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