A Discussion of Dynamic Configuration Technology of Highly Complex System in Information Era

Zeyong Jiang, Tingdi Zhao, Fuchun Ren and Nuo Zhao

ABSTRACT

Current highly integrated and complex system will cause huge property losses and casualties, if security accident occurs. Dynamic reconfiguration technology has become a practical and effective solution to ensure safety operation of complex system through reconfiguration after a fault occurs in system. However, dynamic reconfiguration technology provides new ideas and methods for security of complex system; meanwhile, it also brings the issues that system behavior tends to be more complex, so that it is difficult to implement effective and credible analysis and evaluation. Therefore, this paper makes a brief discussion of current status of dynamic configuration system as well as the issues, and some corresponding advices are also recommended.

INTRODUCTION

Modern systems are developing in the direction of large-scale, highly integration and complexity. There are typical representatives of modern complex large scale systems, such as large transport aircraft, satellite constellation, nuclear facilities control and high speed railway in recent years. Such systems are related to the people's livelihood, and once the security accident occurs, it will probably cause huge property losses and casualties. In order to guarantee the safe operation of complex system and to ensure that after a system fault, it can still function well through reconfiguration.
Therefore, dynamic reconfiguration technology has become a practical and effective solution. At present, system reconfiguration technology has been gradually applied in the field of control, information transmission and other critical safety, such as the Boeing 787 flight control system, advanced integrated avionics system, the third generation of the United States GPS constellation navigation system.

At present, as for complex system such as aircraft integrated avionics and flight control system, under premise of the effective protection of key system reliability, once system encounters a fault to trigger dynamic reconfiguration strategies, complex dynamic reconfiguration system performance of complex fault logic behavior, fault correlation logic chaos, fuzzy safety mechanism, system state management and reconstruction of complex problems caused by dynamic process characteristics, will seriously restrict the safe application of dynamic system reconfiguration. Therefore, dynamic reconfiguration technology provides new ideas and new approaches for security of complex systems, but it also brings the issues that system behavior tends to be more complex, so that it is difficult to implement effective and credible analysis and evaluation. The security analysis and evaluation technology of dynamic reconfiguration system has become one of the important issues in the development of complex systems.

In this paper, we want to make a brief discussion of current status of reconfiguration technology in complex systems, and attempt to figure out some shortages with corresponding advices. The rest of this paper is organized as follows. Section 2 presents an overview of research status of dynamic reconfiguration systems. Current problems are discussed from three aspects in Section 3. And then some advices are given in Section 4. Finally, a conclusion of the paper is provided in Section 5.

RESEARCH STATUS

Status out of China

Dynamic reconfiguration system is a typical form of fault tolerance mechanism, in order to ensure the critical safety systems, such as flight control systems, avionics system still can take some control actions to guarantee the safe operation mechanism of the system after a fault is encountered. Therefore, dynamic reconfiguration technology has become an effective approach to improve the reliability and security of dynamic systems.

At present, in the field of aviation, the research of dynamic reconfiguration technology mainly focus on the technology of flight control system, avionics system and UAV control. The fault tolerant flight control technology, especially the active fault tolerant control technology has been widely used and rapidly developed accompanied by a FBW flight control system. The dynamic reconfiguration flight control system is the advanced development direction of fault tolerant flight control system. In 1982, the United States National Aeronautics and Space Administration (NASA) first proposed reconfigurable flight control system concept, and the United States Air Force Flight Dynamics Laboratory in 1984 carried out reconfigurable flight control system research program. From then on, the research of the key technology of reconfigurable flight control system, reliability and system design, implementation and
validation of flight is beginning [1]. Based on this research, American Grumman
designed control fighter reconstruction [2], especially considering the development
inherent redundancy of aircraft control structure, aiming to make the aircraft
performance insensitive to a single control surface in order to eliminate the critical
flight control surfaces [3]. Since the 1990s, with the development of computer
technology and key technology of reconfigurable flight control system, reconfigurable
control system design gradually tends to develop in the direction of adaptive control.
Reconfigurable flight control system (RFCS) effectively solved the problems of the
reliability and Maintainability (R&M: reliability and Maintainability) in flight control
system and improved survival and reduced hardware redundancy and life cycle cost
(LCC). From May to July, 1996, the United States Air Force conduct a series of flight
tests, using 5 VISTAIF-16 test aircraft, flying nearly 1 hour, to verify a new direct
adaptive reconfiguration controller method called Self-Designing controller (SDC:).
Meanwhile, the United States launched the "flight system reconfiguration of tailless
aircraft and adaptive research plan", with the purpose of developing a reconfigurable
adaptive flight control system of tailless stealth aircraft after 2000[4].

In the field of civil aviation, integrated modular avionics system (IMA) is an
important direction of the large aircraft avionics system development. Integrated
technology of avionics system improved system effectiveness and efficiency
effectively, and both A380 of the European Airbus Company, and B787 of the United
States Boeing, treat aviation electronic system integration technology as core of key
technologies [5]. In integrated avionics system, all functions are based on the system
management to provide support for the mission.

Status in China

In the past decade in China, many researches on reconfiguration systems have
been carried out. Chinese universities and research institutes have also carried out
relevant research, such as Beihang University, National University of Defense
Technology, Nanjing University of Aeronautics and Astronautics, Air Force
Engineering University, Institute of Standardization of Chinese Space, Institute of
Aeronautical Technology of China. Since the 9th Five-Year Plan, Beihang University
has carried out many studies on complex system safety and reconfiguration. So far,
many projects have been undertaken, for example, "Safety Analysis and Assessment
Technology for System Operation" and "Aircraft Fail-safe Analysis and Verification
Technology" for pre-research project, "Integrated Safety Analysis and Design
Technology" and "Research on Resource Integration Safety of Integrated System" for
National Basic Research Program of China (973 Program), "Research on Accident
Rehearsal and Early Warning Technology for Civil Aircraft" for National High
Technology Research and Development Program of China (863 Program) etc. With
years of efforts, many breakthroughs about safety analysis and evaluation technologies
of configuration systems have been made, such as "Multi-dimension Safe-state Space
Theory", "Probability-Consequence-Time Three-dimension Risk Assessment Model",
"Multi-factor Accident Rehearsal Modeling and Analysis Technology", "Multi-view
Hazard Analysis Method" etc.
DISCUSSION OF CURRENT ISSUE

Complex Fault Logic Behavior and Dynamic Process Characteristics

Complexity of logical interaction relation, could lead to the problem of fault propagation or operation inheritances, once a fault occurs in the system. And many aspects of the subject involved in reconfiguration process requires task space for demand, system function space for protection and system resource space as the core of operation. However, due to the huge state space and logic space of system, complicacy of mutual relationship, it is difficult to guarantee the completeness and certainty of conversion process from the task space to feature space and finally to the resource space, resulting in system eventually exceeding security state space of system, and in violation of the security constraints, which makes it difficult to ensure safety and effective operation of system.

System Status Management and Reconstruction of Complexity

Illustrated by the example of typical integrated avionics system, when the hardware fault occurs in the system and the system of configuration management is needed through comprehensive management, i.e. function application is reconfigured to modules of normal operation, in order to achieve the sustained operation of the system task. However, with the increase of comprehensive depth in integrated avionics system, the content that each function is responsible for increases and the supporting object that resources of the components involved in increases, resulting in substantial growth in the state space of the system, and complexity of relationship between function and resource. Therefore it is more difficult and complex to implement system management work.

Security Analysis and Evaluation Technology of Dynamic Reconfiguration Process

Current research on dynamic reconfiguration technology and dynamic reconfiguration system safety and reliability analysis and evaluation research mainly concentrate on reconfiguration strategies, methods, and the field of the safety assessment system based on system function mechanism and the safety and reliability modeling form research, respectively. There are few researches on the characteristics of the evolution in the dynamic reconfiguration process and the related issues about security risk, and systematic and explicit behavior process characteristics, safety mechanism and related technical system of configuration system, are not formed. This also leads to the fact that the current dynamic reconfiguration technology is still faced with many uncertain factors in the application of various types of complex large systems. Therefore, dynamic reconfiguration system cannot fully have an important effect.
ADVICE AND SUBSEQUENT WORK

Based on the Theory of System Security and Technology

Since the end of the last century, the rapid development of strategic weapons, space shuttle and nuclear industry have further promoted the complexity of the system. In research, development and design, the internal problems of each unit and system should be considered, and, relation state of each other increases the potential safety hazard, which makes the system idea based on the concept of security gradually rise. Nancy G. Levenson from MIT carried out the complex system safety research and proposed a new safety theory STAMP (Systems Theoretic material model and processes) where safety is considered as a control problem[6][7]. Hollnagel Eric in 2004 proposed the functional resonance analysis model (FRAM) [8] applying functional resonance theory as the basic principle. Safety analysis theory and technology based on the view of system stress that system engineering thought should research from the overall system situation, instead of the traditional security theory and method which consider traditional hazard as the core and consider the form of "chain of events" as representative, and attach importance to the system unit interaction logic relationship and consider behavior process deviation about safety influence, expanding the understanding of the essence of system security.

The Demand for the Development of Safety Airworthiness

For civil aviation aircraft, It is crucial to ensure safety of system and standard of airworthiness is the minimum safety standard for civil aviation products. At present, due to the fact that dynamic reconfiguration system still exist potential fault logic complexity, and security effect mechanism is still fuzzy, Federal Aviation Administration (FAA) and other airworthiness certification mechanism have not yet solved the issue of dynamic reconfigurable system validation, and there is no corresponding terms in airworthiness regulations to guide the validation work of dynamic reconfiguration system, resulting in the fact that dynamic reconfiguration system is not applied in civil aircraft, and also directly restricting the development of the dynamic reconfiguration system in the field of civil aviation. Therefore, it is related to the future development of civil aviation in China to implement the basic research of airworthiness.

Systematic Security Development Concept of Treating Information as Core and Considering Logic as Carrier

In current information era, software, electronic products account for higher proportion in system, traditional complex system treating hardware platform as core is transferring into systematic complex system considering information as core. Correspondingly, traditional reliability and security concept based on hardware faults has been unable to solve the various issues of current electronic, software and integrated products. Therefore, in the background of establishment of various systems treating information as core and considering logic relationship as carrier, systematic security concept which transfer from physics factors to logic factors should be
concentrated on, which helps engineering and technical personnel to understand and design more safety and effective system products.

CONCLUSION

In conclusion, in the information and systematized era of the 21th century, complex dynamic configuration system is facing distinct challenges in contrast with the past. Engineering and technical personnel with systematic security concept of transferring physics level to operation logic level could have better understanding and design system products with higher safety and efficiency.

REFERENCES