Research on the Key Technologies of Avionics Communication System

Haili Sun [1]

[1] Xi'an Railway Vocational & Technical Institute, Xi'an, Shaanxi, 710014

KEYWORDS: Key Technologies; Avionics Communication System; Technology Development

ABSTRACT: Avionics system presents a comprehensive, modular, network and other trends, with a high degree of resource sharing, data integration and software, highly intensive and so on. Integrated avionics system to ensure a high degree of information sharing, enhance the efficiency of aircraft task execution while facing severe network and information security challenges. Integrated avionics system is not only to prevent the invasion of traditional information security, but also to be able to respond to emergencies, with the ability of active defense. In this paper, avionics systems and aircraft of their own characteristics collaborative networking scene, research integrated avionics system dependability safeguard key technologies.

Introduction

Software features onboard software occupies an important position in the IAS, the implementation of each task aircraft need the help of the onboard software to complete. IAS onboard software brings changes in the following areas: software highly concentrated: the concept of sub-carrier turn evolves into software, software running on a single hardware platform, called integrated area. High-speed parallel processing: Each region consists of a comprehensive set of ultra-large-scale performance computer cluster, whose treatment capacity will reach ten trillion times / sec, and each replaceable processor module LRM (Line Replaceable Module) on the maximum processing capacity get up to 100 million times sec or more, thus requiring on-board software must adapt to the rapid concurrent processing. Software reusability, portability needs enhancement: expansion by a combination of software due to the confluence of a large amount of software and increases the complexity of the software, reduces the reliability of the software, thus affecting the software reusability and portability.

Mission-critical levels and security issues: different levels of tasks share a unified hardware platform, managed by the operating authority of the onboard software to bear, how to effectively prevent errors affect critical low-level mission to produce high-level tasks, and to ensure lawful authority, control over resources, protect the security of information between the tasks and the prevention of the spread of the fault is a new problem caused by functional integration. Deterministic resource use: after data fusion, system resources are no longer private, and shared by multiple tasks, task execution order, the running time and resources required must be arranged in advance, to ensure reliable operation of the IAS, and will not appear needed Resource depletion. Software engineering: Integrated Avionics Software Engineering proposed the concept of a unified operating platform and supports a unified platform to reduce the load mainframe software development and maintenance costs, and enhance the reliability of onboard software. Compared to the previous three generations of avionics systems, the performance indicators IAS have been greatly improved, but the rapid growth of software size reduced reliability, a high degree of shared system resources to make the system more vulnerable to malicious destruction program.

Further development of the structure of the IAS, makes a lot of open components are applied to come as possible, which avoids the inflexibility of dedicated components to some extent, but also affect the security of the system. The open architecture of system performance can be achieved, such as the use of COTS and standard electronic module SEM (Standard Electronic Modular) application platform, is conducive to upgrading technology and components, but also conducive to the expansion of the system with a lower life-cycle costs and upgraded to support scalable systems to reduce system development cost and development cycle. However, the openness of the system also improves the security requirements of the system.

Key Technical Analysis of Avionics Systems

The physical structure of the communication network of interconnected subsystems, called the topology of the communication network. Current common communication network topology includes a single bus topology, a plurality of single-stage and multi-level bus topology bus topology. These three communications network topology not only have a solid theoretical foundation, but also has been proven. All communications subsystem avionics systems are directly connected to the same bus cable 1553B, constitute a single bus topology. This form of simple topologies, traffic at lower avionics communications system, subsystem, or less, may be employed. And avionics communications systems business volume, and more subsystems, a single bus topology can not meet the requirements. Avionics subsystems communication system reasonable classification, and are connected to a plurality of 1553B bus, which constitute more than single-stage bus topology. Assuming that the above plurality of bus is not at the same level, it is a multi-level bus topology. In a multi-level bus topology, a subordinate bus needs to receive and execute control instructions issued by the higher bus. This topology is more complex communication network, adapted to process a variety of functional units, a larger amount of communication traffic avionics communications network.

1553B bus technology supports both static and dynamic bus control program. Static bus control program uses centralized control mode, relying on a fixed bus controller, to achieve the 1553B bus data and information management. This communication control simple control scheme, hardware and software devices are easy to configure for fault detection system is also convenient and accurate, but the single point of failure is likely to cause paralysis of the entire avionics communication system. Dynamic bus control program distributed more bus controllers on 1553B bus, the same time there is only one data bus controller is authorized to manage information on the bus. Control of the bus cycle may be time division or transfer of the way between the bus controller handover. Dynamic bus control scheme is highly reliable, and easy to reconstruct, but it is relatively complex communication control a lot, fault detection more difficult. In addition, the appropriate hardware and software facilities are also more difficult to configure.

Synchronous communications system designed avionics subsystems possess an independent timing clock and multiple clock timing error phenomenon is more common. However, avionics communications systems are for real-time transmission of information has a high demand. This requires the establishment avionics clock synchronization mechanism, providing a unified time for the entire avionics communications systems, subsystems and keep time consistently throughout the flight. It works avionics clock synchronization mechanism for each subsystem configuration bus and an identical length and resolution of real-time clock timer, and after avionics communication system is powered on, automatically begins counting. Avionics bus controller periodically send the bus in real time the timer value to each subsystem, through error timer value and compare your bus

timer value between their system time correction, thereby effecting the entire avionics communication system clock synchronization.

Processing avionics communication system failures can be divided due to the interference and other factors appear accidental temporary failures and system hardware failure caused by a permanent fault. When avionics communication system fails, the bus controller will first according to the system requirements, the dual redundant cables finite retry processing. Suppose the fault disappears, it can be diagnosed hitch system; otherwise, the bus controller determines that the fault is permanent fault and creates files recorded. Meanwhile, the bus controller subsystem will fail under the net, and periodically queries. No bus controller subsystem failure, depending on the type of fault with the status word subsystems flag is a flag which terminal is disabled MBI three treatments and ways.

IAS in the development and improvement process, the security issue has been wide concern. As traditional architecture avionics system and rely mainly on firewall, intrusion detection, virus prevention, redundancy or the like based on historical data to predict the occurrence of events and ultimately achieve the system security. But for credible integrated avionics architecture, the traditional idea of passive defense in this has its limitations, we must adopt a new active defense thinking. In recent decades developed and widely adopted in other areas of trusted computing technology avionics system security provides a strong foundation. This chapter avionics architecture based on trusted the previous chapter, given the technical security of the system under, including key management based on trusted computing technology, multi-level security policy and access control technology.

IAS, a large number of computing, communications, control service and a variety of security classification of data processing code running on the same platform, with a high rate of resource sharing, which improve system resource utilization, but also brought some security problems, so widely used in avionics data / message encryption, authentication, message authentication and other technologies. Since the system uses a key, there must be a key management issue. For example, how to distribute real-time applications and services key; how safe and controlled implementation of key migration system reconstruction; by how promptly erased when security is threatened key system to prevent leakage of critical resources.

In IAS, the multi-level security MLS (Multi-Level Security) according to the sensitivity of the information is divided into different levels of security to prevent security classification of information leaked to the high security low security classification level entity. At present, many use the BLP model in integrated avionics system. BLP model is a computer simulation of military security policy multi-level security model, is typical of the confidentiality of information Multi-level security model, mainly used in military systems, its core idea is to define the direction of flow of information to ensure the confidentiality of the information. It is a static management model, security level model in the main object can not be modified. However, IAS, based on the nature of zoning changes so often based on tasks performed in the main level of security, object. Since the TCG specification primarily for embedded systems, such information is not multi-level security presence avionics system, and did not give a credible multi-level security policy. Multi-level security rules usually allow traffic low security level of information flow to the high level of security partitions, but definitely not in the opposite direction of the flow of information appears. This is too strict for the purposes of the actual system and the lack of flexibility, a lot of classified information does not always flow from top to bottom, such as the main medium should be allowed to read confidential trust less dense object, write a higher security classification of the object, but it can not read a higher security classification of objects, and also do not trust the read

secret information leaked to the low security classification of the object. In a multi-level security, often by default all subjects are not to be trusted. In some systems, in order to take into account of the confidentiality and integrity requirements, we make simply the BLP model and the Biba model. Together, at the same time we look forward to implementation of the system of rules on confidentiality and integrity rules, because at the same time limited by the rules of the process leading to impossible to access any data. Typically, multi-level security level of security is a security sensitivity level, and credible vary, but in practice the two systems are there, and can not replace each other.

Based on credible multi-level security policy to the confidentiality and integrity of information coming in comprehensive and incorporate trusted subject to an access control policy to ensure the security of information. Based access control framework for trusted computing technologies and the implementation method, by means of credible reference monitors provide reliable support for the aircraft avionics systems and network information security access control. Avionics systems for these security technologies under the system provided credible technical support.

Conclusion

Avionics communication system is a complex distributed real-time airborne communications network, involving all electronic devices on the multiplex transmission bus avionics, its top-level design of a direct impact on the performance of the aircraft. Said avionics communication system hierarchy, network topology, the communication control programs, avionics and communication design clock synchronization troubleshooting, etc are the key technical problems avionics communication system proposed in this paper and the Airborne Solutions ACT bus communication network design flight control system for avionics designers and implementers to make specific reference.

Reference:

[1] Xiaorui Wang et al., Control-Based Adaptive Middleware for Real-Time Image Transmission over Bandwidth-Constrained Networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2008,19(6):779-793.

[2] Tei Weikuo, Wang Ruyang, Kwei Jaylin. A class of rate-based real-time scheduling algorithms [J], IEEE Transactions on Computers, 2002,51(6):708-720.

[3] Richard L. Alena, John P. Ossenfort IV, Kenneth I. Laws. Communications for Integrated Modular Avionics. Aerospace Conference, 2007 IEEE. 3-10 March 2007: 1-18.

[4] J. Rushby, B. Randell. A distributed secure system. IEEE Computer, vol. 16, no. 7, pp. 55–67, 1983.