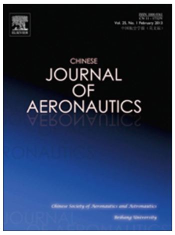
Chinese Journal of Aeronautics, 2013,**26**(2): 363–377

Chinese Society of Aeronautics and Astronautics
& Beihang University

Chinese Journal of Aeronautics

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



Performability analysis of avionics system with multilayer HM/FM using stochastic Petri nets

Wan Jianxiong [a,b], **Xiang Xudong** [a,b], **Bai Xiaoying** [b,c,*], **Lin Chuang** [b],
Kong Xiangzhen [b], **Li Jianxiang** [b]

[a] *School of Computer Science and Communication Engineering, University of Science and Technology, Beijing 100083, China*
[b] *Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*
[c] *Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China*

Received 28 February 2012; revised 18 April 2012; accepted 12 June 2012
Available online 7 March 2013

KEYWORDS

Health monitoring/fault management system;
Integrated modular avionics;
Multilayer;
Performability analysis;
Stochastic Petri nets

Abstract The integrated modular avionics (IMA) architecture is an open standard in avionics industry, in which the number of functionalities implemented by software is greater than ever before. In the IMA architecture, the reliability of the avionics system is highly affected by the software applications. In order to enhance the fault tolerance feature with regard to software application failures, many industrial standards propose a layered health monitoring/fault management (HM/FM) scheme to periodically check the health status of software application processes and recover the malfunctioning software process whenever an error is located. In this paper, we make an analytical study of the HM/FM system for avionics application software. We use the stochastic Petri nets (SPN) to build a formal model of each component and present a method to combine the components together to form a complete system model with respect to three interlayer query strategies. We further investigate the effectiveness of these strategies in an illustrative system.

1. Introduction

The integrated modular avionics (IMA) is an emerging trend in the on-board avionics systems during past decades. It is proposed to address the issue of reducing life cycle cost (LLC), improving the performance of on-board avionics, and facilitating software/hardware updates. Modern military and civil aircrafts like F-22, F-35, Boeing 787 and A-380 are all equipped with IMA systems.

Different from traditional federated avionics systems, which focus on designing a dedicated system for each application, IMA is a highly open system which supports various kinds of avionic applications. The integration of avionics components has the following advantages.[1]

(1) Optimized allocation of spare computing resources. System resources are maintained by the integrator, which can dynamically adjust the resource occupied by each component, adding more flexibility to system resource management.

---

[*] Corresponding author at: Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China. Tel.: +86 10 62772487.
E-mail address: baixy@tsinghua.edu.cn (X. Bai).

Peer review under responsibility of Editorial Committe of CJA.

Production and hosting by Elsevier

1000-9361
http://dx.doi.org/10.1016/j.cja.2013.02.014

(2) Optimized physical equipment weight and power consumption. Dedicated infrastructures are replaced with a general IMA platform which contains a set of common processors, memories, communication channels, etc., resulting in a great reduction of equipment weight and power consumption.
(3) The standardized IMA architecture and interface are widely accepted by the industry, facilitating the development and migration of application.

A main characteristic of the IMA system is the "softwarization" of functional components. Software realization of functional module can improve the resource utilization efficiency and reduce the number of dedicated subsystems. According to a recent report, the software implementation, which has 170 million lines of code and accounts for over 80% of all functional components in the F-22 military flight, has now surged to 800 million lines in the F-35 military flight. The maintenance of the software stability and reliability is the crux to the on-board system management.

Health monitoring/fault management (HM/FM) is introduced in the IMA environment to ensure that the system can still behave well in the presence of software faults.[2] The health monitoring module is responsible for identifying, locating, and reporting the failure of one or more system elements. The fault management module is then activated to take appropriate behavior to conduct trouble-shooting works. Extensive research efforts have contributed to the state-of-the-art HM/FM techniques.[3–5]

Modern avionics systems generally adopt a layered architecture which provides the abstraction necessary to minimize the effect of system changes on user application.[6] IMA with a layered architecture has been advocated by the industry.[6,7] However, to the best of our knowledge, there is no quantified performance analysis of the HM/FM module in a layered IMA environment. We believe this work is of great significance in the sense that it can provide useful information on how to design the HM/FM scheme as well as how to set system parameters to build a cost-effective system.

In this paper, we evaluate the effectiveness of the layered HM/FM scheme in the IMA environment using stochastic Petri nets (SPN). Compared with traditional "lower level" modeling tools like Markov chains (MC) or queueing theory, stochastic Petri nets has the following advantages:

(1) To build a comprehensive model of a complex system is a difficult task, and often results in a huge model which is hard to understand and debug. By using SPN, we could use a "divide and conquer" approach to model the system, i.e., first divide the system into several components, and then establish the sub SPN models for each component, and finally combine sub SPN models together to create an integrated model.
(2) The way sub models are connected reflects the system architecture and behavior, which can be easily expressed by guard functions in the transitions and arches connecting sub models (Such information is usually hard to model using MC). We can then perform comparison studies of the impacts from various architectures and behavior without major changes to the original model.

There are mainly three contributions in this paper, namely:

(1) We build a scalable SPN model for the layered HM/FM. We present SPN sub models for each component separately and propose three monitoring strategies. We give the way to concatenate SPN sub models together to construct a complete model which realizes three strategies. The performance of HM/FM system may be affected by two major factors. (a) Parameters configuration, such as the inter-monitoring time. (b) Time variant factors, e.g., the performance of functional components degrades with time and cannot be renovated. In our SPN model, however, we regard the system as time-invariant and overlook the time-variant factors.
(2) The state space of the Markov chain underlying the complete SPN model grows exponentially with the number of monitored objects, which makes the model intractable for practical systems. Therefore we use time scale decomposition (TSD) technique to design a general method to approximately solve our SPN model.
(3) We conduct a numerical analysis of an illustrative system, which is a prototype system in Allied Standards Avionics Architecture Council (ASAAC) standard of the North Atlantic Treaty Organization (NATO).[8] The results shed light on the design of a cost-effective HM/FM scheme. We show that in our illustrative system, the subordinate layer query blocking time nearly coincides for the subordinate layer query with subordinate layer FM activation (SQSF) scheme and the Subordinate layer query with current layer FM activation (SQCF) scheme. Further, the no subordinate layer query (NSQ) scheme has the worst performance, and the SQCF scheme is generally better than the SQSF scheme. We finally discuss some designing principles for a practical system.

The paper proceeds as follows. Section 2 gives a brief overview of the multilayer HM/FM system of our consideration; Section 3 presents SPN sub models for each component, as well as the method of combining sub models into a complete model with regard to three inter layer query strategies; Section 4 discusses the definition of performance metrics and TSD technique to approximately solve the model; Section 5 conducts a detailed evaluation of the HM/FM system in an illustrative system; Section 6 concludes the paper.

2. Multilayer HM/FM system

2.1. System architecture

The overall layered HM/FM system architecture is shown in Fig. 1. This system is running on a partitioned real-time operation system, typically hosted in an on-board hardware. The health monitoring modules take charge of monitoring all objects periodically.

When an error is found, the health monitoring module will notify a fault management module, which deals with the error.

(1) Health monitoring mechanism. The HM module monitors the health status of objects in real time, which must perform the following tasks. (a) Periodically check the health status of objects by sending an *ARE_YOU_ALIVE*