Article citation info:
WU X, WU X. Mission reliability modeling and evaluation of multi-mission phased mission system based on an extended object-oriented Petri net. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2017; 19 (2): 244–253, http://dx.doi.org/10.17531/ein.2017.2.12.

Xinyang WU
Xiaoyue WU

MISSION RELIABILITY MODELING AND EVALUATION OF MULTI-MISSION PHASED MISSION SYSTEM BASED ON EXTENDED OBJECT-ORIENTED PETRI NET

MODELOWANIE NIEZAWODNOŚCI MISJI ORAZ OCENA SYSTEMÓW WIELOZADANIOWYCH O MISJACH OKRESOWYCH W OPARCIU O ROZSZERZONĄ SIEĆ OBIEKTOWĄ PETRIEGO

Multi-mission phased mission system (MM-PMS) is an extension of phased mission system (PMS) which is required to complete more than one missions for a period of time. Missions in MM-PMS usually have following characteristics: they have different mission starting and duration times; they share common components but with different combinational requirements; they have unequal occurrence probabilities. Therefore, reliability modeling and evaluation of MM-PMS is more complicated than that of PMS. This paper presents a general methodology based on the extended object-oriented Petri net (EOOPN) for mission reliability modeling and evaluation of MM-PMS with these characteristics. The proposed EOOPN model for MM-PMS includes five sub-models depicting MM-PMS at different levels of granularity. To demonstrate the effectiveness of the proposed model, mission reliability evaluation results of a simple MM-PMS case by EOOPN simulation methods are compared with those by binary decision diagram (BDD). Results show that the EOOPN model is suitable to depict the dynamics and to evaluate the reliability of MM-PMS.

Keywords: *Multi-mission phased mission system, extended object-oriented Petri net, mission reliability, reliability modeling, reliability evaluation.*

Wielozadaniowy system o misjach okresowych (ang. multi-mission phased mission system, MM PMS) jest rozszerzoną wersją systemu o misjach okresowych (ang. phased mission system, PMS). MM PMS to system, w którym zachodzi konieczność wykonania więcej niż jednego zadania w danym okresie czasu. Zadania (misje) w MM-PMS zazwyczaj charakteryzują się następującymi cechami: mają różne czasy rozpoczęcia i trwania; mają wspólne elementy, ale występujące w różnych kombinacjach; różnią się prawdopodobieństwem wystąpienia. W związku z tym, modelowanie i ocena niezawodności MM-PMS jest bardziej skomplikowana niż w przypadku PMS. W pracy przedstawiono ogólną metodologię opartą na idei rozszerzonej sieci obiektowej Petriego (EOOPN) służącą do modelowania niezawodności misji oraz oceny MM-PMS o podanych cechach. Proponowany model EOOPN dla MM-PMS obejmuje pięć modeli zależnych przedstawiających MM-PMS na różnych poziomach szczegółowości. Aby wykazać skuteczność proponowanego modelu, porównano wyniki oceny niezawodności misji dla prostego przypadku MM-PMS dokonanej metodami symulacji EOOPN z oceną przeprowadzoną metodą binarnego diagramu decyzyjnego (BDD). Wyniki pokazują, że model EOOPN można z powodzeniem stosować do obrazowania dynamiki oraz oceny niezawodności MM-PMS.

Słowa kluczowe: *Wielozadaniowy system o misjach okresowych, rozszerzona sieć obiektowa Petriego, niezawodność misji, modelowanie niezawodności, ocena niezawodności.*

1. Introduction

Phased-mission system (PMS) is a kind of complex system whose mission could be divided into a number of consecutive independent periods [1, 4]. As an extension of PMS, multi-mission phased mission system (MM-PMS) is used to accomplish several different missions, while a PMS only completes one mission during its mission time. Examples of MM-PMSs abound in many practical applications, such as the tracking, telemetry and command (TT&C) system [13, 17], rail transportation system, etc. For example, a TT&C system is used to support several missions like tracking different spacecrafts or receiving data from different spacecrafts for a period of time. These missions may have different starting times and duration times, but occupy same ground resources. Failure of these missions could lead to serious consequence, such as failure to launch the spacecraft or failure to receive useful information. Hence, it is necessary to evaluate the mission reliability of MM-PMS before its being putted into operation.

In general, mission reliability is defined as the probability to successfully complete a prescribed mission under given conditions [13]. So far, mission reliability analysis of PMS has attracted many researchers. Generally, there are two kinds of reliability evaluation methods: analytical methods and simulation method. Combinational method is one of the most effective analytical methods in analyzing non-repairable PMS which are mainly based on binary decision diagrams (BDD) algorithm, but has to combine with state-based approaches to deal with repairable PMS [7, 13]. State-based approaches could consider each possible state of the repairable systems [9]. However, they may suffer state space explosion problems when there are large number of components. Modular or hierarchical methods are provided to balance the drawbacks of the previous two approaches [5, 6]. But they have to make many hypothesis and could not fully consider the repairable cases; Simulation methods have less restriction and stronger representation power, but are time consuming to gain high accuracy [1, 3]. As research continues, more literature has addressed mission reliability analysis of PMS with more complicated cases, such as with repairable component [4, 11] , common cause failures [13, 14], imperfect fault coverage [15], multi-states [17]. How-

ever, to the best of our knowledge, mission reliability of MM-PMS has not been systematic studied.

Reliability evaluation of MM-PMS is more complicated than that of PMS because of its following characteristics: different missions in a MM-PMS have different mission starting times and phase duration times; missions in a MM-PMS are not independent due to overlapping phase durations and sharing common components; missions in a MM-PMS may have different importance degrees for conflict resolution; different missions may have unequal occurrence probabilities. Considering these characteristics, in this paper, the reliability of MM-PMS is defined as the proportion of successfully completed missions weighted by mission importance degree, and we present a simulation method for mission reliability modeling and evaluation of MM-PMS based on an extended object-oriented Petri net (EOOPN) model.

Petri net (PN) is an adaptable and widely used tool for dynamic system modelling and simulation, which combines the advantage of state-based methods and simulation methods [3,10,18]. To satisfy the requirement of complex system modelling, considerable work has been done on the extensions of PN models [1,2,10]. The proposed EOOPN in [11] was suitable for modeling of complex system. It introduced the concept of logic transitions to describe the complicated logic relations between the various system components and broadcast place to transmit information to the large number of objects in the model simultaneously. Compared with other PN models, EOOPN had been demonstrated to have good readability and reusability. However, the EOOPN model for PMS in [11] did not consider multi-missions with different mission starting times, missions with overlapping durations, with different importance degrees and occurrence probabilities. As a result, the model in [11] has difficult in reliability evaluation of MM-PMS. In this paper, we further extend the EOOPN by introducing a competitive-handling mechanism which is used to deal with component sharing and conflict in overlapping durations.

The rest of this paper is organized as follows. Section 2 presents the mission reliability definition of the MM-PMS. Section 3 provides the EOOPN model for mission reliability evaluation of MM-PMS and outlines the simulation procedure. Section 4 illustrates the proposed method via an example. The results obtained by the proposed methods are compared with a BDD based analytical method to show its effectiveness for mission reliability evaluation of MM-PMS. Finally, section 5 presents some conclusions.

2. Mission reliability definition and model assumptions

2.1. Mission reliability definition of MM-PMS

Reliability of MM-PMS depends on the component reliability parameters, mission duration times, mission logic structures of components, mission importance, and mission occurrence probability. Suppose that a system consists of n components and has to accomplish m missions, the mission importance degree of mission M_i is W_i ($i \in \{1,2,...,m\}$), and the occurrence probability of a mission M_i is P_i ($i \in \{1,2,...,m\}$).

Supposed that the reliability distributions and parameters of each component are given, according to the law of large numbers, the sample average value can be viewed as an approximated of true value, so the point estimated value of the reliability of MM-PMS including m missions could be evaluated based on Monte-Carlo sample method after Nth simulation.

When the missions in a MM-PMS are independent (there is no conflict among each mission), we have:

$$R = \sum_{j=1}^{N} \sum_{i=1}^{m} W_i P_i R_i / N ,$$

where R_i is the mission reliability of mission M_i, W_i is the importance of mission M_i and P_i is the occurrence probability of mission M_i.

When there are conflicts among missions, only the mission with higher W_i can be executed. In this case, the above equation should be changed with the real MM-PMS examples.

2.2. Assumptions

In the sequel, the following assumptions of MM-PMSs are made [1, 11, 17]:

1) The phases durations of each mission are fixed, and phases of each mission are ordered in a predetermined sequence;
2) A mission is considered to be failed if any one of its phases fails;
3) Maintenance resources are adequate, and repair is carried out immediately after failure occurs;
4) A component is as good as new after its repair;
5) A component has three modes: free, busy and failure;
6) A phase task has four states: activation waiting, activation, success and failure;
7) The importance degree and the occurrence probability of a mission are predefined fixed values.

3. EOOPN models for reliability evaluation of MM-PMS

EOOPN model is designed to facilitate mission reliability simulation and analysis of complex systems [11]. It consists of subnets to encapsulate internal behaviors of an object, broadcast place to transmit shared information without time delay, logic transitions (similar to the logic gates in fault tree) to depict logics and arcs linking subnets and logic transitions.

3.1. The general EOOPN specification

As introduced in [11], EOOPN is defined as a tri-tuple (S_N, F, D_{dr}), where:

S_N is a finite set of extended CPN model drawn as a package icon (▭); the extended CPN is defined as an eight-tuple $(P, F, D_{dr}; S, C;\ Pre, Post;\ M_0)$: P is a non-empty finite set of places with three kinds of places, they are simple place drawn as an ellipse ⬭, information place drawn as a circle and broadcast place drawn as a circle with two vertical bars ⊗; D_{dr} and F are defined as follows; S is a non-empty finite set of colors. C is a color function to set place color and transition color. Pre and $Post$ are pre and post mappings between places and transitions. M_0 is the initial places markings;

F is a finite set of arcs, via which subnets transfer tokens. EOOPN defines two kinds of arcs: simple arc, drawn as an arrow (⟶), and information arc, drawn as an arrow with dashed line (⇢). Tokens will not be removed from the output place after a transition fired when it is linked by an information arc;

D_{dr} is a finite set of logic transitions (Delay transition ▮, AND transition ▱, OR transition ▱, N/R transition R/N, and Probability transition r) [11]. Probability transition and Delay transition have more than one transition modes defined by transition-colors. Different transition-colors in Delay transition represents different transition

modes with different transition delay times, and that of probability transition means different firing probabilities.

3.2. EOOPN reliability Models for MM-PMS

S_N of EOOPN in [11] is used to represent a single phase or a component, in this paper, it can also represent a single mission. Additionally, token of EOOPN in [11] has a unique 'ID' to separate each other, an attribute 'state' depicting its state, an attribute 'priority' deciding its firing order. There are three kinds of tokens defined in this paper: mission token, which has a 'task' attribute to record the phase ID in execution state in the mission; phase token, which has a 'path-set' attribute to record all the minimal-paths of the phase task; For example, a phase has two components 1 and 2. If the two components are parallel, its 'path-set' attribute is 1+2. If the two components are serial, its 'path-set' attribute is 1*2; component token, which has an 'occupant' attribute to record the phase ID it working in. These attributes are designed to solve component conflict in simulation of MM-PMS reliability evaluation.

Transition is used to change the state of a component, a phase or a mission. All kinds of transitions in [11] have difficulty in correctly and clearly changing states of missions, phases and components during phase overlapping durations. When two or more missions have overlapping duration, we have to judge whether these missions have conflict. Thus, another kind of logic transition is added called comparison transition drawn as C. Before activate the missions, a corresponding comparison transition will fire. Firstly, the comparison transition will obtain the phase ID in execution or the phase ID needing to be activated from 'task-state' attribute of the missions. Then, according to the unique IDs, the corresponding phase tokens can be found. The comparison transition will compare the 'path-set' attributes of these phases. When their path-sets are same, these phases are common phases. The phase task in execution could continue and the phases needed to be activated can start. When there is a minimal path (we call it feasible path in the following) of the phase needing to be activated has no common component with those in a minimal path of the phase in execution, the phase needing to be activated has no conflict with the phases in execution. In this case, the comparison transition will send a release information to the components in the feasible path, and thus the phase needing to be activated will be activated immediately. When there is no feasible path of the phase needing to be activated, task conflict will occur. In this case, the comparison transition will compare the 'priority' attribute of these missions. The mission with higher priority can be continued or be successfully activated, while the mission with lower priority will be terminated or failed in activation.

Fig. 1 uses an example with two missions to explain the algorithm of the comparison transition. It has three kinds of output results named as case1, 2, and 3. Five kinds of EOOPN sub-models are defined for mission reliability evaluation of MM-PMS to ensure model generality. They are: multi-mission model (MMM), controlling the starting time and duration time of each mission; mission state model (MSM), reflecting the states of a mission on real time; phase execution model (PEM), depicting the states of each phase on real time (failed or executing); phase logic model (PLM), describing the phase mission logic; component execution model (CEM), governing the change of component state according to its failure time distribution, repair time distribution and work duration time.

In the following part of this section, we will introduce the preceding models in detail.

3.2.1. CEM for MM-PMS

Component is the basic unit to support mission implementation. CEM is designed to depict the change of component state. During the whole system mission, each component is assumed to be in one of the three states: free, busy, or failure. Fig. 2 shows a general CEM for a repairable component, with the symbols explained as follows:

111-mp1: storing activation request place storing activation request from the phase execution model, capacity is 1;
111-mp2: storing release request from the phase execution model, capacity is 1;
p1: component in free state;
p2: component in busy state;
p3: component in failure state;
b1: the latest state information of a component token;
ADR1: enabled when p1 has a free component token and mp1 has a cooperation activation request token for the component token, an instantaneous transition;
ADR2: enabled when p2 has a busy component token and 111-mp2 has a release request token for the component token, an instantaneous transition;
t1: component fails. The delay time is governed by failure distribution of the enabled token;
t2: component repairs. The delay time is governed by repair distribution of the enabled token.

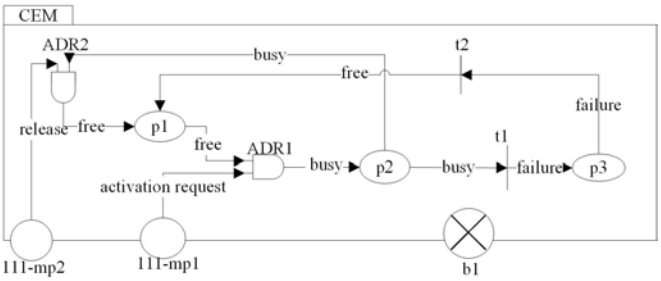


Fig. 2. A general CEM

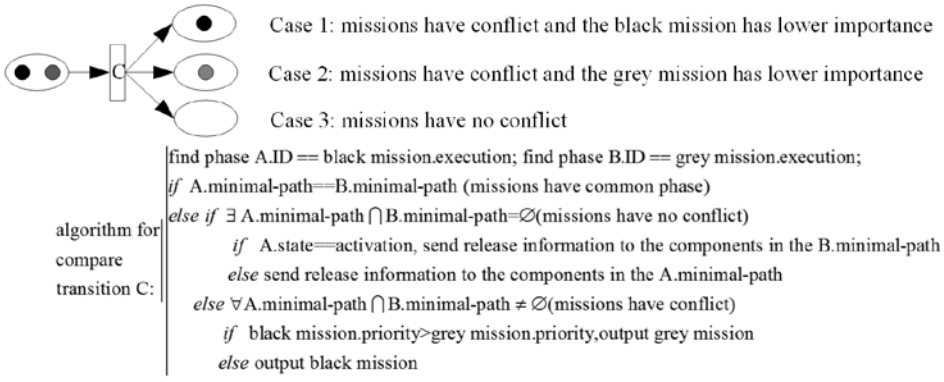


Fig. 1. Example of comparison transition

The notes on the arc are used to depict the required input tokens states that enable a transition or the output tokens states after the transition fires.

Initially, a component token in the 'free' state is put in p1. ADR1 will fire after 111-mp1 receives an activation request token. After ADR1 fires, the token state in p1 will be updated to 'busy' and be transmitted to p2. Meanwhile, its attribute 'occupant' will be updated to the task activation request token ID in 111-mp1. If there is no component failure occurring before 111-mp2 receives the token release information, ADR2 fires,

and the component token will be released and sent back to p1. If component failure occurs, t2 fires and sends a component token in 'failure' state to p3. The simulation clock will be advanced according to failure occurrence time. During this period, once the component state changes, the latest state will be transmitted to b1 and be broadcasted by b1 without time delay. Arcs from transitions ADR1, ADR2, t1 and t2 to b1 are not shown in Fig. 2 for better readability. Transitions t1 and t2 have different types of transition colors. The actual choice of transition colors depends on the component that enables the transition. Their firing time are sampled by the Monte-Carlo methods. Besides, places with capacity equal to 1 meaning the token in them will be replaced by the new arrival.

3.2.2. PLM for MM-PMS

In this paper, PLM is designed to depict phase mission logic. Its input information is the state of each related components, and the output information is the mission state of this phase (a phase token is a kind of information token). PLM of a particular phase can be transformed from its fault tree model (FT) directly. Fig. 3 uses a series structure as an example to illustrate the transformation approach. From which we observe that PLM elements with grey color are totally consistent with the FT model. Therefore, the PLM model of a phase can be easily built after its phase FT model is determined.

The meaning of the places and transitions in Fig. 3 are given below:

11-mp1: phase token in activation state, capacity is 1;
ADR1: enabled when 11-mp1 has activation request tokens and b1 has component states, instantaneous transition;
ADR2: enabled when component a and b are in free states, instantaneous transition;
ODR1: enabled when either component a or b is in failure states, or at least one of them is occupied by other task, instantaneous transition;
b1: the latest states of components and mission states of phases.

When 11-mp1 receives a phase token in activation, ADR1 fires and the related components states information will be sent to the corresponding places. The arc from mp1 to ADR1 is an information arc. That is, token in mp1 will not be removed after ADR1 fires. Thus, until the phase finish time or phase failure occurrence, any of the components states change will enable ADR1. PLM can generate three kinds of phase state: 1) 'activation', when the related components in 'free' state match the reliability logic, ADR2 fires and phase token state in b1 is updated to 'activation'; 2) 'failure', during the phase duration time, once the failure logic of the phase is matched, ODR1 will fire and token state of this phase in b1 will be updated to 'failure'. Different from PMS, phase task in MM-PMS has two failure modes: one is caused by component failure, and the other is caused when the required components occupied by other missions. As mentioned above, a component token has an 'occupant' attribute recording the phase task ID which occupied it. If the information of the occupant of a token is not equal to the ID of this PLM Petri net, it means this token has been occupied by other phases with higher importance. Thus, arcs from 'a' or 'b' to 'ODR1' are noted with 'failure or occupant.ID! = PLM.ID ' which are used to depict component failure or occupied by other missions respectively. Except for the above two cases, phase token state remains unchanged (the original phase token state is 'activation waiting').

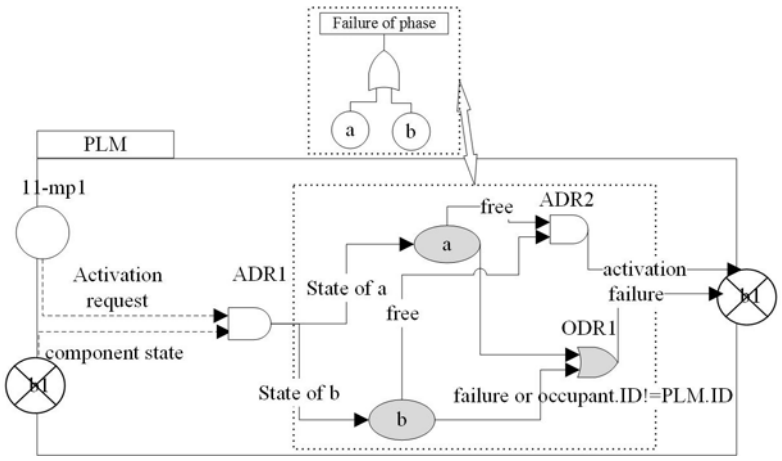


Fig. 3. A PLM example with series failure logic

3.2.3. PEM for MM-PMS

PEM is designed to control the phase task process according to the phase state from PLM. Different from PMS, there are three kinds of failure modes in PEM for MM-PMS: 1) activation failure, components supporting this phase is occupied by another mission with higher mission importance degree before mission starts; 2) component failure, components supporting this phase fail during the phase duration; 3) conflict failure, components working in this phase taken away by another mission with higher mission importance degree during the phase task duration. PEM for MM-PMS considering these three kinds of failures is shown in Fig. 4. The meaning of the places and transitions in it are given below:

1-mp1: phase task activation request from MSM, capacity is 1;
1-mp2: component activation request to CEM, capacity is 1;
p1: phase task activation request to obtain state information from PLM, capacity is 1;
p2: phase task activation request to activate phase task, capacity is 1;
p3: phase state from PLM, capacity is 1;
p4: phase task in execution state;
mp3: phase task finishing information from MSM, capacity is 1;
mp4(result_place): phase task in success state;
mp5: release information to CEM, capacity is 1;
mp6: phase interrupt information from MSM, capacity is 1;
b1: the latest states information of the phase;
t1: request to activate phase task, instantaneous transition;
t2: fail to activate phase task, delay transition;
ADR1: enabled when p1 has activation request token and b1 has phase state tokens, instantaneous transition;
ADR2: enabled when p3 has phase in 'activation waiting' state token and p2 activation request token, instantaneous transition;
ADR3: enabled when mp3 has a release token and p4 has a phase token in execution state, instantaneous transition;
ADR4: enabled when p3 has a phase state token in failure state and p4 has a phase token in execution state, instantaneous transition;
ADR5: enabled when mp6 has a interrupt information and p4 has a phase token in execution state, instantaneous transition.

After a PEM model being initialized, b1 will receive a phase token in 'activation waiting' state. When mp1 receives a phase activation request information, t1 fires and sends the request information to p1, p2. Token in p1 is used to enable ADR1 to obtain the lasted phase state information. Token in p2 is used to enable ADR2 to start the phase task.

Arc from p1 to ADR1 is an information arc. Once the phase state changes, ADR1 will fire. Hence, p3 can obtain the latest phase state. When the latest phase state is 'activation', i.e., the components supporting this phase task are available, ADR2 will fire and put a phase token in execution state to p4, a component activation request token to 1-mp2 to activate the corresponding CEM. When the latest state of the phase is 'activation waiting', i.e., the phase task cannot be

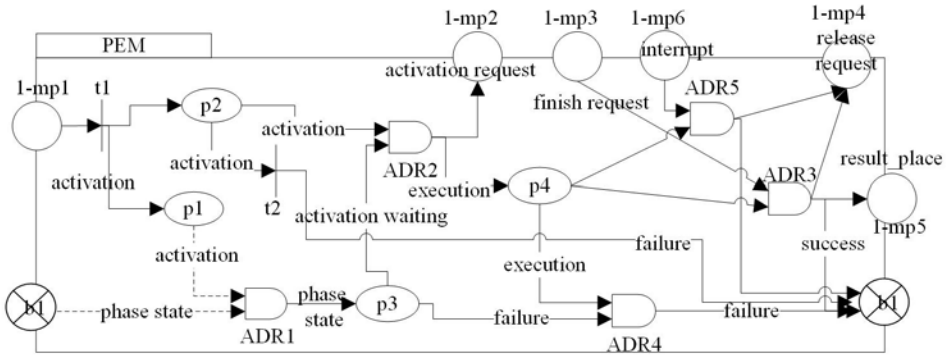


Fig. 4. A general PEM

activated at time moment. Transition t2 is a delay transition whose delay time is equal to the tolerant activation buffer time of the phase. In engineering, it is equal to the interval time between the latest start time of the phase mission and the present time. For example, if the delay time of t2 is 5, it means the phase task can be activated during $[t, t+5]$, where t is the firing time of transition t1. Therefore, if the latest phase state turns to 'activation' during this period, phase task also can still be activated (ADR2 will fire). Otherwise, t2 will fire and b1 will update the phase state to 'failure' (activation failure).

If ADR2 fires, phase task begins to execute. Under this situation, if p3 receives a 'failure' phase state token before mp3 receives a finishing request token, ADR4 will fire immediately and b1 will update the phase state to 'failure' (component failure). Besides, if mp6 receives a task interrupt token, ADR5 will fire and b1 will update the phase state to 'failure' (conflict failure). Only when the above two kinds of failures do not occur, will ADR3 fire and send a phase success token to mp4, and b1 update the phase state to 'success'. Place mp4 is a result_place used to estimate the reliability of each phase.

3.2.4. MSM

MSM controls the simulation process of a mission. Fig. 5 is an example MSM with two phases. From which, we observe the two parts in the dashed rectangle are identical. They are used to activate the corresponding phase task and update the mission state according to the phase state from PEM. In cases that a mission has more phases, add same number of dashed rectangle parts. The meaning of the places and transitions in Fig. 5 are given below:

mp1: phase activation request to PEM and PLM, capacity is 1;
p1(p4, p5): phase token with ID phase1(phase 2) in execution state, capacity is 1;
p2, p3(p6): phase token with ID phase1(phase 2) in success state, capacity is 1;
1-mp1(2-mp1): phase token with ID phase1 (phase 2) in activation state, capacity is 1;
1-mp3(2-mp3): phase token with ID phase1 (phase 2) in success state, capacity is 1;
mp3: information token in success state;
mp4: information token in failure tate;
mp5: mission interrupt information from MMM;
t1 (t3): activate phase task 1 (2), instantaneous transition;
t2 (t4): terminate phase task 1(2), delay transition whose delay time is equal to the duration time of phase 1 (2);
ADR1 (ADR3): enabled when p1(p5) has phase token and b1 has phase failure state, instantaneous transition;
ADR2 (ADR4): enabled when p2(p6) has phase token and b1 has phase success state, instantaneous transition;

After place mp1 receives a mission activation request, transition t1 will fire and send phase token in activation state to 1-mp1 to activate PEM for phase 1, and will send a token represent mission in 'activation' state in p1 to enable ADR1. When p1 has tokens, transition t2 is enabled. It can fire after the duration time of the phase. The firing priority of ADR1 is higher than that of t1. Therefore, if the latest phase state turns to failure before t2 could fire, ADR1 will fire, and send a token representing mission in 'failure' state to mp3. If not, t2 will fire, and send a phase token in 'success' state to p3. A phase task could be activated when its previous phases end in success. As a result, only when place p3 has token, could t3 fire to start phase task 2. The next phases will go on in the same way as the first phase. Arcs from transitions ADR1, ADR3 and ADR4 to b1 are not shown in Fig. 5 for better readability. Place mp5 is used to receive the mission interrupt information from MMM and transmit the information to the PEMs. Note that b1 is a global broadcast place. The whole EOOPN for a MM-PMS has only one b1.

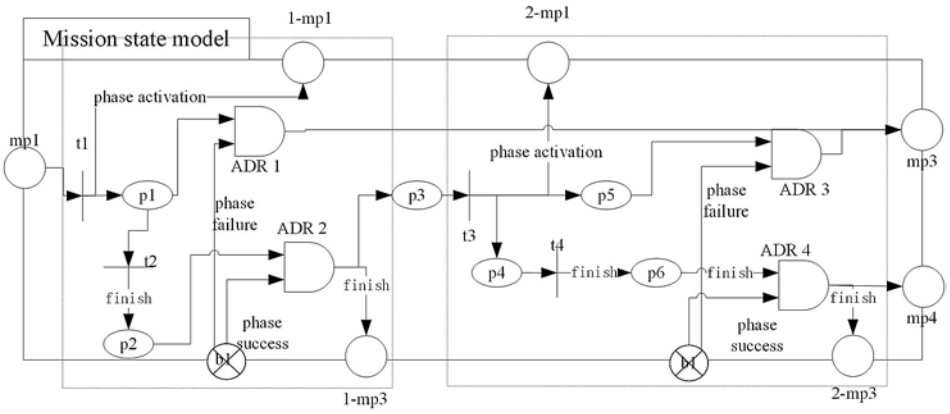


Fig. 5. A MSM with two phases

3.2.5. MMM for MM-PMS

MMM is used to activate and terminate all the missions. The activation of a mission depend on its planned activation time point and occurrence probability. Fig. 6 shows a general MMM for MM-PMS. The meaning of the places and transitions are given below:

m-mp1: missions in waiting state;
m-mp2: mission activation request to MSM;
m-mp3: mission interrupt information to MSM;
p1: mission in activation judgement state;
p2: missions in execution state;
$m_1(m_n)$: mission $m_1(m_n)$ in execution state;
$r_1(r_n)$: result place for mission $m_1(m_n)$
t1: delay transition and the delay time depends on the mission planned starting time;

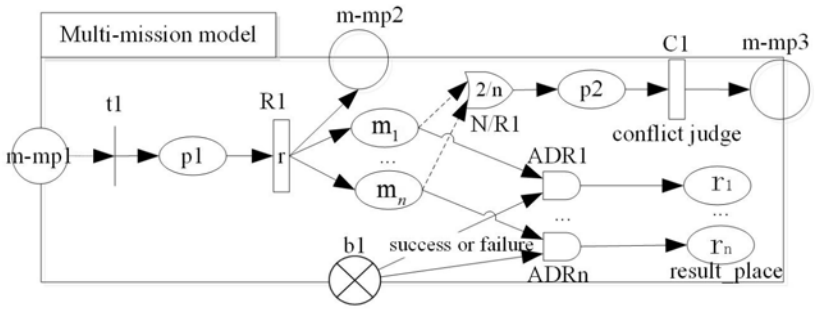


Fig. 6. A general MMM

R1: probability transition, the occurrence probability depends on different missions;

N/R1: enabled when two or more places have mission tokens, instantaneous transition;

ADR1 (ADRn): enabled when $m_1(m_n)$ has mission token and b1 has mission success or failure state token to terminate mission 1(n) , instantaneous transition;

C1: comparison transition, instantaneous transition.

Different mission tokens in place m-mp1 are used to start different missions. Transition t1 has different transition colors used to depict different mission starting time. For example, supposed that there are two missions M_1 and M_2. Both M_1 and M_2 can enable transition t1, and t1 will have two corresponding transition colors. Given that M_1 occurs every 100 hours and M_2 occurs every 150 hours, t1 fires with transition color M_1 firstly and the simulation clock will be pushed to 100h. Note that arc from m-mp1 to t1 is an information arc, so a mission could happen more than once during the whole mission time. Then when the simulation time is pushed to 150h, t1 fires with transition color M_2. As a probability transition, R1 has different transition colors to represent different mission occurrence probabilities. If a mission is activated, its corresponding token will be put into the execution state places. During the mission duration, if there is another mission occurs, N/R1 will fire. Then the comparison transition C1 will fire. If there exists mission conflict, the interrupt information for the phases of a mission will be transmitted to m-mp3. If not, all the missions could continue. When the latest state of a mission in b1 turns to 'failure' or 'success', the corresponding transition ADR will fire and transmit the mission state to the corresponding result_place which is used to estimate the system mission reliability.

Fig. 7 shows the interactions among the five sub-models. Simulation begins with the MMM. When m-mp2 has tokens, a mission activation request will be transferred to the corresponding MSM. Then MSM will send the phase activation request to PEM and PLM. PEM will send component activation request to CEM. PLM begins to receive the latest state information of components of this phase from broadcast place and updates phase state in terms of task logic. PEM also begins to monitor the phase process in real time. When simulation reaches a mission's first phase finish time, MSM transfers the finish request to PEM. After receives the finish request, PEM will update the mission state according to the phase state. Meanwhile, PEM will send release information to relevant CEMs. If the phase state is success, the mission state is in execution. Otherwise, the mission state is failure. Until the state of the last phase of a mission is success, the mission's state will be updated to success, and this information will be transferred to MSM. Besides, when task conflict occurs, MMM will send an interrupt information to the MSM then the MSM will transmit the information to the related PEM.

Simulations of the five sub-models are done by movement of tokens among places in or between different object models through firing of transitions. The reliability of each mission can be estimated by statistics of the tokens in the result_place in MMM, and the reliability of each phase can be estimated by the statistics of the tokens in the result_place in PEM.

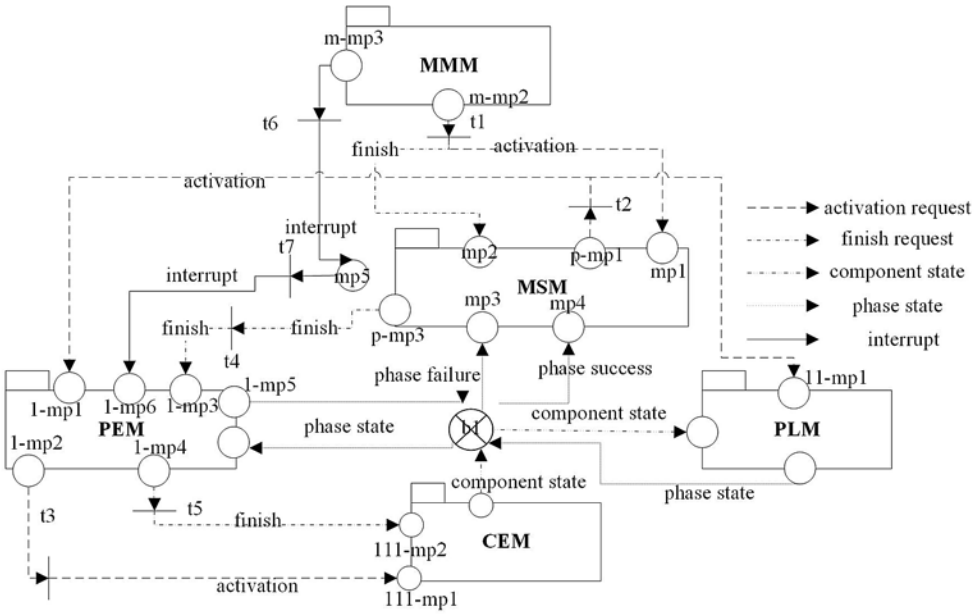


Fig. 7. Interaction between sub-models

4. Case Study

In this section, an example MM-PMS is used to illustrate the procedure and verify the effectiveness of the proposed EOOPN simulation method.

Supposed that an example MM-PMS has 12 binary components and two missions. The reliability block diagram for the first system mission and the second system mission are shown in Fig. 8. The starting times of missions A and B are the same, and the phase duration times of them are $\mathbf{T_A} = (100,160,100,150)^T$ and $\mathbf{T_B} = (200,180,160)^T$. The failure time distribution of each component follows exponential distribution, with failure rates as shown in Table 1.

4.1. An example with non-repairable component

To verify the effectiveness of the model and the simulation method, the BDD analytical algorithm proposed by Xing and Levitin [13] is used. Generally, the BDD method applied in mission reliability evaluation of PMS requires that the components are non-repairable. For comparison purpose, the components in the example MM-PMS are supposed to be non-repairable. The BDD models for mission A and mission B are shown in Fig. 9. We use two different cases shown in Table 2.

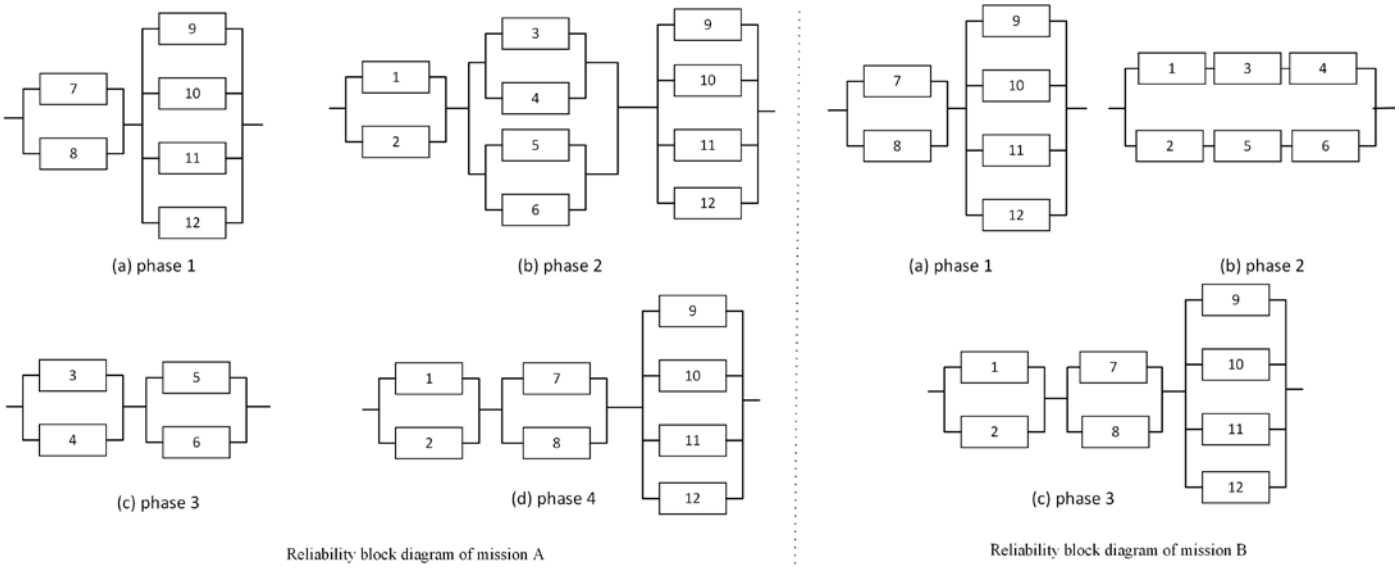


Fig. 8. Reliability block diagram of missions A and B

*Table 1. Failure rate of each component *10^{-3}*

	Mission A				Mission B		
Components	1	2	3	4	1	2	3
1,2	0.0	0.15	0.0	0.15	0.0	0.12	0.15
3,4,5,6	0.0	0.3	0. 2	0.0	0.0	0.2	0.0
7,8	0.11	0.0	0.0	0.12	0.11	0.0	0.12
9,10	0.2	0.15	0.0	0.3	0.2	0.0	0.3
11,12	0.05	0.15	0.0	0.13	0.05	0.0	0.13

In case one, both mission A and mission B will occur, and their occurrence probabilities are both equal to 1.

Table 3 shows the conflict resolution for mission A and mission B in each time interval. From which we observe that conflict occurs when system mission moves to phase 3 of mission A. Mission B has higher importance degree. Thus, only mission B could be executed.

Although in this case, only mission B could succeed, the system reliability is not equal to the mission reliability of B, for mission A also be executed before conflict occurs. According to the system structure function in Table 3, the MM-PMS is divided into 5 phases, and BDD models for the MM-PMS is shown in Fig. 10.

By the BDD analytical algorithm, mission reliability of the MM-PMS is obtained as 0.5921.

In case two, mission A and mission B have different occurrence probabilities. When both mission A and mission B occur, only mission B continues. When only mission A occurs, mission reliability of the MM-PMS could be calculated based on the mission reliability of the mission A. Based on the BDD algorithm, in this case, mission reliability of the MM-PMS is equal to 0.8696.

Table 2. Two different cases

	Case one		Case two	
	importance	occurrence probability	importance	occurrence probability
Mission A	1	1	1	1
Mission B	2	1	2	0.3

The EOOPN modeling and simulation procedure of these two cases are the same, except with different simulation parameters. The simulation steps are as follows:

Step 1: build the MMM. Put two information tokens with color A and B to represent mission A and B in place m-mp1 in Fig. 6 to activate the simulation. Priority attribute of the token representing mission A is 1 in both case one and two, while that of the token

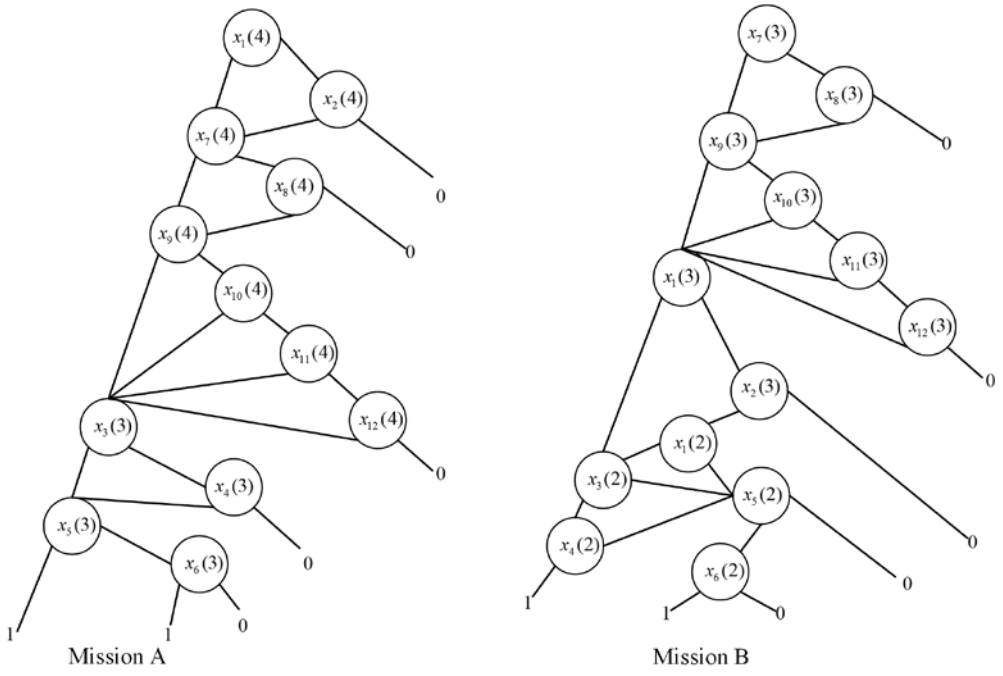


Fig. 9. BDD models for mission A and mission B

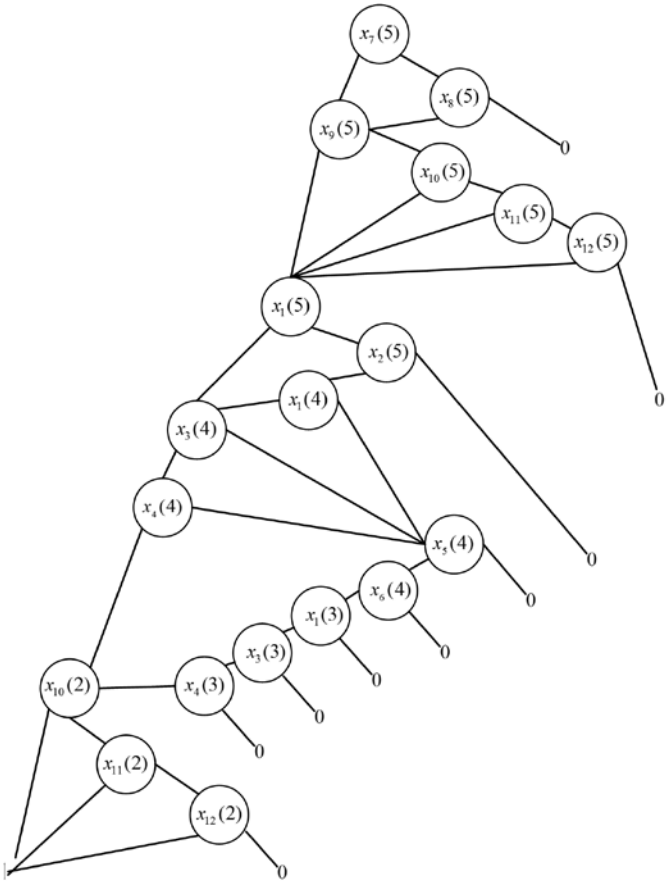


Fig. 10. BDD model for MM-PMS in case one

representing mission B is 2. R1 has two transition colors to represent different occurrence probabilities of Mission A and Mission B. In case one, two transition colors of R1 are 1 and 1, but in case two, they are 1 and 0.3.

Step 2: build the MSM. There are two missions in total, as a result, we need to build two MSMs. Mission A is be supported by three phases, and so add another two phases in Fig. 5 to obtain MSM for mission A. Similarly, add another one phases in Fig. 5 and then obtain MSM for mission B.

Step 3: generate PEMs and PLMs. We have to create five PLMs according to the five different kinds of phase mission failure logic.

Step 4: generate CSMs. All the components are non-repairable, when the failure mode that enabled transition t2 is component failure, the firing time after enabled is set to a constant larger than the system mission time. In this way, components are treated as non-repairable.

Step 5: initial these Models. Place the information tokens in MMM and facility tokens in CEM. Add transition colors to each delay transitions and probability transitions according to practical cases.

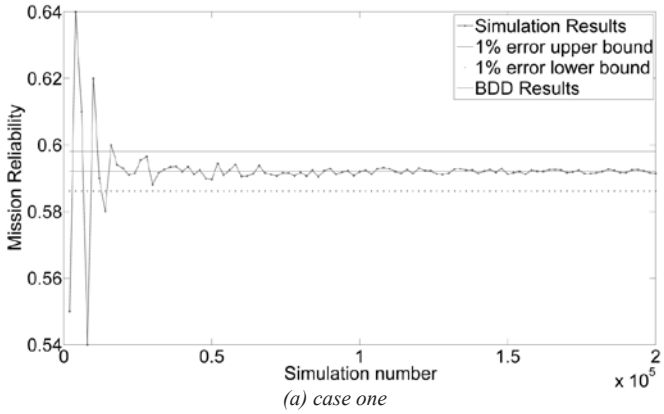
Step 6: run the simulation for Nth times, and estimate the MM-PMS reliability.

Mission reliability evaluation results of the MM-PMS in these two cases by the proposed EOOPN method and the BDD analytical method are compared in Fig. 11. From which we observe that these two methods obtain almost the same reliability results in the above two cases, which shows the effectiveness of the simulation method to estimate the reliability of MM-PMS.

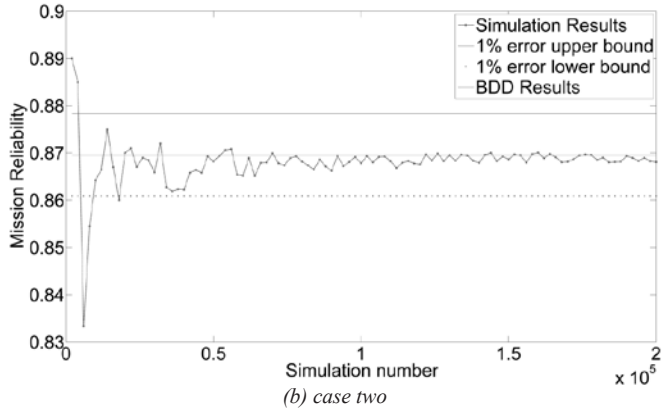
An EOOPN Modeling & Simulation software tool coded in C# has been developed [18].

4.2. Other applications of the EOOPN model for MM-PMS

4.2.1. Reliability estimation of MM-PMS with repairable components



(a) case one



(b) case two

Fig. 11. Convergence of mission reliability

Table 3. Conflict resolution for mission A and mission B

Time	Minimal path f A	Minimal path of B	Conflict	System structure function
(0,100]	{7,9}...{7,12}{8,9}...{8,12}	{7,9}...{7,12}{8,9}...{8,12}	**No**	(7+8)(9+10+11+12)
(100,200]	{1,3,9}...{1,6,12} {2,3,9}...{2,6,12}	{7,9}...7,12} {8,9}...{8,12}	**No**, release 9 for A	A:(1+2)(3+4+5+6)(9) B:(7+8)(10+11+12)
(200,260]	{1,3,9}...{1,6,12} {2,3,9}...{2,6,12}	{1,3,4} {2,5,6}	**No**, release 3, 4 for B	A:2(5+6)(9+10+11+12) B:134
(260,380]	{3,5},{3,6},{4,5}{4,6}	{1,3,4} {2,5,6}	**Yes**, terminate A	B:134+256
(380,540]	\	{1,7,9}...{1,8,12} {2,7,9}...{2,8,12}	Only mission B	(1+2)(7+8) (9+10+11+12)

Traditional methods (e.g. combinational method and BDD based method) have difficulty in reliability evaluation of PMS with repairable component. EOOPN model can be applied in this case without much complexity. Let the mission duration time and failure time distributions for each component of the given MM-PMS as in the example of

section 4.1. Repair distributions and parameters for each component are shown in Table 4.

The simulation steps are similar with that in section 4.1. The main difference is the initialization of transition t2 in CEM in step 4. Transition t2 should be attached with several transition colors to represent different repair distributions when failure mode is component failure.

After 20 million simulation runs, the mission reliability of MM-PMS in case one is estimated as 0.6041, and mission reliability of MM-PMS in case two is estimated as 0.8762.

4.2.2 Component sensitivity analysis of MM-PMS

Component sensitivity analysis is mainly used to evaluate the component importance to the mission. We use case one as an example.

Firstly, the Birnbaum structural importance of each component is computed. The definition of Birnbaum structural importance of component c_i for MM-PMS is : $I_i^B = \frac{\partial R}{\partial r_i} | r_1 = ... = r_n = \frac{1}{2}$. Fig. 12 shows the Birnbaum structural importance for each component, from which

Table 4. Input repair parameters of each component

		Mission A				Mission B		
Components	distribution	1	2	3	4	1	2	3
1,2	μ	0.0	0.015	0.005	0.015	0.0	0.012	0.015
3,4,5,6	μ	0.0	0.03	0.02	0.02	0.0	0.02	0.02
7,8	μ	0.011	0.012	0.01	0.012	0.011	0.0	0.012
9,10	μ	0.02	0.015	0.04	0.03	0.02	0.0	0.03
11,12	μ	0.05	0.015	0.016	0.013	0.05	0.0	0.013

we find components 3 and 4 are relatively more sensitive to the mission reliability of MM-PMS.

Then, the component reliability influence on the system mission is studied. Fig. 13 shows the change of the mission reliability of the given MM-PMS with component reliabilities. From which, we observe that components 3 and 4 are relatively more sensitive to the mission reliability of MM-PMS. It is consistent with the conclusion above. Thus, it is more effective to improve the reliability of a component with higher Birnbaum structural importance.

5. Conclusions

This paper proposes a simulation method based on an EOOPN model for reliability modeling and evaluation of MM-PMS. Five general and relative independent sub-models are presented, which depict MM-PMS at different levels. In this way, the sub-models are easier

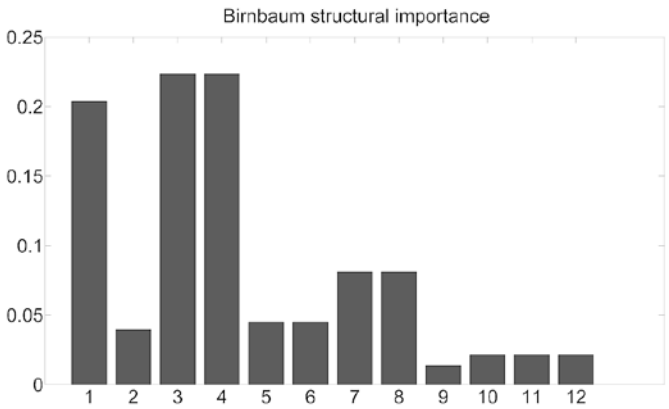


Fig. 12. Birnbaum structural importance for each component

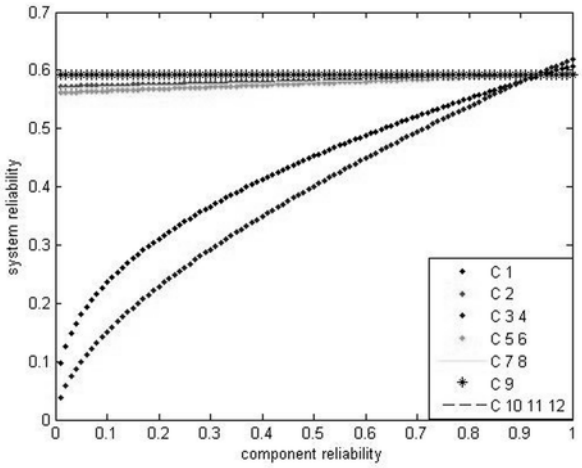


Fig. 13. Component reliability against the mission reliability

to be understood, and easier to be rebuilt with the change of practical MM-PMS.

The proposed EOOPN model allows missions in MM-PMS with different mission starting times, phase duration times, occurrence probabilities and mission importance degrees, and it is demonstrated to be effective and efficient in modeling MM-PMS. Compared with traditional methods for PMS, the EOOPN model could be used for evaluating the mission reliability of MM-PMS in more complex situations such as component repairable. Besides, the EOOPN model could be used to analysis components sensitivities. However, unlike existing analytical methods, only simulation results can be obtained by EOOPN.

References

1 Chew SP, Dunnett SJ, Andrews JD. Phased mission modelling of systems with maintenance-free operating periods using simulated Petri nets. Reliability Engineering & System Safety 2008; 93(7): 980-94, https://doi.org/10.1016/j.ress.2007.06.001.

2. Jensen K. A brief introduction to coloured petri nets. Tools and Algorithms for the Construction and Analysis of Systems. Springer Berlin Heidelberg 1997: 203-8, https://doi.org/10.1007/978-3-642-60794-3_15.

3. Kowalski, M; Magott, J; Nowakowski, T; Werbinska-Wojciechowska, S. Analysis of transportation system with the use of Petri net. Eksploatacja i Niezawodnosc-Maintenance and Reliability 2011; 1: 48-62.

4. Lu, JM; Lundteigen, MA; Liu, YL; Wu, XY. Flexible truncation method for the reliability assessment of phased mission systems with repairable components. Eksploatacja i Niezawodnosc-Maintenance and Reliability 2016; 18(2): 229-236, https://doi.org/10.17531/ein.2016.2.10.

5. Mo Yuchang, Xing L, Amari S V. A Multiple-Valued Decision Diagram Based Method for Efficient Reliability Analysis of Non-Repairable Phased-Mission Systems. IEEE Transactions on Reliability 2014; 63(1):320–330, https://doi.org/10.1109/TR.2014.2299497.

6. Ou Y, Dugan J B. Modular solution of dynamic multi-phase systems. IEEE Transactions on Reliability 2004; 53(4):499−508, https://doi.org/10.1109/TR.2004.837305.

7. Schneeweiss W G. Tutorial: Petri nets as a graphical description medium for many reliability scenarios. Reliability, IEEE Transactions on, 2001; 50(2): 159-164, https://doi.org/10.1109/24.963123.

8. Tang Z, Dugan J B. BDD-based reliability analysis of phased-mission systems with multimode failures. IEEE Transactions on Reliability 2006; 55(2): 350-360, https://doi.org/10.1109/TR.2006.874941.

9. Wu X, Yan H, Li L. Numerical method for reliability analysis of phased-mission system using Markov chains. Communications in Statistics-Theory and Methods 2012; 41(21): 3960-3973, https://doi.org/10.1080/03610926.2012.697969.

10. Wu X, Zhang W, Sha J.Generalized object oriented Petri net model for reliability analysis of communication network. System Engineering and Electronics 2000; 22(3):84-6.(in Chinese)

11. Wu X, Wu X. Extended object-oriented Petri net model for mission reliability simulation of repairable PMS with common cause failures. Reliability Engineering & System Safety 2015; 136: 109-119, https://doi.org/10.1016/j.ress.2014.11.012.

12. Xing L, Amari SV. Reliability of Phased-Mission Systems, in Handbook of Performability Engineering, Chapter 23, Editor: Krishna B. Misra, Springer-Verlag, August 2008, 349-368, https://doi.org/10.1007/978-1-84800-131-2_23.

13. Xing L, Levitin G. BDD-based reliability evaluation of phased-mission systems with internal/ external common-cause failures. Reliability Engineering & System Safety 2013; 112(1):145-53, https://doi.org/10.1016/j.ress.2012.12.003.

14. Xing L. Reliability evaluation of phased-mission systems with imperfect fault coverage and common-cause failures. IEEE Transactions on Reliability 2007; 56(1): 58-68, https://doi.org/10.1109/TR.2006.890900.

15. Xing L, Amari S V, Wang C. Reliability of k-out-of-n systems with phased-mission requirements and imperfect fault coverage. Reliability Engineering & System Safety 2012; 103: 45-50, https://doi.org/10.1016/j.ress.2012.03.018.

16. Yang X, Wu X. Mission Reliability Assessment of Space TT&C System by Discrete Event System Simulation. Quality and Reliability Engineering International 2014; 30(8): 1263-1273, https://doi.org/10.1002/qre.1546.

17. Yu H, Yang J, Peng R, et al. Reliability evaluation of linear multi-state consecutively-connected systems constrained by m consecutive and n total gaps. Reliability Engineering & System Safety 2016; 150: 35-43, https://doi.org/10.1016/j.ress.2016.01.010.

18. Yu H, Wu X. A Petri net software for mission reliability evaluation of PMS. Chinese Control and Decision Conference (CCDC), 27th. 2015: 6040-6044, https://doi.org/10.1109/ccdc.2015.7161894.

19. Zhang X, Wu X. Modeling and algorithm to mission reliability allocation of spaceflight TT&C system based on radial basis function neural network. Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012 International Conference on. IEEE, 2012: 63-68, https://doi.org/10.1109/icqr2mse.2012.6246188.

Xinyang WU
Xiaoyue WU
College of Information System and Management
National University of Defense Technology
No.109, Deya Road, Changsha, China
E-mail: wuxinyang525@126.com