55.

[30] Sklet S. Safety barriers: definition, classification, and performance. J Loss Prev Process Ind 2006;19:494–506.

[31] Haugen S, Lundteigen MA, Hokstad P, Håbrekke S. Reliability prediction method for safety instrumented systems–PDS method handbook 2010 edition, 2013.

[32] Zhang N, Fouladzad M, Barros A. Optimal imperfect maintenance cost analysis of a two-component system with failure interactions. Reliab Eng Syst Saf 2018;177: 24–34.

[33] Liu Y, Rausand M. Reliability effects of test strategies on safety instrumented systems in different demand modes. Reliab Eng Syst Saf 2013;119:235–43.

[34] Alizadeh S, Siriramula S. Unavailability assessment of redundant safety instrumented systems subject to process demand. Reliab Eng Syst Saf 2018;171: 18–33.

[35] Meng H, Kloul L, Rauzy A. Modeling patterns for reliability assessment of safety instrumented systems. Reliab Eng Syst Saf 2018;180:111–23.

[36] Xie L, Lundteigen MA, Liu Y. Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures. ISA Trans 2021.

[37] Azizpour H, Lundteigen MA. Analysis of simplification in Markov-based models for performance assessment of Safety Instrumented System. Reliab Eng Syst Saf 2019; 183:252–60.

[38] Ding L, Wang H, Jiang J, Xu A. SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram. Reliab Eng Syst Saf 2017;165:170–87.

[39] Yu H, Zhao Y, Mo L. Fuzzy reliability assessment of safety instrumented systems accounting for common cause failure. IEEE Access 2020;8:135371–82.

[40] Gascard E, Simeu-Abazi Z. Quantitative analysis of dynamic fault trees by means of Monte Carlo simulations: event-driven simulation approach. Reliab Eng Syst Saf 2018;180:487–504.

[41] Guo H, Zheng C, Ju H-H-C, Fernando T. A critical review of cascading failure analysis and modeling of power system. Renew Sustain Energy Rev 2017;80:9–22.

[42] Wu S, Zhang L, Lundteigen MA, Liu Y, Zheng W. Reliability assessment for final elements of SISs with time dependent failures. J Loss Prev Process Ind 2018;51: 186–99.

[43] Abdelnoor W, Nassar D, Shereshevsky M, Gradshteyn N, Gunnalan R, Ammar HH, et al. Error propagation in software architectures. In: 10th International Symposium on Software Metrics; 2004. p. 384–93.

[44] 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; 127:14–30.

[45] Murphy D, Nguyen D. Study of two-component system with failure interaction. Naval Res Logist Q 1985;32:239–47.

[46] Xie L, Lundteigen MA, Liu Y. Reliability and barrier assessment of series-parallel systems subject to cascading failures. Proc Inst Mech Eng, Part O: J Risk Reliab 2020;234:455–69.

[47] Levitin G, Xing L, Ben-Haim H, Dai Y. Reliability of series-parallel systems with random failure propagation time. IEEE Trans Reliab 2013;62:637–47.

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

[49] Rausand M, Hayland A. System reliability theory: models, statistical methods, and applications. 2nd. Hoboken, New Jersey, USA: John Wiley & Sons; 2004.

[50] Jin H, Lundteigen MA, Rausand M. Uncertainty assessment of reliability estimates for safety-instrumented systems. Proc Inst Mech Eng, Part O: J Risk Reliab 2012; 226:646–55.