Reliability analysis of static and dynamic fault-tolerant systems subject to probabilistic common-cause failures

L Xing[1]*, **P Boddu**[1], **Y Sun**[2], and **W Wang**[3]

[1]University of Massachusetts Dartmouth, North Dartmouth, Massachusetts, USA
[2]University of Rhode Island, Kingston, Rhode Island, USA
[3]Applied Materials, Santa Clara, California, USA

The manuscript was received on 19 May 2009 and was accepted after revision for publication on 8 October 2009.

DOI: 10.1243/1748006XJRR260

Abstract: Fault-tolerant systems designed with redundancy techniques are typically subject to common-cause failures, which are multiple dependent component failures caused by a shared root cause or a common cause (also known as a shock). There are two types of shocks: fatal and non-fatal. A fatal shock (FS) will fail all components of a system. A non-fatal shock (NFS) will affect only a subset of system components. Most of the existing shock models have assumed that the occurrence of an NFS results in deterministic and simultaneous failures of the affected components. In practice, however, the occurrence of an NFS may result in failures of different components with different probabilities of occurrence. This behaviour is referred to as probabilistic NFS. In this paper, we consider the effects of probabilistic NFS in the reliability analysis of fault-tolerant systems. Both an explicit method and an implicit method are proposed for incorporating probabilistic NFS in the reliability analysis of static systems. A Markov approach combined with the Poisson decomposition law is proposed for incorporating probabilistic NFS in the reliability analysis of dynamic systems. The proposed approaches are illustrated through the analyses of several examples.

Keywords: binary decision diagram, probabilistic common-cause failure, Markov model, Poisson decomposition law, reliability, total probability theorem, static system, dynamic system

1 INTRODUCTION

Fault-tolerant systems are designed to provide continuous and correct functions even in the presence of hardware failures or software errors. Redundancy techniques are commonly used for designing fault-tolerant systems with the aim of enhancing the system reliability and availability. But the introduction of redundancies can facilitate the occurrence of common-cause failures (CCF), which are failures of multiple components owing to a shared root cause or a common cause, and which can contribute significantly to the overall system unreliability and unavailability [**1**, **2**]. Common causes (also known as shocks) can be sabotage, computer viruses, malicious attacks, human errors, design weaknesses, or extreme environmental conditions such as floods and lightning strikes. The damage from a shock can be fatal or non-fatal. A fatal shock (FS) causes all the system components to fail simultaneously; a non-fatal shock (NFS) causes only a subset of components within the system to fail. Furthermore, NFS can be divided into deterministic NFS and probabilistic NFS. The occurrence of a deterministic NFS results in deterministic and guaranteed failures of components affected by the shock, whereas the occurrence of a probabilistic NFS results in failures of different components with different occurrence probabilities [**3**].

Presently, there are two types of approaches for considering effects of CCF in the analysis of system

**Corresponding author: Electrical and Computer Engineering, University of Massachusetts Dartmouth, 285 Old Westport Road, North Dartmouth, MA 02747, USA.*
email: lxing@umassd.edu

reliability: explicit approaches (see, for example, references [**4**] to [**6**]) and implicit approaches (see, for example, references [**7**] to [**11**]). The basic idea of the explicit approaches is to model the occurrence of each shock as a basic event shared by all components affected by the shock in the system model (for example, the system fault tree). The system reliability is then computed by evaluating the expanded system model using any conventional reliability analysis method. The basic idea of the implicit approaches is to develop the system model and reliability expression without considering the effects of CCF. The system reliability is then computed by evaluating the resultant expression but with some special treatment for including the contributions of CCF. Both explicit and implicit approaches are mostly applicable for addressing deterministic shocks, i.e. the occurrence of a shock leads to deterministic and guaranteed failures of the affected components; they cannot address probabilistic NFS. A binomial failure rate (BFR) model [**1**, **12**] can be used to address probabilistic NFS. But this model is only applicable to the analysis of systems where all the system components are *s*-identical and *s*-independent, and fail with the same fixed probability, given the occurrence of a shock. In practice, however, the system components may behave *s*-dependently and may not be *s*-identical. Moreover, when a shock hits the system, it is not inevitable that all the system components will be affected equally: a subset of system components can be affected in a different probabilistic way.

The current paper proposes methods that are applicable for incorporating probabilistic shocks in the reliability analysis of both static systems and dynamic systems with non-identical components. Here, the term ‘static systems’ means that all the system components behave *s*-independently, and the system failure criteria can be fully expressed in terms of combinations of component fault events. The term ‘dynamic systems’ means that some system components behave *s*-dependently in terms of function and/or sequence. In other words, the dynamic systems are typically subject to one or more of the following behaviours: functional dependence, sequence dependence, priorities of fault events, and cold spares [**13**]. More specifically, both an explicit method and an implicit method will be proposed for the reliability analysis of static systems subject to probabilistic shocks: a Markov approach combined with the Poisson decomposition law will be proposed for the reliability analysis of dynamic systems subject to probabilistic shocks.

The remainder of the paper is organized as follows. Section 2 presents an overview of the problem to be addressed, assumptions used in the analysis, as well as the modelling of probabilistic shocks. Section 3 describes the two CCF analysis methods for static systems. Section 4 presents the Markov-based approach for CCF analysis in dynamic systems. Section 5 gives the conclusions as well as directions for future work.

2 PROBLEM STATEMENT

This paper considers the problem of reliability evaluation of static and dynamic fault-tolerant systems subject to probabilistic CCF. The general assumptions used in the analyses are described below, as well as the modelling of probabilistic CCF in the system fault tree analysis.

2.1 Assumptions

1. A fault-tolerant system can be subject to CCF from multiple independent shocks (fatal or non-fatal) with different probabilities of occurrence.
2. A system component may be affected by multiple shocks. A shock group (SG) is defined as a set of components affected by the same shock. This assumption implies that a single system component may belong to more than one SG.
3. Each non-fatal shock, denoted by NFS_i, can hit the system with either a constant rate of $\lambda_{\mathrm{NFS}i}$ or a fixed probability of $p_{\mathrm{NFS}i}$. Also, define $p_{iA} =$ Pr(component A fails | NFS_i occurs).
4. Each fatal shock, denoted by FS_i, can hit the system with either a constant rate of $\lambda_{\mathrm{FS}i}$ or a fixed probability of $p_{\mathrm{FS}i}$. Each FS_i causes the deterministic and guaranteed failure of all the system components.

It is noted that the accuracy of the reliability analysis results depends not only on the system model construction and evaluation, but also on realistic estimation of the occurrence probabilities of shock events as well as the failure parameters of system components. There are some existing approaches, for example fault injection to estimate the component-level failure probabilities and distributions [**14**, **15**], and some parametric models (such as the basic parameter model, the beta model, the alpha factor model, and the multiple Greek letter model) to estimate the occurrence probabilities/rates of common-cause shock events [**16–19**]. However, the problem of parameter estimation is not covered in this work. Instead, the focus is on system-level reliability evaluation with the consideration of effects from probabilistic CCF; assume $p_{\mathrm{NFS}i}$, $\lambda_{\mathrm{NFS}i}$, $p_{\mathrm{FS}i}$, $\lambda_{\mathrm{FS}i}$, p_{iA}, and component failure probabilities are given as input parameters of the problem.

2.2 Modelling of probabilistic CCF

In general, dynamic fault trees (DFT) [**13**] will be used to represent the structure function of the system subject to CCF. In particular, to model the probabilistic non-fatal shocks, a gate called the probabilistic CCF (PCCF) gate is used (Fig. 1), which is modelled after the functional dependency (FDEP) gate [**13**]. The single trigger input of the PCCF gate represents the event of a shock occurring. The one or more dependent events represent failures of components affected by the shock, and they are forced to occur with certain probabilities when the trigger event occurs. Note that separate occurrence of any of the dependent basic events has no effect on the occurrence of the trigger event. Refer to examples in sections 3 and 4 for the application of the gate in the system DFT modelling. When fatal shocks hit the system, all the system components fail, and thus the whole system fails. Therefore each fatal shock event will be connected to the top OR gate of the system fault tree model directly.

3 PROBABILISTIC CCF ANALYSIS FOR STATIC SYSTEMS

This section presents two combinatorial approaches for the reliability analysis of static systems subject to PCCF. The proposed methods will be illustrated via the analysis of an example static system subject to multiple FS and NFS, as described in section 3.1.

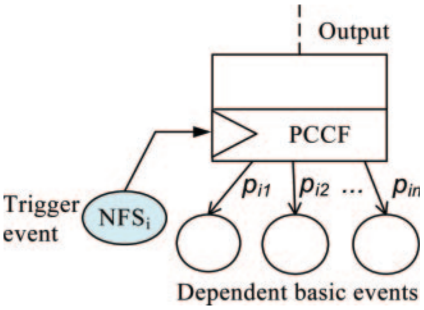

Fig. 1 The PCCF gate

3.1 An example static system

Figure 2 shows the dynamic fault tree model of a five modular redundancy (5MR) system subject to two non-fatal shocks and two fatal shocks: NFS$_1$, NFS$_2$, FS$_1$, and FS$_2$. Without considering the effects of those shocks, the system fails when either three or more than three components fail.

In the example 5MR system, the occurrence of NFS$_1$ would cause components A, B, and E to fail with probabilities p_{1A}, p_{1B}, and p_{1E} respectively. The occurrence of NFS$_2$ would cause C and E to fail with probabilities p_{2C} and p_{2E}, respectively. The two NFS are modelled using the PCCF gate described in section 2 in the system DFT model. The occurrence of FS$_1$ or FS$_2$ would cause all the five components and thus the whole system to fail with a probability of 1. Therefore they are connected to the top OR gate of the DFT model directly. According to assumption 2 in section 2.1, the SG for those shocks are: $\mathrm{SG}_{\mathrm{NFS1}} = \{A, B, E\}$, $\mathrm{SG}_{\mathrm{NFS2}} = \{C, E\}$, and $\mathrm{SG}_{\mathrm{FS1}} = \mathrm{SG}_{\mathrm{FS2}} = \{A, B, C, D, E\}$.

The following parameter values are used in the analysis.

1. Failure probabilities of components owing to s-independent causes: $q_A = q_B = q_C = q_D = q_E = 0.1$. Note that for simplicity of illustration, all the five components are assumed to fail with the same fixed probability; but the present approach for static systems is applicable to components with any arbitrary time-to-failure distributions.
2. Occurrence probabilities of shocks: $p_{\mathrm{NFS1}} = 0.01$, $p_{\mathrm{NFS2}} = 0.02$, $p_{\mathrm{FS1}} = 0.0003$, and $p_{\mathrm{FS2}} = 0.001$.
3. Conditional component failure probabilities owing to non-fatal shocks: $p_{1A} = 0.3$, $p_{1B} = 0.6$, $p_{1E} = 0.7$, $p_{2C} = 0.6$, $p_{2E} = 1$.
4. Mission time: $t = 1000$ h.

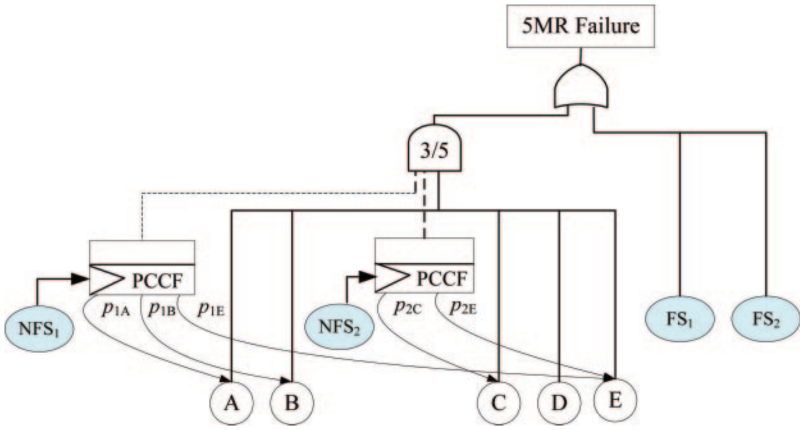

Fig. 2 DFT model of the 5MR system with shocks

3.2 Method 1: an explicit method

This method generalizes the idea of the conventional explicit method for dealing with deterministic shocks to handle probabilistic shocks in the static system reliability analysis. In the conventional explicit method, each shock is modelled as a repeated input event shared by all components affected by the shock in the system fault tree mode. For PCCF, because the occurrence of an NFS does not necessarily result in the guaranteed failure of components affected by the shock, but may cause the affected components to fail with different probabilities, it is necessary to model each non-fatal shock NFS$_i$ as multiple different input events, one for each component affected by NFS$_i$. Denote the input event for component A affected by NFS$_i$ as NFS$_{iA}$. The occurrence probability of NFS$_{iA}$ is computed as the occurrence probability of the shock ($p_{\mathrm{NFS}i}$) multiplied by p_{iA}, which is defined as the conditional probability that A fails given the occurrence of NFS$_i$ (section 2).

Consider the example 5MR system described in section 3.1. Applying the above generalized explicit method, an expanded fault tree model is obtained as shown in Fig. 3. Specifically, since NFS$_1$ affects A, B, and E, it is modelled as three input events NFS$_{1A}$, NFS$_{1B}$, and NFS$_{1E}$ with occurrence probabilities of $p_{\mathrm{NFS1}} \times p_{1A}$, $p_{\mathrm{NFS1}} \times p_{1B}$, and $p_{\mathrm{NFS1}} \times p_{1E}$, respectively. Similarly, NFS$_2$ is modelled as two input events NFS$_{2C}$ and NFS$_{2E}$ with occurrence probabilities of $p_{\mathrm{NFS2}} \times p_{2C}$ and $p_{\mathrm{NFS2}} \times p_{2E}$ respectively. The two fatal shocks are modelled as basic events contributing to the top OR gate, i.e. the entire system failure directly.

The resultant expanded fault tree model can be evaluated using any traditional fault tree reliability analysis approach, such as inclusion/exclusion or sum-of-disjoint products based on cut/path-sets, and binary decision diagram (BDD)-based methods. Among the existing methods, it has been shown that the BDD-based method is more efficient and thus it will be used in the present analysis [**13**, **20**]. Based on Shannon decomposition theory, a BDD is a directed acyclic graph with two sink nodes labelled by constants '0' and '1', representing the system/subsystem being operational and failed respectively. Each non-sink node in the BDD model is associated with a Boolean variable and has two outgoing edges, indicating the non-occurrence (left edge) and occurrence (right edge) of the failure event represented by the node. The unreliability of the system/subsystem is given by the sum of probabilities for all the paths from the root to the sink node '1'. Each of those paths represents a disjointed combination of component failures and non-failures leading to the system/subsystem failure.

To obtain the system unreliability considering the effects of both fatal and non-fatal shocks, the whole system BDD can be generated from the expanded fault tree model, and then evaluated. Alternatively and more efficiently, the evaluation can be performed using a two-level hierarchical method: in the lower level, a BDD is built for each component subsystem, considering the component failures resulting from both independent causes and all non-fatal shocks; in the upper level, a system BDD is built upon component subsystems (referred to as super-nodes) and all fatal shocks. The failure probability of each super-node is the total component failure probability calculated using the corresponding lower-level component subsystem BDD.

Consider the example 5MR system; Figs 4(a) and (b) show the BDD for component subsystems A and E respectively. The BDD for component subsystems B and C are similar to Fig. 4(a) because all of them are subject to failures owing to s-independent cause and one non-fatal shock (NFS$_1$ or NFS$_2$). The evaluation of those BDD produces the total failure (TF) probability of components A, B, C, and E in the 5MR system as

$$\mathrm{TF}_A = q_A + (1 - q_A) p_{\mathrm{NFS1}} p_{1A} = 0.1027 \qquad (1)$$

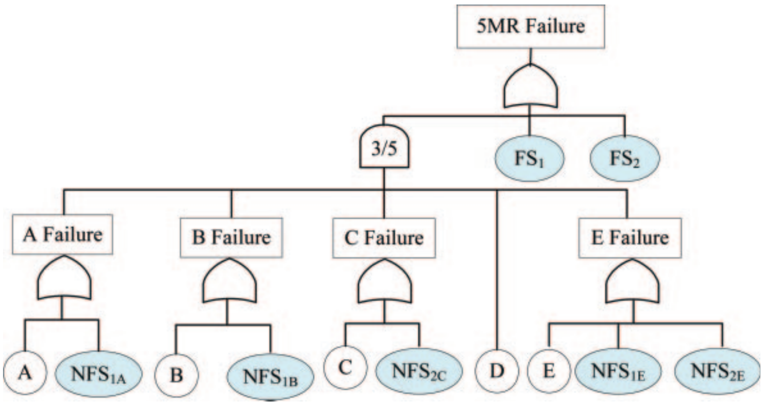

Fig. 3 Expanded fault tree model of the 5MR system

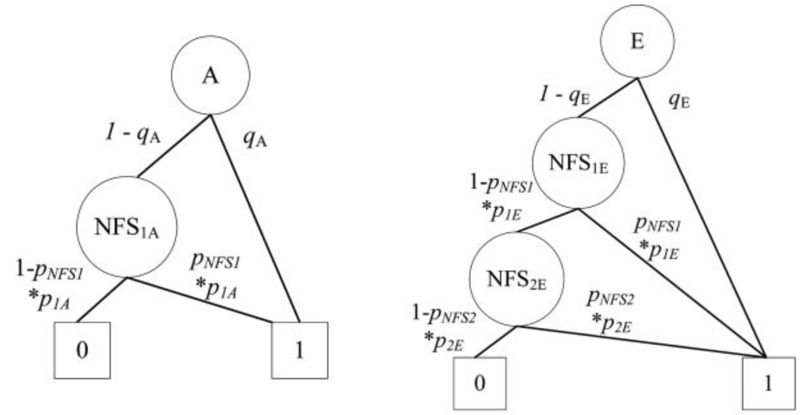

Fig. 4 BDD of component subsystems at the lower level: (a) BDD of component subsystem A; (b) BDD of component subsystem E

$$\mathrm{TF}_B = q_B + (1 - q_B)p_{\mathrm{NFS1}}p_{1B} = 0.1054 \tag{2}$$

$$\mathrm{TF}_C = q_C + (1 - q_C)p_{\mathrm{NFS1}}p_{1C} = 0.1108 \tag{3}$$

$$\begin{aligned}\mathrm{TF}_E &= q_E + (1 - q_E)^* p_{\mathrm{NFS1}}{}^* p_{1E} \\ &\quad + (1 - q_E)^*(1 - p_{\mathrm{NFS1}}{}^* p_{1E})^*(p_{\mathrm{NFS2}}{}^* p_{2E}) \\ &= 0.1242\end{aligned} \tag{4}$$

Since component D is not affected by any NFS, its TF probability is simply the failure probability owing to the s-independent cause, i.e. $\mathrm{TF}_D = q_D = 0.1$.

Figure 5 shows the upper level BDD model of the expanded fault tree in Fig. 3. The evaluation of this BDD gives the overall 5MR system unreliability with the consideration of effects from both fatal and non-fatal shocks as 0.012 061.

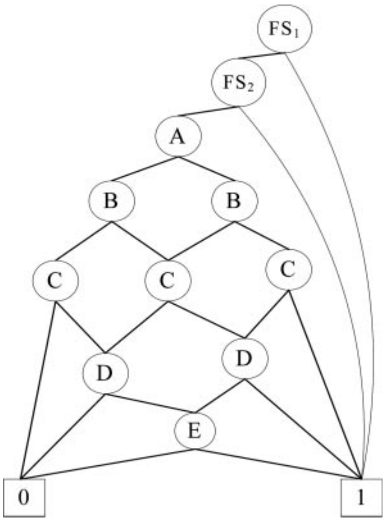

Fig. 5 Upper-level BDD model

3.3 Method 2: an implicit method

The basic idea of the implicit method is to generate the system-level model without considering the effects of non-fatal shocks, but to include the contributions of NFS in the model evaluation. Specifically, the implicit method can be described as a three-step process.

1. Build the reliability model of the system (for example, BDD) with the consideration of fatal shocks, but without considering the effects of NFS, as shown in Fig. 5 for the example 5MR system.
2. Evaluate the TF probability for each component subject to NFS. The contributions of NFS to the entire system unreliability will be included in this step based on a total probability theorem-based method to be detailed in section 3.3.1.
3. Evaluate the system reliability model built in step 1 using the TF probabilities calculated in step 2 as the component failure probabilities.

3.3.1 *Evaluation of component's total failure probability*

The special treatment for including the contributions of NFS is conducted through the evaluation of each component's TF probability based on the total probability theorem.

Consider the example 5MR system in section 3.1. Ignoring all the fatal shocks, component A can fail due to either some independent cause or non-fatal shock NFS$_1$. The TF probability of component A, denoted by TF$_A$, can be calculated using the total probability theorem as

$$\begin{aligned}\mathrm{TF}_A &= \Pr\left(A|\overline{\mathrm{NFS}_{1A}}\right)\times \Pr\overline{(\mathrm{NFS}_{1A})} \\ &\quad + \Pr(A|\mathrm{NFS}_{1A})\times \Pr(\mathrm{NFS}_{1A}) \\ &= q_A(1 - p_{\mathrm{NFS1}}p_{1A}) + 1\times p_{\mathrm{NFS1}}p_{1A} \\ &= q_A + (1 - q_A)p_{\mathrm{NFS1}}p_{1A}\end{aligned} \tag{5}$$

This expression matches that obtained via the evaluation of the lower-level BDD for component A in equation (1).

For component E, which is subject to two non-fatal shocks NFS$_1$ and NFS$_2$, to apply the total probability theorem, a non-fatal shock event (NFSE) space is first constructed: $\Omega_{\text{NFSE}} = \{\text{NFSE}_1, \text{NFSE}_2, \text{NFSE}_3, \text{NFSE}_4\}$. Each event in the space is a distinct and disjoint combination of NFS that affects component E (that is, NFS$_{1E}$ and NFS$_{2E}$) as follows

$$\text{NFSE}_1 = \overline{\text{NFS}_{1E}} \cap \overline{\text{NFS}_{2E}}, \quad \text{NFSE}_2 = \text{NFS}_{1E} \cap \overline{\text{NFS}_{2E}}$$

$$\text{NFSE}_3 = \overline{\text{NFS}_{1E}} \cap \text{NFS}_{2E}, \quad \text{NFSE}_4 = \text{NFS}_{1E} \cap \text{NFS}_{2E}$$

The occurrence probability of NFSE$_i$, denoted by Pr(NFSE$_i$), can easily be calculated based on the occurrence probabilities of the relevant non-fatal shocks. In this work, since all the shocks are assumed to be s-independent (assumption 1 in section 2.1), Pr(NFSE_i) for component E can be calculated as follows: $\Pr(\text{NFSE}_1) = (1 - p_{\text{NFS1}} * p_{1\text{E}})^*(1 - p_{\text{NFS2}} * p_{2\text{E}})$, $\Pr(\text{NFSE}_2) = (p_{\text{NFS1}} * p_{1\text{E}})^*(1 - p_{\text{NFS2}} * p_{2\text{E}})$, $\Pr(\text{NFSE}_3) = (1 - p_{\text{NFS1}} * p_{1\text{E}})^*(p_{\text{NFS2}} * p_{2\text{E}})$, $\Pr(\text{NFSE}_4) = (p_{\text{NFS1}} * p_{1\text{E}})^*(p_{\text{NFS2}} * p_{2\text{E}})$. Actually the implicit method can also handle other types of s-relationship between the NFS in the total failure probability evaluation, while the explicit method of section 3.2 cannot. For example, if two non-fatal shocks NFS$_1$ and NFS$_2$ are mutually exclusive or disjointed, then those occurrence probabilities should be calculated as: $\Pr(\text{NFSE}_1) = 1 - p_{\text{NFS1}} * p_{1\text{E}} - p_{\text{NFS2}} * p_{2\text{E}}$, $\Pr(\text{NFSE}_2) = p_{\text{NFS1}} * p_{1\text{E}}$, $\Pr(\text{NFSE}_3) = p_{\text{NFS2}} * p_{2\text{E}}$, and $\Pr(\text{NFSE}_4) = 0$.

Based on the NFSE space, the total probability theorem can be applied to calculate the TF probability of component E as

$$\text{TF}_E = \sum\nolimits_{i=1}^{4} [\Pr(E|\text{NFSE}_i) * \Pr(\text{NFSE}_i)] \qquad (6)$$

Apparently, $\Pr(E|\text{NFSE}_i) = 1$ for $i = 2, 3, 4$, since either NFS$_1$ or NFS$_2$ or both have occurred, the component E fails. In the case of no NFS occurring, $\Pr(E|\text{NFSE}_1)$ is actually q_E, which is the failure probability of E resulting from some independent causes. Therefore, the calculation of the TF probability of component E for the case where NFS$_1$ and NFS$_2$ are independent can be expanded as

$$\begin{aligned} TF_E &= \sum\nolimits_{i=1}^{4} [\Pr(E|\text{NFSE}_i) \times \Pr(\text{NFSE}_i)] \\ &= q_E \times (1 - p_{\text{NFS1}} \times p_{1E}) \times (1 - p_{\text{NFS2}} \times p_{2E}) \\ &\quad + 1 \times (p_{\text{NFS1}} \times p_{1E}) \times (1 - p_{\text{NFS2}} \times p_{2E}) \\ &\quad + 1 \times (1 - p_{\text{NFS1}} \times p_{1E}) \times (p_{\text{NFS2}} \times p_{2E}) \\ &\quad + 1 \times (p_{\text{NFS1}} \times p_{1E}) \times (p_{\text{NFS2}} \times p_{2E}) \\ &= q_E + (1 - q_E) \times p_{\text{NFS1}} \times p_{1E} + (1 - q_E) \\ &\quad \times (1 - p_{\text{NFS1}} \times p_{1E}) \times (p_{\text{NFS2}} \times p_{2E}) \end{aligned} \qquad (7)$$

This expression matches that obtained via the evaluation of the lower-level BDD for component E in equation (4).

Based on the above discussions on calculating the TF probability of components subject to one or two NFS, the total probability theorem-based method can be expanded to the evaluation of components subject to any finite number of NFS. In general, consider a component K subject to m non-fatal shocks. The m non-fatal shocks partition the event space into 2^m disjointed subsets or NFSE, i.e. NFSE_i, $i = 1, 2, \ldots, 2^m$. As shown in the following equations, each NFSE$_i$ is a distinct and disjoint combination of NFS that affect component K, i.e. NFS$_{1K}$, NFS$_{2K}$, $\ldots$, NFS$_{mK}$

$$\text{NFSE}_1 = \overline{\text{NFS}_{1K}} \cap \overline{\text{NFS}_{2K}} \cap \ldots \cap \overline{\text{NFS}_{(m-1)K}} \cap \overline{\text{NFS}_{mK}}$$

$$\text{NFSE}_2 = \overline{\text{NFS}_{1K}} \cap \overline{\text{NFS}_{2K}} \cap \ldots \cap \overline{\text{NFS}_{(m-1)K}} \cap \text{NFS}_{mK}$$

$$\text{NFSE}_{2^m-1} = \text{NFS}_{1K} \cap \text{NFS}_{2K} \cap \ldots \cap \text{NFS}_{(m-1)K} \cap \overline{\text{NFS}_{mK}}$$

$$\text{NFSE}_{2^m} = \text{NFS}_{1K} \cap \text{NFS}_{2K} \cap \ldots \cap \text{NFS}_{(m-1)K} \cap \text{NFS}_{mK}$$

Each NFS$_{iK}$ has the occurrence probability of $p_{\text{NFS}i} \times p_{iK}$. Based on the total probability theorem, the TF probability of component K is calculated as

$$\text{TF}_K = \sum\nolimits_{i=1}^{2^m} [\Pr(K\text{fails}|\text{NFSE}_i) \times \Pr(\text{NFSE}_i)] \qquad (8)$$

Note that reference [**21**] proposed an approach called the efficient decomposition and aggregation (EDA) approach, which is also based on the total probability theorem for CCF analysis. The EDA approach and the approach presented above for evaluating the TF probability of a component subject to non-fatal shocks are different in two ways:

1. In the method described above, the total probability theorem is applied at the component level for evaluating the TF probability of a component subject to NFS; in the EDA approach, the total probability theorem is applied at the system level for evaluating the failure probability of the entire system subject to CCF.
2. The method here handles probabilistic NFS, the occurrence of which results in failures of different components with different probabilities; the EDA approach can only handle deterministic non-fatal shocks, the occurrence of which result in the deterministic and guaranteed failures of components affected by the shocks. Actually, deterministic shocks are special cases of probabilistic shocks with all the conditional probabilities p_{iA} being 1.

3.4 Discussions

Both the proposed explicit method (section 3.2) and the proposed implicit method (section 3.3) are combinatorial and are based on the efficient BDD model.

Also, both methods are applicable to systems with components having any arbitrary time-to-failure distributions. The explicit method can be inefficient for large-scale systems because it may involve adding a large number of input basic events to the system fault tree model. However, its computational efficiency can be improved using the proposed two-level hierarchical BDD-based method. Another limitation/problem of the proposed explicit method is that it is only applicable to analysing static systems subject to *s*-independent shocks. In contrast, the proposed implicit method can handle other types of *s*-relationship between the non-fatal shocks, as illustrated in section 3.3.1.

As a comparison with the unreliability of the 5MR system subject to both probabilistic NFS and FS (0.012 061), the unreliability results for the 5MR system were also generated in another two scenarios.

1. The 5MR system is not subject to any shocks. The system unreliability can be calculated simply based on combinatorial theory as

$$\begin{aligned}\mathrm{UR}_{5\mathrm{MR}} &= C_5^3(0.1)^3(0.9)^2 + C_5^4(0.1)^4(0.9) + C_5^5(0.1)^5 \\ &= 0.008\,56\end{aligned}$$

2. The 5MR system is subject to two fatal shocks (FS_1, FS_{12}), and two non-fatal shocks (NFS_1, NFS_2). But these two non-fatal shocks are deterministic. Applying the EDA approach of reference [**21**] for deterministic CCF or the explicit method of section 3.2 or the implicit method of section 3.3 for probabilistic CCF with all the conditional probabilities p_{iA} being 1, the system unreliability is obtained as 0.024 94.

Observing the difference of results for those three scenarios, it is concluded that failure to consider CCF or probabilistic CCF leads to underestimated system unreliability. Also, the effects of CCF or probabilistic CCF on the system unreliability are more pronounced as the occurrence probabilities of shocks and/or the conditional probabilities p_{iA} become larger.

4 PROBABILISTIC CCF ANALYSIS FOR DYNAMIC SYSTEMS

This section presents a Markov chain-based approach for the reliability analysis of dynamic systems subject to probabilistic CCF. The proposed methods will be illustrated via the analysis of an example dynamic system subject to fatal and non-fatal shocks, as described in section 4.1.

4.1 An example dynamic system

Figure 6 shows the fault tree model of a dynamic system subject to a non-fatal shock NFS_1 and a fatal shock FS_1. The system contains a cold standby sparing subsystem modelled by a cold spare (CSP) gate, in which P_2 is a primary component and P_s is a cold spare. The cold spare is unpowered and thus cannot fail (unless it is hit by a shock) before it is switched to replace the failed primary component. Without considering the effects of shocks, the system fails when all the three components have failed.

The occurrence of NFS_1 causes P_1 and P_s to fail with probabilities p_{11} and p_{1S} respectively. The occurrence of FS_1 causes all the three components, and thus the whole system, to fail with probability 1. The SG for the two shocks are $\mathrm{SG}_{\mathrm{NFS1}} = \{P_1, P_s\}$ and $\mathrm{SG}_{\mathrm{FS1}} = \{P_1, P_2, P_s\}$.

Since the proposed method for probabilistic CCF analysis in dynamic systems is based on Markov chains, both the component time-to-failures due to *s*-independent causes and the shock occurrence times follow the exponential distribution. The following parameter values are used in the analysis:

(a) the constant failure rates of components due to *s*-independent causes: $\lambda_{P1} = 1\mathrm{e}-5/\mathrm{h}$, $\lambda_{P2} = 1\mathrm{e}-5/\mathrm{hr}$, $\lambda_{Ps} = 1\mathrm{e}-5/\mathrm{h}$;
(b) the constant occurrence rates of shock: $\lambda_{\mathrm{NFS1}} = 5\mathrm{e}\text{-}5/\mathrm{h}$, $\lambda_{\mathrm{FS1}} = 9\mathrm{e}\text{-}5/\mathrm{h}$;
(c) conditional component failure probabilities due to the non-fatal shock NFS_1: $p_{11} = 0.3$, $p_{1S} = 0.9$;
(d) mission time: $t = 1000$ h.

4.2 Markov approach for dynamic systems

For systems subject to dynamic behaviours of functional dependence, sequence dependence, priorities

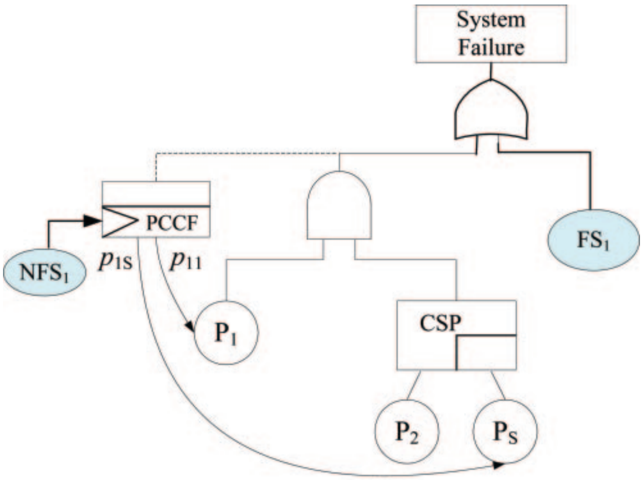

Fig. 6 DFT model of an example dynamic system with shocks

of fault events, and/or cold spares, Markov chain-based methods have been used for the system reliability analysis [**13**]. However, owing to the simultaneousness of the probabilistic occurrence of multiple component failures resulting from a shock, the traditional Markov chain-based methods, which consider the component failures one by one, cannot be directly applied to the reliability analysis of dynamic systems with probabilistic shocks. The current authors propose combining the Markov approach with the Poisson decomposition property [**22**] to address the above problem.

As shown in Fig. 7, according to the Poisson decomposition property [**22**], if a Poisson stream with rate λ branches out into multiple output paths or substreams such that each path occurs with a fixed probability p_i, then these output substreams are also Poisson with rates being λ times the respective occurrence probability of the output path, i.e. $\lambda \times p_i$.

Consider the occurrence of NFS_1 in the example in section 4.1: applying the Poisson decomposition law, the stream (or transition in the Markov solution) representing the occurrence of NFS_1 can be subdivided into four output substreams, each representing a disjoint combination of occurrence/non-occurrence of components affected by NFS_1. Specifically, they are 'neither P_1 nor P_s fails'; 'P_1 fails and P_s does not fail'; 'P_1 does not fail and P_s fails'; and 'both P_1 and P_s fail'. The transition rates associated with those four output paths are shown in Fig. 8.

Figure 9 illustrates the complete Markov model for the example dynamic system of Fig. 6, where the effects of probabilistic NFS are incorporated via the Poisson decomposition law. Since the occurrence of a fatal shock results in failures of all system components, and therefore the failure of the entire system, there is a direct transition from each non-absorbing state to the absorbing state (i.e. the system failure state, denoted by F) with the transition rate of λ_{FS1}. Specifically, the Markov model is developed starting with an initial state (P_1, P_2, P_{S}) representing all the three components functioning. The failure of P_1 would lead to the state (P_2, P_{S}) representing P_2 working, P_{S} in the cold standby state, and P_1 failed. The transition rate from state (P_1, P_2, P_{S}) to state (P_2, P_{S}) includes the failure rate due to independent cause (λ_{P1}) and the failure rate due to the non-fatal shock ($\lambda_{\mathrm{NFS1}} \times p_{11} \times p'_{1\mathrm{S}} = \lambda_{\mathrm{NFS1}} \times p_{11}{}^{*}(1 - p_{1\mathrm{S}})$). From ($P_2$, P_{S}), the failure of P_2 would lead to state (P_{S}); the failure of P_{S} would lead to state (P_2). P_2 can fail only due to the independent cause with the rate of λ_{P2}. The component P_{S} can fail in the cold standby condition only when it is hit by the shock, and the transition from state (P_2, P_{S}) to state (P_2) is thus associated with the rate of ($\lambda_{\mathrm{NFS1}} \times (1 - p_{11}) \times p_{1S} + \lambda_{\mathrm{NFS1}} \times p_{11} \times p_{1S}) = \lambda_{\mathrm{NFS1}} \times p_{1\mathrm{S}}$. From the state ($P_{\mathrm{S}}$), the failure of P_{S} would lead to the absorbing state (F). The rate of transition from (P_{S}) to (F) includes the failure rate of P_{S} due to independent cause (λ_{PS}) and the failure rate due to the non-fatal shock, i.e. ($\lambda_{\mathrm{NFS1}} \times (1 - p_{11}) \times p_{1\mathrm{S}} + \lambda_{\mathrm{NFS1}} \times p_{11} \times p_{1\mathrm{S}}) = \lambda_{\mathrm{NFS1}} \times p_{1\mathrm{S}}$). Other states and transitions in the Markov model of Fig. 9 can be similarly developed.

Evaluating the Markov model of Fig. 9 using the input parameters provided in section 4.1, it is possible to obtain the unreliability of the example dynamic

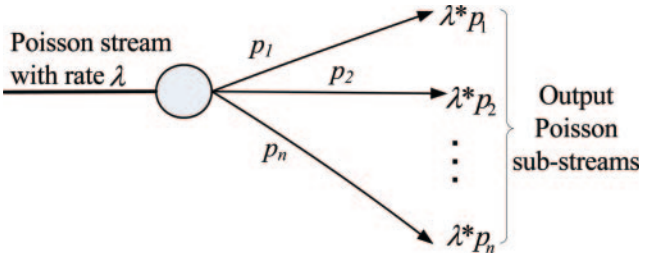

Fig. 7 The Poisson decomposition law [**22**]

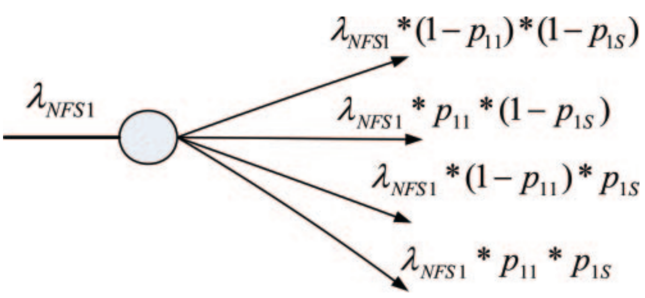
λ_{NFS1}
$\lambda_{NFS1}{}^*(1-p_{11})^*(1-p_{1S})$
$\lambda_{NFS1}{}^*p_{11}{}^*(1-p_{1S})$
$\lambda_{NFS1}{}^*(1-p_{11})^*p_{1S}$
$\lambda_{NFS1}{}^*p_{11}{}^*p_{1S}$

Fig. 8 Application of Poisson decomposition law

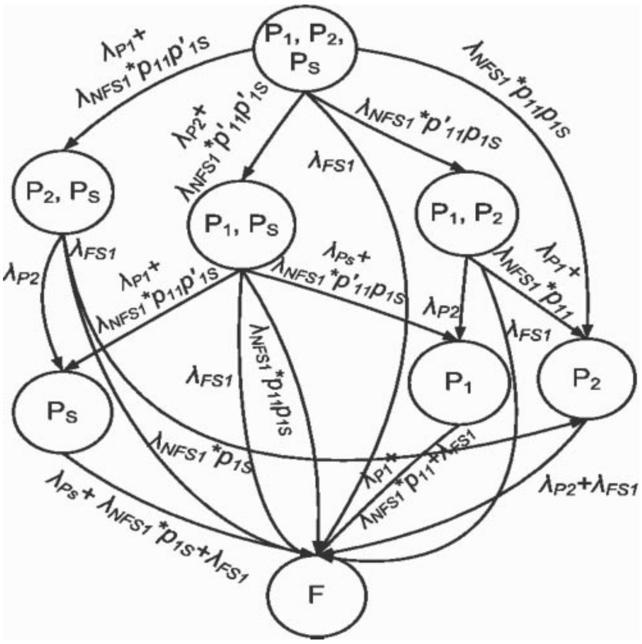
P1, P2, Ps
P2, Ps
P1, Ps
P1, P2
Ps
P1
P2
F
λ_{P1}+ $\lambda_{NFS1}{}^*p_{11}p'_{1S}$
λ_{P2}+ $\lambda_{NFS1}{}^*p'_{11}p'_{1S}$
$\lambda_{NFS1}{}^*p'_{11}p_{1S}$
$\lambda_{NFS1}{}^*p_{11}p_{1S}$
λ_{FS1}
λ_{P2}
λ_{FS1}
λ_{P1}+ $\lambda_{NFS1}{}^*p_{11}p'_{1S}$
λ_{Ps}+ $\lambda_{NFS1}{}^*p'_{11}p_{1S}$
λ_{P2}
λ_{P1}+ $\lambda_{NFS1}{}^*p_{11}$
λ_{FS1}
λ_{FS1}
$\lambda_{NFS1}{}^*p_{11}p_{1S}$
$\lambda_{NFS1}{}^*p_{1S}$
λ_{P1}+ $\lambda_{NFS1}{}^*p_{11}$+λ_{FS1}
λ_{P2}+λ_{FS1}
λ_{Ps}+ $\lambda_{NFS1}{}^*p_{1S}$+λ_{FS1}

Fig. 9 Markov model of the example dynamic system

system considering the effects from both non-fatal and fatal shocks as 0.6003 at mission time of 1000 h.

4.3 Discussions

As illustrated through the analysis of the example dynamic system, the proposed Markov solution can successfully handle the probabilistic NFS in the system reliability analysis. However, a major disadvantage of the proposed solution is that it worsens the state space explosion problem of the traditional Markov methods. Owing to this problem, the proposed Markov-based method is suitable only for solving dynamic systems of very limited size and subject to a small number of NFS. Some research efforts have been expended in the modularization technique [**23**], which has been used to minimize the use of the Markov model in the system reliability solution while retaining the efficiency of combinatorial models as much as possible. The adaption of the existing modularization technique for handling probabilistic NFS as well as other efficient solutions will be explored in future work, to provide a viable solution to the reliability analysis of large-scale dynamic systems subject to probabilistic CCF.

5 CONCLUSIONS AND FUTURE WORK

In this paper, both an explicit method and an implicit method were proposed for incorporating the effects of PCCF in the reliability analysis of static systems. Both methods are combinatorial and are based on the efficient BDD models. For incorporating the effects of probabilistic CCF in the reliability analysis of dynamic systems, a Markov model combined with the Poisson decomposition law was proposed. The proposed methods are able to evaluate systems subject to multiple different shocks. In addition, they are applicable to cases in which a single component can be affected by multiple shocks. Basics and advantages of the proposed approaches were illustrated through the analyses of examples.

As previously mentioned, one direction of the current authors' future work is to investigate efficient solutions to the reliability analysis of large dynamic systems subject to probabilistic shocks. Another direction is to investigate the impact of jamming attacks on the reliability of wireless sensor networks (WSN) via the probabilistic shock models. It is well-known that WSN are vulnerable to various attacks [**24**, **25**]. This is due to the fact that WSN are usually deployed in unattended environments; the sensor nodes have limited amount of resources (e.g. power); and the networks are self-organized and lack central control. Among all possible attacks, jamming attack is one of the most powerful and hateful attacks that exploit the shared nature of the wireless medium in order to prevent devices from transmitting and receiving. As a direct consequence, a cheap jammer can bring down many neighbouring sensor nodes. Currently, the jamming and anti-jamming techniques are evaluated through simulations (see, for example, references [**26**] to [**29**]). However, the simulation-based comparisons are highly application dependent, time-consuming, and lack consensus on evaluation criteria. As a consequence, it is very difficult to compare different jamming and anti-jamming techniques in a unified framework. In future work, the authors will tackle the above problem via a theoretical analysis method, in particular, applying the proposed probabilistic CCF analysis theories to sensor networks where various jamming and anti-jamming techniques are used. Their goals are to evaluate the impact of different jamming attacks upon network reliability, and to compare different anti-jamming techniques in the context of improving network reliability performance. The third direction of their future work is to investigate approaches for quantifying the parameters needed for probabilistic CCF models.

ACKNOWLEDGEMENTS

This work was supported in part by the National Science Foundation under grant no. 0614652. An earlier version of this paper was presented at the 55th Annual Reliability and Maintainability Symposium [**30**]. The authors appreciate the feedback given to them on this topic by conference attendees.

REFERENCES

1 **Borcsok, J., Schaefer, S.,** and **Ugljesa, E.** Estimation and evaluation of common cause failures. In Proceeding of the Second International Conference on *Systems*, Sainte-Luce, France, 2007.

2 **Mitra, S., Saxena, N. R.,** and **McCluskey, E. J.** Common-mode failures in redundant VLSI systems: a survey. *IEEE Trans. Reliability*, 2000, **49**(3), 285–295.

3 **Xing, L.** and **Wang, W.** Probabilistic common-cause failures analysis. In Proceedings of the Annual Reliability and Maintainability Symposium, Las Vegas, Nevada, January 2008.

4 **Dai, Y., Xie, M., Poh, K. L.,** and **Ng, S. H.** A model for correlated failures in N-version programming. *IIE Trans.*, 2004, **36**(12), 1183–1192.

5 **Vaurio, J. K.** Fault tree analysis of phased mission systems with repairable and non-repairable components. *Reliability Engng and System Safety*, 2001, **74**(2), 169–180.

6 **Fleming, K. N.** and **Mosleh, A.** Common-cause data analysis and implications in system modeling. In Proceedings of the International Topical Meeting on *Probabilistic safety methods and applications*, San Fransisco, California, 1985, vol. 1: 3/1–3/12, EPRI NP-3912-SR.

7 **Vaurio, J. K.** An implicit method for incorporating common-cause failures in system analysis. *IEEE Trans. Reliability*, 1998, **47**(2), 173–180.

8 **Tang, Z.** and **Dugan, J. B.** An integrated method for incorporating common cause failures in system analysis. In Proceedings of the Annual Reliability and Maintainability Symposium, Los Angeles, California, January 2004, pp. 610–614.

9 **Tang, Z., Xu, H.,** and **Dugan, J. B.** Reliability analysis of phased mission systems with common cause failures. In Proceeding of the 51st Annual Reliability and Maintainability Symposium, Alexandria, Virginia, January 2005, pp. 313–318.

10 **Xing, L.** Reliability evaluation of phased-mission systems with imperfect fault coverage and common-cause failures. *IEEE Trans. Reliability*, 2007, **56**(1), 58–68.

11 **Xing, L., Shrestha, A., Meshkat, L.,** and **Wang, W.** Incorporating common-cause failures into the modular hierarchical systems analysis. *IEEE Trans. Reliability*, 2009, **58**(1), 10–19.

12 **Chae, K. C.** System reliability using binomial failure rate. In Proceedings of the Annual Reliability and Maintainability Symposium, Los Angeles, California, January 1988, pp. 136–138.

13 **Dugan, J. B.** and **Doyle, S. A.** New results in fault-tree analysis. *Tutorial notes annual reliability and maintainability symposium*, Philadelphia, Pennsylvania, January 1997.

14 **Hsueh, M., Tsai, T. K.,** and **Iyer, R. K.** Fault injection techniques and tools. *IEEE Computer*, 1997, **30**(4), 75–82.

15 **Cukier, M., Powell, D.,** and **Ariat, J.** Coverage estimation methods for stratified fault-injection. *IEEE Trans. Computers*, 1999, **48**(7), 707–723.

16 **Modarres, M.** *What every engineer should know about reliability and risk analysis*, ch. 6, 1993 (Marcel Dekker, New York).

17 **Vaurio, J. K.** Uncertainties and quantification of common cause failure rates and probabilities for system analyses. *Reliability Engng and System Safety*, 2005, **90**(2–3), 186–195.

18 **Xie, L., Zhou, J.,** and **Wang, X.** Data mapping and the prediction of common cause failure probability. *IEEE Trans. Reliability*, 2005, **54**(2), 291–296.

19 **Hokstad, P., Maria, A.,** and **Tomis, P.** Estimation of common cause factors from systems with different numbers of channels. *IEEE Trans. Reliability*, 2006, **55**(1), 18–25.

20 **Rauzy, A.** New algorithms for fault tree analysis. *Reliability Engng and System Safety*, 1993, **40**, 203–211.

21 **Xing, L., Meshkat, L.,** and **Donohue, S. K.** Reliability analysis of hierarchical computer-based systems subject to common-cause failures. *Reliability Engng and System Safety*, 2007, **92**(3), 351–359.

22 **Trivedi, K. S.** *Probability and statistics with reliability, queuing, computer science applications*, 2001 (John Wiley, New York).

23 **Gulati, R.** and **Dugan, J. B.** A modular approach for analyzing static and dynamic fault trees. In Proceedings of the Annual Reliability and Maintainability Symposium, Philadelphia, Pennsylvania, January 1997, pp. 57–63.

24 **Wood, A.** and **Stankovic, J.** Denial of service in sensor networks. *IEEE Computer*, 2002, **35**(10), 54–62.

25 **Perrig, A., Stankovic, J.,** and **Wagner, D.** Security in wireless sensor networks. *Commun. ACM*, 2004, **47**(6), 53–57.

26 **Li, M., Koutsopoulos, I.,** and **Poovendran, R.** Optimal jamming attacks and network defense policies in wireless sensor networks. In Proceedings of IEEE INFOCOM, May 2007, Anchorage, AK, pp. 1307–1315.

27 **Xu, W., Ma, K., Trappe, W.,** and **Zhang, Y.** Jamming sensor networks: attack and defense strategies. *IEEE Networks*, 2006, **20**(3), 41–47.

28 **Ma, K., Zhang, Y.,** and **Trappe, W.** Mobile network management and robust spatial retreats via network dynamics. In Proceedings of the IEEE International Conference on *Mobile ad hoc and sensor systems*, Washington, DC, November 2005.

29 **Noubir, G.** and **Lin, G.** Low-power DoS attacks in data wireless LANs and countermeasures. *ACM SIGMOBILE Mobile Computing and Commun. Rev.*, 2003, **7**(3), 29–30.

30 **Xing, L., Boddu, P.,** and **Sun, Y.** System reliability analysis considering fatal and non-fatal shocks. In Proceedings of the 55th Annual Reliability and Maintainability Symposium, Fort Worth, Texas, January 2009, pp. 436–441.

APPENDIX

Notation

A	a system component
B, C, D, E	components in the example static system
FS_i	a fatal shock
m	number of non-fatal shocks
NFS_i	a non-fatal shock
NFS_{iA}	an event in which the shock NFS_i occurs and component A is affected
NFSE_i	a non-fatal shock event
p_{iA}	Pr(component A fails | NFS_i occurs)
$p_{\mathrm{FS}i}$	occurrence probability of FS_i
$p_{\mathrm{NFS}i}$	occurrence probability of NFS_i
$Pr(\mathrm{NFSE}_i)$	occurrence probability of NFSE_i
P_1, P_2, P_s	components in the example dynamic system
q_A	failure probability of A
$\mathrm{SG}_{\mathrm{FS}i}$	shock group of FS_i
$\mathrm{SG}_{\mathrm{NFS}i}$	shock group of NFS_i
t	mission time
TF_A	total failure probability of component A
$\mathrm{UR}_{5\mathrm{MR}}$	unreliability of a 5MR system

λ_A	constant failure rate of component A
$\lambda_{\mathrm{FS}i}$	constant occurrence rate of FS_i
$\lambda_{\mathrm{NFS}i}$	constant occurrence rate of NFS_i

Acronyms

The singular and plural of an acronym are always spelled the same.

BDD	binary decision diagram
BFR	binomial failure rate
CCF	common-cause failure
CSP	cold spare
DFT	dynamic fault tree
EDA	efficient decomposition and aggregation
FDEP	functional dependency
FS	fatal shock
NFS	non-fatal shock
NFSE	NFS event
PCCF	probabilistic CCF
SG	shock group
TF	total failure
WSN	wireless sensor network
5MR	five modular redundancy