A COMPUTER WITH OPERATIONAL REDUNDENCY AND INTEGRATED ONBOARD NETWORKING AS BASE FOR AVIONICS OF ZERO MAITENANCE EQUIPMENT

A. Avakyan*, I. Boblak*, V. Bukov*, V.Chernyshov*,
Yu. Sheynin, V. Shurman*, E. Suvorova****
*** Institute of Aircraft Equipment, Zhukovskii, Russia***
**** State University of Aerospace Instrumentation, St. Petersburg, Russia***
v_bukov1@mail.ru ; sheynin@aanet.ru

Keywords: fault-tolerant computing environment, SpaceWire technology

Abstract

The results concerning the creation of reliable distributed airborne network are considered. A uniformed computation module is designed in compliance with future requirement specifications and has internal operational redundancy. Correction of any airborne equipment failure is assumed to be made automatically by means of system reconfiguration based on a designed computer with operational redundancy (COR).

The paper presents the developments of a next generation onboard networking for IMA2G that is based on the SpaceWire networking technology and its further evolution. Here are some examples of applying typical avionics subsystems (cockpit functions, cabin functions flight control, maintenance) on SpaceWire based interconnection.

The Project is sponsored by the Russian Ministry of Education and Sciences under the Government Regulation No. 218.

1 Introduction

The concept of Integrated Modular Avionics (IMA) [1] has been broadly accepted by aviation experts and industry. The objectives, capability [2] and architectures [3] of the IMA are essentially universal and are reflect all modern concepts concerning highly reliable integrated avionics packages.

At the same time the IMA concept has not provided direct advantages for final customers, such as airlines, which want to reduce costs and time during the whole life of aircraft, while passengers obtain maximum comfort. This fact has forced a market for IMA to be unclear.

Later an updated concept, Integrated Modular Avionics of Second Generation (IMA2G) appeared [4]. The main objectives were improvements to meet the paramount interests of airlines (reliability, maintenance, etc.).

Simultaneously other concepts related to direct advantages for customers were developed, namely Integrated Vehicle Health Management (IVHM) in USA [5], Onboard Active Safety System (ONBASS) in Europe [6], and Avionics of Zero Maintenance Equipment (AZME) in Russia [7]. The appropriate projects are aimed to solve problems to reach a new level of capacity for aircraft systems.

1.1 Maintenance Efforts

Immense maintenance costs and time for both aircraft as a whole and aircraft equipment in particular is a great problem for aviation.

According to the paper [8], maintenance costs for short-range and midi-range aircraft (150 passengers) are about $750 for a flight hour. So, the overall maintenance costs during the lifetime are $51 million and equal to an aircraft price.

At the same time estimation accomplished at the Institute of Aircraft Equipment shows that annual maintenance costs for conventional avionics are equal to or exceed the annual purchase costs. This must be added with the fact that the maintenance of conventional avionics causes inevitable delays of aircraft flights in airports.

Zero Maintenance Equipment (ZME) is such airborne equipment that is designed to automatically recover without personnel intervention for a given time.

Avionics that is created with substantial reduction of maintenance efforts gives to airlines undeniable advantages in operating airship cost (approximately 50 %), possibilities of realizing more compact flight timetable and using airports equipped with a low level of surface facilities.

1.2 Main Directions of AZME Concept Implementation

The following directions concentrate the cardinal progress of airborne equipment from the standpoint of ZME concept.

1.2.1 Fault-tolerant data-processing network with operational redundancy

A distributed network with a number of uniformed computation modules (UCMs) is assumed. Such an UCM must be designed in compliance with future requirement specifications, have internal operational redundancy and be produced on the basis of a "System on a Chip" modern technology. It is supposed that combination of several UCMs and signal processors gives a platform for information handling. If the area of UCM application is too large, utilization of failed UCM may be more preferable than repair.

Just this direction is the subject of this report.

1.2.2 Element-wise redundancy of airborne equipment

It is assumed that in the future all functional (spatially segregated) systems have to contain "inside" a redundant number of independent sensors or execution units in combination with necessary controllers. Computation and communication facilities, which provided by UCMs, are "outside" of these systems in terms of priorities: these units are firstly elements of an airborne network and then parts of functional systems.

1.2.3 Advanced systems for gathering and calculating information about airborne equipment for analysis during flight and taxi

It is assumed that airborne equipment will contain possible (physically feasible) built-in testing. Signals of corresponding units will be used for ground aids and firstly for urgent decisions for system reconfiguration and crew operations.

1.2.4 High-performance algorithms for localization directly controllable and uncontrollable failure

It is assumed that all airborne systems, both accessible and inaccessible to built-in testing, are checked with high-performance algorithms of "inverse logic", which are based on the application of logic models for failure propagation in the system [9]. Such algorithms must be added with algorithms of current analysis of system functioning efficiency, which allows the system structure optimization in real time.

1.2.5 Algorithms for profound reconfiguration of airborne systems based on element-wise redundancy of systems and airborne network

It is assumed that results of failure localization will be used to make decision to remove (replace) failed airborne elements without or with minimal degradation of system functionality. The double redundancy of an airborne network (elements on a chip and chips in an airborne network) is planned to be used.

1.2.6 Systems and channels for distributing flight situation for a timely decision

It is assumed that in any case a digital channel must be used to deliver operating data to the ground personnel for the preparation of extraordinary arrangements, if necessary.

2 Design a Fault-Tolerant Platform

The main objective is to create a closed technology to design, produce and upgrade an airborne network firstly and equipment in whole secondly that realize the policy of non-attended systems (between 600-hour scheduled operations).

The long-term plan of the development of this scientific and technical direction envisages the next stages:

1. Develop the design principles and a closed design and production technology for airborne computational environment (ACE) with integration of the IMA and AZME concepts (by 2015).
2. Develop a package of airborne equipment with ACE and conventional (structurally and functionally separated) terminal systems (by 2019).
3. Develop the principles and technical solutions for structural and module separation of basic airborne terminal systems (by 2019).
4. Develop the basic zero maintenance package of airborne equipment with the operational redundancy for the computational environment and modular terminal systems (by 2023).

At the first stage the Institute of Aircraft Equipment (NIIAO) together with the St. Petersburg State University of Aerospace Instrumentation (SUAI) sponsored under the Russian Government Regulation No 218, have prepared a complex project to create the up-to-date high-efficiency closed technology to design and produce the ACE hardware and software package.

3 Architectures of Airborne Package

3.1 Typical Architecture

The architecture of the first-generation system of the IMA consists of one or more platforms and contains interfaces with other aircraft systems and different users (flight crew, attendants, personnel, etc.). The IMA platform provides the capability to manage resources used together, check the operational state of systems and support the protection of the resources used together.

An appropriate architecture is shown in Fig. 1.

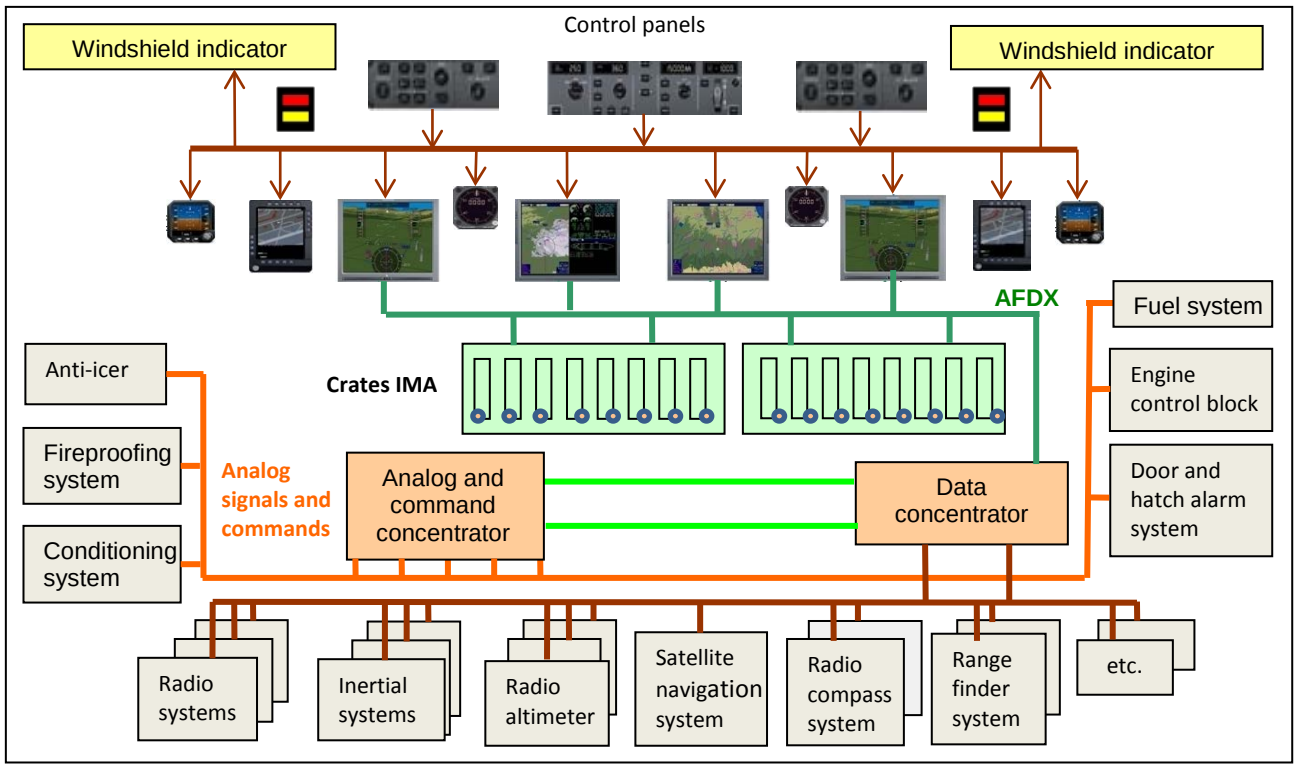

Fig. 1. “Typical” architecture of an integrated avionics package

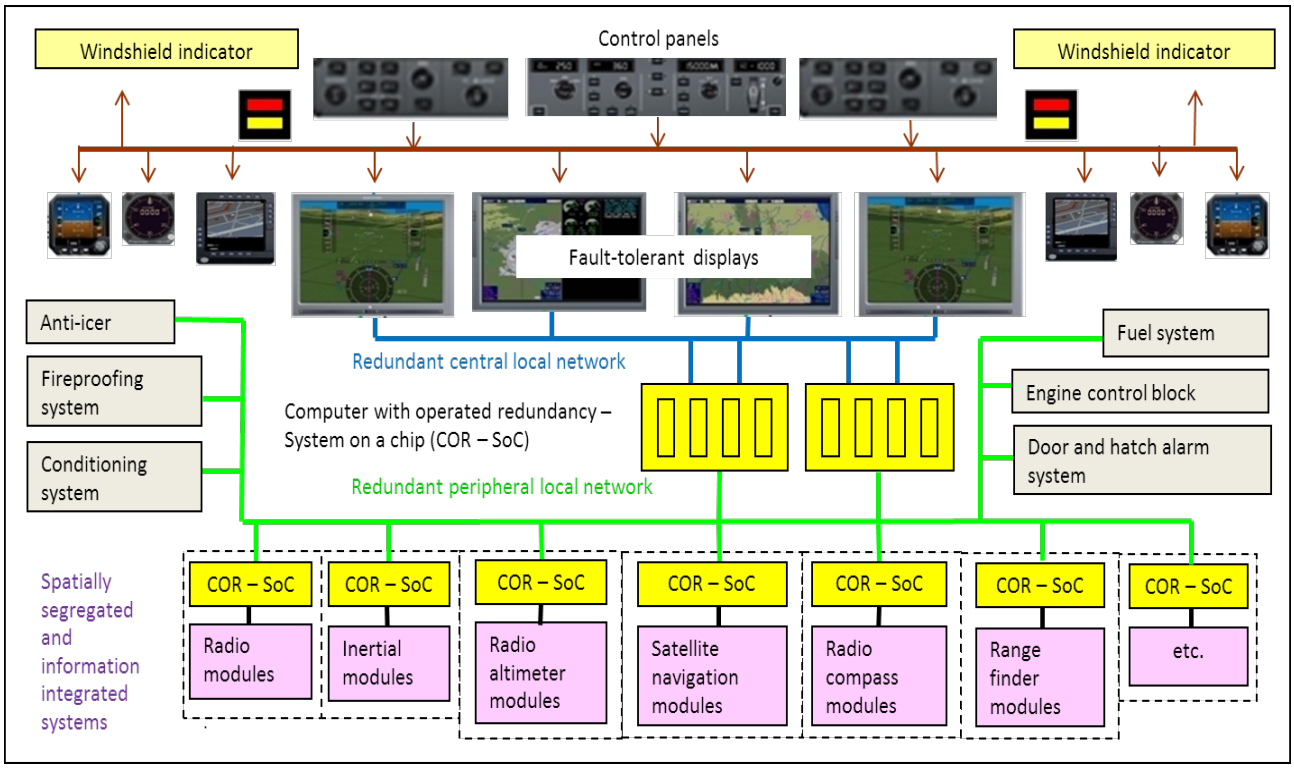

Fig. 2. “Perspective” architecture of an integrated avionics package

Two computation stations designed to be installed in crate form. This is the architecture basis, or so-called “computational kernel”. All computations related to aircraft function implementation and also to control of a technical state are provided in this kernel. Serial interfaces are used for data communication: high-speed FibreChannel (ARINC 818) for video and map information, and also full-duplex Ethernet (ARINC 664) for communication with data concentrators for reception from sensors and for connection between the stations.

So, in the case in question the considerable concentration of computational resources takes place. It simplifies the solution of a number of problems related to computational resources handling, however, causes difficulties in achieving the package vitality when a failure occurs. In addition, the excessive concentration of calculations hampers and raises the costs of both package development and its subsequent modification.

3.2 Perspective Architecture

Here the computational interconnect environment of a package is examined as an information-management computer network system, where the resource integration is provided by organizing connections between its elements on the basis of a networking technology. Such a system must provide the capability of program-driven reconfiguration in the process of regular operation (flight) to optimize the descriptions of fault tolerance as the productivity, providing probability of failure in the mode of maximum fault tolerance no more than 10^{-9} and the productivity in the mode of burst performance no less than 1 - 2 milliard flops.

Such task redistribution among the resources is mostly feasible, if:

- computational resources are homogeneous to the maximum attainable degree, connections between resources are regular (thus, for example, the most effective application of the sliding reservation is possible for the use of added-on equipment);
- the repetition factor of reservation of the centralized computational resources is high enough;
- the participation in replacing a failed equipment can accept all computational

resources: not only centralized, spatially concentrated resources within one structurally-functional module (unit, container) and incorporated by a system chassis, but also resources that are dispersed on the entire aircraft and connected by information exchange channels;

- the possible solution of any task using any computational resource are not limited to functional specialization of resources;
- information generators (sensors) are accessible to all processing devices through the integrated environment of informative exchange. Heterogeneity (physical, informative) of sensors is compensated by adapting facilities: by local concentrators and processing devices, network comptrollers;
- the descriptions of information exchange environment provide access time to the remote calculable resources, comparable with local access.

Fig. 2 shows the suggested structure for airborne computer environment. Two fundamental features, that require attention, include:

- ✓ separate modules which form the information basis of the functionally complete systems are used here instead of these systems;
- ✓ all computational resources (Computers with Operational Redundancy – COR) are either universal units or behave as a number of compatible calculators.

The channels used for information exchange do not limit this structure. Practically any advanced interface can take place.

4 Computer with Operated Redundancy

When developing a computer platform for IMA2G, the following basic principles are taken into account.

A. Redundancy of platform elements. This principle results from the fact that the attained level of reliability for modern components is insufficient to satisfy requirements for avionics platform reliability.

B. Automatic (steady and remittent) renewal fault recovery and failure correction. This principle provides the implementation of exploitation of platform between 600-hour scheduled platform operations without maintenance.

C. Localization and correction of hardware and software errors. The current methods of validation and verification of circuit technology and developed programs do not provide the desired reliability of platform operation.

When implementing the first principle, it is necessary to define the structure of redundancy, i.e. the level of backup for platform elements, and then to define the degree of backup. Research has showed that for computer platforms the rational element of backup is an interface computation path.

The typical interface computation path of a platform, as a rule, consists of the next large-sized parts:

- a low-frequency interface which is used by the computer system to connect to sensors (often it is a general-purpose interface like ARINC-429, CAN, etc.);
- a computation module used for information processing;
- a high-frequency output interface (AFDX, FibreChannel, SpaceWire);
- path switchboards on the platform input and output.

A variant of the COR architecture is shown in Fig. 3.

Four interface computation paths provide necessary redundancy to safety the airworthiness requirements and flight regularity.

The switchboards of high-frequency interfaces and modules of integrated low-frequency output operate the redundancy, and also information output on a front-end interface.

When creating the systems that have the maximum faultlessness (the intensity of function faults resulting in a catastrophic situation must not exceed 10-9 faults per flight hour [10]), it is a necessary to develop systems with two-level backup.

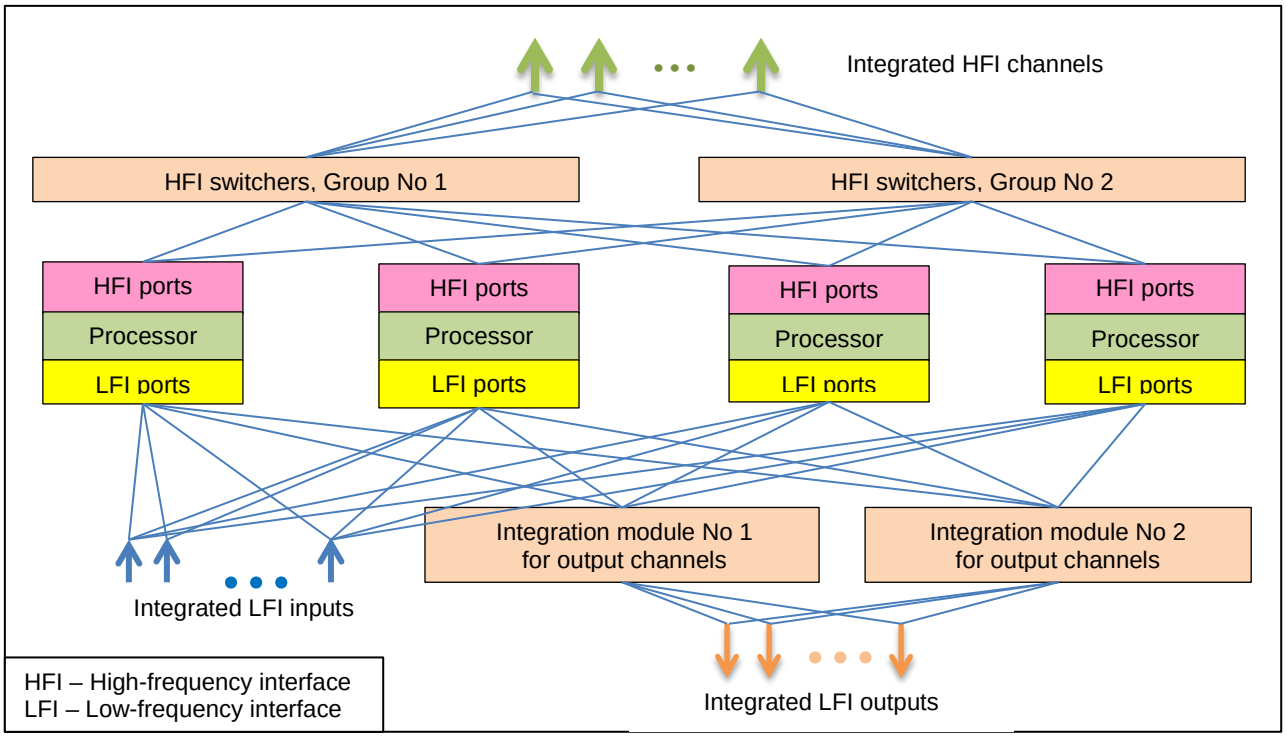

Fig. 3. Structure of a computer with operational redundancy

The first system must be a majority check system, as it is impossible to correct a fault during one second with other control methods. For determination of a failed path in the majority check system, it is necessary, at least, to have a basic path and two backup paths.

The second system (system of the second level) controls the majority check system, providing its faultless work between scheduled operations.

An appropriate method was developed, approved and patented in Russian Federation as "Method and computer system for fault-tolerant information processing for aircraft critical functions".

The pre-production model of the COR is made. Fig. 4 gives its overview.

Fig. 4. Computer with operational redundancy (COR)

The COR with the suggested structure is assumed to be used in aircraft integrated packages with interconnections either within a network or in a point-to-point configuration.

5 Integrated Networking for IMA2G

Further integration in IMA2G should cover data processing in a distributed modular electronics (DME) architecture, as well as command and control, I/O and signalling tasks. In a DME on-board architecture it should be supported by an Integrated Communications Network (ICN). It should provide a communication entity that could support all types of traffic in the distributed on-board avionics:

- Sensor buses with high-rate data steams;
- Command buses, that needs command packets with deterministic delivery time;
- Data buses for distributed processing, with low latency delivery of data packets;
- Signal lines with hard real-time signals distribution with ultra-low latency.

The Integrated Networking ARchitecture (INAR) for IMA2G and AZME has been developed, which is based on SpaceWire / SpaceFibre networking technology [11], Fig. 5.

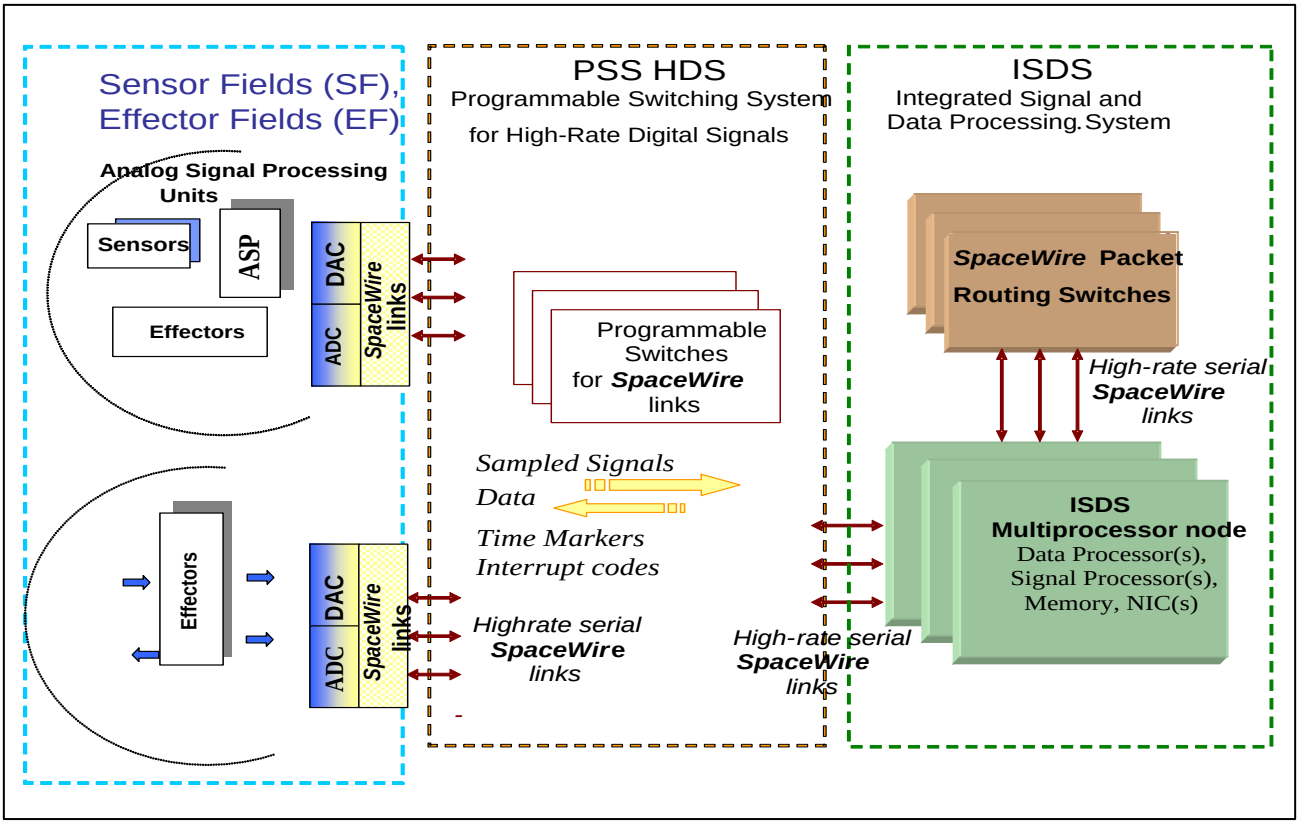

Fig. 5. SpaceWire/SpaceFibre-based integrated networking architecture for IMA2G/AZME

The INAR gives a basis for building a scalable networking infrastructure with compact and light-weight routing switches, ready for scalability and duplications for redundancy. It provides high-rate communications (up to 400 Mbit/s for SpaceWire, 1-6 Gbit/s for SpaceFibre links), better latency than other networking technologies, efficient and compact implementation in chips.

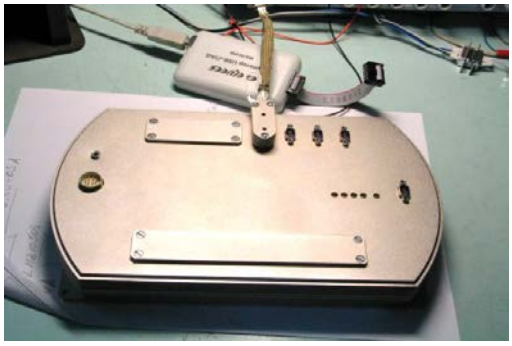

Fig. 6. SpaceWire routing switcher for airborne networks

The INAR provides an integral network infrastructure for all types of traffic in the DME: high-rate data streams, command packets with deterministic delivery time, data packets for distributed processing and I/O, common time ticks distribution, ultra-low latency distribution of hard real-time signals. Interfacing INAR to other interconnections (ARINC429, CAN, AFDX, and FibreChannel) for gradual evolution of avionics is provided by gateway nodes.

The pre-production model of network is made in accordance with the aviation requirements. Fig. 6 gives the overview of this unit.

Methodology and tools for INAR-based onboard networks design and configuration has been developed.

6 System Level Fault-Tolerance with Operational Redundancy

System-level fault-tolerance is supported by INAR for building a fault-tolerant network infrastructure. The INAR provides the construction of scalable network interconnections with operational redundancy, adaptive and redundant packets and signal tokens. Automatic recovery from transient faults

is an inherent feature of SpaceWire / SpaceFibre protocols at several layers. Automatic recovery after persistent faults is done by intelligent SpaceWire and/or SpaceFibre routing switches. Traffic partitioning ensures the protection of packet flows in the network from spurious coupling between them. Trusted interconnection interface of end nodes provides the protection from end node applications malfunctioning that could disturb system operation.

Redundant sets of end nodes, such as computation modules/CNOR, peripheral modules, I/O modules, along with transparent tasks migration to available operating end nodes, provide system-level operational redundancy.

For fault-tolerance support in the AZME at the system level, the basic features of the SpaceWire technology are used:

- ✓ automatic detection of a link connection fault or break, that is built in the Symbol, Exchange levels' protocols;
- ✓ automatic connection recovery after a transient fault in a link;
- ✓ adaptive routing, which is built in the Network level protocol, that provides automatic selection of an alternative route if an initial output port of a routing switch appears to be not connected, faulty or busy on a forwarded packet arrival;
- ✓ fault-tolerance and recovery mechanisms built in the basic SpaceWire protocols for Time Codes and Distributed Interrupts distribution, that know how to pave their ways to any node in the network with bypassing failed switches and links;
- ✓ no restrictions on the interconnection graph topology, that gives a full capability for building any types of a redundant interconnection topology;
- ✓ clustering network facilities (regional logical addressing) that enable communications to be placed in a region in correlation with easily monitored, controlled (and disabled, if there is a risk of fault propagation) packets for inter-region transition in dedicated points of the clustered interconnection;
- ✓ reconfigurablility of tracing logical connections between the nodes due to route alignment in interconnection routing switches without any changes in the logical connection setup for the end nodes.

Tools for suggested fault-tolerant network infrastructure design and system-level DME configuration have been developed.

7 Demonstration

7.1 General structure of the demonstrator

A demonstrator was developed to demonstrate capacity and to research the behavior of the advanced computational environment. It includes the functional and structural prototypes of system components and the segments of a local central and peripheral airborne network.

The demonstrator of a central computer network contains two types of fault-tolerant equipment:

- Fault-tolerant computer with the operational redundancy (COR) on the basis of the triple backup (4 equivalent paths) of a processor module with the "each with each" connections (see Fig. 3).
- Fault-tolerant segment built on the basis of mini-blocks that contain a processor and SpaceWire network (see Fig. 5).

A computer is attended with AFDX and SpaceWire as well as contains hardware of graphic comptrollers (GC) with the DVI interface to deliver flight navigation and map information to video monitors. Thus, video information acts from the computer in displays not directly, but through the "cloud" of SpaceWire switchboards.

Fig. 7 shows the structure of this demonstrator.

There is a segment on the base of SpaceWire interface and data/signals concentrators in a peripheral computer network. The concentrators are attended with AFDX and SpaceWire and can also co-operate with the local signal concentrators of airborne equipment (using CAN).

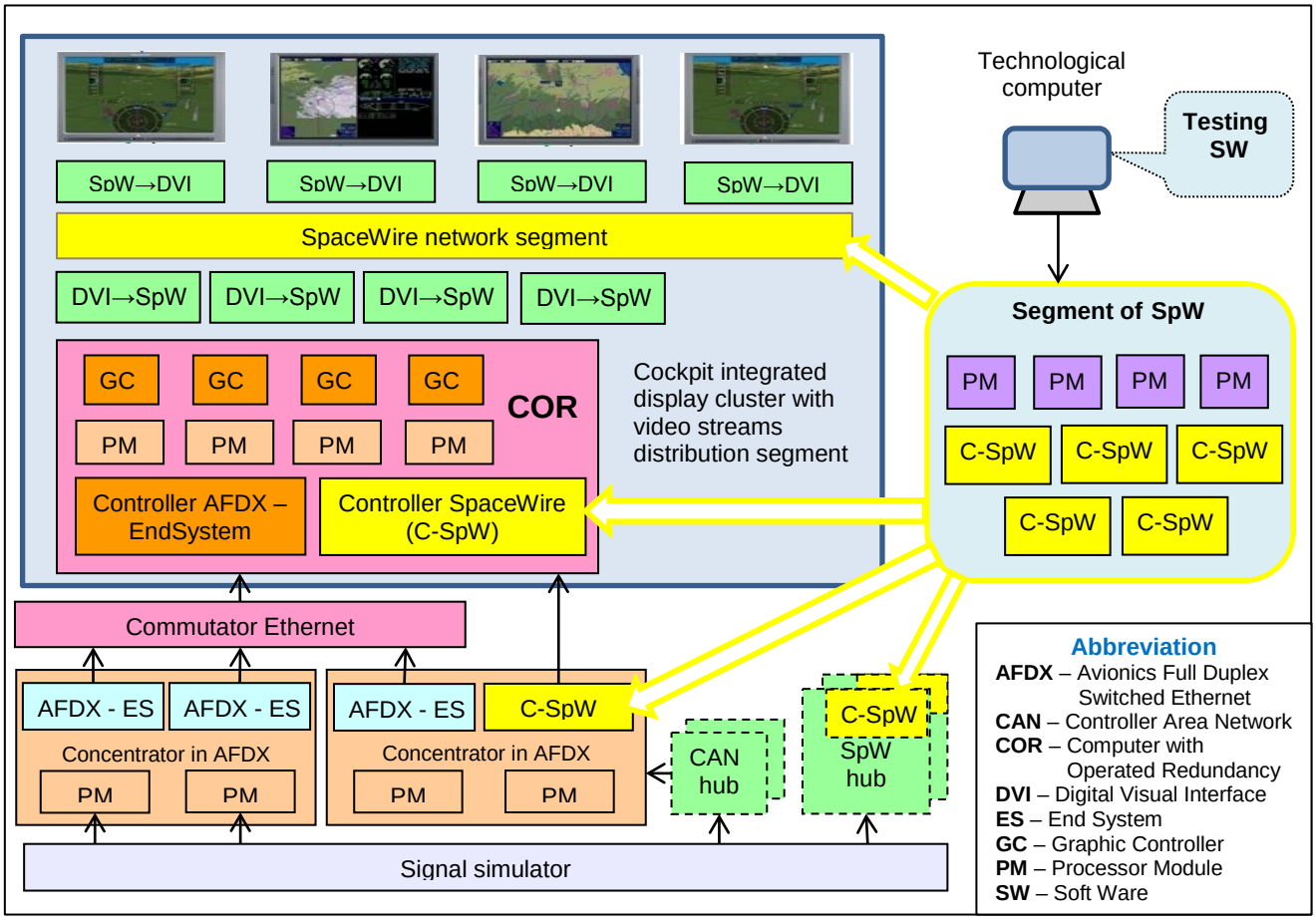

Fig. 7. Demonstrator of a local network segment

The demonstrator allows research and measurements for such parameters as

- carrying capacity and time parameters of different network configurations in a wide range of descriptions of data flow structure and intensity;
- algorithms efficiency for redundancy and equipment reconfiguration management;
- possible reduction of productivity indices and reliability of computational facilities;
- really attainable repetition factor for fault tolerance;
- hardware and software organization efficiency for information collection and preprocessing processes;
- airborne equipment management efficiency;
- efficiency of internetwork cooperation.

The Video streams distribution segment (see Fig. 7) provides efficient and robust video data delivery from the COR(s) to the cockpit displays, building task oriented, Cockpit Integrated Display Cluster for IMA2G/AZME.

7.2 Video streams distribution network segment in the cockpit

Video streams routing, multicasting or broadcasting from multiple sources to multiple displays are provided by native SpaceWire features and is easily controlled by configuration and dynamic reconfiguration of routing tables in the SpaceWire switches. Thus better workload repartition between Pilot Flying and Non Flying data and more efficient cockpit displays field organisation are achieved.

Format of SpaceWire packets makes it easy to package natural video data units into SpaceWire packets. For instance, a video frame, say 2 Mbits/frame, could be packaged in a single SpaceWire packet, without its cutting into fragments, packing/unpacking them in a separate packet each, etc. It simplifies

interfacing video sources/sinks to the network and increases useful throughput for video streams delivery.

Redundant topology of the SpaceWire network segment provides fault-tolerance of the video streams distribution. Adaptive routing that is a native SpaceWire feature, automatically, on the fly, switches data streams to healthy links bypassing faulty ones without network management system interference. Network operation recovery after transient faults in links and nodes is embedded in the SpaceWire protocol stack at several layers and is done automatically by respective FSM in nodes and link controllers.

8 Conclusion

Correction of any failure in airborne equipment is assumed to be made automatically by system reconfiguration based on the designed fault-tolerant network and the computer with operational redundancy.

The Integrated Networking ARchitecture (INAR) gives a basis for building scalable networking infrastructure with compact and light-weight routing switches, ready for scalability and duplications for redundancy.

The usage of a computational environment, that includes suggested solutions, provides an opportunity to implement a traditional human-aided equipment service (disassembly, rebuilding and assembly) during routine maintenance only. In the limit, this service has not to be provided during the life cycle of an aircraft.

Naturally such a goal may be achieved on assumption of developmental work for other directions listed above in this paper.

References

[1] DO-297. *Integrated modular avionics (IMA) development guidance and certification considerations*. RTCA Inc., Washington, 2005.

[2] Watkins C B. Integrated Modular Avionics: Managing the Allocation of Shared Intersystem Resources. *25th Digital Avionics Systems Conference (DASC)*, Portland, Oregon, October 2006.

[3] Garside R and Pighetti J F. Integrating Modular Avionics: A New Role Emerges. *26th Digital Avionics Systems Conference (DASC)*, Dallas, Texas, October 2007.

[4] Hainaut D. Towards the next generation of integrated modular avionics. *Sixth European Aeronautics Days*. Madrid / Spain. 30 March – 1 April, pp 135. 2011.

[5] Gorinevsky D and Mah R. *NASA IVHM RTI Architecture: Working Document.* April 20, NASA NNA08BC21C, 2009.

[6] Schagaev I. Concept of Active System Safety. *Proc 15th IFAC Symp. on Automatic Control in Aerospace*, Bologna/Forli, Italy, 2001.

[7] Bukov V N, Kutahov V P and Bekkiev A Yu. Avionics of zero maintenance equipment. *International congress of the aeronautical sciences*. CD ISBN 978-0-9565333-0-2, Report 7-1-1. 2010.

[8] Butz X. Integrierte modulavionik – ein direkter weg zu ausfallsithern systemen. *Daimler Chrysler Aerospace Airbus Kreetslag* 10, D-21129, Gamburg, 2005.

[9] Bukov V N, Bronnikov A M and Selvesyuk N I. Algorithm of Fault Troubleshooting of Airborne Equipment Based on Mixed Directed Graph. *Safety Flight Problems*, No 2, pp 57-71, 2010 (in Russian).

[10] *Airworthiness requirements for the transport category* (АП-25). Moscow. 1993 (in Russian).

[11] *SpaceWire-links, nodes, routers and networks*. Standard ECSS-E-ST-50-12C, July. 2008.

Copyright Statement