Chinese Journal of Aeronautics, (2016), 29(3): 799–813

Chinese Society of Aeronautics and Astronautics
& Beihang University

Chinese Journal of Aeronautics

cja@buaa.edu.cn
www.sciencedirect.com

Modeling of reliability and performance assessment of a dissimilar redundancy actuation system with failure monitoring

Wang Shaoping [a,*], Cui Xiaoyu [a], Shi Jian [a], Mileta M. Tomovic [b], Jiao Zongxia [a]

[a] School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China
[b] College of Engineering and Technology, Old Dominion University, Norfolk, VA 23529, USA

Received 11 May 2015; revised 17 July 2015; accepted 7 August 2015
Available online 20 October 2015

KEYWORDS

Dissimilar redundancy actuation system;
Electro-hydraulic actuation system;
Fault monitoring;
Generalized stochastic Petri nets;
Performance degradation

Abstract Actuation system is a vital system in an aircraft, providing the force necessary to move flight control surfaces. The system has a significant influence on the overall aircraft performance and its safety. In order to further increase already high reliability and safety, Airbus has implemented a dissimilar redundancy actuation system (DRAS) in its aircraft. The DRAS consists of a hydraulic actuation system (HAS) and an electro-hydrostatic actuation system (EHAS), in which the HAS utilizes a hydraulic source (HS) to move the control surface and the EHAS utilizes an electrical supply (ES) to provide the motion force. This paper focuses on the performance degradation processes and fault monitoring strategies of the DRAS, establishes its reliability model based on the generalized stochastic Petri nets (GSPN), and carries out a reliability assessment considering the fault monitoring coverage rate and the false alarm rate. The results indicate that the proposed reliability model of the DRAS, considering the fault monitoring, can express its fault logical relation and redundancy degradation process and identify potential safety hazards.

1. Introduction

As one of the key subsystems in aircraft, the actuation system is mainly used to transmit and distribute secondary energy power and conduct actuations, accomplishing flight control and operation by fulfilling preset missions. If a failure has occurred in the system, a minor outcome could result in a failed mission, but a disastrous outcome can result in fatal plane crash. Therefore, the performance and reliability of the actuation system are of critical importance to aircraft safety, maneuverability, and flight quality.[1,2]

In order to improve the reliability and safety of an actuation system, the dissimilar redundancy technology has been widely adopted in modern aircraft design.[3,4] Airbus 380 was the first aircraft to introduce a system with a combination of dissimilar hydraulic power/electronic power and hydraulic

* Corresponding author. Tel.: +86 10 82338933.
E-mail address: shaopingwang@vip.sina.com (S. Wang).
Peer review under responsibility of Editorial Committee of CJA.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.cja.2015.10.002

Nomenclature

Abbreviation	*Meaning*
DRAS	dissimilar redundant actuation system
DMM	dynamic Markov model
M	motor
EN	evidential networks
DFTA	dynamic fault tree analysis
MSS	multi-state system
FMD	fault monitoring devices
FMCR	failure monitoring coverage rate
MCR	monitoring coverage rate
GSPN	generalized stochastic Petri nets
HA	hydraulic actuator
HS	hydraulic source
HAS	hydraulic actuation system including HA and HS
EHA	electro-hydraulic actuator
ES	electrical supply
EHAS	electro-hydraulic actuation system including EHA and ES
DFM	direct failure mode
GFM	gradual failure mode
CTMC	continuous-time Markov chain
$GSPN_{HAS}$	description for GSPN-based reliability model of HAS
$GSPN_{EHAS}$	description for GSPN-based reliability model of EHAS
HS_{up}	operational state of HS
HS_{dn}	failed state of HS
HA_{eup}	equivalent operational state of HA
HA_{edn}	equivalent failed state of HA
HAS_{up}	operational state of HAS
HAS_{dn}	failed state of HAS
ES_{up}	operational state of ES
ES_{dn}	failed state of ES
EHA_{eup}	equivalent operational state of EHA
EHA_{edn}	equivalent failed state of EHA
$EHAS_{up}$	operational state of EHAS
$EHAS_{dn}$	failed state of HAS
$EHAS_{bp}$	back-up state of EHAS
$GSPN_{DRAS}$	description for GSPN-based reliability model of DRAS
$DRAS_{up}$	operational state of DRAS
$DRAS_{dn}$	failed state of DRAS
$HAS/EHAS_{ud}$	state that undetected failure existed in HAS/EHAS
$HAS/EHAS_{fd}$	state that failures are detected in HAS/EHAS
$HAS/EHAS_{fa}$	state that false alarm occurred in HAS/EHAS
$HAS/EHAS_{nfa}$	state that no false alarm occurred in HAS/EHAS
$HAS/EHAS_{vup}$	HAS/EHAS is in operational state from the view of detection signal
$HAS/EHAS_{vdn}$	HAS/EHAS is in failure state from the view of detection signal
HA_{lf}	light failure state of HA
HA_{mf}	middle failure state of HA
HA_{sf}	secure failure state of HA

Variable	*Meaning*
i	input current of HA
u	input voltage of EHA
θ	deflection angle of the control surface
λ	failure rate
μ	repair rate
P_m	monitoring coverage probability of FMD
P_{fa}	false alarm probability of FMD
$S_{HAS/EHAS/DRAS}$	marking vector of GSPN for HAS/EHAS/DRAS
S_{IDEAL}	state space of DRAS in an ideal situation with no FMD
$M_{HAS0/EHAS0/DRAS0}$	initial states of S in HAS/EHAS/DRAS
$K_{HAS/EHAS/DRAS}$	capacities of each element in $S_{HAS/EHAS/DRAS}$
$T_{HASt/EHASt}$	timed transition set of GSPN for HAS or EHAS
$\Lambda_{HAS/EHAS}$	Transition rate set associate with $T_{HASt/EHASt}$
$T_{HASit/EHASit}$	immediate transition set of GSPN for HAS or EHAS
T	dynamic transition behavior set
M_0	initial identification of a system in GSPN model
F	arc set of GSPN
W	arc weight set of GSPN
S_d	marking set to express whether the fault of HAS/EHAS is detected or false alarm occurred
S_v	marking set to describe if HAS/EHAS is normal from the view of detection signal
S_{INT}	Integral state space of DRAS with FMD
P_{eup}	equivalent operational probability of HA
P_{edn}	equivalent failure probability of HA
λ_e	equivalent failure rate of HA

actuators/electro-hydrostatic actuators aiming to avoid severe outcomes resulting from common cause failures in the actuation system.[5] Although the dissimilar redundant technology has enhanced system mission reliability, it has also increased the overall complexity due to the multiple redundancy design. Shi et al.[6] analyzed a triplex-redundancy airborne hydraulic actuation system and found that the number of system states has increased nine times due to the applications of redundancy techniques. In addition to the normal operating and complete failure states, the system is loaded with a great number of performance degrading states. In other words, the redundancy design in the power and actuation system makes an aircraft experience significant redundancy and performance degradation processes. The redundancy degradation affects not only the general performance, but also the general availability of the system because there are very complicated transitions within the redundancy degradation and between normal and fault states. It is concluded from the analysis of redundancy system failure mechanisms that the degradation failure process is closely related to the system architecture, equipment

reliability parameters, and redundancy transition strategies. Therefore, in order to gain better understanding of the reliability advantages of the DRAS, it is essential to conduct comprehensive research on all possible system states and transition paths from normal state to complete failure state.

Traditional reliability modeling methods, reliability block diagram (RBD) and fault tree analysis (FTA), construct logic relations between component reliability and system reliability in accordance with the system structural composition and function, but they fail to represent the dynamic redundancy degradation and state transitions of DRAS. In addition, NP-hard problem occurs when we calculate the minimum cut set of a large fault tree, as presented by Nystrom et al.[7] Yang et al.[8] applied evidential networks (EN) approach to the problem of the reliability of a redundant servo actuation system. His approach could not describe existing states and dynamic transitioning while the system is working. Distefano[9] and Ranjbar et al.[10] presented the analytical method of system dynamic reliability, and employed the dynamic Markov model (DMM) to illustrate states and behavior of the system. The authors approach was based on two-state assumption (normal and failed), which is unable to demonstrate in detail the entire degradation process from full-up state to failure. As the number of system components linearly increase, the system's state space will experience exponential increase, which means that DMM has exponential complexity.[11] DRAS is a typical multi-state system (MSS) performing its task with degraded performance levels. Levitin[12] proposed the universal generating function (UGF) method for MSS reliability analysis. A comprehensive review of MSS reliability theory and its applications can be found in the work by Lisnianski and Levitin,[13] where different approaches for assessing MSS reliability are presented in detail. An extension of Boolean models to the multi-valued case, stochastic process and Monto-Carlo simulation are also highlighted by Liu and Huang.[14] However, these methods could not describe the performance of FMD, which is necessary in DRAS. Yao[3] proposed a dynamic fault tree analysis model (DFTA) of an airplane fly-by-wire system. The approach included the dynamic timing of system failures, but did not consider state transition paths of the system redundancy degradation.

Furthermore, to ensure proper functioning of DRAS, FMDs are included in DRAS. FMD monitors the system states in real time, and isolates and cuts out faulty units. Multiple factors, including detection precision, layout of sensors, selection of failure thresholds, and other external interferences, collectively affect the performance of FMD. The performance of FMD is commonly denoted by failure monitoring coverage probability and false alarm probability. In actual application with monitoring coverage rate limits, FMD are unable to 100% correctly detect and isolate DRAS, which may have significant impact on the system safety. In extreme cases, failing to detect a fatal fault (complete failure in a single channel, HAS or EHAS, in DRAS) may cause disastrous consequences. However, when false alarms occur in FMD, it does not necessarily mean that all alarms or transitions are responses to real systemic faults, but rather, perfect or comparatively sound devices may be mistakenly switched off, thus lowering the utilization of the DRAS and affecting the mission reliability of the system. As a result, FMD often becomes the weak link in the entire redundancy system design.[15] The advantages of GSPN resulted in development of a triplex-redundancy hydraulic actuation system. The related reliability model of three parallel hydraulic actuators revealed how failure detection rates affected system reliability on the basis of the redundancy architecture, according to Shi et al.[6] However, they did not discuss degradation of actuator performance, nor false alarms from FMD.

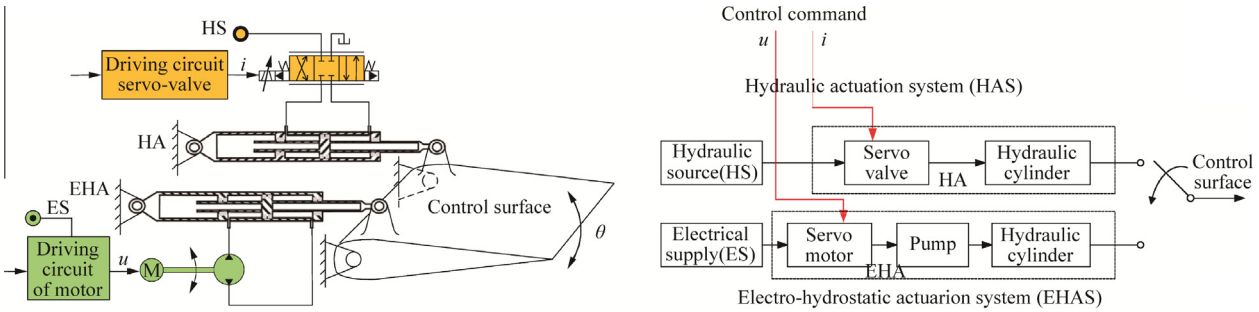
The DRAS, in general, experiences performance degrading processes and fault sequences, different redundancy monitoring transition strategies, and potential faults which have significant impact on the system reliability. Thus, there is a need to develop a method to model the reliability of DRAS with fault monitoring. The Markov process[10], which is commonly applied for system reliability modeling, requires predefinition for all state transitions when it is used in analyzing performance degradation and fault dynamic sequence, which makes the problem difficult to solve. The problem of using the Markov process approach to DRAS with monitoring devices is even more difficult due to significant complexity of the system. For such a complex system, to pre-define accurately all potential states is virtually impossible and any minor change in the system structure would require significant effort to reconfigure the model. Additional difficulty is presented by the fact that the current reliability model cannot manifest potential safety hazards due to introduction of FMD. Therefore, it is important to propose a new model applicable to the reliability and safety analysis of DRAS. GSPN is a modeling and analysis tool for distributed systems, particularly suited to describe the order, concurrency, conflict, and synchronous relationship of the process or component in a system. Meanwhile, as a special directed network, Petri net can reflect state changes and provide intuitive development of a system by means of a graphic model.[16–19]

This paper firstly studies the state transitions in the light of the characteristics of DRAS. A reliability model is constructed and solved using GSPN, and then the weak link of the dissimilar redundant system is identified. The detection probability and false alarm probability are considered as FMD is calculated, and the system fault logical relation and redundancy degrading process are presented. Finally, the causes and probability of potential safety hazards are analyzed, and the methods for improvement of system safety are discussed.

2. Reliability modeling for the dissimilar redundancy actuation system

The architecture and block diagram of a DRAS is shown in Fig. 1, where the power supply includes hydraulic power (HS) and electric power (ES), and its actuation system is composed of an HA and an EHA. Energy for the HA is supplied by a central hydraulic power unit, whereas the EHA has integrated electric power and local hydraulic units. The system represents a typical dissimilar redundancy architecture in terms of power supply and actuation system.[20,21]

As indicated in Fig. 1, the HAS consists of central hydraulic power supply (HS) and a hydraulic actuator (HA) including a servo valve and a hydraulic cylinder. The EHAS consists of electric power (ES) and an electro-hydraulic actuator (EHA) including a piston pump and a hydraulic cylinder. An FMD is set up in each channel to guarantee safe and reliable operation, early fault detection, timely fault isolation, and rapid maintenance of system failures. Normally, the HAS works



(a) Architecture of DRAS (b) Principle block diagram of DRAS

Fig. 1 Architecture and principle block diagram of DRAS.

alone as a primary driver of control surfaces, while the EHAS serves as a backup to the HAS. The hydraulic cylinder of the EHA is in a back-up state with two hydraulic chambers connected. If the HAS breaks down and its failure is correctly detected, the failed HAS will be isolated and cut off, which will cause the EHAS to carry on the mission of actuating control surfaces. If the EHAS is to malfunction, the aircraft will have to substitute it with other control surface combinations to realize the flight control.

2.1. State transition analysis of the dissimilar redundancy system

Deriving from the DRAS working principle and its failure occurrence and development process, we use λ_{HAS} and λ_{EHAS} to represent the failure rate for the HAS and the EHAS, respectively, as well as μ_{HAS} and μ_{EHAS} as repair rates. P_m and P_{fa} represent the monitoring coverage probability and the false alarm probability of FMD. Then the main DRAS states can be defined as indicated in Table 1.

Based on the above state definitions, DRAS state transition relations are illustrated by Fig. 2. The figure represents a diagram of state transitions based on the Markov process. It depicts the system redundancy degradation and failure processes. In the DRAS, an FMD is required to detect the working states of HAS and EHAS, whereas in a single HAS or EHAS, an FMD is not required. Here, P_m represents the monitoring coverage probability of FMD and P_{fa} represents the false alarm probability of FMD.

DRAS states, in Fig. 2, are divided into three groups. The first group, represented with solid circles, includes DRAS functional states (1, 2, 3, 11, 12, and 13). State 1, represented with two concentric solid circles, means that HAS operates and EHAS is in standby mode normally. States 2, 3, 11, 12, and 13 are DRAS redundancy degradation states and are represented with a single solid circle. The second group of states, represented with dashed line circles, includes DRAS complete failure states (4, 5, 6, and 7). The third group of states, represented with triangles, includes DRAS potential hazardous states (8, 9, and 10). The probability on the edge between two nodes indicates the state transfer probability. As the states are clearly described in Table 1, it is straightforward to understand the parameters, the failure rate λ and the maintenance rate μ of the components (HAS and EHAS), as well as the monitoring coverage probability P_m and the false alarm probability P_{fa} of FMD in DRAS.

Table 1 System state definition.

States	Description
1	HAS operates and EHAS standby normally: DRAS is normal
2	HAS breaks down and is correctly detected, and then EHAS operates: DRAS redundancy degrading
3	False alarm occurs as HAS normally operates, and then EHAS is switched into the system: DRAS redundancy degrading
4	Both HAS and EHAS break down and are correctly detected, in this case DRAS loses its function completely: DRAS failed
5	HAS breaks down and is correctly detected, however, false alarm occurs as EHAS operates normally: DRAS becomes invalid
6	False alarm occurs as HAS and EHAS operate normally: DRAS becomes invalid
7	False alarm occurs as HAS operates normally, and EHAS experiences breakdown and is correctly detected: DRAS becomes invalid
8	False alarm occurs as HAS operates normally, and EHAS experiences breakdown but is not detected: DRAS is in danger
9	HAS breaks down and is correctly detected, furthermore, EHAS breaks down but is not detected: DRAS is in danger
10	HAS breaks down but is not detected, and HAS fails: DRAS in danger
11	HAS operates, while EHAS experiences breakdown and is under maintenance: DRAS redundancy degrading
12	HAS operates, but the fault in EHAS is not detected, that is false backup: DRAS redundancy degrading
13	HAS operates, and EHAS is normal but is mistaken for fault: DRAS redundancy degrading

If the failure detection threshold value set in FMD is too high, or if FMD is out of order, an actual HAS failure may not be detected correctly. As a result, DRAS will not be able to cut off the failed HAS and switch operation to EHAS. In this case, the control surface driven by DRAS will be out of control, and the aircraft will be in a hazard state. This particular failure of DRAS is described as a transition from state 1 to state 10, as shown in Fig. 2. Alternately, if the failure of EHAS is not detected due to FMD's incomplete detection coverage of DRAS in state 3, the control surface driven by DRAS may also be out of control, and the aircraft will be in a hazard state. This failure process of DRAS is described as a transition

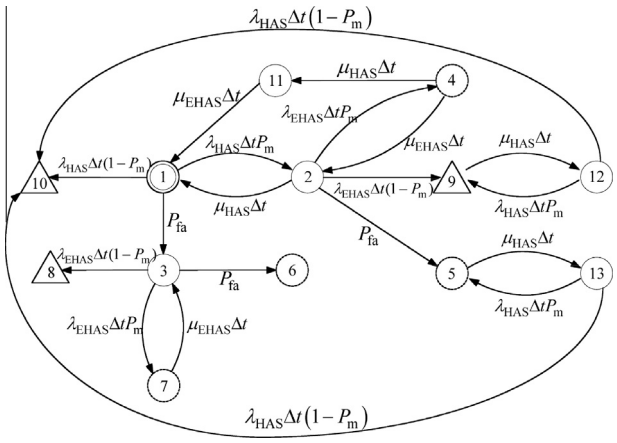


Fig. 2 DRAS state transitions based on the Markov process.

from state 3 to state 8, as shown in Fig. 2. Therefore, missed detection and false alarm of FMD can create potential safety problems to the aircraft, affecting aircraft safety and its reliability. Furthermore, when DRAS is in state 1, HAS may be wrongly cut off and switched to state 3 because of the false alarm of FMD or occasional intermittent interferences. At that instant, if the EHA also reports a false alarm, then the overall system will soon be regarded as in a fault state. Transitions 1-3-7/6 and 1-2-5 show that false alarms can cause DRAS to drop into failure sooner, reduce the system utilization, and have negative effect on mission-accomplishing reliability. Consequently, when establishing a reliability model for DRAS, the FMD performance factor is of vital importance to the accuracy of the model.

The Markov model approach is unable to reveal the working states of internal components in HAS and EHAS. The multiple states and complicated models render the solution of the Markov model even more difficult. Furthermore, both HAS and EHAS are closed-loop control systems, the performance of which may downgrade with an increase in service time.[22] Therefore, the reliability model of HAS/EHAS cannot be simply described with two states (i.e., operational and failed). Failure of HAS/EHAS can be divided into two modes: direct failure mode (DFM) and gradual failure mode (GFM). DFM is a failure mode in which a failure once occurs will directly cause failure in HAS and/or EHAS. In the case of HAS, typical DFMs include short-circuiting and disconnect of servo valve coil, seizing of the servo valve spool or hydraulic cylinder, and fatigue failure of the piston rod. Alternately, in the case of EHAS, typical DFMs include motor winding short-circuiting and disconnect, and damage of core insulation. GFM is a progressive failure mode, where the development and occurrence of GFM happen over a period of time. This failure mode includes failures such as leakage caused by the wear of hydraulic cylinders, abrasion of servo valve spools, and parameter fluctuation of various system components. The Markov model which takes into account the failure features of HAS/EHAS becomes unwieldy, thus making finding the solution increasingly difficult, and thus GSPN is introduced. A continuous-time GSPN with finite position and timed transition is isomorphic to a one-dimensional continuous-time Markov chain.[23] To describe the fault-maintenance process of a complex system, the dynamic operation of an actual system is simulated by marked flow in a reliability model based on GSPN. Meanwhile, as a mathematical tool, GSPN is obtained by establishing state equation, algebraic equation and simulation, which simplifies the reliability modeling and solving process of a complex system.

2.2. GSPN depiction of DRAS

Generalized stochastic Petri nets (GSPN) are generally defined as $\mathrm{GSPN} = (S, T; F, K, M, \Lambda)$, under the condition that $S \cup T \neq \emptyset$, $S \cap T = \emptyset$, $F \subseteq (S \times T) \cup (T \times S)$, and $\mathrm{dom}(F) \cup \mathrm{con}(F) = S \cup T$.[24] $S = \{s_1, s_2, ..., s_m\}$ is the set of repository, $T = \{t_1, t_2, ..., t_n\}$ is the set of timed transition, and the elements in F are called arcs. $K = \{k_1, k_2, \ldots, k_l\}$ is the capacity function set of repository S and W is the weight function which connects the timed transition and the arcs of repository. M_0 is the initial identification of a system. $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ is the set of the average trigger rate of the timed transition, where the reciprocal of λ is the average time delay of the timed transition. In the reliability analysis, λ is represented for failure/maintenance rate distribution of a component. $\mathrm{dom}(F) = \{x|\exists y : (x, y) \in F\}$ and $\mathrm{con}(F) = \{x|\exists y : (y, x) \in F\}$ are the domains of definition and range, respectively.

2.2.1. Assumptions

Assumption 1: Both the failing and repairing times of each component in DRAS can be represented by the exponential distribution.

Assumption 2: HAS is the main actuation system to drive the rudder, while EHAS is the backup system. Once HAS fails, EHAS replaces HAS and drives the control surface. HAS will take over once it is repaired.

Assumption 3: FMD is used to detect failures in both HAS and EHAS. The isolation and switching of redundancy configuration are executed once FMD detects the faults. FMD is assumed to have limited fault monitoring coverage and false alarming probability in DRAS.

2.2.2. Definitions

Definition 1: The GSPN-based reliability models of HAS and EHAS are described as:

$$\mathrm{GSPN}_{\mathrm{HAS}} = (S_{\mathrm{HAS}}, T_{\mathrm{HAS}}; F_{\mathrm{HAS}}, K_{\mathrm{HAS}}, W_{\mathrm{HAS}}, M_{\mathrm{HAS0}}, \Lambda_{\mathrm{HAS}}) \tag{1}$$

$$\mathrm{GSPN}_{\mathrm{EHAS}} = (S_{\mathrm{EHAS}}, T_{\mathrm{EHAS}}; F_{\mathrm{EHAS}}, K_{\mathrm{EHAS}}, W_{\mathrm{EHAS}}, M_{\mathrm{EHAS0}}, \Lambda_{\mathrm{EHAS}}) \tag{2}$$

Definition 2: The GSPN-based model of the DRAS in an ideal situation without FMD is described as:

$$\mathrm{GSPN}_{\mathrm{IDEAL}} = \mathrm{GSPN}_{\mathrm{HAS}} \cup \mathrm{GSPN}_{\mathrm{EHAS}} \cup \mathrm{GSPN}_{\mathrm{DRAS}} \tag{3}$$

Definition 3: The integrated GSPN model of the DRAS with FMD is described as:

$$\mathrm{GSPN}_{\mathrm{INT}} = \mathrm{GSPN}_{\mathrm{IDEAL}} \cup \mathrm{GSPN}_{\mathrm{FMD}} \tag{4}$$

where $\mathrm{GSPN}_{\mathrm{FMD}}$ is:

$$\mathrm{GSPN}_{\mathrm{FMD}} = (S_{\mathrm{F}}, T_{\mathrm{F}}; F_{\mathrm{F}}, K_{\mathrm{F}}, W_{\mathrm{F}}, M_{\mathrm{F0}}, \Lambda_{\mathrm{F}}) \tag{5}$$

2.2.3. Model description

In order to effectively describe the operational/failed status of components and subsystems, we define $S_{\mathrm{HAS}} = \{\mathrm{HS}_{\mathrm{up}}, \mathrm{HS}_{\mathrm{dn}},$

$HA_{eup}, HA_{edn}, HAS_{up}, HAS_{dn}\}$ as the marking vector of $GSPN_{HAS}$. The elements in S_{HAS} describe the operational and failed states of HS, the equal functional and equal failed states of HA, and the operational and failed states of HAS. The initial states of S_{HAS} are defined as $M_{HAS0} = \{1, 0, 1, 0, 1, 0\}$ which indicates that HAS and its components are all operational. Here, $\#(HS_{up}) = 1$ indicates that the hydraulic source is normal, and $\#(HS_{dn}) = 1$ indicates that a fault has occurred in the HS. The detailed description of each element in S_{HAS} is provided in Section 2.2.4. $K_{HAS} = \{1, 1, 1, 1, 1, 1\}$ defines the capacity of each element in S_{HAS}. $T_{HASt} = \{t_{HAS1}, t_{HAS2}, t_{HAS3}, t_{HAS4}\}$ is the timed transition set of $GSPN_{HAS}$, and defines all dynamic failing/repair processes of each component in HAS. The transition rate set associated with T_{HASt} is $\Lambda_{HAS} = \{\lambda_{HS}, \mu_{HS}, \lambda_{HA}, \mu_{HA}\}$. The elements in Λ_{HAS} represent for the failure rate of HS, the repair rate of HS, the failure rate of HA, and the repair rate of HA, respectively. The immediate transition set $T_{HASit} = \{t_{HASi1}, t_{HASi2}, t_{HASi3}\}$ is defined in $GSPN_{HAS}$ to describe logical judgment processes, which take less time than the timed transitions. The dynamic transition behavior can then be described as $T_{HAS} = T_{HASt} \cup T_{HASit}$, and $T_{HASt} \cap T_{HASit} = \emptyset$. F_{HAS} is the arc set of the model, and the values of the arc set W_{HAS} are all 1.

The purpose of the EHAS is to serve as a back-up system to the HAS. It has three operating states – normal, failure, and back-up. We define $S_{EHAS} = \{ES_{up}, ES_{dn}, EHA_{eup}, EHA_{edn}, EHAS_{up}, EHAS_{dn}, EHAS_{bp}\}$ as the marking vector of EHAS. The elements in S_{EHAS} describe the operational and failed states of ES, the equal functional and equal failed states of EHA, and the operational, failed, and back-up states of EHAS. $K_{EHAS} = \{1, 1, 1, 1, 1, 1, 1\}$ is the capacity set of the elements in S_{EHAS}. Depending on the states transition processes in EHAS, we define the time dependent transition set of EHAS as $T_{EHASt} = \{t_{EHAS1}, t_{EHAS2}, t_{EHAS3}, t_{EHAS4}\}$, and the transition rate set associated with T_{EHASt} as $\Lambda_{EHAS} = \{\lambda_{ES}, \mu_{ES}, \lambda_{EHA}, \mu_{EHA}\}$. The elements in Λ_{EHAS} represent the failure rate of ES, the repair rate of ES, the failure rate of EHA, and the repair rate of EHA, respectively. The immediate transition set is defined as $T_{EHASit} = \{t_{EHASi1}, t_{EHASi2}, t_{EHASi3}\}$, and it represents the logical judgment between markings in EHAS. Here, $T_{EHAS} = T_{EHASt} \cup T_{EHASit}$ and $T_{EHASt} \cap T_{EHASit} = \emptyset$. F_{EHAS} is the arc set and the values of the arc set W_{EHAS} are all 1. The logical relationship between HAS and EHAS of DRAS is active-standby. $GSPN_{DRAS}$ is used to describe the DRAS model, and the marking vector $S_{DRAS} = \{DRAS_{up}, DRAS_{dn}\}$ represents the operational and failed states of DRAS. $S_{IDEAL} = S_{DRAS} \cup S_{HAS} \cup S_{EHAS}$ describes the state space of DRAS in an ideal situation with no FMD. The initial state of the system is $M_{DRAS0} = \{1, 0\}$, and the capacity vector of each marking is $K_{DRAS} = \{1, 1\}$.

For the purpose of performance analysis of FMD, the marking set $S_d = \{HAS_{ud}, HAS_{fd}, EHAS_{ud}, EHAS_{fd}, HAS_{nfa}, HAS_{fa}, EHAS_{nfa}, EHAS_{fa}\}$ is used to express whether a fault of HAS and/or EHAS is detected or isolated and whether a false alarm has occurred. The marking set $S_v = \{HAS.vup, EHAS.vup\}$ is defined to describe if HAS/EHAS has a normal detection signal. $S_{INT} = S_{HAS} \cup S_{EHAS} \cup S_{DRAS} \cup S_d \cup S_v$ represents the integral state space of DRAS with FMD

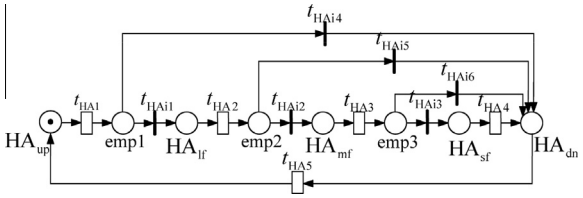


Fig. 3 GSPN model of HA performance degradation process.

2.2.4. GSPN model of DRAS

(1) GSPN model analysis of HAS

According to the fault behavior analysis of HA and EHA described in Section 2.1, HA is a position closed-loop control system where fault behaviors include both direct failure process and progressive failure process caused by the performance degradation of components. The resulting HA's GSPN model, based on performance degradation, is shown in Fig. 3.

According to the GSPN model, in Fig. 3, HA can function normally in the initial condition, i.e., $\#(HA_{up}) = 1$. After a period of time t_{HA1}, HA may encounter DFM with a probability of $P(t_{HAi4})$, and then a token is transmitted directly from HA_{up} to HA_{dn}. The failure that HA may encounter could also be a GFM with a probability of $P(t_{HAi1})$, and then HA is considered to be in the light failure state (HA_{lf}). Here, $P(t_{HAi4}) + P(t_{HAi1}) = 1$. The transfer rate of the timed transition t_{HA1} is λ_1, and then $P(t_{HAi4})\lambda_1$ describes the failure rate of HA from a normal operating state to complete failure, while $P(t_{HAi1})\lambda_1$ describes the failure rate of HA from a normal operating state to a light failure state. As the operational time is increasing, HA may encounter further performance degradation until down (HA_{dn}), or after a light failure state (HA_{lf}), a middle failure state (HA_{mf}) token is directly transmitted to HA_{dn} with a probability of $P(t_{HAi5})$ or $P(t_{HAi6})$. Here, $P(t_{HAi5}) + P(t_{HAi2}) = 1$ and $P(t_{HAi6}) + P(t_{HAi3}) = 1$. temp $i (i = 1, 2, 3)$ represent temporary states in GSPN modeling of the HA performance degradation process. The failed HA will be repaired after transition t_{HA5} where the transfer rate is μ.

It can be seen from Fig. 3 that the GSPN model of the HA performance degradation process has five steady states: working normally, the light failure state, the middle failure state, the serious failure state, and complete failure. If we use numbers 0, 1, 2, 3, and 4 to represent the five states, then the continuous-time Markov chain (CTMC) model of HA, which is equivalent to the GSPN model, can be represented as shown in Fig. 4.

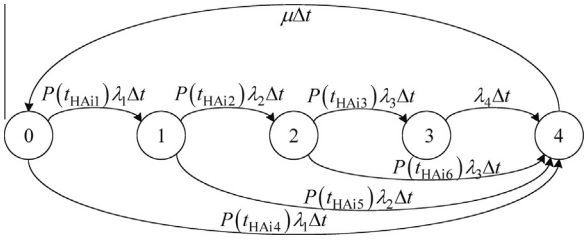


Fig. 4 CTMC model of HA performance degradation process.

The probability of state transfer is shown on the edge between two nodes in Fig. 4. $P(t_{\mathrm{HAi}t})$ represents the probability of an immediate timed transition, λ_i represents the failure rate of different degraded HA, and μ represents the maintenance rate from a complete failure state to a functional state.

According to the CTMC model shown in Fig. 4, the state transition equation is obtained as:

$$\begin{bmatrix}\dot{P}_0(t)\\ \dot{P}_1(t)\\ \dot{P}_2(t)\\ \dot{P}_3(t)\\ \dot{P}_4(t)\end{bmatrix}=\begin{bmatrix}-P_{\mathrm{HAi1}}\lambda_1-P_{\mathrm{HAi4}}\lambda_1 & 0 & 0 & 0 & \mu\\ P_1\lambda_1 & -P_{\mathrm{HAi2}}\lambda_2-P_{\mathrm{HAi5}}\lambda_2 & 0 & 0 & 0\\ 0 & P_{\mathrm{HAi2}}\lambda_2 & -P_{\mathrm{HAi3}}\lambda_3-P_{\mathrm{HAi6}}\lambda_3 & 0 & 0\\ 0 & 0 & P_{\mathrm{HAi3}}\lambda_3 & -\lambda_4 & 0\\ P_{\mathrm{HAi4}}\lambda_1 & P_{\mathrm{HAi5}}\lambda_2 & P_{\mathrm{HAi6}}\lambda_3 & \lambda_4 & -\mu\end{bmatrix}\begin{bmatrix}P_0(t)\\ P_1(t)\\ P_2(t)\\ P_3(t)\\ P_4(t)\end{bmatrix} \tag{6}$$

The initial condition is:

$$\begin{bmatrix}P_0(0)\\ P_1(0)\\ P_2(0)\\ P_3(0)\\ P_4(0)\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix} \tag{7}$$

The steady probabilities of these states of HA can be obtained as follows:

$$\begin{cases}P_0=\frac{\mu\lambda_2\lambda_3\lambda_4}{G}\\ P_1=\frac{\mu P_{\mathrm{HAi1}}\lambda_1\lambda_3\lambda_4}{G}\\ P_2=\frac{\mu P_{\mathrm{HAi1}}\lambda_1 P_{\mathrm{HAi2}}\lambda_2\lambda_4}{G}\\ P_3=\frac{\mu P_{\mathrm{HAi1}}\lambda_1 P_{\mathrm{HAi2}}\lambda_2 P_{\mathrm{HAi3}}\lambda_3}{G}\\ P_4=\frac{\lambda_1\lambda_2\lambda_3\lambda_4}{G}\end{cases} \tag{8}$$

where $G=\lambda_1\lambda_2\lambda_3\lambda_4+\mu\lambda_2\lambda_3\lambda_4+\mu P_{\mathrm{HAi1}}\lambda_1\lambda_3\lambda_4+\mu P_{\mathrm{HAi1}}\lambda_1 P_{\mathrm{HAi2}}\lambda_2\lambda_4+\mu P_{\mathrm{HAi1}}\lambda_1 P_{\mathrm{HAi2}}\lambda_2 P_{\mathrm{HAi3}}\lambda_3$.

The HA can still fulfill its function in the all four states 0, 1, 2, and 3, so the equivalent operational probability of HA (P_{eup}) and the equivalent failure probability of HA (P_{edn}) are:

$$\begin{cases}P_{\mathrm{eup}}=P_0+P_1+P_2+P_3\\ P_{\mathrm{edn}}=P_4\end{cases} \tag{9}$$

In order to facilitate the reliability analysis, the failure and repair process can be equivalent to a transition between an operational state and a failure state. The simplified GSPN model is shown in Fig. 5.

According to the GSPN structure in Fig. 5, the equivalent operational probability of HA is:

$$P_{\mathrm{eup}}=\frac{\mu_{\mathrm{e}}}{\lambda_{\mathrm{e}}+\mu_{\mathrm{e}}} \tag{10}$$

where $\mu_{\mathrm{e}}=\mu$. Accordingly, the equivalent failure rate of HA is:

$$\lambda_{\mathrm{e}}=\frac{1-P_{\mathrm{eup}}}{P_{\mathrm{eup}}}\cdot\mu \tag{11}$$

The parameters of the HA model, the values of failure rate $\lambda_i(i=1,2,3,4)$, and the maintenance rate μ, according to Li et al.[25] are provided in Table 2. The probability of HA's immediate timed transition is assumed based on experience. The value of λ_{e} can then be calculated from Eqs. (9)-(11) as

$$\lambda_{\mathrm{e}}\approx 1.7\times 10^{-4} \tag{12}$$

Combined with the failure process of HS, the dynamic GSPN model of the HAS can be established as shown in Fig. 6.

As indicated in Fig. 6, the hydraulic actuator (HA) and the hydraulic power supply (HS) can operate normally in the initial condition, #($\mathrm{HA_{eup}}$) = 1, #($\mathrm{HS_{up}}$) = 1, and #($\mathrm{HAS_{up}}$) = 1. When the timed transition t_{HAS1} is triggered, the operating state of HS is changed from a normal working state to a failure state, and the triggering rate depends on the failure rate λ_{HS}. Transition t_{HAS2} simulates the restoration process of HS,

Table 2 Parameters of the HA model.

Parameter	Value	Parameter	Value
$P(t_{\mathrm{HAi1}})$	0.9	$P(t_{\mathrm{HAi2}})$	0.8
$P(t_{\mathrm{HAi3}})$	0.6	$P(t_{\mathrm{HAi4}})$	0.1
$P(t_{\mathrm{HAi5}})$	0.2	$P(t_{\mathrm{HAi6}})$	0.4
$\lambda_i\,(i=1,2,3,4)$ (h)	5.2×10^{-4}	μ (h)	6.8×10^{-4}

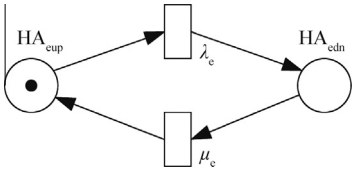


Fig. 5 Simplified GSPN model of HA.

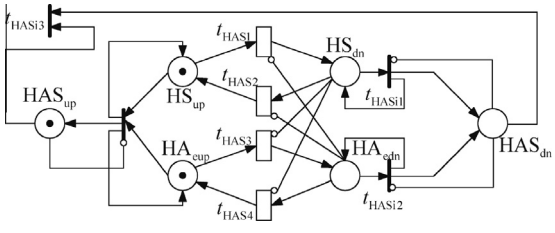


Fig. 6 GSPN model of HAS.

Table 3 GSPN model states of HAS.

States	Description
0	Both the HS and the HA are operating, and the HAS operates well
1	The HS fails, but the HA can still work. The HAS fails
2	The HS is working, but the HA loses its function due to direct or gradual failure, and the HAS fails

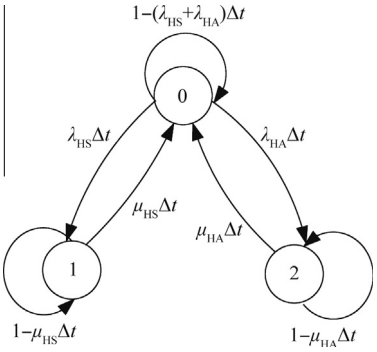


Fig. 7 CTMC model of HAS.

and its triggering rate depends on the maintenance rate μ_{HS}. The HA's state transition principle is similar to that of the HS, and the transition rates of t_{HAS3} and t_{HAS4} are λ_{HA} and μ_{HA}. HAS_{up} describes the operational state of HAS, and iff $\#(HS_{up}) = 1 \cap \#(HA_{eup}) = 1$, then $\#(HAS_{up}) = 1$, which means that HAS can work normally when both HS and HA are working well. HAS.dn represents the fault occurring in HAS, and iff $\#(HS_{dn}) = 1 \cup \#(HA_{edn}) = 1$, then $\#(HAS_{dn}) = 1$, which means that failure of either HA or HS can lead to HAS failure.

Analysis of the reachable markings in Fig. 6 indicates that three reachable states of HAS can be obtained as shown in Table 3.

According to the states description of HAS in Table 3, the CTMC model equivalent to HAS's GSPN model is shown in Fig. 7. In Fig. 7, states 0, 1, and 2 of HAS are described as in Table 3. The probability of state transferring is shown on the edge between two states. The sum of probability of one state transferring to another state or remaining in its state is 1. In Fig. 7, λ represents the failure rate and μ stands for the maintenance rate.

Based on the CTMC model of the HAS, the state transition equation is obtained as:

$$\begin{bmatrix} \dot{P}_0(t) \\ \dot{P}_1(t) \\ \dot{P}_2(t) \end{bmatrix} = \begin{bmatrix} -(\lambda_{HS}+\lambda_{HA}) & \lambda_{HS} & \lambda_{HA} \\ \mu_{HS} & -\mu_{HS} & 0 \\ \mu_{HA} & 0 & -\mu_{HA} \end{bmatrix}^{T} \begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \end{bmatrix} \quad (13)$$

where $P_i(t)$ is the probability of state i.

The initial condition is:

$$[P_0(0)\ \ P_1(0)\ \ P_2(0)] = [1\ \ 0\ \ 0] \quad (14)$$

The result for HAS's reliability can be obtained accordingly. The steady state availability of HAS is:

$$P = \lim_{t\to\infty} P_0(t) = \lim_{s\to 0} s \cdot \frac{1}{s+s\left(\frac{\lambda_{HS}}{s+\mu_{HS}}+\frac{\lambda_{HA}}{s+\mu_{HA}}\right)} = \left(1+\frac{\lambda_{HS}}{\mu_{HS}}+\frac{\lambda_{HA}}{\mu_{HA}}\right)^{-1} \quad (15)$$

Given the transition rate values in Eq. (15), $\lambda_{HS} = 2\times10^{-4}$/h, $\lambda_{HA} = \lambda_e = 1.7\times10^{-4}$/h, $\mu_{HS} = 7.2\times10^{-4}$/h, and $\mu_{HA} = \mu_e = 6.8\times10^{-4}$/h.[25] The steady state availability is determined to be 0.6545.

The EHAS serves as the back-up system for HAS. If EHAS malfunctions and is subsequently repaired, the state of EHAS will be transferred from the fault state to the back-up state. That is, there will be three states for EHAS in the DRAS model: working, fault, and back-up. The GSPN model which describes the dynamic failure process of EHAS is similar to the HAS model, and will be shown in DRAS modeling.

(2) GSPN reliability model for the ideal DRAS without FMD

The working mechanism of DRAS is cold backup. In the beginning, HAS is working, and EHAS is in the back-up

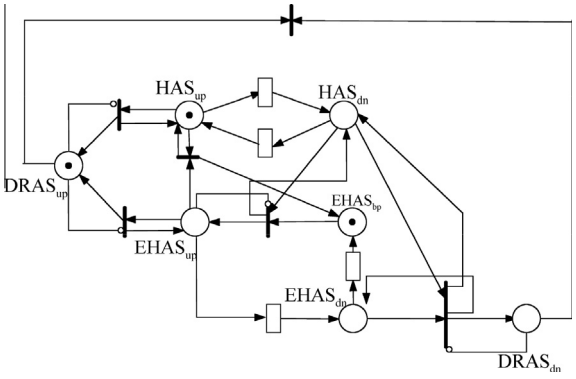


Fig. 8 GSPN model for working mechanism of DRAS.

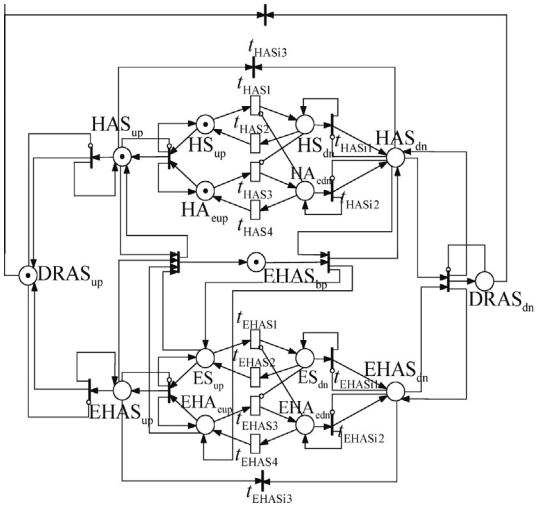


Fig. 9 GSPN model for DRAS without FMD.

Table 4 GSPN model parameters of EHAS.[25]

Parameter	Value	Meaning
λ_{ES}	1.0×10^{-4}/h	The triggering rate of time transition t_{EHAS1} and also the failure rate of ES
μ_{ES}	7.1×10^{-4}/h	The triggering rate of time transition t_{EHAS2} and also the maintenance rate of ES
λ_{EHA}	1.3×10^{-4}/h	The triggering rate of time transition t_{EHAS4} and also the equivalent failure rate of EHA
μ_{EHA}	7.3×10^{-4}/h	The triggering rate of time transition t_{EHAS4} and also the maintenance rate of EHA

Table 5 Accessible states and steady-state probability of the ideal DRAS reliability model.

State	HS_{up}	HA_{up}	ES_{up}	EHA_{up}	HAS_{up}	$EHAS_{up}$	$EHAS_{bp}$	$DRAS_{up}$	$DRAS_{dn}$	Probability
M_0	1	1	0	0	1	0	1	1	0	0.621248
M_1	1	0	1	1	0	1	0	1	0	0.13812
M_2	1	0	0	1	0	0	0	0	1	0.011624
M_3	0	1	1	1	0	1	0	1	0	0.150389
M_4	1	0	1	0	0	0	0	0	1	0.014404
M_5	1	1	1	0	1	0	0	1	0	0.02074
M_6	0	1	1	0	0	0	0	0	1	0.015666
M_7	0	1	0	1	0	0	0	0	1	0.012338
M_8	1	1	0	1	1	0	0	1	0	0.015471

mode, and DRAS is functioning well, thus: $\#(HAS_{up}) = 1$, $\#(DRAS_{up}) = 1$, and $\#(EHAS_{bp}) = 1$. If HAS fails and EHAS is in the normal backup state, EHAS resumes the function of the failed HAS to drive the rudder. In this case, $EHAS_{bp}$ is marked with a token, and DRAS is still functioning. If EHAS also fails, DRAS loses it function completely, expressed as iff $\#(HAS_{dn}) = 1 \cap \#(EHAS_{dn}) = 1$, and $\#(DRAS_{dn}) = 1$. When EHAS is repaired, it returns to the back-up state, and $EHAS_{bp}$ regains the token. The working mechanism logic of DRAS can be demonstrated by GSPN shown in Fig. 8.

To correctly clarify the relations between component failure, subsystem failure, and overall DRAS failure, we can set up a reliability model for an ideal condition with no failure monitoring devices, as shown in Fig. 9.

Since the model is very complex compared to the GSPN model of HAS, computer simulation is adopted to solve the problem. Model parameters for EHAS are given in Table 4. When we operate the model in Fig. 9 and 86 states can be accessed, 9 of which have effective tokens, as shown in Table 5.

In Table 5, M_0 indicates that all components in both HAS and EHAS are in proper service. States M_1 and M_3 represent a failure in HAS due to an HS or HA fault, but all components in EHAS work well, so DRAS runs normally. States M_2, M_4, M_6, and M_7 indicate that some have failed in both the HAS and EHAS, thus leading to overall system failure. States M_5 and M_8 indicate that HAS is in service, while EHAS is in the repair state due to ES or EHA failure, and the system is still operating.

It can be concluded from the above description that states M_0, M_1, M_3, M_5, and M_8 denote the normal operating state of DRAS, so availability of the system is described as:

$$P = P(M_0) + P(M_1) + P(M_3) + P(M_5) + P(M_8) = 0.945968 \tag{16}$$

In comparison with the availability of a single HAS in Section 2.2.4 (1), the adoption of the dissimilar redundancy working mode (EHAS) can highly improve the availability of the DRAS.

(3) Comprehensive GSPN model taking FMD's monitoring coverage probability and false alarm probability into account in DRAS

In the ideal model in Fig. 9, when HAS fails and EHAS is in the back-up state, the system will immediately switch to EHAS to drive the control surface; if the EHAS also breaks down, and the fault in HAS is not fixed, the DRAS will be considered to be in the failure status. In an actual DRAS, the HAS channel requires a fault monitoring device to check whether failure occurs and then makes transition when failure is detected. In the same way, EHAS also needs to be equipped with a monitoring device to detect and determine whether the system fails and then takes possible remedial actions. Affected by factors related to the system complexity and FMD reliability, the devices have certain indicators such as monitoring coverage probability and false alarm probability. If failure cannot be accurately detected, then potential failure and hazard states may result. Therefore, to better describe actual situations, a GSPN dynamic reliability model considering FMD performance is developed and presented in this paper. The system is shown in Fig. 10.

In the model in Fig. 10, instantaneous transitions t_{HASi5}, t_{EHASi5}, t_{HASi4}, and t_{EHASi4}, containing probability, represent the failure monitoring coverage probability and the fault missed detection probability of FMD, and $P(t_{HASi4}) + P(t_{HASi5}) = 1$, $P(t_{EHASi4}) + P(t_{EHASi5}) = 1$. The states $\#(HAS_{fd})$ and $\#(EHAS_{fd})$ indicate that failures are successfully detected, and the states $\#(HAS_{ud})$ and $\#(EHAS_{ud})$ represent undetected/false failures. Instant transitions t_{HASi7} and t_{EHASi7} indicate that FMD has reported false alarms, while t_{HASi6} and t_{EHASi6} indicate that FMD can correctly identify DRAS working states, and $P(t_{HASi6}) + P(t_{HASi7}) = 1$, $P(t_{EHASi6}) + P(t_{EHASi7}) = 1$. The states $\#(HAS_{fa})$ and $\#(EHAS_{fa})$ indicate existences of false alarms in the system, and the state $\#(HAS_{nfa})$ and $\#(EHAS_{nfa})$ indicate that token false alarms have not occurred. The states $\#(HAS_{vup})$ and $\#(EHAS_{vup})$ stand for HAS/EHAS running well from the view of the signal.

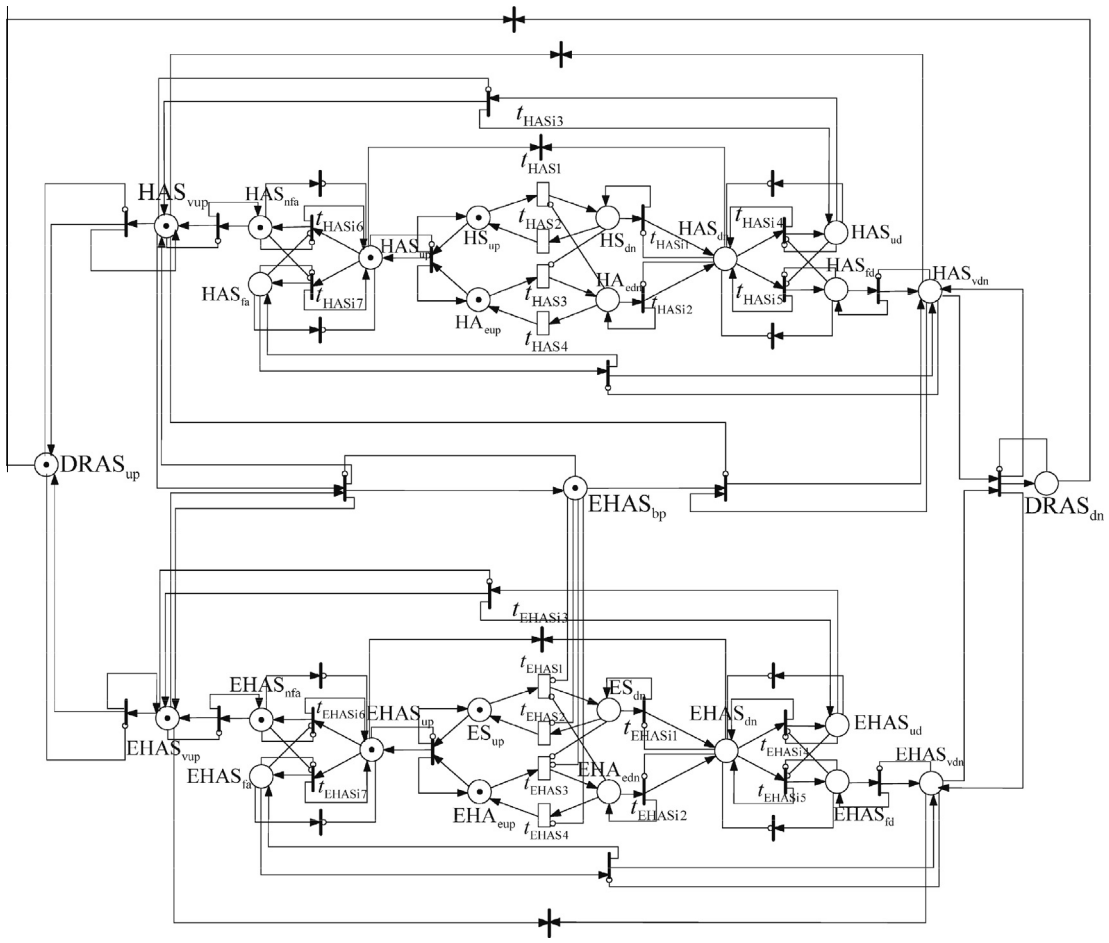


Fig. 10 Comprehensive GSPN model of an actual DRAS considering FMD performance.

Various system states can be seen from the GSPN model of an actual DRAS considering FMD performance

- When HAS fails, i.e., #(HAS_{dn}) = 1, the failure can be detected by FMD with a probability of $P(t_{HASi5})$, and then #(HAS_{fd}) = 1, #(HAS_{vdn}) = 1; therefore, DRAS switches to EHAS.
- Alternately, if the failure is not detected with a probability of $P(t_{HASi4})$, then #(HAS_{ud}) = 1, #(HAS_{vup}) = 1, and DRAS mistakenly regards HAS as functioning normally, without switching, so the DRAS is in danger.
- When HAS fails, i.e., #(HAS_{dn}) = 1∩#(HAS_{fd}) = 1∩#(HAS_{vdn}) = 1∩#($EHAS_{bp}$) = 1, then EHAS is activated. As time passes by, if EHAS fails, that is, #($EHAS_{dn}$) = 1, the failure is detected at a probability of P_{EHASi5}, and then #($EHAS_{fd}$) = 1, #($EHAS_{vdn}$) = 1, and #($DRAS_{dn}$) = 1, so the control surface driven by this DRAS is invalidated, and the flight control system will take measures for isolation and remediation.
- Alternately, if the EHAS failure is not detected at a probability of P_{EHASi4}, then #($EHAS_{ud}$) = 1 and #($EHAS_{vup}$) = 1, so the DRAS is running at risk.
- During EHAS failure, if HAS is fixed, then DRAS switches back to HAS. When false alarms have not occurred in HAS, #(HAS_{nfa}) = 1, #(HAS_{vup}) = 1, and #($DRAS_{up}$) = 1.
- If a false alarm occurs in HAS, then #(HAS_{fa}) = 1, #(HAS_{vdn}) = 1, and #($DRAS_{dn}$) = 1, so DRAS identifies a failure by wrong determination, thus reducing availability.
- Similarly, when false alarms happen while EHAS is running, then #($EHAS_{vdn}$) = 1 and #($DRAS_{dn}$) = 1.

Assuming that the monitoring coverage probabilities of FMD in HAS and EHAS are $P(t_{HASi5}) = P(t_{EHASi5}) = 0.9$ and that the fault alarm probabilities of FMD in HAS and EHAS are $P(t_{HASi7}) = P(t_{EHASi7}) = 0.05$, we have 496 accessible tokens, 36 of which have valid states, as shown in Table 6.

Analysis of DRAS accessible states provided in Table 6 reveals the following:

- State M_0 indicates that HAS is in the normal service and is correctly detected, EHAS is in the proper backup standby mode, and DRAS is functioning well, which is the desired/ideal system state.
- States M_8 and M_{13} indicate that HAS is in the normal service and is correctly detected, but EHAS fails, with failure being detected and repaired (ES or EHA failure respectively), and at this moment, DRAS is functioning, but with degraded redundancy.

Table 6 Accessible states in the comprehensive GSPN model of DRAS considering FMD performance.

State	HS_{up}	HA_{up}	HAS_{up}	HAS_{fd}	HAS_{nfa}	HAS_{vup}	ES_{up}	EHA_{up}	$EHAS_{up}$	$EHAS_{fd}$	$EHAS_{nfa}$	$EHAS_{vup}$	$EHAS_{bp}$	$DRAS_{up}$	Probability
M_0	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0.564567
M_1	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0.131395
M_2	1	0	0	1	0	0	1	1	1	0	1	1	0	1	0.117153
M_3	1	0	0	0	0	1	1	1	1	0	1	1	1	1	0.014987
M_4	1	1	1	0	0	0	1	1	1	0	1	1	0	1	0.025388
M_5	1	1	1	0	0	0	1	0	0	1	0	0	0	0	0.004014
M_6	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0.012722
M_7	0	1	0	1	0	0	1	0	0	1	0	0	0	0	0.013891
M_8	1	1	1	0	1	1	1	0	0	1	0	0	0	1	0.017583
M_9	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0.010843
M_{10}	1	1	1	0	0	0	0	1	0	1	0	0	0	0	0.002825
M_{11}	1	0	0	1	0	0	0	1	0	0	0	1	0	1	0.002041
M_{12}	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0.009426
M_{13}	1	1	1	0	1	1	0	1	0	1	0	0	0	1	0.013028
M_{14}	0	1	0	0	0	1	1	1	1	0	1	1	1	1	0.017346
M_{15}	1	1	1	0	1	1	0	1	0	0	0	1	1	1	0.008135
M_{16}	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0.002086
M_{17}	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0.002503
M_{18}	1	0	0	0	0	1	1	0	0	1	0	0	0	1	0.000278
M_{19}	1	0	0	1	0	0	1	0	0	0	0	1	0	1	0.002298
M_{20}	1	1	1	0	1	1	1	0	0	0	0	1	1	1	0.009725
M_{21}	0	1	0	0	0	1	0	1	0	1	0	0	0	1	0.000217
M_{22}	0	1	0	0	0	1	1	1	1	0	0	0	0	1	0.000166
M_{23}	1	1	1	0	1	1	1	1	1	0	0	0	0	1	0.008361
M_{24}	1	0	0	1	0	0	1	1	1	0	0	0	0	0	0.002438
M_{25}	1	1	1	0	0	0	0	1	0	0	0	1	0	1	0.000445
M_{26}	1	1	1	0	0	0	1	0	0	0	0	1	0	1	0.000545
M_{27}	1	0	0	0	0	1	1	0	0	0	0	1	1	1	0.000246
M_{28}	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0.002983
M_{29}	0	1	0	0	0	1	1	0	0	0	0	1	1	1	0.000422
M_{30}	1	0	0	0	0	1	0	1	0	1	0	0	0	1	0.000204
M_{31}	0	1	0	0	0	1	1	0	0	1	0	0	0	1	0.00029
M_{32}	0	1	0	0	0	1	0	1	0	0	0	1	1	1	0.000234
M_{33}	1	0	0	0	0	1	1	1	1	0	0	0	0	1	0.000156
M_{34}	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0.00079
M_{35}	1	0	0	0	0	1	0	1	0	0	0	1	1	1	0.00027

- State M_{23} indicates that HAS is working properly and is correctly detected, and EHAS is in normal service, but false alarms lead to judgment that DRAS is unavailable, hence DRAS is in redundancy degradation.
- States M_{15} and M_{20} indicate that HAS is in normal service and correct detection, and EHAS is in the back-up status, but a fault actually exists in EHAS, without being detected by FMD, so it is in invalid backup, and DRAS is in redundancy degradation.
- States M_1 and M_2 indicate that HAS fails and is identified by FMD (HA or HS failure respectively), and then the system enters EHAS, functioning well, so by the time system redundancy is downgraded.
- State M_4 indicates that HAS is working well but makes false alarm and gets isolation, and then the system switches to EHAS, in degraded redundancy.

To combine the above six scenarios and nine states, the functioning probability (P_A) of DRAS can be worked out, which represents the DRAS availability.

$$\begin{cases} P_A = \sum_i P(M_i) = 0.895335 \\ i = 0, 1, 2, 4, 8, 13, 15, 20, 23 \end{cases} \tag{17}$$

Further analysis of DRAS accessible states provided in Table 6 reveals the following:

- States M_6, M_7, M_9, and M_{12} indicate that HAS is in malfunction and is detected, and DRAS transits to EHAS, which is in failure and is detected, so DRAS is in the normal failure state.
- States M_{24} and M_{28} indicate that HAS is in malfunction and is detected, and DRAS switches to EHAS when it is working properly but reports false alarms, so DRAS is in the normal failure state.
- States M_5 and M_{10} indicate that HAS is functioning well but its false alarm makes it blocked, and DRAS activates EHAS that fails and is detected, so DRAS breaks down.
- State M_{34} indicates that HAS is normal but it reports false alarms and gets isolated, so DRAS selects EHAS which functions well but reports false alarm, so DRAS fails.

In all of the above-mentioned four scenarios and nine states, DRAS cannot operate normally, and gives alarms. Therefore, the system failure probability, also known as unavailability (P_{UA}), can be determined as follows

$$\begin{cases} P_{UA} = \sum_i P(M_i) = 0.059932 \\ i = 5, 6, 7, 9, 10, 12, 24, 28, 34 \end{cases} \tag{18}$$

Further analysis of DRAS accessible states provided in Table 6 reveals the following:

- States M_{25} and M_{26} indicate that HAS is in good condition but it alarms falsely and is isolated, EHAS is selected but faults occur in EHAS (due to separate failures of ES and EHA) and are not detected, and the detection system is under impression that DRAS is functioning well, but in fact it is in the hazard state.

Table 7 Comparison of three system availability based on the GSPN model.

System	HAS	Ideal DRAS without FMD	DRAS considering P_m and P_{fa}
Availability	0.6545	0.945968	0.895335

- States M_{11}, M_{16}, M_{17}, and M_{19} indicate that HAS has faults (HS and HA failures respectively) which are detected and blocked, EHAS transfers to a working state, which is in a failure state (ES and EHA failures respectively) and is undetected, and the monitoring system is under impression that DRAS is in a good working condition, but it is actually in the hazard state.
- States $M_3, M_{14}, M_{18}, M_{21}, M_{22}, M_{27}, M_{29}, M_{30-33}, M_{35}$ reflect that HAS is in problem but is not spotted by FMD, so the DRAS is in the hazard state.

To summarize, the incidence rate of hazard states (P_D) is:

$$P_D = \sum_i P(M_i) = 0.044733, \quad i = 3, 14, 18, 21, 22, 27, 29, 30, 31, 32, 33, 35 \tag{19}$$

The above results are consistent with the analysis in Section 2.1. A comparison provided in Table 7 indicates that the introduction of FMD may leave the system in danger. In addition, the system reliability with FMD's monitoring coverage probability and false alarm probability taken into account is lower than that in an ideal situation (without FMD). The analytical results correspond to system behaviors observed in practice.[6]

3. Analysis of impact of FMD performance on DRAS reliability and safety

According to the reliability analysis models, the reliability outcome is often higher than the actual value because there is no consideration of impact of FMD performance on system reliability. However, if the performance of FMD is too poor, it will cause potential danger to the system by drastically lowering the system reliability. Hence, the effects of FMD performance on system reliability need to be studied.

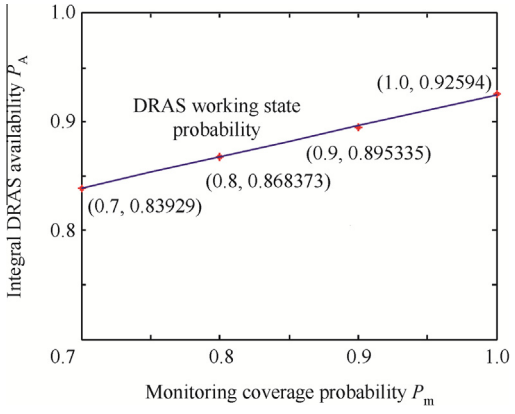


Fig. 11 Relationship between the working state probability and the monitoring coverage probability.

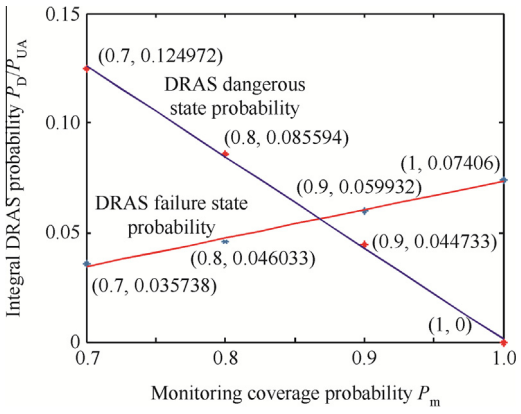


Fig. 12 Relationship between the dangerous state probability, the failure state probability, and the monitoring coverage probability.

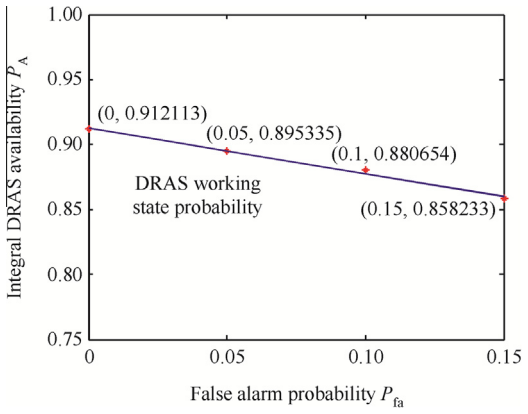


Fig. 13 Relationship between the working state probability and the false alarm probability.

3.1. Impact analysis of FMD's monitoring coverage probability on DRAS

Assuming that the false alarm probability is $P(t_{HASi7}) = P(t_{EHASi7}) = 0.05$, and by simulating the model shown in Fig. 10, we can determine how the probabilities of the working, hazard, and failure states of the EHAS change with the monitoring coverage probability, as shown in Figs. 11 and 12.

At a given false alarm probability of $P(t_{HASi7}) = P(t_{EHASi7}) = 0.05$, we use the least squares method to fit the numerical data, Fig.11, and the resulting relationship is given by $P_A = 0.2869P_m + 0.6384$, where P_m is monitoring coverage probability and P_A is availability of integral DRAS. We can conclude that by improving the monitoring coverage probability by 1%, the availability of DRAS would increase by 0.29%.

In addition, we have applied the least squares method to fit the numerical data in Fig. 12, and the relationship between the dangerous state probability (P_D) in DRAS and the monitoring coverage probability (P_m) is $P_D = -0.4158P_m + 0.4172$, while the relationship between the failure state probability (P_{UA}) in DRAS and the monitoring coverage probability is $P_{UA} = 0.1289P_m - 0.0556$. We can conclude that by improving the monitoring coverage probability by 1%, the probability of DRAS's dangerous state would decrease by 0.42%, while the unavailability would increase by 0.13%.

From Figs. 11 and 12, it can be observed that as the monitoring coverage probability increases, potential faults in the system can be gradually identified and isolated, and the system reliability can be improved. At the same time, since the faults are easier to identify, the possibility of danger from missed detection is substantially reduced, and the failure rate increases.

3.2. Impact analysis of FMD's false alarm probability on DRAS

Assuming that the monitoring coverage probability is $P(t_{HASi5}) = P(t_{EHASi5}) = 0.9$, we can determine how the probabilities of the working, dangerous, and failure states of DRAS change with the false alarm probability, as shown in Figs. 13 and 14.

Assuming that the monitor coverage probability is $P(t_{HASi5}) = P(t_{EHASi5}) = 0.9$, we can apply the least squares method to fit the numerical data in Fig. 13. The function in Fig. 13 is $P_A = -0.3526P_{fa} + 0.9130$. P_{fa} is the false alarm probability and P_A is the availability of integral DRAS. We can observe that 1% degradation of the false alarm probability increases the availability of DRAS by 0.35%.

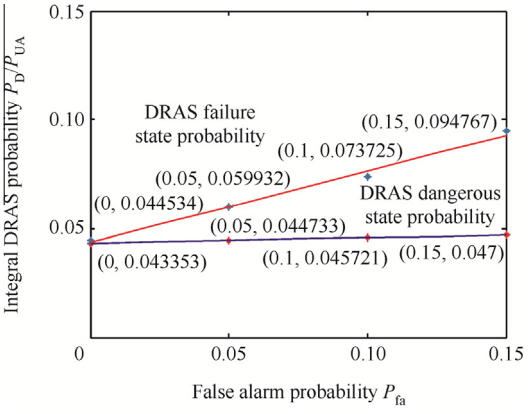


Fig. 14 Relationship between the dangerous state probability, the failure state probability, and the false alarm probability.

From Fig. 14, the relationship between the failure state probability (P_{UA}) of DRAS and the false alarm probability (P_{fa}) can be described as $P_{UA} = 0.3290P_{fa} + 0.0436$, and the relationship between the dangerous state probability (P_D) and the false alarm probability is $P_D = 0.0239P_{fa} + 0.0434$. We can observe that 1% degradation in the false alarm probability decreases the unreliability of DRAS by 0.33% and the probability of a dangerous state of DRAS would decrease by 0.02%.

It is observed from Figs. 13 and 14 that as the false alarm probability is increasing, the misjudgment rate in the working state increases, hence the components cannot be fully used within a life span, so the reliability drops and the failure rate increases. Alternately, the probability of states M_{25} and M_{26} will increase as the false alarm probability increases, thus further leading to a rising possibility of the hazard state.

4. Conclusions

This paper has established a reliability model with GSPN based on the analysis of DRAS architecture and its characteristics.

The paper has presented a study of different system states and transition relations, and discussed the impacts of the monitoring coverage rate and the false alarm rate of failure monitoring devices on system reliability. The major findings are as follows:

(1) The explicit performance degrading processes and fault sequences as well as different redundancy monitoring transition strategies and potential faults have significant effects on DRAS. Reliability modeling for DRAS based on GSPN can clearly describe the dynamic redundancy degradation and state transitions process.
(2) The dissimilar redundant working mode can greatly improve the availability of a large aircraft actuation system compared to a single HAS. In a dissimilar redundancy actuation system, HS/ES and HA/EHA make DRAS experience significant redundancy and performance degradation processes between normal and fault states. The dissimilar system architecture and redundancy transition strategies give better understanding of the reliability advantages of DRAS.
(3) Due to the limitations of FMD in DRAS, there are circumstances when system failure cannot be accurately detected or a well-functioning system is reported with false alarms. If a fault is not detected, the system will be in a potentially hazardous situation. In the DRAS reliability model, as presented, an increase of the monitoring coverage rate and a reduction of the false alarm rate would reduce the probability for the system entering a dangerous state.

Based on the above analysis, it can be concluded that focusing only on redundancy when designing a redundant system is not sufficient and more attention should be paid to improving the failure monitoring devices and designing improved failure monitoring plans. However, this means an increase in the cost of design, so in system design, all comprehensive factors should be taken into account and reasonable design parameters should be selected.

Therefore, when designing a redundancy system, caution should be taken when designing and testing FMD performance. The GSPN model set up in this paper can serve as an accurate reliability assessment for an airplane DRAS, and can also be readily applied in reliability modeling and analysis for other electromechanical systems.

Acknowledgments

This study was supported by the National Basic Research and Development Program of China (No. 2014CB046402), the National Natural Science Foundation of China (No. 51175014), and "111" Program of China.

References

1. Yang J, Huang HZ, Sun R. Reliability analysis of aircraft servo-actuation systems using evidential networks. *Int J Turbo Jet-Engines* 2012;**29**(2):59–68.
2. Wang SP, Tomovic MM, Shi J. Integrated reliability metrics to assess fault tolerant control system. *Proceedings of the IEEE international conference on systems, man and cybernetics;* 2007 Oct 7–10; Montreal, Canada. Piscataway, NJ: IEEE Press; 2007. p. 1310–5.
3. Yao YP, Yang XJ, Li PQ. Dynamic fault tree analysis for digital fly-by-wire flight control system. *15th AIAA/IEEE digital avionics systems conference;* 1996 Oct 27–31. Piscataway, NJ: IEEE Press; 1996. p. 479–84.
4. Zhu XF. Guarantee and implementation of reliability of the hydraulic systems. *Ordnance Ind Autom* 2008;**27**(5):74–6 Chinese.
5. Goupil P. AIRBUS state of the art and practices on FDI and FTC in flight control system. *Control Eng Pract* 2011;**19**(6):524–39.
6. Shi J, Wang SP, Wang K. GSPN-based reliability model of the aircraft hydraulic actuator system. *Acta Aeronaut Astronaut Sin* 2011;**32**(5):920–33 Chinese.
7. Nystrom B, Austrin L, Ankarback N, Nilsson E. Fault tree analysis of an aircraft electric power supply system to electrical actuators. *PMAPS 2006. International conference on probabilistic methods applied to power systems;* 2006 Jun. 11–15; Stockholm, Sweden. Piscataway, NJ: IEEE Press; 2006. p. 1–7.
8. Yang JP, Wen D, Huang HZ, Sun R, Wan H, Sun R. Reliability analysis of aircraft servo-actuation systems based on the evidential networks with imprecise information. *International conference on quality, reliability, risk, maintenance, and safety engineering;* 2011 Jun 17-19; Xi'an, China. Piscataway, NJ: IEEE Press; 2011. p. 187–94.
9. Distefano S, Xing LD. A new approach to modeling the system reliability: dynamic reliability block diagrams. *2006 Reliability and maintainability symposium;* 2006 Jan 23-26; Newport Beach, USA. Piscataway, NJ: IEEE Press; 2006. p. 189–95.
10. Ranjbar AH, Kiani M, Fahimi B. Dynamic Markov model for reliability evaluation of power electronic systems. *2011 International conference on power engineering, energy and electrical drives;* 2011 May 11–13; Malaga, Spain. Piscataway, NJ: IEEE Press; 2011. p. 1–6.
11. Kim K, Park KS. Phased-mission system reliability under Markov environment. *IEEE Trans Reliab* 1994;**43**(2):301–9.
12. Levitin G. The universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliab Eng Syst Saf* 2004;**84**(3):285–92.
13. Lisnianski A, Levitin G. *Multi-state system reliability: assessment, optimization and application*. Singapore: World Scientific Publishing Co Pte Ltd; 2003. p. 283–49.
14. Liu Y, Huang HZ. Reliability and performance assessment for fuzzy multi-state elements. *Proc Inst Mech Eng Part O: J Risk Reliab* 2008;**222**(4):675–86.
15. Shi J, Meng YX, Wang SP, Bian MM, Yan DG. Reliability and safety analysis of redundant vehicle management computer system. *Chin J Aeronaut* 2013;**26**(5):1290–302.
16. Liu TS, Chiou SB. The application of Petri nets to failure analysis. *Reliab Eng Syst Saf* 1997;**57**(2):129–42.
17. Shi J, Wang SP, Shang YX. Petri-nets based availability model of fault-tolerant server system. *2008 IEEE conference on robotics, automation and mechatronics;* 2008 Sep 21-24; Chengdu, China. Piscataway, NJ: IEEE Press; 2008. p. 444–9.
18. Volovoi V. Modeling of system reliability Petri nets with aging tokens. *Reliab Eng Syst Saf* 2004;**84**(2):149–61.
19. Kanoun K, Ortalo-Borrel M. Fault-tolerant system dependability-explicit modeling of hardware and software component interactions. *IEEE Trans Reliab* 2000;**49**(4):363–76.
20. Tao JF, Wang SP, Jiao ZX. Reliability analysis with performance for triple redundant actuator. *J Syst Simul* 2004;**16**(1):38–41.
21. Wang SP, Cui MS, Shi J. Performance degradation and reliability analysis for redundant actuation system. *Chin J Aeronaut* 2005;**18**(4):359–65.
22. Carneiro JS, Ferrarini L. Reliability analysis of power system based on generalized stochastic Petri nets. *Proceedings of the 10th international conference on probabilistic methods applied to power systems;* 2008 May 25–29; Rincon, USA. Piscataway, NJ: IEEE Press; 2008. p. 1–6.

23. DeLong T, Smith DT, Johnson BW. Dependability metrics to assess safety-critical systems. *IEEE Trans Reliab* 2005;**54** (3):498–505.
24. Su C, Shen G. Development for system reliability modeling and simulation based on generalized stochastic Petri net (GSPN). *MIE China* 2007;**36**(9):45–8 [Chinese].
25. Li Q, Wang SP, Shi J, Wang SJ, Jiao ZX. Reliability modeling analysis for hydraulic/electro-hydrostatic dual redundant actuation system. *2014 IEEE Chinese conference on guidance, navigation and control (CGNCC);* 2014 Aug 8–10; Yantai, China. Piscataway, NJ: IEEE Press; 2014. p. 2757–62.

Wang Shaoping received her B.S., M.S., and PhD degrees in mechatronic engineering from Beihang University in 1988, 1991, and 1994, respectively. She is a "Cheung Kong" Chaired Professor in the School of Automation Science and Electrical Engineering at Beihang University. Her main research interests are mechatronics, control, reliability, and fault diagnosis.