Reliability Engineering and System Safety 136 (2015) 109–119

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Extended object-oriented Petri net model for mission reliability simulation of repairable PMS with common cause failures

Xin-yang Wu*, Xiao-Yue Wu

College of Information Systems and Management, National University of Defense Technology, Changsha, China 410073

ARTICLE INFO

Article history:
Received 26 March 2014
Received in revised form
18 November 2014
Accepted 27 November 2014
Available online 12 December 2014

Keywords:
Common cause failures
Extended object-oriented Petri net
Mission reliability
Modelling and simulation
Phased-mission system

ABSTRACT

Phased Mission Systems (PMS) have several phases with different success criteria. Generally, traditional analytical methods need to make some assumptions when they are applied for reliability evaluation and analysis of complex PMS, for example, the components are non-repairable or components are not subjected to common cause failures (CCF). However, the evaluation and analysis results may be inapplicable when the assumptions do not agree with practical situation. In this article, we propose an extended object-oriented Petri net (EOOPN) model for mission reliability simulation of repairable PMS with CCFs. Based on object-oriented Petri net (OOPN), EOOPN defines four reusable sub-models to depict PMS at system, phase, or component levels respectively, logic transitions to depict complex components reliability logics in a more readable form, and broadcast place to transmit shared information among components synchronously. After extension, EOOPN could deal with repairable PMS with both external and internal CCFs conveniently. The mission reliability modelling, simulation and analysis using EOOPN are illustrated by a PMS example. The results demonstrate that the proposed EOOPN model is effective.

1. Introduction

Complex systems (e.g., electronic system, aerospace system and nuclear power system) usually consist of several subsystems with different functions, and their mission execution processes are usually divided into a number of consecutive independent phases. For example, a mission execution process of an aircraft includes take-off, ascent, level flight, descent and landing phases, and each phase can be further divided into finer phases. In reliability literature, such systems are often modeled as phased mission system (PMS) [1–3].

Mission reliability of PMS is defined as its ability to successfully complete prescribed tasks in the mission profile under given conditions. Generally, there are several challenges to evaluate and analyze the mission reliability of PMS. They are: 1) the state of a component at the beginning of a phase depends on its state at the end of the previous phase; 2) components play different roles in different phases, for different phases may have different reliability logic requirements; 3) components may have different reliability parameters in different phases, because the system may be exposed in different environment in different phases; 4) the effects of CCF should not be neglected. CCF can be divided into two types: internal CCF (propagated failures originating from elements within the system) and external CCFs (e.g., sudden changes in environmental or power-supply disturbances) [14,27]. Redundancy technology is usually adopted for critical mission PMS to improve its mission reliability. However, it may be invalid when the external CCF occurs. Besides, the redundancy technology may increase the joint failure probabilities of PMS if it causes the propagated failure, because the failure of any element in a common cause group (CCG) can cause the failure of the entire group with some probability [4,5].

In general, the reliability analysis of PMS is addressed by two kinds of methods: Analytical methods and simulation methods [6,7]. Analytical methods can be further classified into three categories: 1) combinatorial methods [8–10]. Combinatorial methods are mainly based on binary decision diagram (BDD) algorithms which are effective in analyzing non-repairable PMS; 2) state-based approaches [11]. State-based approaches are mainly based on Markov model, which can consider each possible state of the repairable systems, but may have state space explosion problem with large number of components; 3) modular methods [12]. Modular methods are developed to analyze repairable PMS with large number of components. They could avoid the drawbacks of the previous two approaches to some extent. However, these approaches mainly apply to small-scale PMS problems due to the high computational complexity problem. Simulation methods

* Corresponding author. Tel.: +00 86 0731 13755095650.
E-mail addresses: wuxinyang525@126.com (X.-y. Wu), xiaoyuewucn@gmail.com (X.-Y. Wu).

http://dx.doi.org/10.1016/j.ress.2014.11.012
0951-8320/

Acronyms

BDD	Binary decision diagrams
BP	Broadcast place.
CCF	Common cause failure.
CCG	Common cause group.
CPN	Colored Petri net.
CSM	Component state model.
EOOPN	Extended objected-oriented Petri net.
MP	Message place.
OOPN	Objected-oriented Petri net.
PMM	Phase mission model.
PMS	Phased mission system.
PN	Petri net.
PSM	Phase state model.
RBD	Reliability block diagram.
SMM	System mission model.

NOTATIONS

P	Finite set of places.
T	Finite set of transitions.
A	Finite set of arcs.
S	Finite set of non-empty colors
C	Color function
Pre	Pre-mappings from $C(t)$to$C(p)$
$Post$	Post-mappings from $C(p)$to$C(t)$
M_0	The initial marking of EOOPN
S_N	Finite set of extended colored Petri nets
F	Finite set of arcs same as A
D_{dr}	Finite set of logic transitions
$e_i(p)$	Failure propagation probability for component i
$f_i(p)$	Common cause occurrence probability for component i

typically offer greater generality in system representation, but often demand much more computational time [13].

Petri net (PN) combines the merits of analytical methods and simulation methods. It has become a widely used tool for dynamic system modelling and simulation, since the computational time of applying PN for this type of simulation is acceptable [15,16]. PN has an intuitive graphical representation and its extension has been attracted more and more attention. For example, colored PN (CPN) defines complex data types (color) for its tokens [17,18], objected-oriented PN (OOPN) combines object-oriented concepts into PN [19].

Recently many researchers have attempted to use PN for modelling the reliability analysis of PMS. Chew describes the use of PN for reliability modelling of the MFOP and phased mission scenario, in which phase fault tree is transformed to PN model directly [15]. Winfrid shows that PN models could be a graphical description medium for many reliability scenarios, but are unsuitable when the PMS has lots of components [16]. Yang et al. use colored Petri net (CPN) to set up reusable general model for PMS. However, the numbers of nodes in the model grows exponentially with the number of phases [17]. Yang et al. propose an XML-based schema named RML to formally represent data and information used in building reliability model of TT&C system, and introduced an extended OOPN to perform mission reliability simulation [19].

However, above PMS methods do not take the CCF into consideration. Existing works considering CCFS have various limitations, such as focusing on either internal CCF or external CCF [5,20,21], having a single common cause that affects all the system components [22], considering CCFs in the analysis process rather than in the modelling stage [23,24], including a large number of CCF basic events in the system modelling [25,26], and only being applicable to systems with non-repairable components [14,20,21,27,28]. This work presents an extended OOPN (EOOPN) model for mission reliability simulation of repairable PMS subject to both internal and external CCFs. In particular, we consider two kinds of external causes. One causes the components of a CCG to fail directly while the other one only leads to the degradation of the components in the CCG.

The rest of this article is organized as follows. Section 2 introduces the formal specification of EOOPN and describes its ability for encapsulation and hierarchical modelling. Section 3 presents the mission reliability modelling approach by EOOPN for reliability evaluation of PMS with CCF in two cases in detail. Section 4 gives the simulation method and illustrates the given method through a typical PMS example with different kinds of CCFs. Finally, section 5 presents the conclusions and future research works.

2. Specification of EOOPN

EOOPN model is designed to facilitate mission reliability simulation and analysis of repairable PMSs. As shown below, it defines three new elements: subnet, logic transitions with "transition-colors" and broadcast place (BP). As the basic element of EOOPN, subnet uses an extended CPN to depict a component, a phase or a system. Subnets communicate and collaborate with each other through information carried by arcs between them. Logic transitions are used to describe the complicated logic relations between the various system components which are more convenient than traditional transitions. BP is introduced for transmitting information to large number of subnets in the model simultaneously. In this way, the topology structure of the EOOPN model is greatly simplified.

2.1. Colored Petri net

The subnet of EOOPN model extends the classic CPN which is defined as an 8-tuple $(P, T, A; S, C; Pre, Post; M_0)$ [18], where:

- P is a finite set of places, each of which is drawn as an ellipse (⬭);
- T is a finite set of transitions, each of which is drawn as a thin bar (▯);
- $A \subseteq P \times T \cup T \times P$is a finite set of arcs, each of which is drawn as an arrow($\rightarrow$);
- S is a non-empty finite set of colors;
- C is color function, $C = C(t) \cup C(p), t \in T, p \in P$, where $C(p)$ is the color set with places and $C(t)$ is the color set with transitions;
- Pre is the mapping from $C(t)$to$C(p)$;
- and $Post$ is the mapping from $C(p)$to$C(t)$;
- M_0 is the initial marking and $M_0 \in \mu C(p)$, where $\mu C(p)$ is a multi-set of $C(p)$.

2.2. EOOPN

EOOPN is defined as a 3-tuple (S_N, F, D_{dr}), where:

- S_N is a finite set of extended CPN model, each of which corresponds to either a phase or a component, drawn as a package icon (🗀);