Original Article

Institution of MECHANICAL ENGINEERS

Journal of SYSTEMS AND CONTROL ENGINEERING

Proc IMechE Part I:
J Systems and Control Engineering
201X, Vol XX(X) 1–14

DOI: 10.1177/0959651813515204
pii.sagepub.com
SAGE

Fault severity analysis of the time-dependent mechanical systems by the revised Time Petri net

Jianing Wu[1], Shaoze Yan[1] and Yongxia Gu[1,2]

Abstract

This article presents a fault severity analysis model to assess the fault severity at different time intervals by the revised Time Petri net, which reveals the principle of the time-dependent failure and explores the weak links in the mechanical system. A revised Time Petri net is introduced in this article by extending the tuples of the ordinary Time Petri net. The basic functional units are defined by the revised Time Petri net logic symbols, and the time firing schedule as well as the state diagram which reflects the characteristics of the mechanical system is used to assist in modeling the fault propagation of the mechanical system in the early phase of design. A numerical example of the spacecraft solar array illustrates the revised Time Petri net–based modeling method, investigates the fault mechanism and realizes the weak links of the system. The proposed method is demonstrated by analyzing the failure history data of 100 spacecraft solar arrays to get proportion of the failures at the most dangerous time intervals. The results also reveal some special phenomena related to the time-dependent failure in the mechanical system of the solar array.

Keywords

Revised Time Petri net, fault severity, time-dependent mechanical systems

Date received: 17 July 2013; accepted: 8 November 2013

Introduction

In recent times, complex mechanical systems and precision instrument need not only the stronger structure but also the higher reliability of performance, especially in the nuclear power plant and the manned space shuttles.[1–4] So, the fault severity analysis of the mechanical system is very important to the engineers for improving the reliability and enhancing the performance of the mechanical system especially in the early stage of design. Modeling the mechanical systems and analyzing the properties of them are well-accepted ways for achieving the fault mode, fault mechanism and the fault severity of the mechanism, considering the recorded faults in history and the faults with higher risk.[5,6] The complex mechanical systems are always time dependent, which can be thought of as a system which experiences different working periods as time passes.

It is recognized that graphical tools are fit for modeling the fault behavior of the mechanical systems. For instance, as graphical tools, fault tree analysis (FTA) model, reliability block diagram (RBD), the dynamic fault tree and the basic Petri net have been most widely applied in modeling the working principle of the mechanical systems and investigating the failure mechanism embedded in the system.[5–7] As the statistical data-based methods, FTA and RBD analyze the working principle of the mechanical system and model the system by the event symbols and logical connections. The fault severity analysis is realized by calculating the importance of the events. However, here are some shortcomings in these models. First, the connections between the events may not satisfy the logic link such as the AND gate or OR gate in FTA model. Some complex behavior, such as the collision and concurrency, cannot be modeled by the FTA. Second, the complex mechanical systems always operate according to one time schedule. It is worth noting that the results of some

[1]State Key Laboratory of Tribology, Department of Mechanical Engineering, Tsinghua University, Beijing, P.R. China
[2]School of Material Science and Mechanical Engineering, Beijing Technology and Business University, Beijing, P.R. China

Corresponding author:
Shaoze Yan, State Key Laboratory of Tribology, Department of Mechanical Engineering, Tsinghua University, Beijing 100084, P.R. China.
Email: yansz@tsinghua.edu.cn

faults might be opposite. Namely, for example, one certain fault F_1 may be unprevailing in the time interval T_1. However, in the time interval T_2, the fault F_1 will be the fatal one. Unfortunately, this property cannot be accurately reflected by the FTA model. Third, the previous studies of modeling the time-dependent mechanical system limit the objective to the production lines and the manufacturing assembly lines whose connections among all the units are obvious and can be easily identified. The effective methodologies of evaluating the other complex mechanical systems are rarely reported in the literature. Finally, in the early stage of design, the probability of events cannot be collected in the early stage of design when it lacks enough fault or failure data. As a result, the FTA and RBD cannot be used for fault severity analysis of the mechanical systems.

The dynamic fault tree proved to be a powerful tool to model the fault mechanism of the distributed systems.[8] However, the dynamic fault tree cannot be easily extended because it lacks the strong background of mathematical description. Furthermore, the dynamic fault tree cannot accurately reflect the property of time sequence, which could not be used for fault severity analysis of the time-dependent mechanical system.

The Petri net–based methodologies may be the possible way of solving the problems listed above.[9–18] The pioneer work can be traced to 1960s when the classical Petri nets were first defined by C. A. Petri.[8] The basic Petri net known for the advantages of clear graphical description and concise mathematical iteration algorithm is considered. Unfortunately, the basic Petri net is constructed by the 5-tuple model, which cannot concern the time-related properties. Moreover, some extended forms of Petri nets have been applied in modeling the characteristics of the distributed systems. For instance, Gao et al.[19] proposed the fuzzy reasoning Petri net and applied it to investigate the fault propagation mechanism and to diagnose the faults in the turbine machine. An approach for modeling and analysis of time critical, dynamic and complex systems using stochastic Petri nets together with fuzzy sets is presented in Tüysüz and Kahraman.[20] Note that we emergently need a tool to reflect the behavior and properties of time sequence. It is worth noting that the Time Petri nets (TPNs) are the Petri nets in which two times, a and b ($0 \leqslant a \leqslant b, a \neq \infty$), are associated with each transition. The times a and b, for transition t, are relative to the moment at which t was last enabled. It is a regulation for the TPN that firing a transition takes no time. It has been proved that TPN is a powerful tool for investigating the fault mechanism of the time-dependent systems. Berthomieu and Diaz[10] proposed a TPN-based method which allows one to formally verify time-dependent systems. This new method is successfully applied to a simple illustrative example, the specification and verification of the alternating bit protocol. Holliday and Vernon[13] invented a generalized TPN and demonstrated the use of the techniques on the famous Dining Philosopher Problem. As a result, TPN may be an effective tool to establish the model of time-dependent mechanical system. So the revised Time Petri net (RTPN) based on the conception of time sequence is introduced in this article to present a fault severity analysis model to assess the fault severity at different time intervals. The conventional TPN lacks some necessary graphical descriptions for our research. So, the main contribution of this article is extending the graphical description of TPN and then making it fit for fault severity analysis of the time-dependent mechanical systems.

From the details shown above, the main objective of this article is to establish one model of the time-dependent mechanical systems and to explore the fault severity of them. Due to the fact that it lacks sufficient design data in the conceptual phase of design, a method is needed to collect the useful empirical data. In this article, we use the Delphi method[21,22] as the tool to gather the knowledge of experts to determine the dangerous faults in the system. Then, basic functional units that can reflect some special behavior of the mechanical system are defined by employing the 10-tuple RTPN model generated from the classical 7-tuple TPN. The fault severity analysis is completed by the fault injection technique, the simulation RTPN model and the severity index. A numerical study of the proposed method is proposed by the case of spacecraft solar array.

This article is organized as follows. We shall first introduce the definition of the RTPN model in section "Definition of the RTPN model." The basic functional units depicted by the RTPN model are shown in section "Basic functional units depicted by RTPN." Section "Fault severity analysis method" devotes to the modeling method for the different working principles by using the RTPN. A case study and the demonstration of the method are described in section "A numerical study" and section "Validation and reliability improvement strategy." The last section concludes the article.

Definition of the RTPN model

In this section, the definition and the characteristics of the RTPN model are described.

Classical TPN

A classical TPN is a tuple set (P, T, B, F, Mo, SIM) which satisfies the following:[10]

1. P is a finite nonempty set of place p_i ($i = 1, 2, 3, ..., n_p$), where n_p is the number of the places.
2. T is a finite nonempty set of transitions t_j ($j = 1, 2, 3, ..., n_t$), where n_t is the number of the transitions.
3. B is the backward incidence function

$$B : T \times P \rightarrow N \tag{1}$$

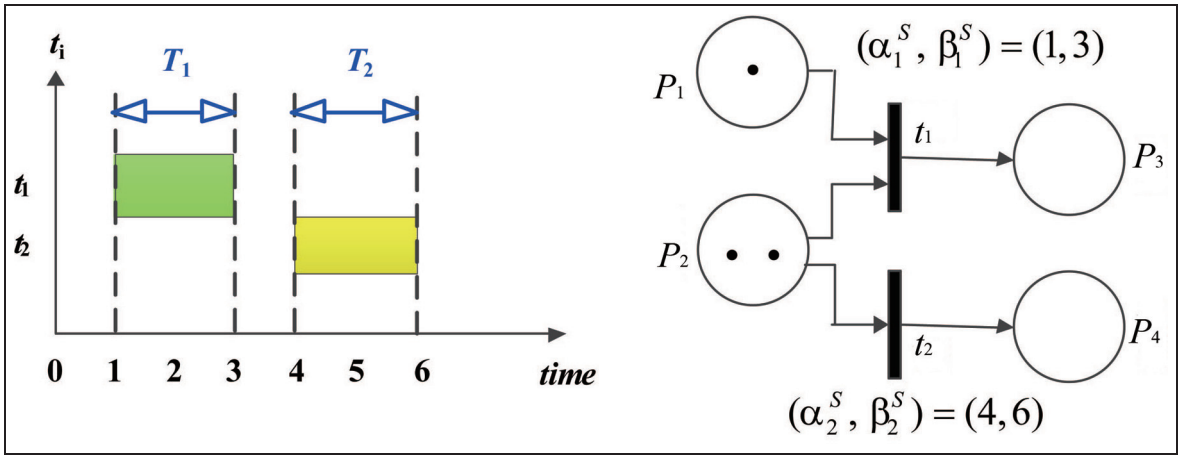

Figure 1. The typical TPN model.

where N is the set of nonnegative integers.

4. F is the forward incidence function

$$F : P \times T \rightarrow N \tag{2}$$

5. Mo is the initial marking function

$$Mo : P \rightarrow N \tag{3}$$

(P, T, B, F and Mo together define a Petri net).

6. SIM is a mapping called static interval

$$SIM : \mathrm{T} \rightarrow Q^a \times (Q^a \cup \infty) \tag{4}$$

where Q^a is the set of positive rational numbers. The SIM can be defined as constrained static rational values satisfying the following constraints for each transition t_i

$$\mathrm{SIM}(t_i) = (\alpha_i^S, \beta_i^S) \tag{5}$$

where α_i^S and β_i^S are rational numbers such that

$$\begin{aligned} &0 \leqslant \alpha_i^S \leqslant \infty, 0 \leqslant \beta_i^S \leqslant \infty, \\ &\alpha_i^S \leqslant \beta_i^S \quad \text{if } \beta_i^S \neq \infty \text{ or} \\ &\alpha_i^S < \beta_i^S \quad \text{if } \beta_i^S = \infty \end{aligned} \tag{6}$$

Assuming that transition t_i is enabled at an absolute time τ_{Abs}, then t_i may not fire, while being continuously enabled, before time $(\tau_{Abs} + \alpha_i^S)$ and must fire before or at the latest at time $(\tau_{Abs} + \beta_i^S)$. Furthermore, if a pair (α_i^S, β_i^S) is not defined, then it is implicitly assumed that the corresponding transition is a classical Petri net transition and so has the pair[10]

$$(\alpha_i^S = 0, \beta_i^S = \infty) \tag{7}$$

associated with it. Nicely and importantly, TPN contains the restriction of Petri nets. Moreover, the time interval matrix SIM is used to record the static time interval which is expressed as

$$SIM = \begin{bmatrix} \alpha_1^S & \alpha_2^S & \cdots & \alpha_i^S & \cdots & \alpha_{n_t}^S \\ \beta_1^S & \beta_2^S & \cdots & \beta_i^S & \cdots & \beta_{n_t}^S \end{bmatrix}^T_{n_t \times 2} \tag{8}$$

Figure 1 shows one typical TPN model with three places P_1–P_3 and two transitions t_1–t_2. Figure 1(a) shows the timed firing schedule of the typical TPN model displayed in Figure 1(b). From Figure 1, the transitions t_1 and t_2 can be only fired at the time intervals $[1, 3]$ and $[4, 6]$. After firing following the rule listed from equations (1) to (8), the tokens will be delivered to the upper places P_3–P_4. So the matrix SIM is defined as

$$SIM = \begin{bmatrix} 1 & 4 \\ 3 & 6 \end{bmatrix}^T_{2 \times 2} \tag{9}$$

The timed fire schedule is defined as the sets of time intervals $\{T_1, T_2\}$ as shown in Figure 1(a).

RTPN model

Figure 2 represents a typical RTPN model with seven places and five transitions. The RTPN extends the classical TPN into a 10-tuple model, namely, the tuples (P, P^+, P^-, P^*, T, T^L, B, F, Mo and SIM). Figure 2 shows the typical RTPN model and its notations.

The definition of tuples is discussed as follows:

1. *The place of normal performance P*. The performance keeps normal, which is defined by the place symbol P. As shown in Figure 2, the places P_3 and P_4 are the typical places of normal performance. If this place gets the token, it reflects the normal states of the corresponding subsystems' components, or units are normal without any anomaly. The matrix $P = [p_{ij}]_{i=1,2,\ldots,N;\, j=1,2,\ldots,T} (p_{ij} = 0, 1)$ records the state of the place of normal

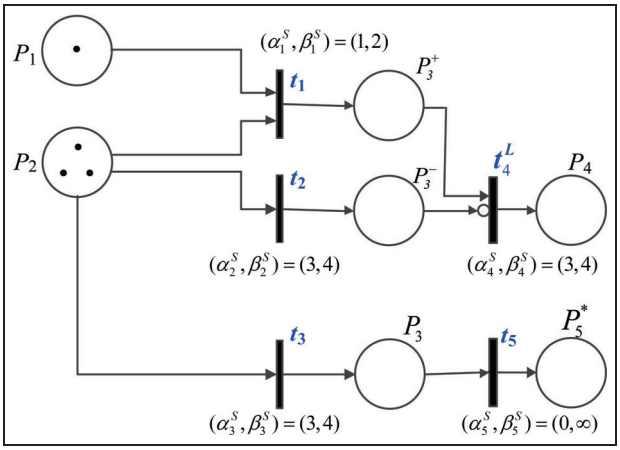

Figure 2. The typical RTPN model.

performance, in which N is the number of the normal performance places and T is the number of time points.

2. *The place of better performance* P^+. The place with the notation "+" shows that the performance changes to better state when it gets the token. This generally occurs in the deployable hinges which are only deployed once in the whole life of the mechanical system. The hinges cannot be stuck in the course of deployment, but if the hinges are stuck after locking of the mechanism, the previous fault is helpful for strengthening the structure of the mechanism. This type of place is graphically depicted as P_3^+ in Figure 2. The matrix $P^+ = [p_{ij}^+]_{i=1,2,...,n_B;\ j=1,2,...,T}(p_{ij}^+ = 0,1)$ records the state of the place of better performance, in which n_B is the number of the better performance places.
3. *The place of worse performance* P^-. The performance of the components turns worse, but it does not result in the failure of the total subsystems/components/units. This place is defined by the circle with the mark "-." The transition P_3^- of Figure 2 is the typical place of worse performance. The matrix $P^- = [p_{ij}^-]_{i=1,2,...,n_W;\ j=1,2,...,T}(p_{ij}^- = 0,1)$ records the state of the place of worse performance, in which n_W is the number of the worse performance places.
4. *The place of failure performance* P^*. The subsystems/components/units fail when the fault occurs. This always happens in the key components and the weak links of the mechanical system, such as the fracture in the driving bar, the explosion of the pressure vessel and the stuck in the sliding bearings. The matrix $P^* = [p_{ij}^*]_{i=1,2,...,n_F;\ j=1,2,...,T}$ $(p_{ij}^* = 0,1)$ records the state of the place of failure performance, in which n_F is the number of the failure performance places.
5. *The ordinary transition* T. T is a finite nonempty set of transitions t_j (j = 1, 2, 3, ..., n_o), where n_o is the number of the ordinary transitions. It will appear in the sequel that it may be convenient to view it as an ordered set $\{t_1, t_2, \ldots t_j, \ldots\}_{n_O \times 1}$. Note that the ordinary transition T has the property of time sequence as expressed in equations (1)–(7).
6. *The locking transition* T^L. The token is sent to the next transition via the arc and then the transition will be locked and all the information below will not be delivered upward. This type of transition is called the locking transition denoted by the symbol t_4^L in Figure 2, and the most significant feature of such a transition is that it has the notation of a circle. T^L is a finite nonempty set of transitions $t_j^L (j = 1, 2, 3, \ldots, n_L)$, where n_L is the number of the ordinary transitions. The ordered set of the locking transition can be expressed by $\{t_1, t_2, \ldots, t_j, \ldots\}_{n_L \times 1}$. If the locking arc gets the token, the transition will be locked and cannot be fired again. The directed arc leading to the locking transition has no properties of time duration. Namely, the action of locking is not controlled by the constraint $SIM(t_i) = (\alpha_i^S, \beta_i^S)$. Take the transition t_4^L in Figure 2 as an example; the token will be transmitted to the transition t_4^L if the place P_3^- gets the token. The place t_4^L is locked instantly and we will not consider the time interval $(\alpha_4^S, \beta_4^S) = (3,4)$. It should be noted that a locking transition only fires once, and once it has fired, it never fires again.
7. *The backward incidence function B*

$$B : T \times P \to N \tag{10}$$

where N is the set of nonnegative integers. Namely, the graphical description of this function is the directed arcs from transitions to places, which connect the transitions to the places and deliver the token upward.

8. *The forward incidence function F*

$$F : P \times T \to N \tag{11}$$

And, the graphical description of this function is the directed arcs from the places to transitions, which transmit the tokens from the places to the upper transitions.

9. *The initial marking function Mo*

$$Mo : P \to N \tag{12}$$

(P, T, B, F and Mo together define a Petri net).

10. *A mapping called static interval SIM*

$$SIM : \mathrm{T} \to Q^a \times (Q^a \cup \infty) \tag{13}$$

where Q^a is the set of positive rational numbers. The properties of the tuple SIM are the same as the SIM defined in section "Classical TPN" by equations (8) and (9).

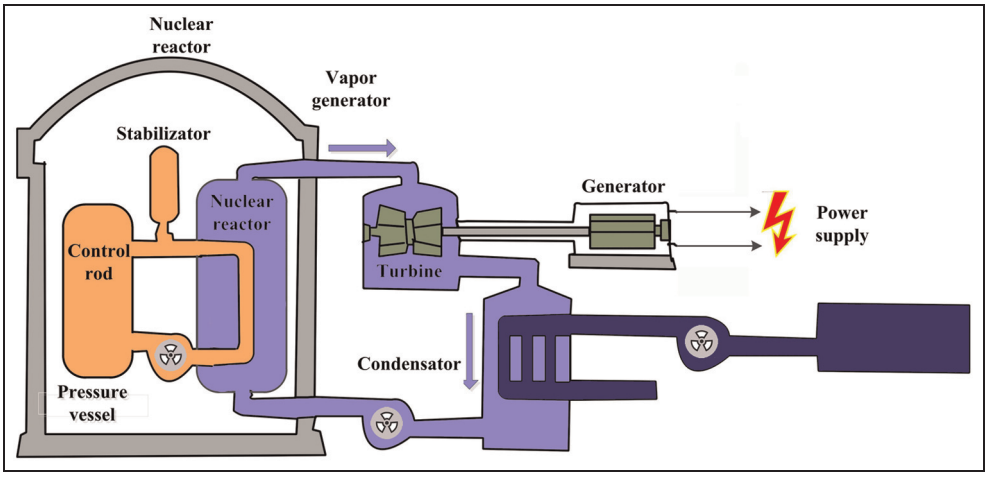

Figure 3. Schematic of the nuclear power station.

Basic functional units depicted by RTPN

The complex mechanical system has a variety of time-dependent units.[23] Figure 3 represents the operation principle of the nuclear power station which can be treated as one complex mechanical system.[24] The heat is produced by the fission in a nuclear reactor. Directly or indirectly, water vapor is produced. The pressurized steam is then usually fed to the steam turbine. The turbine drives the generator to produce electricity. After the steam turbine has expanded and partially condensed the steam, the remaining vapor is condensed in a condensator. The water is then pumped back into the nuclear reactor and the cycle begins again. In this working cycle, the unit of turbine, the unit of vapor generator and the unit of condensator work in the absolute time intervals (α_1^S, β_1^S), (α_2^S, β_2^S) and (α_3^S, β_3^S). There are two typical examples of the time-dependent properties in this system.

1. The unit of turbine can only be activated after the vapor generator works. Namely, the time parameters must satisfy $\alpha_1^S > \alpha_2^S$.
2. The unit of condensator can only be applied after the turbine works, so the time parameters must satisfy $\alpha_3^S > \alpha_1^S$.

The states of the system which do not satisfy equations (1) and (2) are considered as the anomalies. To illustrate the special characteristics of the time-dependent mechanical system, the four types of basic functional units by TPN are shown in Figure 4. The following introduces the definition of the units.

1. *Type I*. The performance turns worse after the fault happened while the system is not totally out of service. This always happens in the mechanical system, such as the insufficiency of the preload in belt drive, the slight wear in the bearings and the small crack on the interface. The basic functional unit of worse performance is shown in Figure 4(a). The places $\{P_1, P_2, P_F, P_2^-\}$ represent the lower place, the upper place of normal performance, the place of failure and the place of worse performance, respectively. If the place P_F gets the token, the transition t_1 will be locked and P_2 cannot get the token any more. Then, the token will be sent to the place P_2^-. The parameters satisfy

$$\alpha_1^S = \alpha_2^S, \beta_1^S = \beta_2^S \tag{14}$$

2. *Type II*. The performance becomes better after the fault happened, which generally occurs in the hinges that are only deployed once in the whole life of the mechanical system.[22,23] The deadlocking is the fatal fault in the course of deployment (Figure 5(a)). However, if the hinges of deployable structure are stuck after locking of the mechanism, it is helpful for strengthening the structure of the mechanism because the deadlocking will eliminate the clearance and enhance the stiffness of the structure (Figure 5(b)).

The graphical description of this type is shown in Figure 4(b), and equation (14) is also satisfied in this type of functional units.

3. *Type III*. This type represents the condition that the state will not change after the fault happened. This kind of phenomenon can be found in the independent components of some distributed systems which will not influence the state of each other when the fault occurs. The mechanism of this kind of unit is shown in Figure 4(c). The place of fault P_F will not influence the state of the unit, and the token will be transmitted to place P_2 which represents the ordinary performance of the unit. The time parameters satisfy

$$\alpha_1^S = 0, \beta_1^S = \infty \tag{15}$$

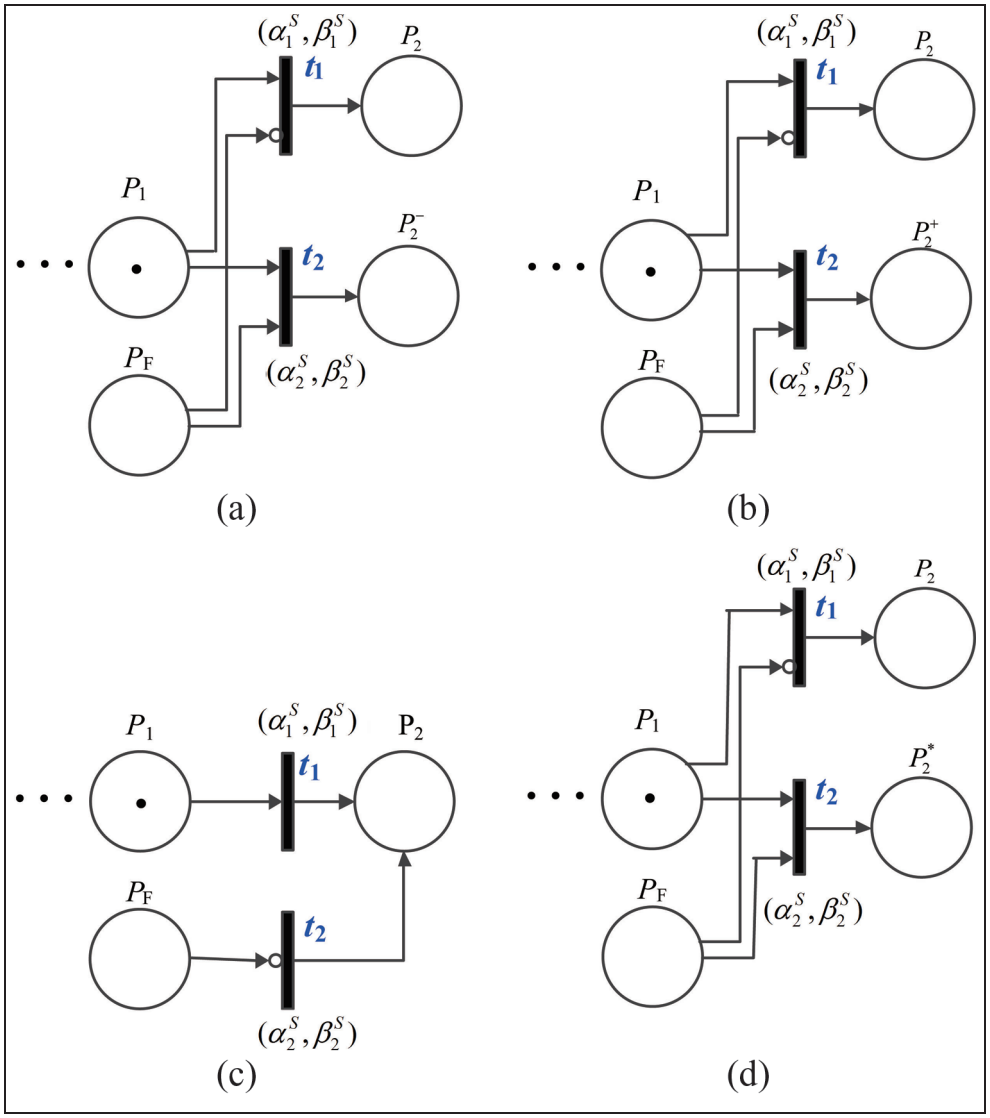

Figure 4. Basic functional units defined by RTPN (a) Type I (b) Type II (c) Type III (d) Type IV.

which indicates that t_2 is a transition of an ordinary Petri net.

4. *Type IV*. The system fails when the fault occurs. This always happens in the key components and the weak links of the mechanical system, such as the fracture in the driving bar, the explosion of the pressure vessel, the stuck in the sliding bearings and the fracture of the belt. As illustrated in Figure 6, the production line fails when the belt is broken in every time interval of the working. The graphical description is shown in Figure 4(d), and equation (14) is also suitable for this type of functional units.

Fault severity analysis method

Comprehensive analysis of the fault severity can deal with the common time-dependent fault mechanisms of the mechanical system and allows for recording the course of fault propagation. The flowchart of the proposed method is shown in Figure 7. On the basis of the working principle of the mechanism, the time series and the work steps can be identified. Then, the experts' knowledge and Delphi method are adopted to preliminarily determine the dangerous faults that will be considered. The RTPN model is established referring to the experts' knowledge and the basic functional units to analyze the severity of dangerous fault. The simulation will present the fault severity in different time intervals after the faults are injected to the system. Finally, the time-dependent strategy for reliability improvement can be figured out in order to restore the weak links of the mechanical system. The new method is outlined by the following five steps.

Step 1: analysis of the working principle

The first step is to analyze working principle of the mechanical system. The functional block diagram is used to investigate the time-dependent working principle. Figure 8(a) shows an example of the functional

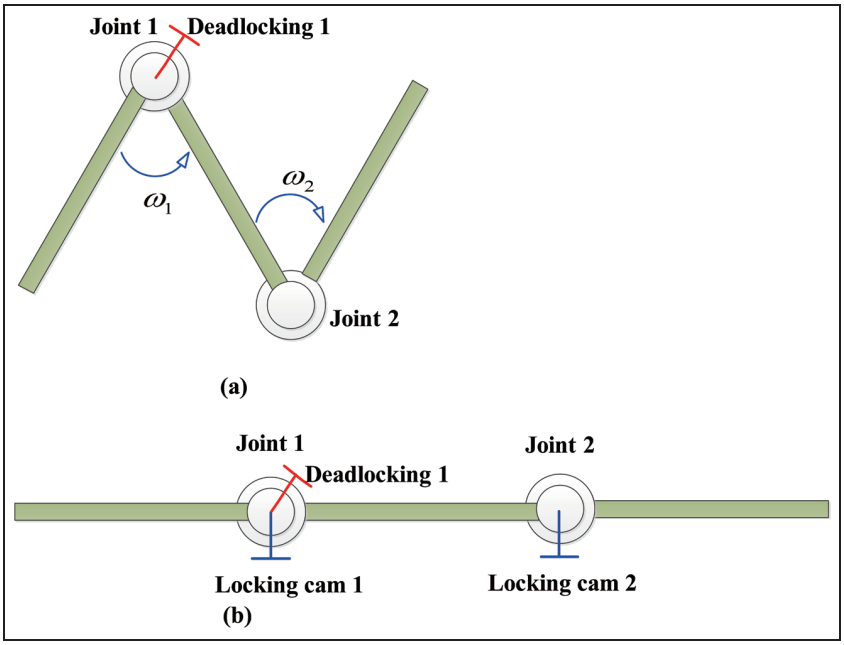

Figure 5. The deployable structure (a) the deployable mechanism in the process of deployment (b) the deployable mechanism after being locked.

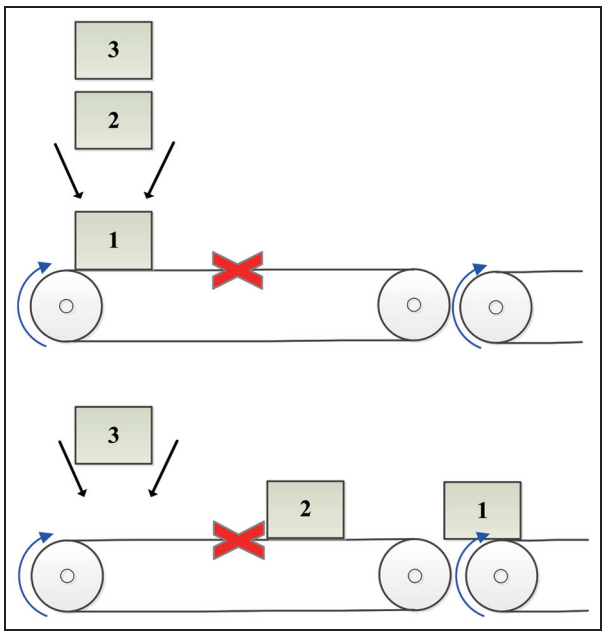

Figure 6. The conveyor belt mechanism.

block diagram. The system is decomposed into three or four layers, namely, the system, the subsystems, the units and the components. Through preliminary analysis, the time series of the different units can be identified (Figure 8(b)).

Step 2: fault mode analysis

According to the functional block shown in Figure 8, the Delphi method is used to realize the main faults of the system, concerning knowledge of the experts and the small amount of history data.[18,19] Table 1 collects the judgment of different experts with the score scale [0, 100]. The score of the ith bottom places can be computed as follows

$$\theta^i = \frac{\sum_{j=1}^{N} X_{ji}}{100N} (i = 1, 2, \ldots, n) \tag{16}$$

where X_{ji} is the score of the ith fault provided by jth expert, and there are N experts and n kinds of faults. The ranking of most significant fault modes can be obtained according to the scores calculated by equation (16).

Step 3: establishment of the RTPN model

The faults drawn by Step 2 are considered in building the RTPN model of the mechanical system. A RTPN-based system is established to structure the time-dependent working principle of the mechanical system by using the basic functional units defined in section "Basic functional units depicted by RTPN."

Step 4: simulation

The time vector of ith time interval is $T_i = \{t_{i1}, t_{i2}, \ldots, t_{in_i}\}$, in which n_i is the number of the time points in the time interval. The faults are injected in the system at the jth time point of the ith time interval. Then, RTPN model will transport the token from the lower place to the upper place, and the state of all the places will be recorded during the fault propagation in the system.

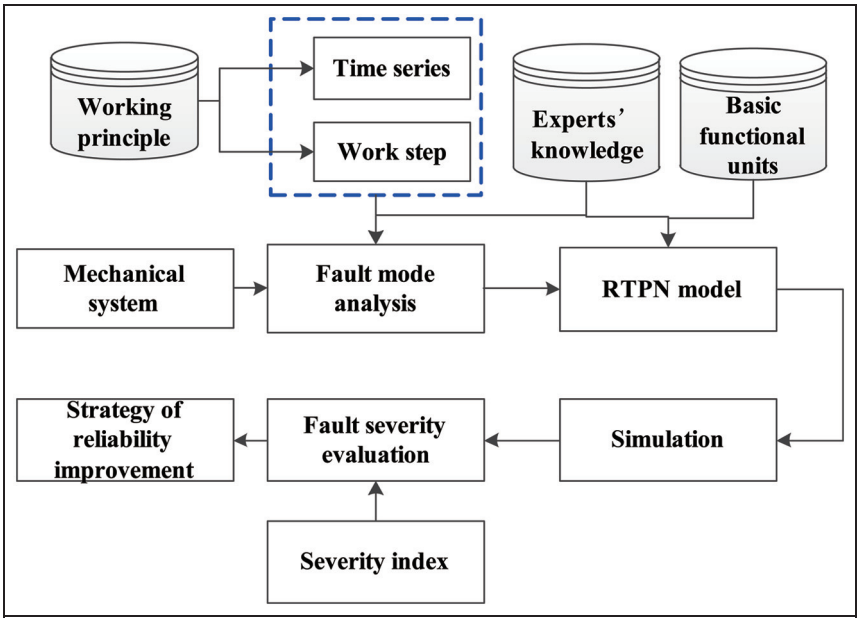

Figure 7. Flowchart of the proposed method.
RTPN: revised Time Petri net.

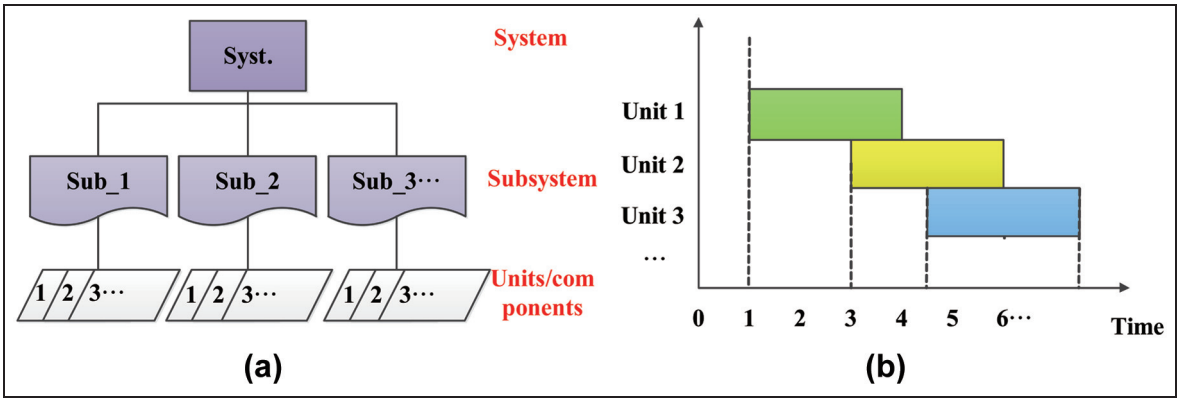

Figure 8. (a) The functional block diagram and (b) the time firing schedule.

Table 1. Data collection table of Delphi method.

Score scale: 0–100	Expert I	Expert II	Expert III	...	Expert *N*
Fault 1	X_{11}	X_{21}	X_{31}	...	X_{N1}
Fault 2	X_{12}	X_{22}	X_{32}	...	X_{N2}
⋮	⋮	⋮	⋮	⋮	⋮
Fault *i*	X_{1i}	X_{2i}	X_{3i}	...	X_{Ni}
⋮					
Fault *n*	X_{1n}	X_{2n}	X_{3n}	...	X_{Nn}

Step 5: fault severity evaluation

The states after the fault injection can be categorized as the following four types: the better performance, the normal performance, the lower performance and the fatal failure (Figure 9). By the simulation of the unit i ($i = 1, 2, 3, ..., n_u$), the times of states after the different faults happen can be recorded as shown in Table 2.

Then, the fault severity of the ith fault on the jth time interval can be measured by the severity index

$$s_{ij} = \frac{N_{ij4}}{\sum_{k=1}^{4} N_{ijk}} \tag{17}$$

If the parameter s_{ij} is higher, the jth fault is more serious in the ith time interval. As a result, for the jth fault,

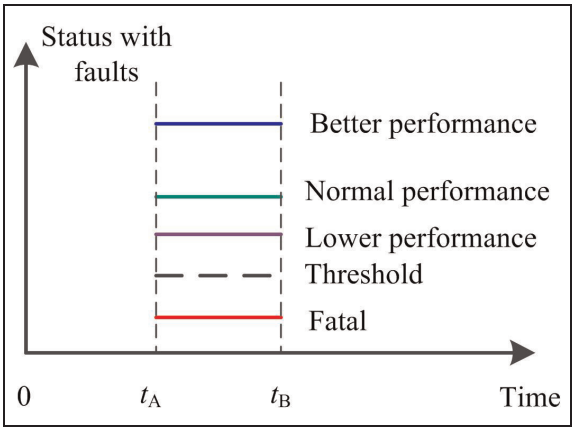

Figure 9. State diagram with faults on one certain time interval.

the relative important time interval can be found by ranking the fault severity indices. It is helpful for engineers to judge the "sensitive time interval" for different faults of the mechanical system.

A numerical study

Step 1: analysis of the working principle

In this section, the typical solar array is introduced to demonstrate the correctness and feasibility of the proposed method. The solar array is one of the most vital parts of the spacecraft which profoundly influences the reliability of the whole spacecraft system.[23–28] Therefore, behavior modeling and failure analysis play an important role in design, manipulation and maintenance of the solar array.

As shown in Figure 10, the entire running process includes three stages, that is, the deployable solar array is first folded, then deployed and locked and finally oriented to the sun to generate power for satellite. Take the solar array of DFH-3 satellite launched in 1997 as an example; the hold-down and release mechanism contains seven explosive bolts (CT_1–CT_7) that must be cut off by the knives after the instruction of deployment transmitted from the satellite in orbit.[28–31]

In general, the solar array mechanism consists of three kinds of mechanisms, that is, the hold-down and release mechanism, the deployable-locking mechanism and the orientation mechanism. The structure of the hold-down and release mechanism is graphically sketched in Figure 10(a). As shown in Figure 10(b), the solar array is composed of four panels. In addition, the deployable mechanism is the hinge, consisting of the driving spring, locking spring, closed cable loop (CCL) and pins with clearances. The hinges are marked from the satellite to the outside of the solar array as H_1, H_2, H_3 and H_4. The driving torsion springs (DS_1–DS_4) are often arranged in the hinges to drive the solar array, and the locking torsion springs (LS_1–LS_4) are used to make the solar array fixed after deployment. The CCLs meet the requirement of motion coordination and synchronization during deployment, which are organized as CCL_1, CCL_2 and CCL_3 in Figure 10(c). The solar array is oriented to the sun by orientation mechanism that is composed of the stepping motor and the harmonic reducer.[23,24]

Step 2: fault mode analysis

According to the working principle of the spacecraft solar array, the functional block diagram which shows the fault modes is illustrated in Figure 11.

By the Delphi method, the preliminary determination of the important failure is scored by the five invited experts in the research field of spacecraft engineering. The results show that the following five types of failure mode are selected as the objective of the study. They are the failure of the cutters, the failure of the CCLs, the failure of the driving torsion spring, the deadlocking of the hinges and the failure of the locking torsion spring. These five types of failures are considered in the following steps.

Step 3: establishment of the RTPN model

As the state diagram shown in Figure 12, the working history is separated into four parts. The meaning of the time intervals T_A–T_D is shown in Table 3. The durations are t_A = 1 day, t_B = (1 day + 10 min), t_C = (1 day + 10 min) and t_D = (1 year + 1 day + 11 min).[28] The number of time points is set as $n_1 = n_2 = n_3 = n_4 = 100$.

Referring to the states of the system after fault injection in Figure 12, the four streams representing the performance of the components are illustrated in Figure 13(a)–(d). The notations of the timed places and their corresponding durations are shown in Table 4.

Table 2. The times of states after the different faults happen.

	Unit i			
State	Normal performance	Better performance	Worse performance	Failure performance
Time interval T_1	N_{i11}	N_{i12}	N_{i13}	N_{i14}
⋮	⋮	⋮	⋮	⋮
Time interval T_j	N_{ij1}	N_{ij2}	N_{ij3}	N_{ij4}
⋮	⋮	⋮	⋮	⋮

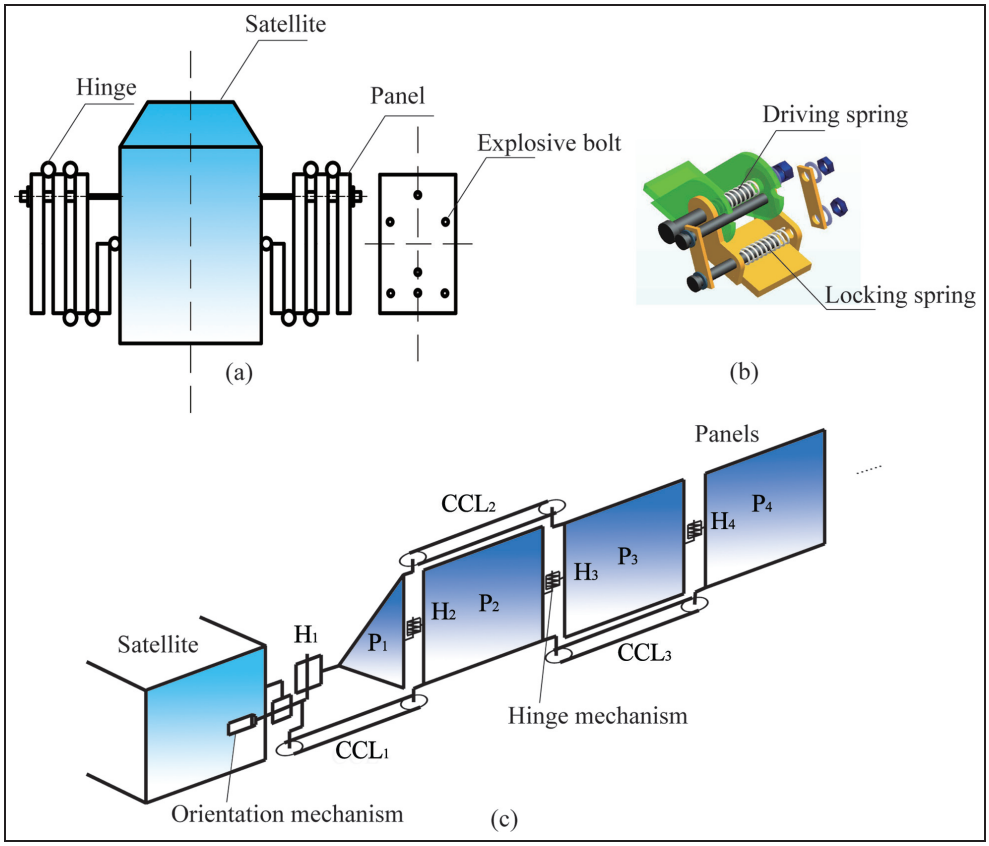

Figure 10. Mechanisms of the solar array (a) the compact solar array (b) the hinge mechanism (c) the deployed solar array. CCL: closed cable loop.

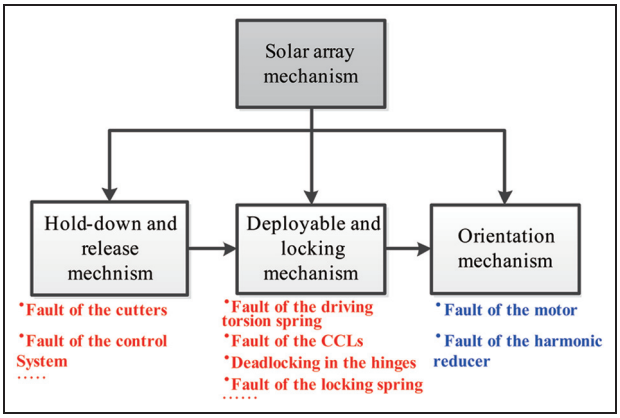

Figure 11. Functional block diagram of the solar array.

Step 4: simulation

The model is built by the software Arena®, and 100 time points are distributed at every time interval. The Arena can be used as the tool to build the structure of the Petri net and can simulate the mechanism of fault propagation in the distributed system. Arena is just a simple tool to get the graphical description from the customers and then to operate by the SIMAN processors. The SIMAN processors are modeled by the basic modules, and the operation is based on the iteration algorithm. In fact, the main algorithm architecture is based on three directives—seize, delay and release, which can realize the function of RTPN. Then, the failure of the cutters, failure of CCLs, deadlocking in the hinges, failure of the driving torsion spring, deadlocking of the hinges and the failure of locking torsion spring are simulated by referring to the RTPN model shown in Figure 13. Then, the fault severity index can be calculated by equation (17).

Table 3. Time intervals and the related failures.

Time interval	Failure
$T_A = [0, t_A)$	Time interval between launch and unlocking of the panels
$T_B = [t_A, t_B)$	Time interval of deployment
$T_C = [t_B, t_C)$	Time interval of locking
$T_D = [t_C, t_D)$	Time interval of orientation

Step 5: fault severity analysis

The simulation results reveal the output properties of the states after the failures happened. Consider the single failure that is injected in the system, there exist four types of states after fault propagation: the normal output, the lower performance, the better performance and the total failure of the system. Figure 14 shows the fault

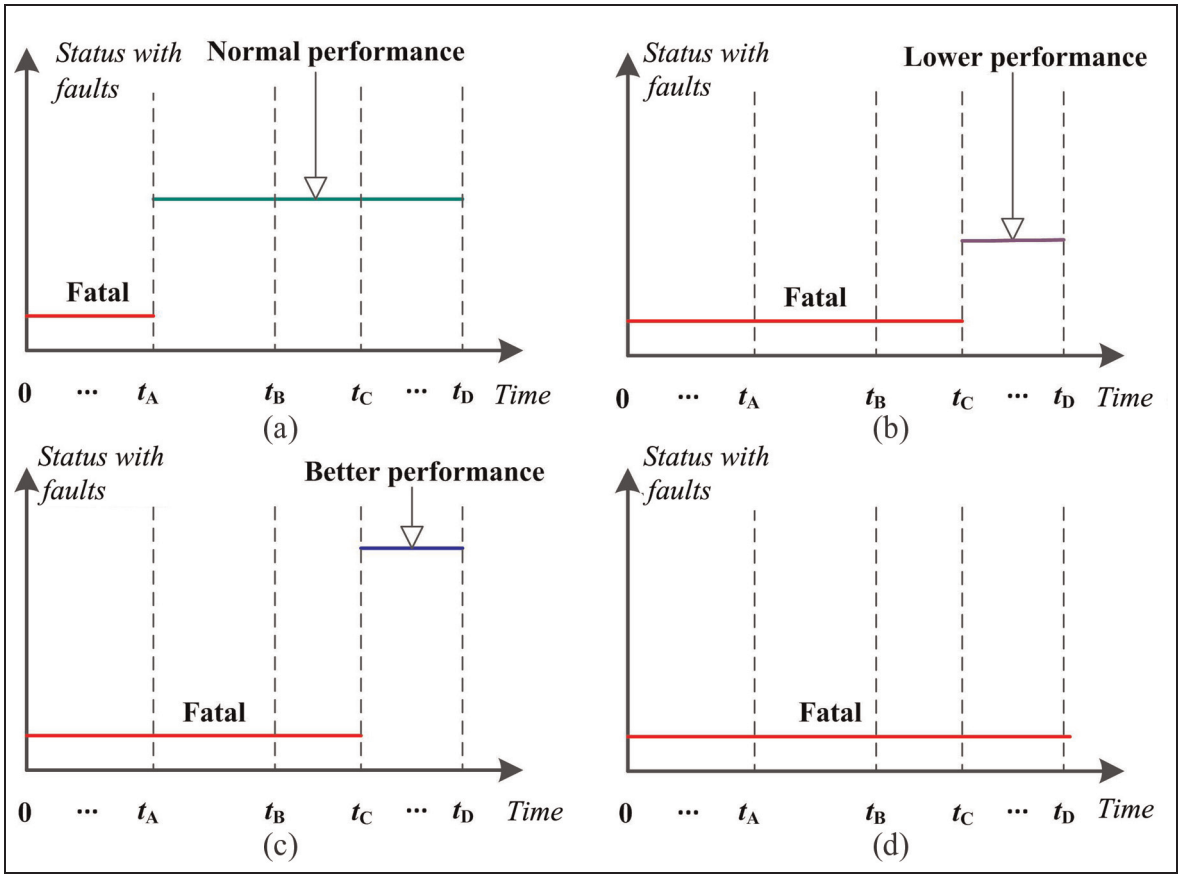

Figure 12. State diagram of the key subsystems: (a) failure of the cutters, (b) failure of CCLs/driving torsion spring, (c) deadlocking of the hinges and (d) failure of the locking torsion spring.

Table 4. Notations of the timed places and corresponding durations.

No.	Fault	Notations	Serial number of transitions	$[\alpha_i^S, \beta_i^S]$	Number of transitions	$[\alpha_i^S, \beta_i^S]$
1	Fault of the cutters	CT_1–CT_7	$4i - 3$ (i = 1, 2, ..., 7)	(0, 1 day)	$4i - 3$ (i = 1, 2, ..., 7)	(0, 1 year + 11 min)
			$4i - 2$ (i = 1, 2, ..., 7)	(0, 1 day)	$4i - 2$ (i = 1, 2, ..., 7)	(0, 1 year + 11 min)
2	Fault of CCLs	CCL_1–CCL_3	$5i + 24$ (i = 1, 2, 3)	(0, 1 day + 11 min)	$5i + 26$ (i = 1, 2, 3)	(0, 1 year)
			$5i + 25$ (i = 1, 2, 3)	(0, 1 day + 11 min)	$5i + 27$ (i = 1, 2, 3)	(0, 1 year)
3	Fault of the driving torsion spring	DS_1–DS_4	$5i + 24$ (i = 4,5, ..., 7)	(0, 1 day + 11 min)	$5i + 26$ (i = 4, 5, ..., 7)	(0, 1 year)
			$5i + 25$ (i = 4, 5, ..., 7)	(0, 1 day + 11 min)	$5i + 27$ (i = 4, 5, ..., 7)	(0, 1 year)
4	Deadlocking of the hinges	H_1–H_4	$6i + 58$ (i = 1, 2, ..., 4)	(0, 1 day + 11 min)	$6i + 60$ (i = 1, 2, ..., 4)	(0, 1 year)
			$6i + 59$ (i = 1, 2, ..., 4)	(0, 1 day + 11 min)	$6i + 61$ (i = 1, 2, ..., 4)	(0, 1 year)
5	Fault of the locking torsion spring	LS_1–LS_4	$4i + 84$ (i = 1, 2, ..., 4)	(0, 1 year + 11 min)	–	–
			$4i + 85$ (i = 1, 2, ..., 4)	(0, 1 year + 11 min)	–	–

CCL: closed cable loop.

severity index at different time intervals, and the faults marked by Nos 1–5 can be inquired in Table 4. It can be concluded from Figure 14 that

1. The fault severity index describes the "time sensitivity" of the faults. The fault of the cutters will be the most dangerous if it happens in the first time interval. Fault of CCLs, fault of the driving torsion spring and deadlocking of the hinges are the vital faults considered in the second time interval.
2. The special properties of the fault "deadlocking of the hinges" can be clearly seen from Figure 14. At the time intervals T_c and T_d, the fault indices are 0% which means the fault "deadlocking of the hinges" cannot lead to the failure of the system after the deployment of the solar array. This is caused by the effect of "better performance" as Type II shown in section ""Basic functional units depicted by RTPN."
3. The fault of the locking mechanism (No. 5) is "sensitive" to the third time interval when the solar arrays are going to lock after deployment. The fault severity index in the last time interval is 5% which indicates that the fault of the locking

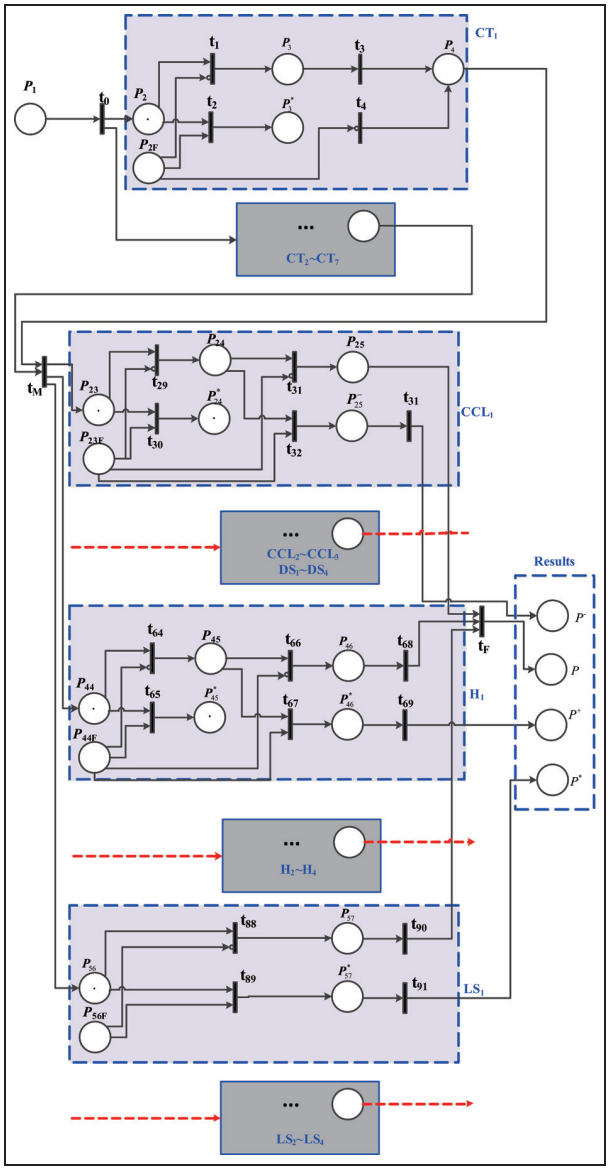

Figure 13. RTPN model of the solar array mechanism.

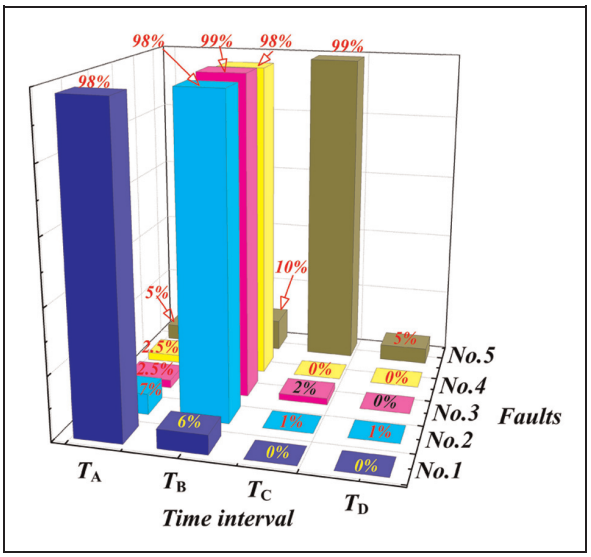

Figure 14. Fault severity index in different time intervals.

mechanism still influences the performance after the course of locking. This is caused by the reason that the locking mechanism connects the structures as a rigid one, and the stiffness will decrease if it is out of service.

The results provide the information of severity ranking among all the failures and the related "dangerous time interval," which are useful for reliability design.

Validation and reliability improvement strategy

The results of the fault severity analysis are demonstrated by the data collection in Table 5. The SpaceTrak Database[32] is adopted for the data collection provided by many of the world's launch providers, satellite insurers, operators and satellite manufacturers. The sample analyzed in this article covers the failure data of 100 spacecraft. The sample was restricted to Earth-orbiting satellites successfully launched between January 1990 and October 2008.[32] Table 5 shows the data collection template of the fault time and fault mode of the spacecraft solar arrays.[33]

According to the actual failure data of the spacecraft solar array, we calculate the proportion of the failure in the most dangerous time intervals (Table 6). The proportions of the failure in the most dangerous time interval are all more than 70%, which validates the correctness of the fault severity analysis.

On the basis of fault severity index shown in Figure 14, the vital links of the solar array can be found. According to the sorting of the fault severity index, the strategies for reliability improvement are illustrated in Table 6.

Conclusion

We attempt to introduce the RTPN-based fault severity method of the complex mechanism in this article. The fault mechanisms are modeled by the functional units of the 10-tuple RTPN model. A numerical example illustrates that the proposed model has the ability of combing the history data and the experts' knowledge, simulating the special behavior of the time-dependent fault propagation and judging the severity of faults which may occur in the complex mechanical systems. The proposed method can also be used in the fault severity analysis of other kinds of complex mechanical systems.

There is a room for future development in the modeling tool which can describe the more complex behavior such as the common cause failure (CCF) and the multi-fault in the system. Another meaningful future research direction is the investigation on the

Table 5. Data collection template of the fault time and fault mode of the spacecraft solar arrays.

Spacecraft unit number	Launch date	Fault date (if fault occurred)	Fault mode	Consequence	Time interval	Censored time (if no failure occurred)
Spacecraft 1	6 Nov 1998	6 Nov 1998	Deadlocking in the hinges	The spacecraft fails totally.	First	–
Spacecraft 2	1 Mar 2002	–	–			2 Oct 2008
Spacecraft 3	1 Mar 1997	3 March 1997	Clearances in the hinges	The loss of location accuracy	Fourth	
⋮	⋮	⋮	⋮			⋮

Table 6. Validation of the fault severity index.

Fault	The most dangerous time interval from the RTPN model	Proportion of the failure in the most dangerous time interval from the database	Strategies for reliability improvement
Fault of the cutters	First	90%	Use the backup cutter
Fault of CCLs	Second	70%	1. Use the cable of new material that is not sensitive to the change of temperature; 2. Use tightener to fasten the cable.
Fault of the driving torsion spring	Second	85%	1. Test the torsion spring on the ground, then find the torque-angle curve to know the characteristics of the torsion spring more deeply; 2. Test the performance of the whole system, using torsion springs with at least 20% remaining torque.
Deadlocking of the hinges	Second	95%	1. Improve the lubrication of the hinges. MoS_2 and graphite are widely used in the spacecraft as solid lubricant. Other lubricants should be tested under the environment of space, in order to choose the better one; 2. Improve the sealing device of the hinges to hold a relatively ale space for the hinges.
Fault of the locking torsion spring	Third	–	1. Use the locking spring with higher stiffness; 2. Use the backup locking springs.

RTPN: revised Time Petri net; CCL: closed cable loop.

mechanism and the propagation rule of the multiple failure modes in the mechanical system, which may provide a hint for thoroughly evaluating the time-dependent failure mechanism of them.

Declaration of conflicting interests

The authors declare that there is no conflict of interest.

Funding

This work was supported by the National Science Foundation of China under Contract No. 50875149 and Beijing Natural Science Foundation under Contract No. 3132030.

References

1. Brandhorst HW Jr and Rodiek JA.Space solar array reliability: a study and recommendations. *Acta Astronaut* 2008; 63: 1233–1238.
2. Harland DM and Lorenz R.*Space systems failures: disasters and rescues of satellites, rocket and space probes*. 1st ed. Berlin: Springer-Praxis, 2005.
3. Xu JP, Guo F and Xu L.Integrated system health management-based state evaluation for environmental control and life support in manned spacecraft. *Proc IMechE, Part I: J Systems and Control Engineering* 2013; 227: 461–473.
4. Shen Q, Jiang B and Cocquempot V.Fault diagnosis and estimation for near-space hypersonic vehicle with sensor faults. *Proc IMechE, Part I: J Systems and Control Engineering* 2012; 226: 302–313.
5. Lee WS.Fault tree analysis, methods, and applications: a review. *IEEE T Reliab* 1985; 34: 194–203.
6. Xiao NC, Li YF and Huang HZ.Reliability analysis method of deployment mechanism of a satellite solar arrays. *J Astronaut* 2009; 30: 1704–1710 (in Chinese).
7. Souza RQ and Álvares AJ.FMEA and FTA analysis for application of the reliability centered maintenance methodology: case study on hydraulic turbines. *Acs Sym Ser* 2008; 3: 803–812.
8. Simeu-Abazi Z, Lefebvre A and Derain JP.A methodology of alarm filtering using dynamic fault tree. *Reliab Eng Syst Safe* 2011; 96: 257–266.
9. Tadao M.Petri nets: properties, analysis and applications. *P IEEE* 1989; 77: 541–579.

10. Berthomieu B and Diaz M.Modeling and verification of time dependent systems using Time Petri net. *IEEE T Software Eng* 1991; 17: 259–273.
11. Gardey G, Lime D and Magnin M.Romeo: a tool for analyzing time Petri nets. In: Etessami K and Rajamani SK (eds) *Computer aided verification*. 1st ed. Berlin: Springer, 2005, pp.418–423.
12. Carlier J and Chrétienne P.Timed Petri net schedules. In: Rozenberg G (ed.) *Advances in Petri nets*. Berlin, Heidelberg: Springer, 1988, pp.62–84.
13. Holliday MA and Vernon MK.A generalized timed Petri net model for performance analysis. *IEEE T Software Eng* 1987; 12: 1297–1310.
14. Nancy GL and Janice LS.Safety analysis using Petri nets. *IEEE T Software Eng* 1987; 3: 386–397.
15. Yuan CY.*Petri nets*. 1st ed. Nanjing, China: Southeastern University Press, 1989 (in Chinese).
16. Trivedi KS, Kulkarni VG, Horton G, et al. Fluid stochastic Petri nets: theory, applications and solution techniques. *Eur J Oper Res* 1998; 105: 184–201.
17. Uzam M.The use of the Petri net reduction approach for an optimal deadlock prevention policy for flexible manufacturing systems. *Int J Adv Manuf Tech* 2004; 23: 204–219.
18. Pedrycz W and Gomide F.A generalized fuzzy Petri net model. *IEEE T Fuzzy Syst* 1994; 2: 295–301.
19. Gao M, Zhou MC, Huang X, et al. Fuzzy reasoning Petri nets. *IEEE T Syst Man Cy A* 2003; 33: 314–324.
20. Tüysüz and Kahraman C. Modeling a flexible manufacturing cell using stochastic Petri nets with fuzzy parameters. *Expert Syst Appl* 2010; 37: 3910–3920.
21. Linstone HA and Turoff M.*The Delphi method: techniques and applications*. 1st ed. Boston, MA: Addison-Wesley Publishing Company, 1975.
22. Rausand M and Høyland A.*System reliability theory: models, statistical methods, and application*. Hoboken, NJ: John Wiley & Sons Inc., 2004.
23. Borkar S.Designing reliable systems from unreliable components: the challenges of transistor variability and degradation. *IEEE Micro* 2005; 25: 10–16.
24. http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm (accessed 1 July 2013).
25. Yuan JJ. *Design and analysis of satellite structures*. 1st ed. Beijing, China: China Astronautic Publishing House, 2004 (in Chinese).
26. Wallrapp O and Wiedemann S.Simulation of deployment of a flexible solar array. *Multibody Syst Dyn* 2002; 7(1): 101–125.
27. Wu JN, Yan SZ and Xie LY.Reliability analysis method of a solar array by using fault tree analysis and fuzzy reasoning Petri net. *Acta Astronaut* 2011; 69: 960–968.
28. Rauschenbach HS.*Solar cell array design handbook: the principles and technology of photovoltaic energy conversion*. 1st ed. Beijing, China: China Astronautic Publishing House, 1994 (in Chinese).
29. Fragnito M and Pastena M.Design of smart microsatellite deployable solar wings. *Acta Astronaut* 2007; 61: 335–544.
30. Metz H, Kiendl M and Roth M.*A mechanism for extending and hauling in a folding structure such as a solar cell panel array*. Patent GB2114812A, UK, 1983.
31. Tanzman JR.Material considerations in the STEREO solar array design. *Acta Astronaut* 2008; 63: 1239–1245.
32. Airclaims Ascend SpaceTrak Database, http://www.ascendworldwide.com (accessed 6 December 2013).
33. Saleh JH and Castet JF. *Spacecraft reliability and multi-state failures: a statistical approach*. 2nd ed.Hoboken, NJ: Wiley, p.11.