1

Introduction

The advances and interdisciplinary integration of science and technology are making modern engineering and computing systems more and more complex. For modern systems (especially those in, e.g. wireless sensor networks, Internet of Things (IoT), smart power systems, space explorations, and cloud computing industries), dynamic behavior and dependence are typical characteristics of the systems or products. System load, operating conditions, stress levels, redundancy levels, and other operating environment parameters are variables of time, causing dynamic failure behavior of the system components as well as dynamic system reliability requirements. In addition, components of these systems often have significant interactions or dependencies in time or functions. Effects of these dynamic and dependent behaviors must be addressed for accurate system reliability modeling and analysis, which is crucial for verifying whether a system satisfies desired reliability requirements and for determining optimal design and operation policies balancing different system parameters like cost and reliability. As a result, reliability modeling and analysis of modern dynamic systems become more challenging than ever.

Traditional reliability modeling methods, such as reliability block diagram [1] and fault tree analysis [2], can define the static logical structure of the system, but they lack the ability to describe dynamic state transfers of the system, and component fault dependencies and propagations. It is difficult or impossible to accurately reflect the actual behavior of modern complex fault-tolerant systems using the traditional reliability models. In other words, failure to address effects of dynamic behavior and dependencies of modem systems makes the reliability analysis results obtained using the traditional reliability models far from the actual system reliability performance, misleading the system design, operation, and maintenance efforts.

Different from the traditional static reliability modeling, the dynamic reliability theory considers that a system failure depends not only on the static logical combination of basic component failure events, but also on the timing of the occurrence of the events, correlations or interrelationship of the events, and impacts of operating environments. Therefore, the dynamic system reliability theory can provide a more accurate representation of actual complex system behavior, more effectively guiding the reliable design of real-world critical systems. The dynamic system reliability theory is the evolution and improvement of the traditional reliability modeling theory, and its research will promote the development and application of complex systems engineering.

This book focuses on dynamic reliability modeling of fault-tolerant systems with imperfect fault coverage, functional dependence, deterministic or probabilistic

Dynamic System Reliability: Modeling and Analysis of Dynamic and Dependent Behaviors,
First Edition. Liudong Xing, Gregory Levitin and Chaonan Wang.

common-cause failures, deterministic or probabilistic competing failures, as well as standby sparing.

Specifically, imperfect fault coverage is an inherent behavior of fault-tolerant systems designed with redundancies and automatic system recovery or reconfiguration mechanisms [3–5]. Just like any system component, the system recovery mechanisms involving fault detection, fault location, fault isolation, and fault recovery will likely not be perfect; they can fail such that the system cannot adequately detect, locate, isolate, or recover from a fault occurring in the system. The uncovered component fault may propagate through the system, causing an extensive damage to the system, sometimes failure of the entire system. Further, it is observed that the extent of the damage from an uncovered component fault occurring in a system with the hierarchical nature may exhibit multiple levels due to the layered recovery [6]. The traditional imperfect fault coverage concept has been extended to the modular imperfect fault coverage to model multiple levels of uncovered failure modes for components in hierarchical systems [7].

Functional dependence occurs in systems where the failure of one component (or, in general, the occurrence of a certain trigger event) causes other components (referred to as *dependent components*) within the same system to become unusable or inaccessible. A classic example is a computer network where computers can access the Internet through routers [8]. If the router fails, all computers connected to the router become inaccessible. It is said that these computers have functional dependence on the router.

In the case of systems with perfect fault coverage, the functional dependence behavior can be addressed as logic OR relationship [9]. However, for systems with imperfect fault coverage, the logic OR replacement method can lead to overestimation of system unreliability because it allows the disconnected dependent components (in the case of the trigger event occurring) to contribute to the system uncovered failure probability if they can fail uncovered. However, since these dependent components were disconnected or isolated, they could really not generate propagation effect or bring the system down [10]. New algorithms are required for addressing the coupled functional dependence and imperfect fault coverage behavior.

In addition to the imperfect fault coverage, common-cause failures are another class of behavior that can contribute significantly to the overall system unreliability [11–13]. Common-cause failures are defined as "A subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are direct results of a shared cause" [11]. Most of the traditional common-cause failure models assumed the deterministic failure of the multiple components affected by the shared root cause. Recent studies extended the concept to model probabilistic common-cause failures, where the occurrence of a root cause results in failures of multiple system components with different probabilities [14–16].

As one type of common-cause failures, a propagated failure with global effect (PFGE) originating from a system component can cause the failure of the entire system [17]. Such a failure can occur due to the imperfect fault coverage or destructive effect of a component failure on other system components (like overheating, explosion, etc.). However, PFGE may not always cause the overall system failure in systems with functional dependence behavior. Specifically, if the trigger event occurs before PFGEs of all the dependent components, these PFGEs can be isolated deterministically and thus cannot affect other parts of the system. On the other hand, if PFGE of any dependent component occurs before the trigger event, the failure propagation effect takes place, crashing

the entire system. Therefore, there exist competitions in the time domain between the failure isolation and failure propagation effects, causing distinct system statuses [18, 19].

The pioneering works on addressing such competing failures in system with functional dependence have focused on deterministic competing failures, where the occurrence of the trigger event, as long as it happens first, can cause deterministic or certain isolation effect to any failures originating from the corresponding dependent components. Recent studies [20, 21] have revealed that in some real-world systems, e.g. systems involving relayed wireless communications, the failure isolation effect can be probabilistic or uncertain. Consider a specific example of a relay-assisted wireless sensor network where some sensors preferably deliver their sensed information to the sink device through a relay node due to wireless signal attenuation. These sensors have functional dependence on the relay node. However, unlike in the deterministic competing failure case, when the relay fails, each sensor is not necessarily isolated because it may increase transmission power to be wirelessly connected to the sink device with certain probability dependent on the percentage of remaining energy. A sensor is isolated only when its remaining energy is not sufficient to enable the direct transmission to the sink node. Similarly, there exist time-domain competitions between the probabilistic failure isolation effect and the failure propagation effect that can lead to dramatically different system statuses. The modeling of such probabilistic competing failures is naturally more complicated than modeling the deterministic competing failure behavior.

Another common dynamic behavior of modern systems, especially life or mission-critical systems requiring fault-tolerance and high-level of system reliability, is standby sparing. In the standby sparing systems, one or several units are online and operating while some redundant units serve as standby spares, which are activated to resume the system mission in the case of the online unit malfunction occurring [3]. Components in the standby sparing systems often exhibit dynamic failure behaviors; they have different failure rates before and after they are activated to replace the failed online component [22–26].

The above described dynamic behaviors abound in real-world systems, as detailed in case studies in subsequent chapters. Due to the existence of these dynamic behaviors, not only the system structure function is seriously affected, but also the system reliability modeling and analysis become more complicated. Ignoring the dynamic and dependence of failures, or simply performing system reliability analysis under the assumption that components behave independently of each other, often leads to excessive errors and even draws wrong conclusions. The following chapters present models and methods to address effects of the dynamic and dependent behaviors for different types of systems, covering binary-state and multi-state systems, single-phase, and multi-phase systems.

The traditional reliability models are mostly applicable to binary-state systems in which both the system and its components assume two and only two states (operation and failure). However, many practical systems are multi-state systems [27–30], such as those involving imperfect fault coverage, standby sparing, multiple failure modes [31], work sharing [32], load sharing [33], performance sharing [34, 35], performance degradation, and limited repair resources [36]. In these systems, both the system and its components can exhibit multiple states or performance levels varying from perfect function to complete failure. The nonbinary property and dependencies among different states of the same component must be addressed in modeling a multi-state system.

In addition to addressing effects of the dynamic behavior for reliability modeling and analysis of multi-state systems, this book considers multi-phase systems, also known as phased-mission systems. Traditional system reliability models generally assume that a system under study performs a single phased mission, during which the system does not change its task and configuration [37]. Due to an increased use of automation in diverse industries such as airborne weapon systems, aerospace, nuclear power, and communication networks, phased-mission systems have become a more appropriate and accurate model for many reliability problems since the 1970s [38, 39]. These systems perform a mission that involves multiple and consecutive phases with possibly different durations. During each phase, the system has to accomplish a specified and often different task. In addition, the system can be subject to different stress levels, environmental conditions, and reliability requirements. Thus, the system configuration, success criteria (structure function), and component behavior may vary from phase to phase [13, 40]. These dynamics as well as statistical dependence across different phases for a given component make reliability modeling and analysis of multi-phase systems more difficult than single-phase systems.

In summary, dynamic reliability models and methods are presented in this book to address effects of single-level or multi-level (modular) imperfect fault coverage, functional dependence, deterministic or probabilistic common-cause failures, deterministic or probabilistic competing failures, standby sparing, multi-state, and multi-phase behaviors.

References

1 Rausand, M. and Hoyland, A. (2003). *System Reliability Theory: Models, Statistical Methods, and Applications*, 2e. Wiley Inter-Science.

2 Dugan, J.B. and Doyle, S.A. (1996). New Results in Fault-Tree Analysis. In: *Tutorial Notes of Annual Reliability and Maintainability Symposium*, Las Vegas, Nevada, USA.

3 Johnson, B.W. (1989). *Design and Analysis of Fault Tolerant Digital Systems*. Addison-Wesley.

4 Arnold, T.F. (1973). The concept of coverage and its effect on the reliability model of a repairable system. *IEEE Transactions on Computers* C-22: 325–339.

5 Dugan, J.B. (1989). Fault trees and imperfect coverage. *IEEE Transactions on Reliability* 38 (2): 177–185.

6 Xing, L. and Dugan, J.B. (2001). Dependability analysis of hierarchical systems with modular imperfect coverage. In: *Proceedings of The 19th International System Safety Conference*, 347–356. Huntsville, AL.

7 Xing, L. (2005). Reliability modeling and analysis of complex hierarchical systems. *International Journal of Reliability, Quality and Safety Engineering* 12 (6): 477–492.

8 Xing, L., Levitin, G., Wang, C., and Dai, Y. (2013). Reliability of systems subject to failures with dependent propagation effect. *IEEE Transactions Systems, Man, and Cybernetics: Systems* 43 (2): 277–290.

9 Merle, G., Roussel, J.M., and Lesage, J.J. (2010). Improving the Efficiency of Dynamic Fault Tree Analysis by Considering Gates FDEP as Static. In: *Proceeding of European Safety and Reliability Conference*, Rhodes, Greece.

10 Xing, L., Morrissette, B.A., and Dugan, J.B. (2014). Combinatorial reliability analysis of imperfect coverage systems subject to functional dependence. *IEEE Transactions on Reliability* 63 (1): 367–382.

11 NUREG/CR-4780. (1988). Procedure for Treating Common-Cause Failures in Safety and Reliability Studies. *U.S. Nuclear Regulatory Commission*; vol. I and II, Washington DC, USA.

12 Fleming, K.N., Mosleh, A., and Kelly, A.P. (1983). On the analysis of dependent failures in risk assessment and reliability evaluation. *Nuclear Safety* 24: 637–657.

13 Xing, L. and Levitin, G. (2013). BDD-based reliability evaluation of phased-mission systems with internal/external common-cause failures. *Reliability Engineering & System Safety* 112: 145–153.

14 Xing, L. and Wang, W. (2008). Probabilistic common-cause failures analysis. In: *Proceedings of the Annual Reliability and Maintainability Symposium, Las Vagas, Nevada* 354–358.

15 Xing, L., Boddu, P., Sun, Y., and Wang, W. (2010). Reliability analysis of static and dynamic fault-tolerant systems subject to probabilistic common-cause failures. *Proc. IMechE, Part O: Journal of Risk and Reliability* 224 (1): 43–53.

16 Wang, C., Xing, L., and Levitin, G. (2014). Explicit and implicit methods for probabilistic common-cause failure analysis. *Reliability Engineering & System Safety* 131: 175–184.

17 Xing, L. and Levitin, G. (2010). Combinatorial analysis of systems with competing failures subject to failure isolation and propagation effects. *Reliability Engineering & System Safety* 95 (11): 1210–1215.

18 Xing, L., Wang, C., and Levitin, G. (2012). Competing failure analysis in non-repairable binary systems subject to functional dependence. *Proc IMechE, Part O: Journal of Risk and Reliability* 226 (4): 406–416.

19 Wang, C., Xing, L., and Levitin, G. (2012). Competing failure analysis in phased-mission systems with functional dependence in one of phases. *Reliability Engineering & System Safety* 108: 90–99.

20 Wang, Y., Xing, L., Wang, H., and Levitin, G. (2015). Combinatorial analysis of body sensor networks subject to probabilistic competing failures. *Reliability Engineering & System Safety* 142: 388–398.

21 Wang, Y., Xing, L., and Wang, H. (2017). Reliability of systems subject to competing failure propagation and probabilistic failure isolation. *International Journal of Systems Science: Operations & Logistics* 4 (3): 241–259.

22 Xing, L., Tannous, O., and Dugan, J.B. (2012). Reliability analysis of non-repairable cold-standby systems using sequential binary decision diagrams. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans* 42 (3): 715–726.

23 Zhai, Q., Peng, R., Xing, L., and Yang, J. (2013). BDD-based reliability evaluation of k-out-of-(n+k) warm standby systems subject to fault-level coverage. *Proc IMechE, Part O, Journal of Risk and Reliability* 227 (5): 540–548.

24 Levitin, G., Xing, L., and Dai, Y. (2013). Optimal sequencing of warm standby elements. *Computers & Industrial Engineering* 65 (4): 570–576.

25 Levitin, G., Xing, L., and Dai, Y. (2014). Cold vs. hot standby mission operation cost minimization for 1-out-of-N systems. *European Journal of Operational Research* 234 (1): 155–162.

26 Levitin, G., Xing, L., and Dai, Y. (2014). Mission cost and reliability of 1-out-of-N warm standby systems with imperfect switching mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 44 (9): 1262–1271.

27 Zang, X., Wang, D., Sun, H., and Trivedi, K.S. (2003). A BDD-based algorithm for analysis of multistate systems with multistate components. *IEEE Transactions on Computers* 52 (12): 1608–1618.

28 Caldarola, L. (1980). Coherent systems with multistate components. *Nuclear Engineering and Design* 58 (1): 127–139.

29 Xing, L. and Dai, Y. (2009). A new decision diagram based method for efficient analysis on multi-state systems. *IEEE Transactions on Dependable and Secure Computing* 6 (3): 161–174.

30 Lisnianski, A. and Levitin, G. (2003). *Multi-state System Reliability: Assessment, Optimization and Applications*. World Scientific.

31 Mo, Y., Xing, L., and Dugan, J.B. (2014). MDD-based method for efficient analysis on phased-mission systems with multimode failures. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 44 (6): 757–769.

32 Levitin, G., Xing, L., Ben-Haim, H., and Dai, Y. (2016). Optimal task partition and state-dependent loading in heterogeneous two-element work sharing system. *Reliability Engineering & System Safety* 156: 97–108.

33 Kvam, P.H. and Pena, E.A. (2005). Estimating load-sharing properties in a dynamic reliability system. *Publications of the American Statistical Association* 100 (469): 262–272.

34 Levitin, G. (2011). Reliability of multi-state systems with common bus performance sharing. *IIE Transactions* 43 (7): 518–524.

35 Yu, H., Yang, J., and Mo, H. (2014). Reliability analysis of repairable multi-state system with common bus performance sharing. *Reliability Engineering & System Safety* 132: 90–96.

36 Amari, S.V., Xing, L., Shrestha, A. et al. (2010). Performability analysis of multi-state computing systems using multi-valued decision diagrams. *IEEE Transactions on Computers* 59 (10): 1419–1433.

37 Ma, Y. and Trivedi, K.S. (1999). An algorithm for reliability analysis of phased-mission systems. *Reliability Engineering & System Safety* 66 (2): 157–170.

38 Esary, J.D. and Ziehms, H. (1975). Reliability analysis of phased missions. In: *Reliability and Fault Tree Analysis: Theoretical and Applied Aspects of System Reliability and Safety Assessment*, 213–236. Philadelphia: SIAM.

39 Burdick, G.R., Fussell, J.B., Rasmuson, D.M., and Wilson, J.R. (1977). Phased mission analysis: a review of new developments and an application. *IEEE Transactions on Reliability* R-26 (1): 43–49.

40 Shrestha, A., Xing, L., and Dai, Y. (2011). Reliability analysis of multi-state phased-mission systems with unordered and ordered states. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans* 41 (4): 625–636.