Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 740936, 12 pages
http://dx.doi.org/10.1155/2014/740936

Research Article

Unavailability Analysis for *k*-out-of-*n*:G Systems with Multiple Failure Modes Based on Micro-Markov Models

Shengjin Tang,[1] Xiaosong Guo,[1] Xiaoyan Sun,[2] Haijian Xue,[1] and Zhaofa Zhou[1]

[1] *High-Tech Institute of Xi'an, Xi'an, Shaanxi 710025, China*
[2] *Suzhou INVO Automotive Electronics Co., Ltd., Suzhou, Jiangsu 215200, China*

Correspondence should be addressed to Xiaosong Guo; guoxiaosong_1957@126.com

Received 2 January 2014; Revised 16 March 2014; Accepted 19 March 2014; Published 24 April 2014

Academic Editor: Carsten Proppe

Markov models are commonly used for unavailability analysis of redundant systems. However, due to the exploding states of Markov models for redundant systems, the states need to be merged to simplify the computation, which is called micro-Markov models. However, how to derive the failure rates and repair rates of the newly developed micro-Markov models has not been studied thoroughly. Therefore, this paper proposes detailed explanations and rules to derive the static unavailability by the micro-Markov models for the *k*-out-of-*n*:G systems with multiple failure modes. Firstly, two properties about applying the Markov models to the repairable system with independent multiple failure modes are presented. Based on these two properties, two rules are proposed for implementing the micro-Markov models. The micro-Markov models provide the exact same results for the repairable *k*-out-of-*n*:G system with multiple independent failure modes and repair mechanisms and approximate results for systems with multiple hybrid failure modes. A case study of safety integrity verification for safety instrumented systems is provided to illustrate the application of the proposed method. The conceptual comparison and numerical examples demonstrate the reasonability and usefulness of the proposed micro-Markov models.

1. Introduction

A *k*-out-of-*n*:G system (hereinafter referred to as *koon* system) is a redundant system where at least *k* out of *n* components (or channels) must be functional for the redundant system to be successful [1–3]. Due to the fault-tolerant ability of the *koon* system, it has been widely used in process industry, oil and gas industry, nuclear industry, and so forth. Reliability analysis for *koon* systems is a classic issue in reliability engineering. For the *koon* system with a single failure mode, it is easy to derive the system reliability whether the system could be repaired immediately or not [4]. However, many systems have multiple failure modes [5–8], which increases the complexity of the reliability analysis. A typical system with multiple failure modes is the safety instrumented system (SIS), which has been widely used in the process industry as an important protection layer to prevent hazardous events or mitigate their consequences [3, 9–11]. Due to the self-diagnostic function of the SIS, the dangerous failure of the SIS can be divided into dangerous detected (DD) failure and dangerous undetected (DU) failure. The DD failure, which is detected by the self-diagnostic function, can be repaired immediately. However, the DU failure can only be detected and repaired in the proof test. As the static unavailability is an important value in the reliability analysis for safety systems [9–25], this paper focuses on the static unavailability evaluation for *koon* systems with multiple failure modes.

There are many modeling techniques for unavailability analysis of *koon* systems with multiple failure modes, for example, simplified equations [9–15], reliability block diagram (RBD) [16], fault tree analysis (FTA) [17, 18], and Markov analysis (MA) methods [19–21]. Rouvroye and Van den Bliek [22] compared these techniques and obtained the following conclusion: FTA and RBD are intuitive and easy to model; however, a new model has to be established for evaluating a new parameter by FTA and RBD. MA covers most aspects that affect reliability and can describe the

dynamic transitions among different system states. Therefore, the MA method has been widely used in the unavailability analysis of complex systems [19–25]. However, the states of Markov models increase explosively as the system becomes more complex, and it is fallible and time-consuming to create Markov models manually. Knegtering and Brombacher [19] proposed micro-Markov models for quantitative safety assessment for SISs, where the RBD of the system is first developed and redefined, and then the micro-Markov models are established from the redefined RBD. However, how to derive the failure rates and repair rates of the newly developed micro-Markov models has not been presented in detail. Guo and Yang [21] presented an automatic Markov modeling method to reduce the burden of computation, where the states that have identical transition rates to common states are merged. However, the states with nonidentical transition rates have not been merged.

Another issue about the micro-Markov models is to transform the nonrepairable failure into the repairable failure. If the failure modes are all nonrepairable, the system reliability can be addressed by the classical probability analysis methods, for example, RBD method [15]. Otherwise, if the failure modes are all repairable, Markov models could be used. However, many systems include repairable and nonrepairable failure modes simultaneously, which is called hybrid failure modes in this paper. Take the SIS for example; the DU failure can be regarded as the nonrepairable failure mode which is only repaired in the proof test, while the DD failure is repairable. For the hybrid failure modes, using the MA method directly could result in heavy computation to derive the analytical formulas of reliability since the system is trapped in the absorbing state of the nonrepairable failure.

There are two main ways to solve this problem. The first way is regarding the repairable failure as a failure with static failure probability, and thus the system reliability can be analyzed by the FTA method [17]. However, it is complex to build the fault trees for highly redundant systems. The second way is transforming the nonrepairable failure as the repairable failure, which is called the approached MA method in [23, 24]. The approached MA method has already been applied to the low redundant system, for example, 1oo1 system, 1oo2 system, and 2oo3 system [20, 23–26], and the accuracy is satisfied. However, whether the approached MA method could be applied to the highly redundant system and how to derive the approached Markov models for a general *koon* system have not been presented in detail.

From the above review of the related researches, it can be observed that there are two main issues remaining to be solved. The first is how to merge the states for the *koon* systems with multiple failure modes, which is central to the micro-Markov models. The second is how to transform the nonrepairable failure as the repairable failure for the general *koon* system. In response to these two issues, a property about applying the Markov models to the repairable system with a single failure mode is first presented. Based on this property, we present a rule for transforming the nonrepairable failure to a repairable failure for the general *koon* system. This is the first contribution of this paper. Secondly, the states of the *koon* system with multiple failure modes are merged, and thus the *koon* system with multiple failure modes can be transformed to that with a single failure mode. A property regarding this transformation is proposed. This is the second contribution of this paper since the states can be merged reasonably. Then, two rules are proposed for implementing the micro-Markov models based on these two properties. Additionally, we present a case study about the safety integrity verification of the SIS and obtain the simplified equations. Finally, a conceptual comparison and a numerical example are presented to illustrate the application and usefulness of the proposed method.

The remainder of this paper is organized as follows. Section 2 introduces the associated acronyms, notations, and assumptions. Section 3 presents two properties about applying the Markov models to the repairable system and proposes the mechanism regarding how to merge the states for a general *koon* system. In Section 4, we apply the results obtained in Section 3 to a case study about the safety integrity verification for the SIS and provide a numerical example to illustrate the application and usefulness of the proposed method. Section 5 concludes the paper with a discussion.

2. Acronyms, Notations, and Assumptions

2.1. Acronyms

CCF: common cause failure

DD: dangerous detected failure

DU: dangerous undetected failure

FTA: fault tree analysis

koon: *k*-out-of-*n*:G system

MA: Markov analysis

RBD: reliability block diagram

SIL: safety integrity level

SIS: safety instrumented system.

2.2. Notations

C_n^k: number of combinations of size "k" from a set with "n" components

A_n^k: number of permutations of size "k" from a set with "n" components

DC_D: dangerous diagnostic coverage coefficient

$F(t)$: failure probability function,

MDT: mean down time

MRT: mean repair time

MTTR: mean time to restoration

P_j: the steady state probability of state j

PFD: probability of dangerous failure on demand

PFD_{avg}: average probability of dangerous failure on demand

t_a: the mean time when the system failure due to the undetected failures occurs over the interval $[0, T_1]$

t_d: the duration of time after system failure due to the undetected failures

T_1: proof test interval

λ_D: dangerous failure rate

λ_{DD}: dangerous detected failure rate

λ_{DU}: dangerous undetected failure rate

μ_{DD}: repair rate for dangerous detected failure

μ_j: the repair rate for a *koon* system from state j to state $j-1$

μ_j': the repair rate for a *koon* system from state j to state $j-1$ with considering the CCF

β: beta factor for DU failures

β_D: beta factor for DD failures.

2.3. Assumptions

(i) All the n components in a *koon* system are identical and independent.

(ii) The failure modes in one component are identical with those in other components (i.e., with the same failure rates and repair rates).

(iii) The failure modes in one component are independent of each other and independent of the failure modes in other components.

(iv) The unrepairable failure mode can only be detected in a proof test (T_1), and if detected it is repaired in the time of MRT (mean repair time).

(v) The repairable failure mode can be detected and repaired immediately. If the repairable failure of a component is being repairing, the component is not functioning.

3. Modeling *koon* Systems by the Micro-Markov Models

3.1. A Property of Modeling koon Systems with a Single Repairable Failure Mode. In this subsection, we use the Markov models to model the *koon* system with a single repairable failure mode and derive a property of the modeling process. The property is summarized in the following proposition. The proposition is based on the assumption that the failure of any component is independent of other components.

Proposition 1. *For a koon system, let λ and μ be, respectively, the failure rate and repair rate of a single component and let μ_j be the repair rate from the state with j failed components to the state with $(j-1)$ failed components as shown in Figure 1. (The repair rate from the state with j failed components to the state with $(j-1)$ failed components is affected by the dependence of the repairs. If there are n repair crews existing, then $\mu_j = j\mu$. If only one repair crew exists, then $\mu_j = \mu$. To represent a general condition, we use μ_j to describe the failure rate.) Then the following holds.*

(1) *The mean down time (MDT) of a 1oon system (MDT_{1oon}) is $1/\mu_n$.*

(2) *For any koon system, $\mu_j = 1/MDT_{1ooj}$, where MDT_{1ooj} represents the MDT of a 1ooj system.*

Proof. For a 1oo*n* system, the system fails only in state n and the MDT of the 1oo*n* structure is $1/\mu_n$. For a *koon* system as shown in Figure 1, it can be observed that when the process enters state j with j faults, the repair team will start repairing and will bring the system to state $j-1$ after a mean repair time of $1/\mu_j$. As the j failure components are independent of the other $n-j$ working components, the mean repair time from state j to state $j-1$ ($1/\mu_j$) is equal to the MDT of a 1oo*j* system. This completes the proof. □

The second result of Proposition 1 demonstrates the relationship between the repair rates and the MDTs of the 1-out-of-j systems. This relationship provides a reasonable way to transform the nonrepairable failure to the repairable failure or to combine the multiple failure modes to a single failure mode. Based on Proposition 1, we propose novel micro-Markov models in the following subsection.

3.2. Micro-Markov Models for koon Systems with Multiple Repairable Failure Modes. As mentioned above, multiple failure modes exist widely in redundant systems. Therefore, it is necessary to combine the multiple failure modes to reduce the burden of computation. In the following, we first propose micro-Markov models for *koon* systems with two repairable failure modes as illustrated in Proposition 2. The assumption of Proposition 2 is that the failure and repair of any component are independent of that of other components.

Proposition 2. *For a koon system, each component has two failure modes with failure rates λ_1 and λ_2, and the repair rates of the two components are μ_1 and μ_2, respectively. The state unavailability of the koon system with two failure modes equals a transformed koon system with a single failure mode, whose failure rate and failure rate are $\lambda_m = \lambda_1 + \lambda_2$ and $\mu_m = \lambda_m\mu_1\mu_2/(\lambda_1\mu_2 + \lambda_2\mu_1)$, respectively. Moreover, the transformed koon system has independent failure and repair rate.*

Proof. As the derivation of Proposition 2 changes due to the size of the system, we only give detailed derivation for a duplicate system for an illustrative purpose. The derivation for other systems, for example, one component system and triplicate system, is similar. The Markov states transition diagram for a duplicate system is shown in Figure 2.

From Figure 2(a), we derive the transition matrix for the original duplicate system as follows:

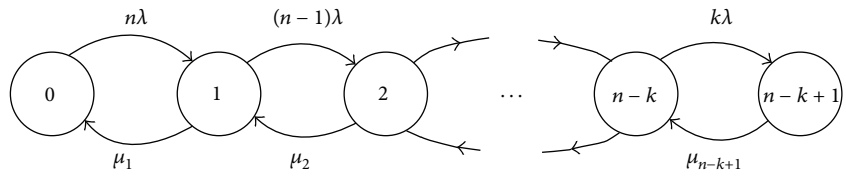

Figure 1: Markov states transition diagram for a *koon* system.

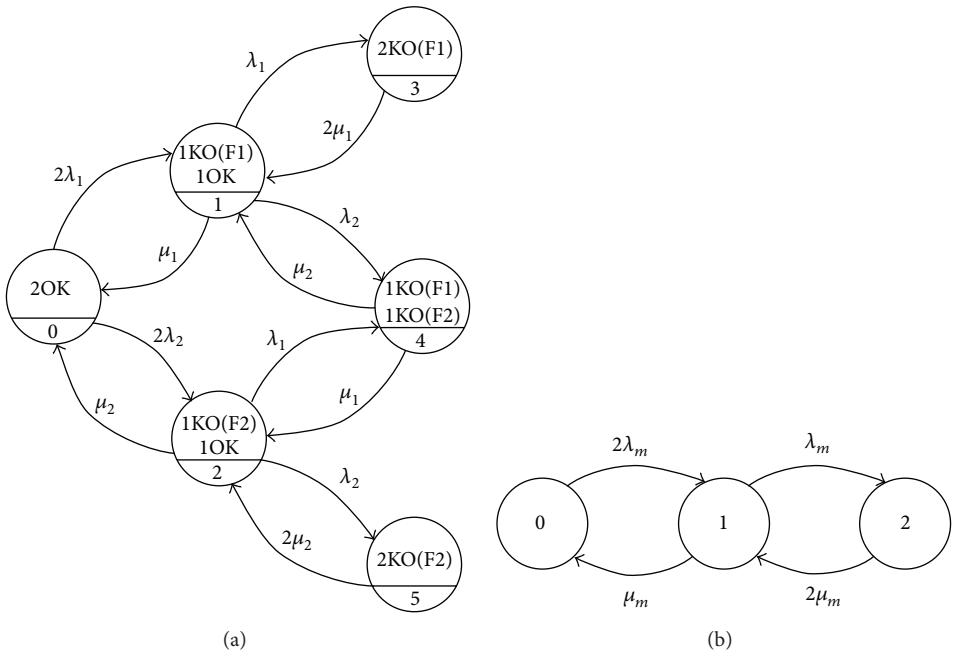

Figure 2: Markov states transition diagram for a duplicate system. ((a) Original duplicate system with two failure modes; (b) transformed duplicate system with a single failure mode).

$$M = \begin{bmatrix} -2(\lambda_1+\lambda_2) & 2\lambda_1 & 2\lambda_2 & 0 & 0 & 0 \\ \mu_1 & -\lambda_1-\lambda_2-\mu_1 & 0 & \lambda_1 & \lambda_2 & 0 \\ \mu_2 & 0 & -\lambda_1-\lambda_2-\mu_2 & 0 & \lambda_1 & \lambda_2 \\ 0 & 2\mu_1 & 0 & -2\mu_1 & 0 & 0 \\ 0 & \mu_2 & \mu_1 & 0 & -\mu_1-\mu_2 & 0 \\ 0 & 0 & 2\mu_2 & 0 & 0 & -2\mu_2 \end{bmatrix}. \tag{1}$$

Let p_j $(j = 0, 1, 2, \ldots, 5)$ represent the steady state probability of state j for the original duplicate system; then, we have

$$\begin{gathered} [p_0 \;\; p_1 \;\; \cdots \;\; p_5]\, M = [0 \;\; 0 \;\; \cdots \;\; 0], \\ p_0 + p_1 + \cdots + p_5 = 1. \end{gathered} \tag{2}$$

By solving the above equations, we have

$$\begin{gathered} p_0 = \frac{\mu_1^2\mu_2^2}{Q}, \qquad p_1 = \frac{2\mu_1\mu_2^2\lambda_1}{Q}, \\ p_2 = \frac{2\mu_1^2\mu_2\lambda_2}{Q}, \qquad p_3 = \frac{\mu_2^2\lambda_1^2}{Q}, \\ p_4 = \frac{2\mu_1\mu_2\lambda_1\lambda_2}{Q}, \qquad p_5 = \frac{\mu_1^2\lambda_2^2}{Q}, \\ \text{where } Q = (\mu_1\mu_2 + \mu_1\lambda_2 + \mu_2\lambda_1)^2. \end{gathered} \tag{3}$$

From Figure 2(b), let P_j $(j = 0, 1, 2)$ represent the steady state probability of state j for the transformed duplicate system; the following result can be obtained after some manipulations:

$$P_0 = \frac{\mu_m^2}{(\lambda_m + \mu_m)^2},$$

$$P_1 = \frac{2\lambda_m\mu_m}{(\lambda_m+\mu_m)^2},$$
$$P_2 = \frac{\lambda_m^2}{(\lambda_m+\mu_m)^2}. \tag{4}$$

Substituting $\lambda_m = \lambda_1 + \lambda_2$ and $\mu_m = \lambda_m\mu_1\mu_2/(\lambda_1\mu_2 + \lambda_2\mu_1)$ into (4) yields

$$P_0 = \frac{\mu_1^2\mu_2^2}{Q} = p_0,$$
$$P_1 = \frac{2\mu_1\mu_2(\mu_1\lambda_2+\mu_2\lambda_1)}{Q} = p_1 + p_2, \tag{5}$$
$$P_2 = \frac{(\mu_1\lambda_2+\mu_2\lambda_1)^2}{Q} = p_3 + p_4 + p_5.$$

This completes the proof. □

Proposition 2 is based on the result of Proposition 1. To transform the multiple failure modes to a single failure mode, the MDT of any 1-out-of-j system is calculated by adding the individual MDTs of the two failure modes, that is, $1/(j\mu_1)$ and $1/(j\mu_2)$, in direct proportion to each failure's contribution to the failure probability of the system. Thus, we have

$$\begin{aligned}\mathrm{MDT}_{1\mathrm{oo}j} &= \frac{\lambda_1}{\lambda_m j\mu_1} + \frac{\lambda_2}{\lambda_m j\mu_2} \\ &= \frac{1}{j}\left(\frac{\lambda_1}{\lambda_m\mu_1} + \frac{\lambda_2}{\lambda_m\mu_2}\right) = \frac{1}{j}\mathrm{MDT}_{1\mathrm{oo}1}.\end{aligned} \tag{6}$$

Similar procedure to derive the system MDT has also been presented in Chapter 9.3 in [27]. Let $1/\mu_m = \lambda_1/\lambda_m\mu_1 + \lambda_2/\lambda_m\mu_2$; that is, $\mu_m = \lambda_m\mu_1\mu_2/(\lambda_1\mu_2 + \lambda_2\mu_1)$; the novel *koon* system with a single failure mode can be derived.

Proposition 2 demonstrates how to transform the *koon* system with two failure modes to that with a single failure mode. It can also be generalized to the *koon* system with multiple failure modes, which is summarized in Proposition 3.

Proposition 3. *For a koon system, each component has l failure modes with failure rates $\lambda_1, \lambda_2, \ldots, \lambda_l$, and the repair rates of these l failure modes are $\mu_1, \mu_2, \ldots, \mu_l$. The state unavailability of the koon system with multiple failure modes equals the transformed koon system with a single failure mode, whose failure rate and the inverse of the failure rate are $\lambda_m = \sum_{i=1}^{l}\lambda_i$ and $1/\mu_m = \sum_{i=1}^{l}\lambda_i/\lambda_m\mu_i$, respectively. Moreover, the transformed koon system has independent failure rates and repair rates.*

Proof. Mathematical induction is used to prove Proposition 3. From Proposition 2, it can be observed that the *koon* system with two failure modes is equivalent to the transformed system with a single failure mode. Assume that the *koon* system with l failure modes is equivalent to the transformed system with a single failure mode with failure rate $\lambda_m = \sum_{i=1}^{l}\lambda_i$ and repair rate, whose inverse is $1/\mu_m = \sum_{i=1}^{l}\lambda_i/\lambda_m\mu_i$. Therefore, the *koon* system with $l+1$ failure modes can be transformed to the system with two failure modes. The failure rates of the two transformed modes are, respectively, λ_m and λ_{l+1}, and the repair rates are μ_m and μ_{l+1}. Based on Proposition 2, the two failure modes of the transformed system could continue to be combined, and thus the failure rate and repair rate of the final transformed system can be written as follows:

$$\lambda_m' = \lambda_m + \lambda_{l+1} = \sum_{i=1}^{l+1}\lambda_i,$$
$$\frac{1}{\mu_m'} = \frac{\lambda_m}{\lambda_m'\mu_m} + \frac{\lambda_{l+1}}{\lambda_m'\mu_{l+1}} = \sum_{i=1}^{l+1}\frac{\lambda_i}{\lambda_m'\mu_i}. \tag{7}$$

This completes the proof. □

Compared with Proposition 1, Propositions 2 and 3, add an assumption that the repair rates are independent. In other words, Propositions 2 and 3 are correct on condition that there are n repair crews for a *koon* system. Although Propositions 2 and 3 may not be strictly correct when the repair rates are not independent, it provides a reasonable way to combine the multiple modes together.

3.3. The Rules of the Micro-Markov Models. Overall, from the above analysis of applying the Markov models to *koon* systems with multiple failure modes, we obtain two rules of the micro-Markov modes.

Rule 1. For a *koon* system, the repair rate from the state with j failed components to the state with $(j-1)$ failed components can be represented by the inverse of the MDT of the 1-out-of-j system.

Rule 2. For a *koon* system with l failure modes, it can be transformed to a novel system with a single failure mode. The failure rate and repair rate of the transformed system fit the following criteria:

$$\lambda_m = \sum_{i=1}^{l}\lambda_i,$$
$$\frac{1}{\mu_m} = \sum_{i=1}^{l}\frac{\lambda_i}{\lambda_m\mu_i}. \tag{8}$$

Note that Rule 1 is strictly correct for the repairable system and Rule 2 is strictly correct for the repairable system with multiple independent failure modes. However, whether these rules could derive satisfactory results for the system with nonrepairable failure modes or hybrid failure modes has not been demonstrated; we address this issue in the next section through a case study.

4. A Case Study

4.1. Safety Integrity Level Verification. Safety instrumented systems (SISs) are widely used in the process industry as

an important protection layer to prevent hazardous events or mitigate their consequences. Safety integrity level (SIL) is proposed to measure how well a SIS performs its intended function by the safety standards: IEC 61508 and IEC 61511 [9, 10]. And SIL verification is to verify that whether the reliability of the SIS meets the required level. For the low demand mode of SIS operation, the SIL of a SIS is defined in terms of the average probability of failure on demand (PFD_{avg}), which could be represented by the static unavailability of the system. The relation between the SIL and the PFD_{avg} is shown in Table 1.

The PFD_{avg} evaluation is concerned with the voting logic of the redundant systems, failure rates, diagnostic coverage, proof test interval, common cause failure (CCF), and some other factors [3]. Since the SIL verification is provided as a case study to validate the results of the micro-Markov models, we mainly consider the dangerous failure and its repair time. The dangerous failure with failure rate λ_D means the failure to perform the protective function when required. Due to the self-diagnostic function of SIS, the dangerous failure can be divided into DU failure and DD failure with the failure rates of λ_{DD} and λ_{DU}, respectively. Consider

$$\lambda_D = \lambda_{DU} + \lambda_{DD}. \tag{9}$$

Additionally, diagnostic coverage of dangerous failure (DC_D), expressed as a percentage, is represented by the ratio of DD failure to the total dangerous failure.

As discussed previously, the repair mechanisms of the DU failure and DD failure are different; thus it is difficult to derive the analytical PFD_{avg} by using Markov models directly. Therefore, the simplification equations of PFD_{avg} have been presented, for example, the typical simplified equations by IEC 61508. However, since IEC 61508 does not give detailed explanations of PFD_{avg} calculations, which are difficult to understand for common safety engineers. Even in the IEC 61508 committee, the issues, how to calculate PFD_{avg} and which models should be used, are controversial [4].

In order to give detailed explanations to the simplified equations by IEC 61508, Zhang et al. [20] redefined the equivalent MDT of the undetected failure and derived the equivalent MDTs of 1oo1 and 1oo2 architectures. Then, the PFD value of a few typical architectures was calculated by the MA method. Guo and Yang [16] calculated the equivalent MDT by using the ratio of steady failure probability to the steady failure frequency and evaluated the PFD value for the most used architectures by the RBD method. However, these obtained results are different from the equations given by the IEC 61508 standard [9], which may confuse the safety engineers. Innal [23] explained the analytical formulas presented in the IEC 61508 by the approached Markov model. This paper attempts to solve this problem by the two rules of the micro-Markov models proposed in Section 2. The key issue of the micro-Markov models is to derive the repair rate of the states, which is handled in the next subsection.

4.2. Equivalent MDT. From Rule 1, it can be observed that the repair rate is determined by the MDT of the 1oo$n$ system. As the DD failure is repairable, we first calculate the MDT of the DU failure, which is called equivalent MDT time for the SISs. It is assumed that the DU failure is only detected in the proof test with the interval of T_1. The MDT is generated from the time of the DU failure to the proof test and the repair time, as shown in Figure 3. In the figure, t is the time when the DU failure occurs, MRT is the mean repair time if the DU failure is detected in the proof test, t_a is the mean time when system failure due to the DU failures occurs over the interval $[0, T_1]$, and t_d is the duration of the down time.

Table 1: SIL for the low demand mode of operation.

SIL	PFD_{avg}
4	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-2}$ to $<10^{-1}$

Zhang et al. [20] gave a clear definition of the equivalent MDT for the DU failure and provided the result of the equivalent MDT for the 1oo1 system and 1oo2 system. However, it is not applicable to the case when the system size changes. Thus, we attempt to calculate the equivalent MDT for a common 1-out-of-n system.

For a 1oo$n$ system, the cumulative distribution function for the DU failure is

$$F(t) = \left(1 - e^{-\lambda_{DU} t}\right)^n. \tag{10}$$

Hence, the mean time when system failure due to the DU failures occurs over the interval $[0, T_1]$ (t_a) can be formulated as

$$\begin{aligned} t_a &= \frac{\int_0^{T_1} tF'(t)\,dt}{\int_0^{T_1} F'(t)\,dt} = \frac{T_1 F(T_1) - \int_0^{T_1} F(t)\,dt}{F(T_1)} \\ &= T_1 - \frac{\int_0^{T_1} \left(1 - e^{-\lambda_{DU} t}\right)^n dt}{\left(1 - e^{-\lambda_{DU} T_1}\right)^n}. \end{aligned} \tag{11}$$

Set $u = \lambda_{DU} t$ and $x = \lambda_{DU} T_1$; then we get

$$\begin{aligned} t_a &= T_1 - T_1 \frac{\int_0^x (1 - e^{-u})^n du}{x(1 - e^{-x})^n} = T_1 - T_1 \frac{\int_0^x \left(u^n + o\left(u^n\right)\right) du}{x\left(x^n + o\left(x^n\right)\right)} \\ &= T_1 - T_1 \frac{(1/(n+1))\, x^{n+1} + o\left(x^{n+1}\right)}{x^{n+1} + o\left(x^{n+1}\right)}. \end{aligned} \tag{12}$$

Since $x = \lambda_{DU} T_1 \ll 1$, t_a can be approximately calculated as

$$t_a \approx \frac{n}{n+1} T_1. \tag{13}$$

From (13), it can be observed that the approximate value of t_a is independent of λ_{DU}.

Referring to Figure 3, the approximation of the equivalent MDT of DU failures for a 1-out-of-n system is

$$\mathrm{MDT}_{1oon}^{DU} = T_1 - t_a + \mathrm{MRT} \approx \frac{1}{n+1} T_1 + \mathrm{MRT}. \tag{14}$$

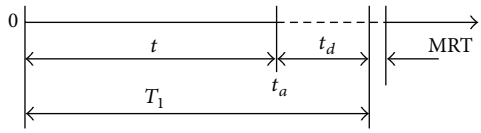

Figure 3: Failure process of the DU failure.

The DD failure is detected by the self-diagnostic function of SISs and can be repaired immediately in the time of MTTR, which denotes the mean time to restoration for the DD failure. It is assumed that the failure and repair rate of the DD failure are independent. Thus, from Proposition 1, the MDT of DD failures for the 1-out-of-n system can be formulated as

$$\mathrm{MDT}_{1oon}^{\mathrm{DD}} = \frac{\mathrm{MTTR}}{n}. \tag{15}$$

Based on Rule 2, the equivalent MDT of the combined two failure modes for the 1-out-of-n system (MDT_{1oon}) can be calculated based on the law of total probability. It is composed of the MDT of the DU failure with a conditional probability $\lambda_{\mathrm{DU}}/\lambda_D$ and the MDT of the DD failure with a conditional probability $\lambda_{\mathrm{DD}}/\lambda_D$. Then, we have

$$\begin{aligned}\mathrm{MDT}_{1oon} &= \frac{\lambda_{\mathrm{DU}}}{\lambda_D}\mathrm{MDT}_{1oon}^{\mathrm{DU}} + \frac{\lambda_{\mathrm{DD}}}{\lambda_D}\mathrm{MDT}_{1oon}^{\mathrm{DD}} \\ &= \frac{\lambda_{\mathrm{DU}}}{\lambda_D}\left(\frac{1}{n+1}T_1 + \mathrm{MRT}\right) + \frac{\lambda_{\mathrm{DD}}}{\lambda_D}\frac{\mathrm{MTTR}}{n}.\end{aligned} \tag{16}$$

After determining the component equivalent MDT for the 1-out-of-n system, the repair rate can be represented by the inverse of the equivalent MDT. Then, the $\mathrm{PFD}_{\mathrm{avg}}$ of the $koon$ system can be analyzed, as illustrated in the next subsection.

4.3. PFD_{avg} Calculation by Micro-Markov Models. For the $koon$ system, the system fails when at least $n - k + 1$ components fail. The micro-Markov state transition diagram could be represented by Figure 1. Let P_j $(j = 0, 1, 2, \ldots, n)$ represent the steady state probability; from Figure 1, we derive the transition matrix as follows:

$$M = \begin{bmatrix} -n\lambda_D & n\lambda_D & & & 0 \\ \mu_1 & -\mu_1 - (n-1)\lambda_D & (n-1)\lambda_D & & \\ \ddots & \ddots & \ddots & & \\ & \mu_{n-k} & -\mu_{n-k} - k\lambda_D & k\lambda_D & \\ 0 & & \mu_{n-k+1} & -\mu_{n-k+1} & \end{bmatrix}, \tag{17}$$

where μ_j is inverse of $\mathrm{MDT}_{1oo j}$.

Let P_j $(j = 0, 1, 2, \ldots, n)$ represent the steady state probability of state j; then we have

$$\begin{aligned}\begin{bmatrix} P_0 & P_1 & \cdots & P_{n-k+1} \end{bmatrix} M &= \begin{bmatrix} 0 & 0 & \cdots & 0 \end{bmatrix}, \\ P_0 + P_1 + \cdots + P_{n-k+1} &= 1.\end{aligned} \tag{18}$$

By solving the above equations, we have

$$\begin{aligned}P_{n-k+1} &= \left[1 + \sum_{j=0}^{n-k} \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_D^{n-k+1-j}}\right]^{-1}, \\ P_j &= \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_D^{n-k+1-j}} P_n \quad \text{for } j < n-k+1.\end{aligned} \tag{19}$$

Then, the PFD_{koon} can be written as

$$\begin{aligned}\mathrm{PFD}_{koon} &= P_{n-k+1} \\ &= 1 \times \left(1 + \sum_{j=0}^{n-k} \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_D^{n-k+1-j}}\right)^{-1}.\end{aligned} \tag{20}$$

4.4. PFD_{avg} Calculation with Considering the CCF. Common cause failure (CCF) is a phenomenon which mitigates the effects of redundancy, and thus it often plays a dominating role for the unavailability of a $koon$ system. CCF is a dependent failure when two or more redundant components fail simultaneously or within a short time interval, due to a shared cause. There are several models for quantification of CCF in SISs, such as β-factor model [9], multiple beta factor (MBF) [28, 29] model, and the PDS model [30]. The β-factor model, as suggested by IEC 61508, is the most popular CCF model due to its simplicity. The β-factor represents the fraction of the total failure rate that can cause all channels to fail. Therefore, the existence of CCF splits the DD failure and DU failure into independent failure parts and CCF parts, which can be, respectively, expressed as follows:

$$\begin{aligned}\lambda_{\mathrm{DU}} &= (1-\beta)\lambda_{\mathrm{DU}} + \beta\lambda_{\mathrm{DU}}, \\ \lambda_{\mathrm{DD}} &= (1-\beta_D)\lambda_{\mathrm{DD}} + \beta_D\lambda_{\mathrm{DD}}.\end{aligned} \tag{21}$$

If the β-factor model is used to model CCF, the CCF part can be regarded as an independent part with the independent failures in the reliability block diagram of the $koon$ system and thus the CCF can be included as an add-on to the system

unavailability. Then, the PFD_{koon} with CCF can be calculated as

$$\begin{aligned}\mathrm{PFD}_{koon}^{\mathrm{CCF}} &\approx 1 \times \left(1 + \sum_{j=0}^{n-k} \frac{(k-1)!\mu'_{j+1}\mu'_{j+2}\cdots\mu'_{n-k+1}}{(n-j)!{\lambda'_D}^{n-k+1-j}} \right)^{-1} \\ &\quad + \beta\lambda_{\mathrm{DU}} \left(\frac{T_1}{2} + \mathrm{MRT} \right) + \beta_D\lambda_{\mathrm{DD}}\mathrm{MTTR},\end{aligned} \tag{22}$$

where $\lambda'_D = (1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_D)\lambda_{\mathrm{DD}}$ and $1/\mu'_j = ((1-\beta)\lambda_{\mathrm{DU}}/\lambda'_D)((1/(j+1))T_1 + \mathrm{MRT}) + ((1-\beta_D)\lambda_{\mathrm{DD}}/\lambda'_D)(\mathrm{MTTR}/j)$. The derived equations of PFD_{koon} in (20) and (22) can also be regarded as simplified equations for the SIL verification.

4.5. Conceptual Comparison. From the above derivation of the PFD_{koon}, it can be observed that there are two main steps of transforming the DU failure and DD failure into a single failure mode. The first is transforming the DU failure as a repairable failure. The second is combining the two failure modes to a single failure mode. In order to compare the results of the micro-Markov models with the actual results, we present a conceptual comparison in this subsection. As the unavailability equations of the CCF part are the same in different methods, we only compare the independent part of the unavailability. The numerical comparison of some typical *koon* systems is presented in the next subsection.

Firstly, the results of transforming the DU failure into a repairable failure are compared with the actual results. For the DU failure, the exact results can be derived by the classic probability method, for example, the RBD method or the FTA method. To implement the comparison, the mean repair time of λ_{DU} is assumed to be zero (i.e., MRT = 0) and the CCF is not considered (i.e., $\beta = 0$ and $\beta_D = 0$). Then, we propose the following proposition.

Proposition 4. *Let PFD_{koon}^{m} and PFD_{koon}^{c} represent the PFD_{avg} calculated by the transformed Markov models and the classic probability method, respectively; then, the following holds on condition that $\lambda_{DU}T_1 \ll 1$:*

(1) $PFD_{koon}^{m} \approx C_n^{n-k+1}(\lambda_{DU}T_1)^{n-k+1}/(n-k+2)$;

(2) $PFD_{koon}^{m} \approx PFD_{koon}^{c}$.

Proof. Let P_j $(j = 0, 1, 2, \ldots, n)$ represent the steady state probability; from Figure 1 and (19), we can obtain that

$$\begin{aligned}P_{n-k+1} &= \left[1 + \sum_{j=0}^{n-k} \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_{\mathrm{DU}}^{n-k+1-j}} \right]^{-1}, \\ P_j &= \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_{\mathrm{DU}}^{n-k+1-j}} P_n \quad \text{for } j < n-k+1,\end{aligned} \tag{23}$$

where $\mu_j \approx (n+1)/T_1$. Then, the PFD_{koon}^{m} can be written as

$$\begin{aligned}\mathrm{PFD}_{koon}^{m} &= P_{n-k+1} \\ &= 1 \times \left(1 + \sum_{j=0}^{n-k} \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_{\mathrm{DU}}^{n-k+1-j}} \right)^{-1}.\end{aligned} \tag{24}$$

For the SIS, it is generally known that $(n+1)/T_1 \gg \lambda_{\mathrm{DU}}$; thus $\mu_j/\lambda_{\mathrm{DU}} \gg 1$. Then, we have

$$\frac{(k-1)!\mu_1\mu_2\cdots\mu_{n-k+1}}{n!\lambda_{\mathrm{DU}}^{n-k+1}} \gg 1 + \sum_{j=1}^{n-k} \frac{(k-1)!\mu_{j+1}\mu_{j+2}\cdots\mu_{n-k+1}}{(n-j)!\lambda_{\mathrm{DU}}^{n-k+1-j}}. \tag{25}$$

It follows that

$$\begin{aligned}\mathrm{PFD}_{koon}^{m} &\approx \frac{n!\lambda_{\mathrm{DU}}^{n-k+1}}{(k-1)!\mu_1\mu_2\cdots\mu_{n-k+1}} = \frac{n!\lambda_{\mathrm{DU}}^{n-k+1}T_1^{n-k+1}}{(k-1)!\,(n-k+2)!} \\ &= C_n^{n-k+1}\frac{(\lambda_{\mathrm{DU}}T_1)^{n-k+1}}{n-k+2}.\end{aligned} \tag{26}$$

Additionally, the exact results derived by the classic probability method could also be simplified as [27, 31]

$$\mathrm{PFD}_{koon}^{c} \approx C_n^{n-k+1}\frac{(\lambda_{\mathrm{DU}}T_1)^{n-k+1}}{n-k+2}, \tag{27}$$

This completes the proof. □

Proposition 4 indicates that when $\lambda_{\mathrm{DU}}T_1 \ll 1$, the transformation of the nonrepairable failure to the repairable failure leads to satisfactory results. In the following, we demonstrate the effect of combining the DU failure and DD failure to a single failure mode. The comparison is made when only one type of failure exists. The results are summarized in Proposition 5.

Proposition 5. *The results of PFD_{koon} evaluated by the micro-Markov models when only one type of failure exists are consistent with the results by the classic probability when only one type of failure is considered.*

Proof. For the SIS, it is generally known that $\mu_j \gg \lambda_D$; thus the PFD_{koon} in (20) can be simplified as

$$\begin{aligned}\mathrm{PFD}_{koon} &\approx \frac{n!\lambda_{\mathrm{DU}}^{n-k+1}}{(k-1)!\mu_1\mu_2\cdots\mu_{n-k+1}} \\ &= A_n^{n-k+1}\prod_{j=1}^{n-k+1}\left[\lambda_{\mathrm{DU}}\left(\frac{T_1}{j+1} + \mathrm{MRT} \right) + \lambda_{\mathrm{DD}}\frac{\mathrm{MTTR}}{j} \right].\end{aligned} \tag{28}$$

Table 2: Comparison of PFD_{avg} equations only considering the DU failure.

System type	This paper	IEC equation	Reference [16]	Reference [20]	Reference [4]
1oo1	$\lambda_{DU}T_1/2$	$\lambda_{DU}T_1/2$	$\lambda_{DU}T_1/2$	$\lambda_{DU}T_1/2$	$\lambda_{DU}T_1/2$
1oo2	$(\lambda_{DU}T_1)^2/3$	$(\lambda_{DU}T_1)^2/3$	$(\lambda_{DU}T_1)^2/9$	$(\lambda_{DU}T_1)^2/4$	$(\lambda_{DU}T_1)^2/3$
2oo2	$\lambda_{DU}T$	$\lambda_{DU}T$	$2\cdot\lambda_{DU}T/3$	$\lambda_{DU}T$	$\lambda_{DU}T$
2oo3	$(\lambda_{DU}T_1)^2$	$(\lambda_{DU}T_1)^2$	$(\lambda_{DU}T_1)^2/3$	$3(\lambda_{DU}T_1)^2/4$	$(\lambda_{DU}T_1)^2$
1oo3	$(\lambda_{DU}T_1)^3/4$	$(\lambda_{DU}T_1)^3/4$	—[a]	—[a]	$(\lambda_{DU}T_1)^3/4$

[a]The PFD_{1oo3} equation is not given in [16, 20].

Table 3: Comparison of PFD_{avg} equations only considering the DD failure.

System type	This paper	IEC equation	Reference [16]	Reference [20]	Reference [4]
1oo1	λ_{DD}MTTR	λ_{DD}MTTR	λ_{DD}MTTR	λ_{DD}MTTR	λ_{DD}MTTR
1oo2	$(\lambda_{DD}\text{MTTR})^2$	$2(\lambda_{DD}\text{MTTR})^2$	$(\lambda_{DD}\text{MTTR})^2$	$(\lambda_{DD}\text{MTTR})^2$	$(\lambda_{DD}\text{MTTR})^2$
2oo2	$2\lambda_{DD}$MTTR	$2\lambda_{DD}$MTTR	$2\lambda_{DD}$MTTR	$2\lambda_{DD}$MTTR	$2\lambda_{DD}$MTTR
2oo3	$3(\lambda_{DD}\text{MTTR})^2$	$6(\lambda_{DD}\text{MTTR})^2$	$3(\lambda_{DD}\text{MTTR})^2$	$3(\lambda_{DD}\text{MTTR})^2$	$3(\lambda_{DD}\text{MTTR})^2$
1oo3	$(\lambda_{DD}\text{MTTR})^3$	$6(\lambda_{DD}\text{MTTR})^3$	—[a]	—[a]	$(\lambda_{DD}\text{MTTR})^3$

[a]The PFD_{1oo3} equation is not given in [16, 20].

If $\lambda_{DD} = 0$ and MRT = 0, (28) can be simplified as

$$PFD_{koon} \approx C_n^{n-k+1}\frac{(\lambda_{DU}T_1)^{n-k+1}}{n-k+2}. \tag{29}$$

It is in accord with the results by the classic probability method when the DU failure is only considered; see (27).

If $\lambda_{DU} = 0$, (28) can be simplified as

$$PFD_{koon} \approx C_n^{n-k+1}(\lambda_{DD}\text{MTTR})^{n-k+1}. \tag{30}$$

It is consistent with the results by the classic probability method; see [31]. This completes the proof. □

From Proposition 5, it can be observed that when only one type of failure exists, the results via the micro-Markov models are in accord with the results when only one type of failure is considered. We further compare the simplified equations through some typical *koon* systems when only one type of failure exists. The simplified equations are illustrated in Tables 2 and 3. The equations presented by [4] are deduced when only one type of failure is considered, which are also consistent with the equations presented by Smith [31] and Rausand and Høyland [27]. It can be observed that only the simplified equations derived in this paper are equal to the equations presented in [4].

The reason why different results are obtained by different references can be explained as follows. The equivalent MDT of a component or the group is an approximation. Different approximation assumptions could obtain different results. Take the 1oo2 system for instance; the group equivalent MDT is approximately equal to $(\lambda_{DU}/\lambda_D)(T_1/3 + \text{MRT}) + (\lambda_{DD}/\lambda_D)(\text{MTTR}/2)$ (see (16)). However, the approximate results from IEC 61508 [16, 20] are $(\lambda_{DU}/\lambda_D)(T_1/3 + \text{MRT}) + (\lambda_{DD}/\lambda_D)\text{MTTR}$, $(\lambda_{DU}/2\lambda_D)(T_1/2 + \text{MRT}) + (\lambda_{DD}/\lambda_D)(\text{MTTR}/2)$, and $(\lambda_{DU}/2\lambda_D)(T_1/3+\text{MRT}) + (\lambda_{DD}/\lambda_D)(\text{MTTR}/2)$, respectively. Therefore, the controversial results are obtained. However, regardless of approximation process, the results by combining the failure modes should be consistent with those when only one type of failure modes is considered. Thus, the group equivalent MDTs in these references have not been accurately approximated. This verifies the results via micro-Markov models to some extent.

4.6. Numerical Comparison. In this experiment, we compare the results by the micro-Markov models with some classic probability methods. Similar to the above subsection, the transformation of the DU failure to a repairable failure is first compared. For simplicity, the calculation of PFD_{avg} by the classic probability method, the presented micro-Markov model in this paper (i.e., (20)), and the simplified equations presented by IEC 61508 are referred to as M_0, M_1, and M_2, respectively. To compare these methods, the M_0 is regarded as a basic method and the relative error is used to implement the comparison. The relative error expressed as a percentage is represented by the ratio of the difference between the result of M_0 and M_1 (or M_2) to that of M_0.

We consider a triple system for an illustrative purpose. With different proof test intervals, the value of $\lambda_{DU}T_1$ changes from 0.033 to 0.263. The compared results are illustrated in Table 4, where RE1 and RE2 represent the relative error of M_1 and M_2, respectively. In Table 4, it can be observed that the relative error increases with the increase of the value of $\lambda_{DU}T_1$ for any *koon* system and the relative error of M_1 is always smaller than that of M_2. This implies that M_1 obtains more accuracy results than M_2. When the value of $\lambda_{DU}T_1$ is small (e.g., $\lambda_{DU}T_1 = 0.033$), the relative error of M_1 and M_2 is able to meet the accuracy requirements. However, for the case that $T_1 = 4$ years, that is, $\lambda_{DU}T_1 = 0.263$, the relative error of M_2 for 3oo3 system is −27.9%. In such circumstances, for M_2, the methods which have more fundamental principles, for example, FTA or RBD method, should be used.

Table 4: Comparison of PFD_{avg} results by M_0, M_1, and M_2.

$\lambda_{DU} = 7.5E-06$/h, $\lambda_{DD} = 0$, MRT = 0 h, 1 year = 8760 h, $\beta = 0$						
System type	T_1 (year)	M_0	M_1	M_2	RE1 (%)	RE2 (%)
1oo3	0.5	$8.52E-06$	$8.44E-06$	$8.86E-06$	$9.79E-01$	$-4.01E+00$
	1	$6.56E-05$	$6.43E-05$	$7.09E-05$	$1.94E+00$	$-8.15E+00$
	4	$3.34E-03$	$3.09E-03$	$4.54E-03$	$7.33E+00$	$-3.60E+01$
2oo3	0.5	$1.04E-03$	$1.03E-03$	$1.08E-03$	$8.21E-01$	$-4.17E+00$
	1	$3.98E-03$	$3.91E-03$	$4.32E-03$	$1.64E+00$	$-8.48E+00$
	4	$5.03E-02$	$4.72E-02$	$6.91E-02$	$6.17E+00$	$-3.73E+01$
3oo3	0.5	$4.77E-02$	$4.70E-02$	$4.93E-02$	$1.54E+00$	$-3.31E+00$
	1	$9.24E-02$	$8.97E-02$	$9.86E-02$	$2.89E+00$	$-6.68E+00$
	4	$3.08E-01$	$2.83E-01$	$3.94E-01$	$8.25E+00$	$-2.79E+01$

Table 5: Comparison of PFD_{avg} results by M_0, M_1, and M_2.

$\lambda_D = 1E-05$/h, $T_1 = 8760$ h, MRT = 24 h, MTTR = 24 h, $\beta = 0$, $\beta_D = 0$						
System type	DC_D (%)	M_0'	M_1	M_2	RE1 (%)	RE2 (%)
1oo3	25	$6.63E-05$	$6.61E-05$	$7.33E-05$	$2.91E-01$	$-1.05E+01$
	50	$2.03E-05$	$2.04E-05$	$2.21E-05$	$-5.14E-01$	$-8.60E+00$
	75	$2.66E-06$	$2.71E-06$	$2.89E-06$	$-1.63E+00$	$-8.64E+00$
2oo3	25	$4.01E-03$	$3.98E-03$	$4.40E-03$	$6.91E-01$	$-9.60E+00$
	50	$1.84E-03$	$1.84E-03$	$1.97E-03$	$1.86E-01$	$-7.07E+00$
	75	$4.81E-04$	$4.84E-04$	$5.06E-04$	$-6.32E-01$	$-5.32E+00$
3oo3	25	$9.28E-02$	$9.03E-02$	$9.93E-02$	$2.67E+00$	$-6.99E+00$
	50	$6.34E-02$	$6.23E-02$	$6.64E-02$	$1.79E+00$	$-4.74E+00$
	75	$3.27E-02$	$3.25E-02$	$3.36E-02$	$8.23E-01$	$-2.51E+00$

In the following, we utilize the method presented in [17] as a basic method to perform the comparison, which has more fundamental principles for the SIS. The method presented in [17] assumes that the unavailability caused by the DD failure is a constant value denoted by $q > 0$. However, the constant value is directly added to the instantaneous unavailability, which is an approximate value. Take the 1oo1 system for example; we have $PFD(t) = q + 1 - e^{-\lambda t}$. However, when $t \to \infty$, the unavailability equals $PFD = q + 1 > 1$. This is not consistent with the assumption that the unavailability is less than or equal to 1. Thus, in this paper, we remedy this deficiency as follows. Essentially, the constant value q can be regarded as a static failure probability. Thus, the instantaneous unavailability can be represented as $PFD(t) = 1 - (1 - q)e^{-\lambda t} = 1 - e^{-\lambda t} + qe^{-\lambda t}$. This is consistent with the assumption. For simplicity, the method presented in [17] is referred to as M_0'. Table 5 gives the compared results, where the value of DC_D changes from 25% to 75%. It is shown that the relative error of M_1 is always smaller than that of M_2. And the maximum value of the relative error of M_1 is 2.67%, which could satisfy the accuracy requirements. Overall, the presented method could obtain the desired results for the SIL verification and can be potentially applied to other *koon* systems.

5. Concluding Remarks

This paper proposes micro-Markov models for the reliability analysis of *koon* systems with multiple failure modes. Two rules are proposed to implement the micro-Markov models. For the repairable *koon* systems with multiple independent failures and repairs, the micro-Markov models could derive the same results with the basic Markov models. For the *koon* systems with hybrid failure modes, approximated and satisfied results could be obtained by the micro-Markov models. A case study regarding the SIL verification for the SIS indicates that when only one type of failure modes exists, the results derived by the micro-Markov models are consistent with the results by the classic probability method when only one type of failure modes is considered. When the DU failure and the DD failure both exist, the results are approximately equal to the results by the methods with more fundamental principles. Additionally, simplified equations are presented for the SIL verification. In summary, the micro-Markov models can be applied to the *koon* systems with multiple failure modes.

In this paper, we mainly discuss how to develop the micro-Markov models for the *koon* systems with multiple failure modes. However, we only use the simple beta factor model to model CCF, which could not distinguish between different *koon* systems. To improve the accuracy of modeling CCF, more advanced CCF models (e.g., the MBF model) should be used, and how to use the micro-Markov models with the MBF model needs to be further exploited. Additionally, as the *koon* system normally works in a finite time zone, it obtains a pessimistic evaluation by using the static unavailability of the repairable failure to represent the average unavailability in the finite time zone. To derive a better evaluation in a finite time zone, the time independent

Markov method should be used. However, for the *koon* system with multiple failure modes, especially for the system with hybrid failure modes, it is different to obtain the exact and closed form solution of the system unavailability. This may encourage the research that is reducing the computation complexity of the time-independent unavailability for *koon* systems.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the National Science Foundation of China under Grant 41174162.

References

[1] S. Eryilmaz, "Consecutive *k*-within-*m*-out-of-*n*:F system with nonidentical components," *Mathematical Problems in Engineering*, vol. 2012, Article ID 106359, 8 pages, 2012.

[2] R. Moghaddass, M. J. Zuo, and W. Wang, "Availability of a general *k*-out-of-*n*:G system with non-identical components considering shut-off rules using quasi-birthdeath process," *Reliability Engineering & System Safety*, vol. 96, no. 4, pp. 489–496, 2011.

[3] M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications*, Wiley Online Library, John Wiley & Sons, New York, NY, USA, 2014.

[4] J. V. Bukowski, "A comparison of techniques for computing PFD average," in *Annual Reliability and Maintainability Symposium, 2005 Proceedings: The International Symposium on Product Quality and Integrity*, pp. 590–595, usa, January 2005.

[5] S. Wang, "Reliability model of mechanical components with dependent failure modes," *Mathematical Problems in Engineering*, vol. 2013, Article ID 828407, 6 pages, 2013.

[6] Q. Yang, Y. Hong, Y. Chen, and J. Shi, "Failure profile analysis of complex repairable systems with multiple failure modes," *IEEE Transactions on Reliability*, vol. 61, no. 1, pp. 180–191, 2012.

[7] J. Wu, S. Yan, and L. Xie, "Reliability analysis method of a solar array by using fault tree analysis and fuzzy reasoning Petri net," *Acta Astronautica*, vol. 69, no. 11-12, pp. 960–968, 2011.

[8] J. Wu and S. Yan, "An approach to system reliability prediction for mechanical equipment using fuzzy reasoning Petri net," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 2013.

[9] IEC 61508, *"Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission, Geneva, Switzerland, 2nd edition, 2010.

[10] IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, International Electrotechnical Commission, Geneva, Switzerland, 2003.

[11] H. Jin, M. A. Lundteigen, and M. Rausand, "Reliability performance of safety instrumented systems: a common approach for both low- and high-demand mode of operation," *Reliability Engineering & System Safety*, vol. 96, no. 3, pp. 365–373, 2011.

[12] L. F. Oliveira and R. N. Abramovitch, "Extension of ISA TR84.00.02 PFD equations to KooN architectures," *Reliability Engineering & System Safety*, vol. 95, no. 7, pp. 707–715, 2010.

[13] J. K. Vaurio, "Unavailability equations for k-out-of-n systems," *Reliability Engineering & System Safety*, vol. 96, no. 2, pp. 350–352, 2011.

[14] H. Jin, M. A. Lundteigen, and M. Rausand, "New PFH-formulas for *k*-out-of-*n*:F-systems," *Reliability Engineering & System Safety*, vol. 111, pp. 112–118, 2013.

[15] H. Jin and M. Rausand, "Reliability of safety-instrumented systems subject to partial testing and common-cause failures," *Reliability Engineering & System Safety*, vol. 121, pp. 146–151, 2014.

[16] H. Guo and X. Yang, "A simple reliability block diagram method for safety integrity verification," *Reliability Engineering & System Safety*, vol. 92, no. 9, pp. 1267–1273, 2007.

[17] A. C. Torres-Echeverría, S. Martorell, and H. A. Thompson, "Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing," *Reliability Engineering & System Safety*, vol. 96, no. 5, pp. 545–563, 2011.

[18] Y. Dutuit, F. Innal, A. Rauzy, and J.-P. Signoret, "Probabilistic assessments in relationship with safety integrity levels by using Fault Trees," *Reliability Engineering & System Safety*, vol. 93, no. 12, pp. 1867–1876, 2008.

[19] B. Knegtering and A. C. Brombacher, "Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by the IEC 61508 standard for functional safety," *Reliability Engineering & System Safety*, vol. 66, no. 2, pp. 171–175, 1999.

[20] T. Zhang, W. Long, and Y. Sato, "Availability of systems with self-diagnostic components—applying Markov model to IEC 61508-6," *Reliability Engineering & System Safety*, vol. 80, no. 2, pp. 133–141, 2003.

[21] H. Guo and X. Yang, "Automatic creation of Markov models for reliability assessment of safety instrumented systems," *Reliability Engineering & System Safety*, vol. 93, no. 6, pp. 829–837, 2008.

[22] J. L. Rouvroye and E. G. Van den Bliek, "Comparing safety analysis techniques," *Reliability Engineering & System Safety*, vol. 75, no. 3, pp. 289–294, 2002.

[23] F. Innal, *Contribution to modelling safety instrumented systems and to assessing their performance critical analysis of iec 61508 standard [Ph.D. thesis]*, University of Technology, 2008.

[24] F. Innal, Y. Dutuit, A. Rauzy, and J.-P. Signoret, "New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 224, no. 2, pp. 75–86, 2010.

[25] Y. Liu and M. Rausand, "Reliability assessment of safety instrumented systems subject to different demand modes," *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 1, pp. 49–56, 2011.

[26] J. V. Bukowski and I. Van Beurden, "Impact of proof test effectiveness on safety instrumented system performance," in *Annual Reliability and Maintainability Symposium (RAMS '09)*, pp. 157–163, January 2009.

[27] M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications*, Wiley Series in Probability and Statistics, John Wiley & Sons, Hoboken, NJ, USA, 2nd edition, 2004.

[28] P. Hokstad and K. Corneliussen, "Loss of safety assessment and the IEC 61508 standard," *Reliability Engineering & System Safety*, vol. 83, no. 1, pp. 111–120, 2004.

[29] P. Hokstad, A. Maria, and P. Tomis, "Estimation of common cause factors from systems with different numbers of channels," *IEEE Transactions on Reliability*, vol. 55, no. 1, pp. 18–25, 2006.

[30] S. Hauge, M. A. Lundteigen, P. Hokstad, and S. Habrekke, "Reliability prediction method for safety instrumented systems-PDS method handbook, 2010 edition," SINTEF report STF50 A, vol. 6031, 2010.

[31] D. Smith, *Reliability, Maintainability and Risk-Practical Methods for Engineers*, Elsevier Butterworth-Heinemann, Burlington, Mass, USA, 2005.