Research on the Safety Mechanism of Complex System Dynamic Reconfiguration Process

Fuchun Ren, Nuo Zhao, Tingdi Zhao and Zeyong Jiang

ABSTRACT

On the premise of ensuring reliable and successful operation of modern safety-critical system, dynamic reconfiguration technology is often needed for the expected or unexpected malfunction. However, with the progress of integration and informatization extent in modern systems, the emerging complicated behavior and dynamic feature of dynamic reconfiguration process also brings some challenges for the application work. To promote the effective embedding of dynamic reconfiguration strategy, the safety mechanism of reconfiguration process is discussed in this paper, while some advises are finally provided based on the state of art of safety theory and technology.

INTRODUCTION

Modern systems represented by large aircraft, satellite constellation and high speed railway are becoming more large-scaled, complex and integrated. To ensure that the systems can still operate safely and effectively after some malfunctions, dynamic reconfiguration technology is often needed to be embedded in the development stage.

From the technology perspective, dynamic reconfiguration can be abstracted into two categories, fault detect and isolation based and online learning based. Various kinds of technology, such as linear quadratic, pseudo-inverse/control mixer, adaptive control/model following, feedback linearization or dynamic inversion, neural network and fuzzy theory are tried in the research and development of dynamic reconfiguration system [1-3].

Fuchun Ren, Tingdi Zhao, Zeyong Jiang. School of Reliability and Systems Engineering, Beihang University, Beijing, China
Nuo Zhao. China Shipbuilding Information Center, Beijing, China
Now in the aerospace domain, dynamic reconfiguration technology is mainly adopted in the flight control system, avionics system. The concept of reconfiguration flight control system was firstly proposed by NASA in 1982. And since 1984 the flight dynamics laboratory of U.S. Air Force has conducted the research on the key reconfiguration technologies including design, development and verification. From 1989 to 1990, 25 times of test flight were carried out to verify the pseudo-inverse based reconfiguration control system [4].

After 1990s, self-adaptive control came to be a new development direction while in 1996 five flight test vehicles were invested by U.S. Air Force to verify a new kind of Self-Designing Controller. Meanwhile, a project for reconfigurable and adaptive flight control system was proposed for the future tailless stealth aircraft, such as R-50 and X-33 [5][6].

In the field of avionics, Integrated Modular Avionics (IMA) is the novel concept of avionics architecture. Currently, IMA has been widely used in aviation domain varying from civil large aircrafts like A380, B787 to military jets like F22, F35. However, in spite of the potential benefits of dynamic reconfiguration technology, with the increasing extent of integration and complex interaction, the dynamic reconfiguration design is facing a verification problem of consistence and integrity, meanwhile the complicated behavior and dynamic feature of dynamic reconfiguration also brings some problems in the application process. To our knowledge, most of the dynamic reconfiguration studies are focusing on the reconfiguration strategy or method [7][8], while the evolution feature and safety mechanism in the dynamic reconfiguration process are rarely discussed, making the real-time online dynamic reconfiguration strategy hard to carry out.

Starting from the behavior characteristics of dynamic reconfiguration process and the principle of system science, this paper makes a study on the behavior feature of dynamic reconfiguration. Three kinds of behavior features are concluded i.e. subject evolution characteristic of dynamic reconfiguration process; logic complexity characteristic of risk mechanism; temporal evolution characteristic of risk. Then to provide a comprehensive solution guidance, some enlightenments coming from the modern safety theory and technology are given. This work tends to provide a fundamental support to the development and application of dynamic configuration and promote the safety-related work in complex system development.

DISCUSSION ON THE BEHAVIOR FEATURE OF DYNAMIC RECONFIGURATION PROCESS

To promote the effective embedding of dynamic reconfiguration strategy, safety mechanism of the reconfiguration should be clear enough. In the process of dynamic reconfiguration, we need to know what is the key elements contributing the risk of reconfiguration process. So in this part, we make a study on the behavior feature of dynamic reconfiguration. Three kinds of behavior features are concluded i.e. subject evolution of dynamic reconfiguration process; logic complexity of risk mechanism; temporal evolution of risk.
Subject Evolution of Dynamic Reconfiguration Process

Different from the physical redundancy technology, dynamic reconfiguration technology is based on the design of function margin. System function-task should be safeguarded in the whole cycle of system operation. And the dynamic reconfiguration process is usually involved with a reconfiguration of multiple related units or modules in complex systems, namely the subject evolution process in dynamic reconfiguration.

Figure 1. Hierarchical structure of integrated avionics.

Here we take an IMA example (see Figure 1) which has a hierarchical structure i.e. task level, function level, and resource level. Since failure is originated from the resource level, the reconfiguration subjects would also be the resources. In result the resource level will be changed, but the function-task level should remain in the former safe operation space. In another word, the validity and completeness of function-task level which make sense to the safety of reconfiguration should be ensured.
Logic Complexity of Risk Mechanism

In the dynamic reconfiguration system, association relationships exist between tasks and functions due to resource sharing and function interaction while a failure of shared resource would influence all the associated tasks and functions.

An IMA example is given in Figure 2, association relationships exist within Integrated Processing Module (IPM)—function A and B share the Integrated Processor of IPM A while function C and D share the Integrated Processor of IPM B [9]. This kind of association brings the logic complexity of risk mechanism since a tiny fault may trigger a very big accident. In contrast with the static view of system architecture, the dynamic interaction and coupling logic of multiple behavior elements makes the system risk mechanism more complicated and deserves a detailed study to recognize the fault association relationships and decompose the logic complexity.

Temporal Evolution of Risk

The sequence characteristic of system reconfiguration will impact the validity and safety of reconfiguration process, while the risk in subject evolution process is the key issue for a successful and safe operation.

Due to the logic complexity and system evolution, risk may have a sequence spreading impact as the fault may spread within the system, for example (see Figure 3), resource 1 fails first and consequently it spreads to operating process 2 and resource 2, then function 2, function 4, operating process 3 and resource 3, ultimately the whole system would get impacted if there were no fault management mechanism.
So, recognizing the fault spread and risk migrating trajectory in the system temporal evolution process and conducting a comprehensive risk management work will improve the safety state of reconfiguration system.

ENLIGHENMENTS FROM MODERN SAFETY THEORY AND TECHNOLOGY

System-theory Based Safety Theory and Technology

In the past few decades, the increased task and function requirements of strategic arms, shuttle and nuclear industry etc. arises the complexity of modern systems. In the design stage of modern systems, the interactive issues among units are becoming the new problems to deal with despite of the inner issues of them, and the system-theory based safety science has become prevalent.

In 2004, Nancy Leveson proposed the Systems-Theoretic Accident Model and Processes i.e. STAMP from the perspective of control theory [10]. Safety is viewed as an emergent feature rather than a component reliability problem under specific system condition and accidents would arise from complex interactions that are not adequately controlled. In the same year, Eric Hollnagel proposed the Functional Resonance Analysis Method i.e. FRAM focusing on the interactions and emergence phenomena in socio-technical systems [11], and revealed that accidents would occur if the vibrations in socio-technical systems overtake the margin or the interactions promote a functional resonance among the system functional logic hierarchies.

Different from the traditional safety theory and technology represented by hazard based and event-chain like methods, the system-theory based safety theory and technology emphasizes a Systems Engineering (SE) based global view for system...
safety. Interactive issues and deviations in system behavior are considered, so the system-theory based safety theory and technology would promote the study and revolution of safety risk problems in complex system dynamic reconfiguration process.

**Information-focused and Logic-subjected System Safety Theory**

In the information era, the proportion of software and electronic products in the system has increased, making a center transfer of the complex systems from hardware platform to information and data space [12]. Correspondingly, traditional hardware failure based reliability and safety theory can no longer address the challenges of modern integrated informational system.

Taking the accident example of “US F15 mistakenly hit “Black Hawk” helicopter in 1994”, if we make an accident analysis from the deep, we would find that it is a typical safety accident due to Systems of System (SoS) complexity, which may be called a lack of “logical completeness”. Many logical defects led to the accident together, including coordination mechanism defects of “information sharing and interaction” between US Air Force and Army, matching defects between the Black Hawk “IFF system” pattern and “communication system”, the lack of surveillance and management for Army helicopter in AWACS mission etc. Another example, the Yong-Wen high-speed rail accident on July 23th 2011 is a typical accident that was caused by the coupling of tiny logic incidents, such as the lightning damage to equipment, communication fault and the monitor screen failure.

So under the progress of integration and informatization extent in modern systems, the information-focused and logic-subjected system safety theory would help engineers achieve a better understanding and design of system products.

**CONCLUSION**

Dynamic reconfiguration technology is a potential effective way to ensure a sustained safe and successful system operation after malfunctions. However, the evolution feature and safety mechanism in the dynamic reconfiguration process are not clear enough now, making the real-time online dynamic reconfiguration strategy hard to carry out. Behavior features including subject evolution of dynamic reconfiguration process, logic complexity of risk mechanism and temporal evolution of risk which are challenging the application of dynamic reconfiguration are discussed in this paper to provide a comprehensive understanding of the safety mechanism in dynamic reconfiguration. Modern safety theory represented by system-theory based safety theory, information-focused and logic-subjected system safety theory would provide enlightenments for safety work in the effective application of dynamic reconfiguration.

**REFERENCES**