Reliability Engineering and System Safety 131 (2014) 175–184

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Explicit and implicit methods for probabilistic common-cause failure analysis

Chaonan Wang [a,*], Liudong Xing [a,*], Gregory Levitin [b]

[a] University of Massachusetts, Dartmouth, MA, USA
[b] The Israel Electric Corporation, Haifa, Israel

ARTICLE INFO

Article history:
Received 24 January 2014
Received in revised form
16 May 2014
Accepted 27 June 2014
Available online 10 July 2014

Keywords:
Probabilistic common-cause failure
External shock
Internal factor
Reliability
Explicit method
Implicit method

ABSTRACT

The occurrence of a probabilistic common-cause failure (PCCF) in a system results in failures of multiple system components with different probabilities. A PCCF can be caused by external shocks or propagated failures originating from some components within the system. This paper proposes an explicit method and an implicit method to analyze the reliability of systems subject to internal or external PCCFs. Both methods can handle any arbitrary types of time-to-failure distributions for the system components. Both of the proposed methods are illustrated through detailed analyses of an example computer system. Applicability and advantages are also discussed and compared for the two methods.

1. Introduction

Common cause failures (CCFs) are failures of multiple components due to a shared root cause or a common cause (CC). The presence of CCFs in a system tends to increase the joint failure probabilities and thus contributes greatly to the overall unreliability of the system [1,2]. Therefore, it is significant to incorporate their effects in the reliability modeling and evaluation of systems subject to CCFs.

CCFs can be caused by some external factors (also known as shocks), such as malicious attacks, computer viruses, human errors, or extreme environmental conditions (hurricane, floods, lightning strikes) [7–9]. They can also be caused by propagated failures originating from some components within the system [3–6]. For example, the destructive effect originating from a system component failure such as fire, overheating, short circuit, blackout, explosion may destroy or incapacitate other system components.

Components affected by the same CC form a common cause group (CCG). The effect from a CCF on its CCG can be deterministic or probabilistic. A deterministic CCF (DCCF) results in guaranteed failures of all components within the CCG; whereas a probabilistic CCF (PCCF) results in failures of different components within the CCG with different occurrence probabilities [10,11]. For a practical example of PCCFs, consider a system of multiple gas detectors installed in a production room [24]. These gas detectors can be purchased at different times and from different companies, and thus be resistant to different levels of humidity. A shared root cause of a potential PCCF event is the increased humidity in the production room. This cause may fail the different gas detectors installed at different locations of the room with different probabilities. To be different from the CCG in the DCCF, we refer the CCG in the PCCF as probabilistic CCG (PCCG) hereafter.

Considerable research efforts have been dedicated to analyzing systems subject to DCCFs. The existing approaches can be classified into explicit and implicit approaches. The basic idea of the explicit approaches is to evaluate an expanded system model which is established by modeling the occurrence of each CC as a basic event shared by all the components affected by this CC (i.e., all the components of its CCG) in the original system model [12–14]. The basic idea of the implicit approaches is to develop the system model without considering the effects of DCCFs first and then evaluate the system model including the contributions of DCCFs by some special treatments [15–18].

To the best of our knowledge, very few works have considered PCCFs. Ref. [19] presents a binomial failure rate model to address PCCFs. However, the model can only be used to analyze systems with *s*-identical and *s*-independent components with the same fixed failure probability given the occurrence of a CC. Ref. [11] proposes more general methods that allow non-identical system components and non-identical component failure probabilities in the case of a CC occurring. However, the methods of [11] have a restrictive assumption that the conditional failure events of

---

* Corresponding author. Tel.: +1 5089998883; fax: +1 5089998489.
E-mail addresses: cwang2@umassd.edu (C. Wang), lxing@umassd.edu (L. Xing), levitin@iec.co.il (G. Levitin).

http://dx.doi.org/10.1016/j.ress.2014.06.024
0951-8320/© 2014 Elsevier Ltd. All rights reserved.

Acronyms

CC	Common Cause
CCF	Common Cause Failure
CCG	Common Cause Group
DCCF	Deterministic Common Cause Failure
FDEP	Functional DEPendency
PCCE	Probabilistic Common Cause Event
PCCF	Probabilistic Common Cause Failure
PCCG	Probabilistic Common Cause Group
BDD	Binary Decision Diagram

Nomenclature

X	a system component
X	local failure event of component X
X_i	failure event of component X caused by the *i*-th CC
X_{TF}	total failure event of component X
q_{iX}	occurrence probability of X_i
q_X	local failure probability of component X
Q_{jX}	total failure probability for component X under *j*-th PCCE
t	mission time
q	fixed failure probability
λ	constant failure rate for exponential distribution
λ_W	scale parameter for Weibull distribution
α_W	shape parameter for Weibull distribution
UR	system unreliability

different components due to the same CC are *s*-independent. Moreover, they are only applicable to external CCs (not internal CCs). In this work, we propose both an explicit method and an implicit method to analyze the reliability of systems subject to PCCFs while relaxing the limitations of the existing methods. The proposed methods are applicable to both internal and external PCCFs. Also, they allow a component to belong to multiple PCCGs with different probabilities.

The remainder of the paper is organized as follows. Section 2 presents an overview of the problem to be addressed. Section 3 presents an illustrative example. Section 4 presents the proposed explicit PCCF analysis method with the example illustration. Section 5 presents the proposed implicit PCCF analysis method with the example illustration. Section 6 discusses and compares the two proposed methods. Section 7 gives conclusions and directions for future work.

2. System description and problem statement

The paper considers the problem of reliability evaluation of systems subject to internal or external PCCFs. The system consists of elements with different individual failure probabilities. Some elements can fail also as a result of different common causes, which can be associated with external factors and with failures of other system components. The probability of failure caused by any common cause event is known for any element. The system structure function, which determines the state of the entire system for any combination of the states of the elements is given.

Fault tree is used to represent the structure function of a system in this paper [20]. The PCCF behavior is modeled by a PCCF gate which is based on the functional dependency (FDEP) gate as shown in Fig. 1 [11]. The input of the PCCF gate represents the trigger event of a CC occurring, which can be either an external shock or failure of an internal system component in this work. One or more dependent events represent failures of components affected by the CC (i.e., components appearing in the PCCG), and they are forced to occur with certain (maybe different) probabilities when the trigger event occurs.

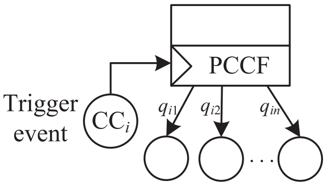

Fig. 1. The PCCF gate.

The following assumptions are used in the proposed methods:

- The component failure event caused by a CC and individual failure event for a component are *s*-independent.
- Failure cascading and loops are not considered, that is, the failure of a dependent component for a PCCF gate cannot trigger another PCCF gate.

3. An illustrative example

Fig. 2 illustrates a computer system consisting of two processors (P_1 and P_2), two buses (B_1 and B_2), Input/output (I/O), and three memory units (M_1, M_2, and M_3). The function of the system requires at least one of the two processors, at least one of the two buses, at least two of the three memory units, and the I/O be operating correctly. Fig. 3 illustrates the system fault tree model.

As shown in Fig. 3, the system is subjected to two external and *s*-independent CCs: CC_1 and CC_2. The occurrence of CC_1 affects processor P_1 and memory unit M_1. The occurrence of CC_2 affects processor P_1, bus B_1 and memory unit M_2. Thus, the two PCCGs are $PCCG_1=\{P_1, M_1\}$ and $PCCG_2=\{P_1, B_1, M_2\}$.

The following parameter values are used in the subsequent analysis using the proposed methods:

- Local or individual failure probabilities of components: $q_{P1}=q_{P2}=q_{B1}=q_{B2}=q_{I/O}=q_{M1}=q_{M2}=q_{M3}=0.01$.
- Occurrence probabilities of CCs: $p_{CC1}=p_{CC2}=0.001$.
- Conditional component failure probabilities conditioned on the occurrence of related CC: $q_{1P1}=0.2$, $q_{1M1}=0.5$, $q_{2P1}=0.3$, $q_{2B1}=0.4$, $q_{2M2}=0.6$. For example, q_{1P1} represents the conditional failure probability of processor P_1 given that CC_1 occurs. In this example, processor P_1 is affected by both CCs but with different probabilities.

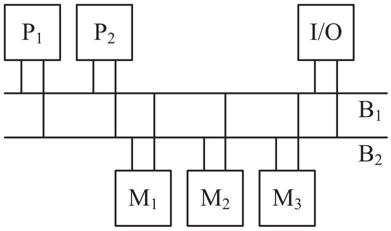

Fig. 2. The example computer system.