System Reliability Analysis Considering Fatal and Non-Fatal Shocks

Liudong Xing, PhD, University of Massachusetts, Dartmouth
Prashanthi Boddu, University of Massachusetts, Dartmouth
Yan (Lindsay) Sun, PhD, University of Rhode Island, Kingston

Key Words: shock, reliability, Poisson decomposition

SUMMARY & CONCLUSIONS

Systems designed with fault-tolerance techniques are typically subject to common-cause shocks. Failure to consider common-cause shocks in the system reliability analysis leads to optimistic results, which makes the reliability analysis less effective in the system design and tuning activities. In this paper, we consider two types of common-cause shocks: fatal and non-fatal in the reliability evaluation of fault-tolerant systems. A fatal shock will fail all components of a system, while a non-fatal shock causes the affected components to fail with different probabilities. Hierarchical combinatorial approaches and a Markov approach have been proposed for incorporating common-cause shocks in the reliability analysis of static and dynamic systems, respectively. The basics of the proposed approaches and effects of common-cause shocks on the system reliability are illustrated through examples.

1 INTRODUCTION

Systems designed with fault-tolerance/redundancy techniques are typically subject to common-cause shocks [1]. Examples of common-cause shocks include extreme environmental conditions, computer viruses, sabotages, power outages, design weaknesses, or human errors [2]. Shocks can be classified into two types: fatal and non-fatal. A fatal shock (FS) will cause the simultaneous failure of all the system components; whereas when a non-fatal shock (NFS) hits the system, a subset of components within the system will fail and they can fail with different probabilities. Failure to consider shocks in the system reliability analysis will lead to optimistic or overestimated results, which makes the reliability analysis less effective in system design and tuning activities. Therefore, it is important to incorporate the effects of both fatal and non-fatal shocks in the system reliability modeling and analysis.

There are many existing common-cause shock models designed for general computer-based systems (see, e.g., [3, 4, 5, 6]). However, most of them have assumed that the occurrence of a non-fatal shock results in the deterministic/guaranteed failure of components affected by that shock. In practice, however, the occurrence of a non-fatal shock may result into failures of different components with different probabilities. A binomial failure rate (BFR) model has been used to address such probabilistic non-fatal shocks [7, 8]. But this model has three limitations: 1) suitable only for systems with all component failures being independent, 2) limiting analysis to scenarios where all the system components fail with the same fixed probability given the occurrence of a shock, and 3) applicable only to systems with $s$-identical components.

In this paper, we first propose two combinatorial methods for incorporating common-cause shocks in the reliability analysis of static systems, for which the system failure criteria can be fully expressed in terms of combinations of component fault events. The methods will be hierarchical, consisting of a total failure probability calculation for each component at the lower level and a combinatorial analysis of reliability for the entire system at the upper level.

For systems subject to dynamic behaviors of functional dependence, sequence dependence, priorities of fault events, and cold spares, Markov chain based methods have been used for the reliability analysis [9]. However, due to the simultaneousness of the occurrence of multiple component failures resulting from a common-cause 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 shocks. We propose to combine the Markov approach with the Poisson decomposition property [10] to address the above challenge. Due to the well-known state space explosion problem, the usage of the Markov model will be kept at a minimum level through the modularization technique that allows the use of the Markov approach only when necessary and retains the efficiency of combinatorial solutions as much as possible [11].

The proposed methods will eliminate the limitations that the existing models have. Furthermore, our methods are able to evaluate a system subject to multiple different shocks. In addition, the proposed methods take into account the cases in which a single component can be affected by multiple shocks. Basics and advantages of the proposed approaches will be illustrated through the analyses of examples.

2 PROBLEM STATEMENT

In this paper, we consider the problem of reliability evaluation of fault-tolerant systems subject to both fatal and non-fatal common-cause shocks. The following assumptions are used in our analyses:
A system can be subject to multiple common-cause shocks with different occurrence probabilities. Each non-fatal shock denoted by $NFS_i$ causes its affected component $A$ to fail with probability $p_{iA} = \Pr(\text{Component } A \text{ fails } | NFS_i \text{ occurs})$. Each non-fatal shock $NFS_i$ can hit the system with either a constant rate of $\lambda_{NFS_i}$ or a fixed probability of $p_{NFS_i}$. Each fatal shock denoted by $FS_i$ causes the deterministic failure of all the system components. Each fatal shock $FS_i$ can hit the system with either a constant rate of $\lambda_{FS_i}$ or a fixed probability of $p_{FS_i}$.

Some parametric models, such as the Basic Parameter model, the Beta model, the Alpha Factor model, and the Multiple Greek Letter model, have been suggested to estimate the occurrence probabilities of common-cause shock events [12]. In this paper, we assume $p_{NFS_i}$, $\lambda_{NFS_i}$, $p_{FS_i}$, $\lambda_{FS_i}$, and $p_{iA}$ are all given as input parameters.

A system component may be affected by multiple shocks. In other words, a single component may belong to more than one common-cause group (CCG), which is defined as a set of components affected by the same common-cause shock.

3  ILLUSTRATIVE EXAMPLES

Two examples of fault tolerant systems will be presented in this section: a static system and a dynamic system. In general, a static system’s failure criteria depends only on the combination of component fault events, while a dynamic system’s failure can be sensitive to the order of occurrence of component fault events. A dynamic system may also contain cold spares and functional dependencies [9]. The two examples will be used to illustrate our proposed methods in Section 4 and Section 5, respectively.

3.1 Example 1: A Static System

Figure 1 shows the fault tree model of a Five Modular Redundancy (5MR) system. The system fails when three or more than three modules fail.

![Figure 1 - Fault Tree Model of the 5MR System](image)

The following scenario is used to illustrate the effects of non-fatal and fatal shocks: the 5MR system is subject to two independent non-fatal shocks and a fatal shock: $NFS_1$, $NFS_2$, and $FS_1$. The occurrence of $NFS_1$ would cause A, B, and E to fail with probabilities $p_{iA}$, $p_{iB}$, and $p_{iE}$, respectively. The occurrence of $NFS_2$ would cause C and E to fail with probabilities $p_{2C}$ and $p_{2E}$, respectively. The occurrence of $FS_1$ would cause all the five components to fail with probability of 1. Thus, $\text{CCG}_{NFS_1} = \{A, B, E\}$, $\text{CCG}_{NFS_2} = \{C, E\}$, and $\text{CCG}_{FS_1} = \{A, B, C, D, E\}$. Using the PCCF gates proposed in [2], the fault tree model of 5MR system considering the above common-cause shock events can be constructed as shown in Figure 2. Note that when the fatal shock hits the system, all the system components fail, thus the whole system fails. So the fatal shock event is connected to the top OR gate directly.

![Figure 2 - Fault Tree of the 5MR System Subject to Shocks](image)

The following parameter values will be used in the analysis:
- Component failure probabilities due to $s$-independent causes: $qA = qB = qC = qD = qE = 0.1$. For simplicity, we assume all the five components fail with the same fixed probability; our approach is applicable to components with any arbitrary time-to-failure distributions.
- Shock occurrence probabilities: $p_{NFS_1} = 0.01$, $p_{NFS_2} = 0.02$, and $p_{FS_1} = 0.001$.
- Component conditional failure probabilities due to non-fatal shocks: $p_{iA} = 0.3$, $p_{iB} = 0.6$, $p_{iE} = 0.7$, $p_{2C} = 0.6$, $p_{2E} = 1$.

3.2 Example 2: A Dynamic System

Figure 3 shows the fault tree model of a dynamic system with a cold standby sparing subsystem. The system fails when all the three components have failed.

![Figure 3 - Fault Tree of the Example Dynamic System](image)

The dynamic system is subject to a non-fatal shock $NFS$ and a fatal shock $FS$. The occurrence of $NFS$ would cause $P_1$ and $P_s$ to fail with probabilities $p_1$ and $p_s$, respectively. The occurrence of $FS$ would cause all the three components to fail with probability of 1. Thus, $\text{CCG}_{NFS} = \{P_1, P_s\}$, and $\text{CCG}_{FS} = \{P_1, P_2, P_s\}$.

The following parameter values will be used in the
analysis:

- Component failure rates due to s-independent causes: $\lambda_{P1} = 1 \times 10^{-5}$/hour, $\lambda_{P2} = 2 \times 10^{-5}$/hour, $\lambda_{Ps} = 3 \times 10^{-5}$/hour.
- Shock occurrence rates: $\lambda_{NFS} = 5 \times 10^{-5}$/hour, $\lambda_{FS} = 6 \times 10^{-5}$/hour.
- Component conditional failure probabilities due to non-fatal shocks: $p_{1} = 0.3$, $p_{s} = 0.2$.

4 HIERARCHICAL COMBINATORIAL APPROACHES

In this section, two hierarchical and combinatorial approaches are presented for the reliability analysis of static systems subject to common-cause shocks. The analysis of Example 1 (Section 3.1) is given to illustrate the proposed methods.

In our previous work in [2], a generalized explicit method has been proposed for incorporating the effects of common-cause shocks into the system reliability analysis. In that method, each shock is modeled as multiple input events, one for each component affected by the shock. For example, applying the generalized explicit method to the example 5MR system described in Section 3.1, an expanded static fault tree model can be obtained as shown in Figure 4. Specifically, since $NFS_1$ affect A, B, and E, it is modeled as three basic events $NFS_{1A}$, $NFS_{1B}$, and $NFS_{1E}$ with probabilities of $p_{NFS_1} * P_{1A}$, $p_{NFS_1} * P_{1B}$, and $p_{NFS_1} * P_{1E}$, respectively. Similarly, $NFS_2$ is modeled as two basic events $NFS_{2C}$ and $NFS_{2E}$ with probabilities of $p_{NFS_2} * P_{2C}$ and $p_{NFS_2} * P_{2E}$, respectively. The fatal shock $FS_1$ is modeled as a basic event contributed to the entire system failure directly. The analysis of the expanded fault tree in Figure 4 gives the system reliability considering the effects of shocks.

To evaluate the expanded fault tree models with the consideration of non-fatal and fatal shocks, a two-level binary decision diagrams (BDD) [9] based method can be used and it is referred to as Method 1 hereinafter. In the lower level, a BDD is built for each component subsystem, considering the failures of the component resulting from both independent causes and all non-fatal shocks. For example, Figure 5 shows the BDD for component $A$ of the example 5MR system, which is subject to failures due to s-independent cause and one non-fatal shock $NFS_1$. Figure 6 shows the BDD for component $E$, which is subject to failures due to s-independent cause and two non-fatal shocks $NFS_1$ and $NFS_2$. The evaluation of each subsystem BDD gives the total failure probability of the corresponding component. In the upper level, a system BDD is built with each node representing a component subsystem. Note that the effects of all fatal shocks are considered in the upper-level system BDD generation and evaluation. Figure 7 shows the upper-level BDD model of the expanded fault tree in Figure 4. The entire system reliability can be obtained via the evaluation of the system BDD using the total failure probabilities calculated at the lower level BDD evaluation.
and non-fatal shocks as 0.011765. The system reliability is thus 0.988235.

An alternative way (referred to as Method 2 hereinafter) to implement the hierarchical approach for the reliability analysis of static systems with shocks is to apply the total probability theorem for calculating the total failure probability of a system component at the lower level, as illustrated by the following examples.

Consider the example 5MR system in Section 3.1. Component A can fail due to either some independent cause (i.e., no shock occurring) or common-cause shock NFS1. The total failure probability of component A, denoted by \( TF_A \), can be calculated using the total probability theorem as:

\[
TF_A = \Pr(A | NFS_1) \cdot \Pr(NFS_1) + \Pr(A | NFS_2) \cdot \Pr(NFS_2)
\]

\[
= q_A \cdot (1 - p_{NFS1} \cdot p_A) + 1 \cdot p_{NFS2} \cdot p_A
\]

\[
= q_A + (1 - q_A) \cdot p_{NFS1} \cdot p_A
\]

This result matches that obtained via the evaluation of the lower-level BDD for component A in Figure 5.

The component E in the example 5MR system is subject to two non-fatal shocks NFS1 and NFS2. To apply the total probability theorem, we construct a shock event (SE) space, \( \Omega_e = \{ SE_1, SE_2, SE_3, SE_4 \} \). Each \( SE_i \) is a distinct and disjoint combination of NFS events that affect component E, i.e., \( NFS_{1E} \) and \( NFS_{2E} \). Specifically, \( SE = NFS_{1E} \cap NFS_{2E} \), \( SE_1 = NFS_{1E} \cap NFS_{2E} \), \( SE_2 = NFS_{1E} \cap NFS_{2E} \), \( SE_3 = NFS_{1E} \cap NFS_{2E} \), \( SE_4 = NFS_{1E} \cap NFS_{2E} \). Let \( \Pr(SE) \) be the occurrence probability of \( SE_i \). \( \Pr(SE) \) can be easily calculated based on the occurrence probabilities of the relevant NFS events and the relationship between the NFSs. In the example 5MR, the two NFSs are s-independent, we can calculate the occurrence probability of each SE as follows:

\[
\Pr(SE_1) = (1 - p_{NFS1} \cdot p_{1E}) + (1 - p_{NFS2} \cdot p_{2E}) \cdot \Pr(SE_2) = (p_{NFS1} \cdot p_{1E} + 1) \cdot (1 - p_{NFS2} \cdot p_{2E}) \cdot \Pr(SE_3) = (1 - p_{NFS1} \cdot p_{1E}) \cdot (p_{NFS2} \cdot p_{2E}) \cdot \Pr(SE_4) = (p_{NFS1} \cdot p_{1E}) \cdot (p_{NFS2} \cdot p_{2E})
\]

Based on the SE space, we can apply the total probability theorem to calculate the total failure probability of component E as:

\[
TF_E = \sum_{SE} \Pr(E | SE) \cdot \Pr(SE)
\]

\[
= q_E \cdot (1 - p_{SE1} \cdot p_{1E}) \cdot (1 - p_{SE2} \cdot p_{2E}) + 1 \cdot p_{SE3} \cdot p_{1E} + 1 \cdot p_{SE4} \cdot p_{1E} \cdot (1 - p_{SE2} \cdot p_{2E}) + 1 \cdot p_{SE4} \cdot p_{1E} \cdot (p_{SE2} \cdot p_{2E}) = q_E \cdot p_{SE3} \cdot p_{1E} + (1 - q_E) \cdot p_{SE4} \cdot p_{1E} \cdot (1 - p_{SE2} \cdot p_{2E}) \cdot (p_{SE2} \cdot p_{2E})
\]

This result also matches that obtained via the evaluation of the lower-level BDD for component E in Figure 6.

Based on the previous discussions for calculating the total failure probability of a component subject to one or two NFSs, we can easily extend the total probability theorem method to components subject to any finite number of NFSs. In general, we need to construct a SE space for the component subject to \( m \) NFSs and then apply the total probability theorem. The \( m \) NFSs will partition the event space into \( 2^m \) disjoint subsets or combinations of NFS events that affect the component \( K \), i.e., \( NFS_{1K}, NFS_{2K}, ..., NFS_{mK} \). Each \( NFS_{iK} \) has the occurrence probability of \( p_{k} \).

In summary, we can describe the hierarchical method based on the total probability theorem (Method 2) as the following three-step process:

1. **Lower-level/component-level evaluation:** calculate the total failure probability of each component subject to NFSs using the total probability theorem based method (equation (1)).

2. **Upper-level/system-level modeling:** build the fault tree model of the system with the consideration of fatal shocks, but without considering the effects of non-fatal shocks.

3. **Upper-level/system-level evaluation:** evaluate the system fault tree model built in step 2 using the total failure probabilities calculated in step 1 as the component failure probabilities. In particular, the BDD based method as described in the upper-level evaluation of Method 1 can be used. For example, evaluating the BDD constructed in Figure 7 with the use of the total failure probabilities obtained in step 1 gives the final reliability of the example 5MR system.

Note that the proposed Method 2 is different from the Efficient Decomposition and Aggregation (EDA) approach proposed in [13], which is also based on total probability theorem, in the following two major aspects:

1. **Method 2 can handle probabilistic non-fatal shocks, the occurrence of which results into failures of different components with different probabilities;** while the EDA approach can only handle deterministic non-fatal shocks, the occurrence of which results in the deterministic/guaranteed failure of components affected by the shock. Deterministic shocks are special cases of probabilistic shocks when all the conditional probabilities \( p_{ik} \) being 1.

2. **In Method 2, the total probability theorem is applied at the component level; while in the EDA approach, the total probability theorem is applied at the system level.**

### 5 MARKOV APPROACH FOR DYNAMIC SYSTEMS

In this section, we propose a Markov chain based approach for the reliability analysis of dynamic systems subject to common-cause shocks. The analysis of Example 2 (Section 3.2) is given to illustrate the proposed method.

As mentioned in the Introduction section, the traditional Markov chain based methods, which consider the component failures one by one, is not adequate for the reliability analysis of dynamic systems with probabilistic shocks. To account for the simultaneous occurrence of the probabilistic occurrence of multiple component failures resulting from a common-cause shock, we propose to combine the Markov approach with the
Poisson decomposition property [10].

According to the Poisson decomposition property, if a Poisson stream with rate $\lambda$ branches out into $n$ output paths or sub-streams such that each path occurs with a fixed probability, then these output paths are also Poisson streams with rates being $\lambda$ times the respective occurrence probability of the output path. Applying the above property to the Markov solution of Example 2, we can divide the stream/transition representing the occurrence of NFS into 4 output streams, each representing a disjoint combination of occurrence/non-occurrence of components affected by NFS. Figure 8 illustrates the decomposition process, where the four output paths represent that given the occurrence of NFS, 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, both $P_1$ and $P_s$ fail, respectively. The transition rates associated with those four output paths are respectively $\lambda_{NFS}*(1 - p_1)*(1 - p_s)$, $\lambda_{NFS}*p_1*(1 - p_s)$, $\lambda_{NFS}*(1 - p_1)*p_s$, $\lambda_{NFS}*p_1*p_s$, as shown in Figure 8.

Figure 8 – Application of Poisson decomposition law

Figure 9 shows the complete state transition diagram in the Markov solution to the example dynamic system (Example 2), incorporating the effects of fatal and non-fatal shocks via the Poisson decomposition law. The development of the diagram starts with an initial state representing all the three components ($P_1$, $P_2$, $P_s$) are working. The failure of $P_1$ would lead to the state ($P_2$, $P_s$) meaning that both $P_2$ and $P_s$ are working, but $P_1$ is failed. The rate associated with the transition from state ($P_1$, $P_2$, $P_s$) to state ($P_2$, $P_s$) includes the failure rate due to independent cause ($\lambda_{P_1}$) and the failure rate due to the non-fatal shock ($\lambda_{NFS}*(1 - p_1)*p_s$). From the state ($P_2$, $P_s$) we would reach state ($P_s$) when $P_2$ fails, and state ($P_2$) when $P_s$ fails. $P_2$ can fail only due to the independent cause with the rate of $\lambda_{P_2}$. Since we assumed that the cold spare component can fail in the standby condition only when it is hit by the shock, $P_s$ will fail before the failure of $P_2$ occurs. The transition from state ($P_2$, $P_s$) to state ($P_2$) will be associated with the rate of $\lambda_{NFS}*(l - p_1)*p_s$. Similarly other transitions and states can be developed. Note that since the occurrence of the fatal shock would result in the failure of all the system components, thus there is a direct transition from each non-absorbing state to the absorbing state (F) with the rate of $\lambda_{FS}$.

The evaluation of the above developed Markov chain using the parameters provided in Section 3.2, we obtain the unreliability of the example dynamic system with the consideration of effects from both non-fatal and fatal shocks as 0.3398. The system reliability is thus 0.6602.

A major disadvantage of the proposed solution is that it worsens the state space explosion problem of the Markov methods. As a result, it is suitable only for systems with small size and with a small number of non-fatal shocks. In practice, the modularization technique [11] can be used to minimize the use of the Markov model while retaining the efficiency of combinatorial solutions as much as possible. More efficient solution will be explored in the future work, to provide a viable solution to the reliability analysis of large-scale dynamic systems subject to non-fatal and fatal common-cause shocks.

6 CONCLUSIONS & FUTURE WORK

In this paper, we presented methods for the reliability analysis of systems subject to fatal and non-fatal shocks. Specifically, two hierarchical combinatorial methods based on binary decision diagrams and the total probability theorem were proposed for incorporating the effects of shocks into the reliability analysis of static systems; a Markov approach combined with the Poisson decomposition law was proposed for incorporating the effects of shocks into the reliability analysis of dynamic systems.

Future directions of this work include investigating more efficient solution to the reliability analysis of dynamic systems subject to shocks and performing more case studies on the reliability analysis of dynamic systems with sequence dependence and/or functional dependence. Another future work is to investigate the impact of jamming attacks on the network reliability via the shock models.

ACKNOWLEDGMENT

This work was supported in part by the National Science Foundation under grant CNS-0614652.

REFERENCES

1. S. Mitra, N. R. Saxena, and E. J. McCluskey, “Common-


**BIOGRAPHIES**

Liudong Xing, PhD
Department of Electrical and Computer Engineering
University of Massachusetts, Dartmouth
285 Old Westport Road,
North Dartmouth, MA, 02747, USA

e-mail: lxing@umassd.edu

Liudong Xing received her M.S., and Ph.D. degrees from the University of Virginia (U.Va.) in 2000, and 2002, respectively. She is now an Associate Professor with the Electrical and Computer Engineering Department, University of Massachusetts, Dartmouth. Dr. Xing served as a program co-chair for IEEE DASC’06, a program vice chair for ICESS’07 and ICPADS’08, and an associate guest editor for the Journal of Computer Science in 2006. She is the Editor for Short Communications in the International Journal of Performability Engineering. Dr. Xing is the recipient of the IEEE Region 1 Technological Innovation (Academic) Award in 2007. Her research interests include dependable computing and networking, reliability engineering, and sensor networks. Her research has been supported by National Science Foundation. She is an author or co-author of over 50 technical papers. She is a senior member of IEEE and a member of Eta Kappa Nu.

Prashanthi Boddu
Department of Electrical and Computer Engineering
University of Massachusetts, Dartmouth
285 Old Westport Road,
North Dartmouth, MA, 02747, USA

e-mail: pboddu@umassd.edu

Prashanthi Boddu received her B.E degree in Electrical and Electronics Engineering from Osmania University, College of Engineering, India in 2006. She is currently pursuing her M.S degree in Electrical and Computer Engineering at University of Massachusetts, Dartmouth. She has been working as a Research Assistant under Dr. Liudong Xing since January 2007. Her area of research focuses on reliability engineering.

Yan (Lindsay) Sun, PhD
Department of Electrical and Computer Engineering
University of Maryland, College Park
4 East Alumni Ave.,
Kingston, RI 02881, USA

e-mail: yansun@ele.uri.edu

Yan (Lindsay) Sun received her B.S. degree with the highest honor from Peking University, Beijing, China, in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Maryland in 2004. She is currently an assistant professor in the Electrical and Computer Engineering Department, University of Rhode Island. Her research interests include network security and wireless communications and networking. Dr. Sun received the Graduate School Fellowship at the University of Maryland from 1998 to 1999, and the Excellent Graduate Award of Peking University in 1998. She received NSF Career Award in 2007. She is a member of the IEEE Communication and Computer Societies.