Design of Airborne Distributed Double Residual Electromechanical Integrated Management System

Kui Chen[a], Jiansheng Wang, Mingliang Hu, Yongguo Wang

Xi'an Aeronautics Computing Technique Research Institute, AVIC, Xi'an, China

[a]282937376@qq.com

Keywords: sDual-redundancy distributed electromechanical system; System fault-tolerant technology; System reconfiguration; Exception handing

Abstract: The Advancement and reliability of the electromechanical system will directly affects the performance of the aircraft, since it is an important part of the aircraft systems. With the sharply increasing of the mount of date and the integration degree of electromechanical system, It is necessary to develop a distributed dual-redundancy electromechanical system which have characteristics of high-speed avionics bus, the ability to detect and reconstruct malfunction. This paper makes a research on the design of distributed dual-redundancy electromechanical system which uses the fault-tolerant technology, system reconfiguration technology and high-speed avionics bus technology, and the composition of the system, working principle, fault tolerance and reconfiguration mechanism, as well as exception handling are mainly discussed. At present, this technology has been successfully used in certain key research projects in our country.

1. Introduction

The aircraft electromechanical system is an important part of the aircraft, and its performance and reliability directly affect the performance and reliability of the aircraft. With the development of the system, the current electromechanical system integrates the power supply subsystem, the power unit subsystem, the hydraulic and pneumatic subsystem, the ice protection subsystem, the fire protection subsystem, the brake subsystem, the landing gear subsystem, the fuel subsystem, etc. There are serious functional overlaps and redundancy in the dedicated controllers of these subsystems, which makes the number of on-board products and the weight of the on-board cables high, and is not conducive to comprehensive control and information fusion within the system, making the electromechanical system further The overall situation is difficult. Therefore, it is necessary to organize and summarize the dedicated controller resources in the electromechanical system, reduce the number of on-board products and the weight of the on-board cable, realize data sharing in the electromechanical system, improve the comprehensive management level of the electromechanical system, and further improve the system reliability. And security, increase system fault tolerance, and realize system fault reconstruction, so as to achieve optimal control management and further integration in the electromechanical system. The use of a distributed dual redundancy system is a more suitable solution.

By adopting a distributed double-duty electromechanical system, the number of products inside the electromechanical system and the total amount of on-board cables can be greatly reduced, and the automatic control of key execution components can be realized at the same time, thereby greatly improving the performance of the electromechanical system, improving the performance of the aircraft platform, and improving Reliability and safety of electromechanical systems. This paper studies the fault-tolerant technology, system reconstruction technology and high-speed aviation bus technology of distributed double-required electromechanical system, which provides a technical platform for the subsequent comprehensive integration of electromechanical systems. Through the application of this technology in electromechanical systems, it fills the domestic on-board The blanks on the advanced electromechanical systems have laid a solid foundation for the development of aircraft platform-level integrated systems.

  DOI: 10.25236/mmmce.2019.153

2. Distributed dual redundancy electromechanical system structure

In this system, it consists of a dual redundancy electromechanical management computer and a configurable number of dual redundancy remote interface units. As the computing and control center for electromechanical systems, UMC collects data collected by all remote interface units through two high-speed aeronautical bus networks.

The internal and external information of the electromechanical is analyzed and comprehensively processed, and the final result is reported to the upper computer. As shown in Figure 1, the electromechanical management computer and the remote interface unit exchange information through a high-speed, intelligent 1394B bus network. The electromechanical management computer completes the integrated processing of the electromechanical system information, and the remote interface unit completes the electromechanical data acquisition, electromechanical actuator drive, and electromechanical data. Upload.

3. Distributed dual redundancy electromechanical system works

In a distributed dual redundancy electromechanical system. The electromechanical management computer and the remote interface unit are double redundant architecture. The A channel of the electromechanical management computer and the A channel of the remote interface unit form a bus network to complete the information exchange; the B channel of the electromechanical management computer and the B channel of the remote interface unit Another bus network completes the information exchange; sets a high-speed cross data link between the A and B channels inside the electromechanical management computer, and realizes data between the two independent electromechanical network data in the A and B channels inside the electromechanical management computer. Sharing; two bus networks work simultaneously. The remote interface unit adopts a unified software and hardware platform, automatically loads the table driver inside the remote interface unit according to different position signals on the aircraft, realizes automatic configuration, and completes the product function at the position. According to the system requirements, the interface of the electromechanical system can adopt the hybrid redundancy connection mode to meet the system security requirements.

In the system, when any one of the electromechanical management computer or the remote interface unit fails at the same time and the function of the node cannot be completed, the product enters the safe mode, and all the bus interface communication and the output interface are blocked from entering the self-locking state. To protect the safety of other electromechanical systems of the aircraft. At the same time, the function module related monitoring mechanism is set inside the electromechanical management computer and the remote interface unit. All nodes in the system have their own fault monitoring, location, and isolation capabilities, and automatically complete resource configuration according to the fault point to realize system resource reorganization after the fault and complete the system function.

4. Fault-tolerant and influential analysis of distributed dual-duplex electromechanical systems

The distributed dual-duty electromechanical system consists of two complete channels. The two channels operate at the same time. The data is shared in real time between the two channels. According to the control strategy, the dual channel works together. According to the characteristics of the system, the system fault tolerance and impact analysis are divided into two levels, namely: node machine level and bus level.

4.1 Node-level fault tolerance and impact analysis

The distributed dual redundancy electromechanical system consists of an electromechanical management computer and a plurality of remote interface units. Due to the different critical degrees of the system tasks, the system tasks are configured with single-node node tasks and two-node machine tasks, and all are configured as dual-channel tasks inside the node machines. Therefore, the node-level fault tolerance and impact analysis in the system are divided into two modes: single-channel fault inside the node machine and dual-channel fault inside the node machine.

When the single-channel fault occurs in the 1-node machine, the fault channel blocks all bus interfaces and puts all the drive output interfaces into a safe state. The node machine enters the single-channel working mode; the signal cross-linked with the node fault channel loses a margin. For the signal only configured to the node machine, the signal is downgraded to a single redundancy mode; for the signal configured to include the node machine and another node machine, the signal is demoted to a dual redundancy working module. In this fault mode, the system redundancy is degraded, and the system functions can be implemented normally.

When the two-node internal two-channel fault occurs, the faulty node machine blocks all bus interfaces and puts all the drive output interfaces into a safe state, and the node machine enters a safe working mode; for the signal only configured to the node machine, the function is lost; The signal to the node machine and another node machine is downgraded to a dual redundancy working module. In this failure mode, one node machine function in the system is lost, the system function is degraded, and the entire function of the system cannot be fully realized.

4.2 Bus-level fault tolerance and impact analysis

The distributed dual-duty electromechanical system consists of two bus networks: an electromechanical internal bus and an avionics bus. According to the system bus structure, bus-level fault tolerance and impact analysis are divided into two modes: electromechanical bus fault and avionics bus fault.

1) According to the characteristics of electromechanical internal bus, the electromechanical internal bus fault can be divided into three modes: root node fault, bus cable fault and remote node fault.

Root node failure: In this failure mode, the network where the faulty root node is located loses the bus network function. All nodes on the network block the bus interface and put all the drive output interfaces into a safe state to enter the safe working mode. The system loses a margin and enters the single-remainder working mode. The system redundancy is degraded, and the system function can be realized normally.

Bus cable failure: In this fault mode, since the entire electromechanical network forms a ring structure, after any cable failure, it will not affect the bus communication function. At this time, the redundancy of the bus network is degraded, which does not affect the normal function; When two or more cable faults occur, the remote node communication function that cannot be connected with the root node is lost, the bus network within the bar cannot complete the normal function, and the electromechanical system loses the redundancy function.

Remote node failure: In this failure mode, the communication function of the failed remote node is lost, which causes the remote node to lose its function, which in turn causes the system to lose a redundancy function. Entering the single-remainder working mode, the system redundancy is degraded, and the system function can be realized normally.

2) The avionics bus failure mode, the distributed dual-duty electromechanical system communicates with the avionics system through two independent bus networks. When one of the networks fails, only the system redundancy is degraded, which does not affect the system function; When the network fails at the same time, the communication function between the electromechanical system and the avionics system is lost, and the electromechanical system completes the internal control function of the electromechanical system according to the electromechanical control rate

5. Distributed Double Residual Electromechanical System Fault Tolerance and Reconstruction

Fault-tolerant and reconfigurable distributed dual-duplex electromechanical systems are implemented by hardware and software.

5.1 Hardware functions and implementation

In order to realize the fault-tolerant and reconfigurable functions of the distributed dual-duty electromechanical system, the following functions are configured on the hardware: watchdog detection function, power supply abnormality detection function, intelligent bus bottom layer verification function, hardware chain function and fault injection detection function.

1) Watchdog detection function. In each node of the system, the FPGA can be configured to configure the watchdog detection function to detect the running state of the processor. When an abnormality occurs, the watchdog alarm signal is linked to the channel control logic of the channel to implement Troubleshoot this channel;

2) Power abnormality detection function. An independent power abnormality detecting circuit is set in each node of the system, and the power signal input to the product and the secondary power source inside the product are detected at the same time. When the external input voltage exceeds the specification, the product generates an alarm message, and records the The alarm information is recorded when the secondary power failure of the product is detected.

3) Intelligent bus underlying verification function. The system uses a large number of intelligent buses, performs cyclic redundancy check, vertical parity check and other verification functions on the bus layer, and reports the results to the software to participate in the system channel control logic.

4) Hardware chain function. When the channel function is lost, the bus output is blocked by the hardware interlock function and the drive output is interlocked to a safe state.

5) Fault injection detection function. The fault injection detection function is set in each node. When the fault is injected from the outside, the channel fault logic inside the node is triggered, causing the node to fail, which is convenient for verifying the channel fault logic function and performing the system fault injection test.

5.2 Software functions and implementation

The distributed double-duty electromechanical system fault-tolerant and reconstruction software can be designed as general-purpose real-time execution software, which mainly performs the following functions: data synthesis processing, fault detection, fault synthesis and resource reconstruction, and exception handling.

1) Data synthesis processing. The data comprehensive processing mainly completes the operating system configuration, the task synchronization between the two channels, and compares and processes the dual-channel shared data realized by the hardware, and stores the calculated result in the specified address, and the supply is called by the software. At the same time, the solved data is cross-transferred and compared to realize dual-channel redundancy data management.

2) Fault detection

Each functional module in the distributed dual-duty electromechanical system reports the health status to the fixed buffer in real time, and the software recognizes the fault flag by periodically reading the buffer status.

The faults of the system can be divided into transient faults and permanent faults. For transient faults, only fault records are recorded, no alarms are reported for the purpose of checking in the system maintenance; for permanent faults, records are recorded, and alarms are reported for faults. The signal participates in the channel fault logic.

3) Fault synthesis and resource reconstruction

The distributed dual-duty electromechanical system adopts the data flow-based fault synthesis and resource reconstruction strategy, that is, each node is internally configured in a dual channel, and only when one of the functional modules in one of the channels fails, the other channel can be completed. Node function; when there is a cross fault in the dual channel, as long as there is a normal function module of the complete channel of the data stream inside the node machine, the node machine automatically runs the resource strategy to ensure that the complete data flow is formed inside the node machine, and the function of the node machine in the system is completed. And the faulty function module identifier is recorded inside the node machine for later troubleshooting; when the same function module failure occurs in the dual channel, the node machine function is lost, and the node machine function cannot be completed.

4) Exception handling

Distributed double-remaining electromechanical system exception handling includes: node machine internal exception handling and electromechanical system exception handling.

The internal processing of the node machine is abnormal. When the operating system is abnormal due to the internal resources of the node machine, different exception handling policies are attached according to the abnormal identifiers of the operating system, and the site of the abnormality is recorded to the inside of the node machine for maintenance. When the internal function of the node machine causes the function module to be abnormal, the internal channel fault logic of the node machine is triggered, and the node machine resource reorganization is triggered, and the scene of the abnormality is recorded to the inside of the node machine.

The electromechanical system is abnormally processed. When the electromechanical system is in an abnormal state, the trigger node machine starts to record all the data of the electromechanical system according to the set step, and is used to recover the fault scene during the maintenance of the electromechanical system.

6. Conclusion

Based on distributed technology, double redundancy fault-tolerant technology and high-speed aviation bus technology, this paper designs and implements a fault identification and resource sharing by studying the system architecture, resource management and fault-tolerant strategies of distributed double redundancy. And a distributed dual-duplex electromechanical system with fault-tolerant reconstruction. The system has the advantages of high reliability, good scalability and reduced number of onboard products. At present, the distributed dual-duplex electromechanical system that uses fault recognition, resource sharing and fault-tolerant reconstruction functions has been successfully applied in a key scientific research project, which not only fills the domestically-made aircraft on the advanced distributed dual-duty electromechanical system. Blank, while laying the technical foundation for the subsequent large-scale integration of aircraft platform.

References

[1] Valentino, G.J.; Johnson, D.L. Advanced photonic subsystems to implement reconfigurable, fault-tolerant avionics. Digital Avionics Systems [C], DASC.20th Conference. 2001.

[2] LeaderS, Friend R.A probabilistic, Diagnostic and Prognostic System for Engine Health and Usage Management [C]//Aero-space Conference Proceedings of IEEE1 [S1I]: IEEE Press, 2000: 185-196.

[3] Shen Yuhua, Aerospace Power Supply System [M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2005.

[4] Shang Lihong, Yan Junbo, Zhang Rui, Jin Huihua. Design of Airborne UMS Distributed Fault Tolerant Computer System[J]. Journal of Beijing University of Aeronautics and Astronautics, 2001, 8(4): 396-398.

[5] Liu Guanzhi, Lin Hui, Li Ying. Design of Double Residual Steering Gear Control System. Micromotor, 2010, 43(1): 50-53

[6] Yin Xin, Zhang Xiaobin, Dong Yanjun, Sun Jia. Design of dual-duration aircraft AC primary power distribution controller based on DSP and FPGA. Measurement and Control Technology, 2014, 33(6): 86-88.