Security Analysis of IMA Primary Processing System Based on DFTA

Yigang Sun
College of Aerospace Automation, Civil Aviation
University of China, Tianjin
ygsun@cauc.edu.cn

Zhen Zhao
College of Aerospace Automation, Civil Aviation
University of China, Tianjin
zhenzhao0523@gmail.com

Hao Li
College of Aerospace Automation, Civil Aviation
University of China, Tianjin
haoli0508@163.com

Zhiyong Fan
Avionics Engineering Faculty, Civil Aviation
University of China, Tianjin, China

Abstract—In order to realize the architectural benefits (increased system scalability, decreased workload, and etc.), the security of the IMA architecture should be put on the first position. IMA architectures utilize shared, configurable computing, communication, and I/O resources. These architectures do lots of benefits to the avionics system integrators. By learning from GENESIS (a new style of synthesis computing platform that comprises IMA and other computing platform, and provides computing , communication and I/O resources for the time-embedded system known as “Hosted Function”), this paper focuses on the composition, function, structure and principle of the primary processing system of IMA platform, and enumerates one model about its characters in component number, communication ways, and placed locations. From the perspective of integrity and availability, the security of IMA architecture is analyzed using the Dynamic Fault Tree Analysis in this paper. The analysis results provide guidance for implementation of Hosted Function in IMA primary processing system.

Keywords-Security; Architecture; DFTA; Primary processing system; IMA

I. INTRODUCTION

Integrated Modular Avionics (IMA) architectures are based upon a set of modular systems that share computing, communication, I/O resources, and etc. In order to conserve computing resources, power resources, and module for the collective set of avionics onboard, IMA architectures increased levels of avionics integration. Thus, the use of intersystem resources can be a new way in the world of systems integration.

An “open systems” architecture known as “GENESIS (Generic Networked Element for Synthesis of Integrated System)” was implemented on the Boeing 787 as the Common Core System (CCS) [1]. The 787 CCS is one of the first examples of an “open system” IMA architecture that was put into practice, this IMA platform can initially host about 70 applications for 20-25 independent suppliers, but is capable of hosting over 100 applications [2].

Since a lot of avionics functions are integrated together using the shared platform resources, the use of intersystem resources would be a new paradigm in the world of systems integration. Then the complexity of the integration process is increased due to the sharing of intersystem resources. So the security of IMA platform appears particularly important. Previous work has addressed modular certification arguments [3], mechanisms for compositional reasoning and modular systems [4], besides, automated selection, sizing, and mapping of IMA modules had discussed in [5]. This paper has a detail description about the composition and integration of IMA primary processing system. By analyzing the integrity and availability of IMA primary processing system, this paper provides guidance for implementation of Hosted Function in IMA primary processing system.

II. PRIMARY PROCESSING SYSTEM OF IMA PLATFORM

A. *Principles of IMA*

IMA architectures are different from traditional “federated” architectures for which each system contains its own dedicated processor, communication channels, and I/O resources. IMA architectures provide a more efficient solution by sharing resources and minimizing resource waste. Multiple systems can be architected and overlaid on the partitioned platform resources to form a highly integrated system with the unique characteristics of full isolation and independence of each individual system.

“Hosted Functions” is referred to that avionics systems hosted on an IMA platform. The shared resources must be allocated among the Hosted Functions within the IMA architecture. For Hosted Functions, they can own unique sensors, effectors, devices and non-platform LRUs that become part of the functional system architecture. Multiple Hosted Functions share the platform resources within a “logical system” environment enforced by partitioning mechanisms that are implemented as part of the platform design. The “logical system” partitioning environment guarantees that Hosted functions are isolated from each other. Fig 1 depicts a type of IMA system architecture [6]. To mitigate the error propagation, high-integrity fault containment mechanisms should be implemented and ensure that when a fault in one Hosted Function or platform component will not initiate failures in all Hosted Function Systems. Redundancy mechanisms are also required to deal with the error propagation across multiple Hosted Functions.

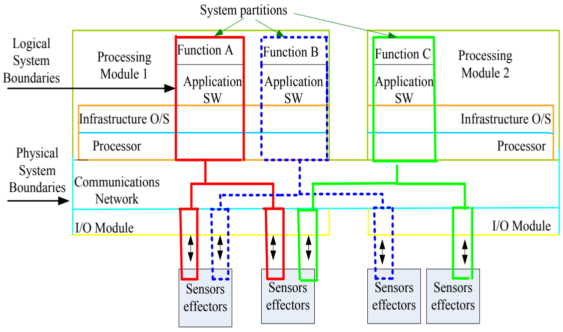

Figure 1 A type of IMA system architecture

B. The primary processing system

As described above, the primary processing system of IMA platform can be obtained. It is proposed to dealing with relevant avionics tasks and providing services for hosted functions. The system is comprised of single or multiple IMA cabinets, data transmission networks and interfaces. To ensuring that each system application can share computing, network, I/O resources, the allocation of these resources is predetermined. The primary processing system of IMA platform can hold the functions of data processing, data transmission, and data conversion based on these shared resources.

It is a real-time distributed computer system which can manage a synthesis processing on data, signal and image. For the expectation of being generally used in any avionics system, at the hardware aspect, IMA primary processing systems should be designed as standard modules and combined with external non-commonly sensors frontend, effectors and application software via interfaces, finally improve interoperability and lower the total costs of equipment lifespan[7]. In view of the mentioned functions, the main components of the IMA primary processing system can be concluded as GPM, AFDX and RDIU [8].

III. SYSTEM FUNCTION AND CORRESPONDING COMPONENTS

A. The function of data processing and General Processing Module (GPM)

The data processing function covers hardware as well as software requirements. It provides resources for Hosted Function for the implementation of aircraft's function. Data processing function can be realized by resources (enough processing time, memory and etc.) supplied for Hosted Function.

GPM is system processing resource, whose main task is realizing the data processing function. It also provides robust classification for environment and infrastructure services (e.g. I/O, health monitoring, the storage and retrieval of non-volatile files based on the ARINC653 standard). Besides, core software is hosted on it. The real-time operating system based on ARINC653 is hosted on every GPM which supplies operating control and resources management in time-spatial division (working time division, space division) for GPM. Functions like data processing, health management, data loading, configuration management and system recovery are hosted on GPM.

The hardware used for GPM can realize fault passive protection, there is no single failure can lead to an incorrect action, meanwhile, there is no situation that not detected fault leads to an incorrect action. GPM owes its independent integrity and redundancy which can meet the availability of Hosted Function.

B. The function of data transmission and Avionics Full Duplex Switched Ethernet (AFDX)

The system provides resources for the data transmission network which makes a connection between data processing resources and other aircraft subsystems based on the ARINC664-P7 standard. The data transmission network is consisted of End System (ES), Switch (SW) and AFDX. Each of the ES in the AFDX is connected with two redundancy channels and each channel is designed matched with the SW, thus, it can improve the availability of data transmission. ES can manage the work status based on the transmission and receiving of data stream in every logical channel. Structure of the AFDX network is shown in Fig 2.

AFDX network is the communication channel of IMA primary processing system. Its structure is disposed in dual star topology. As for each terminal node in topology structure there will be a backup node, the two nodes will connected in a point-to-point way with two independent communication path (channel A and channel B).

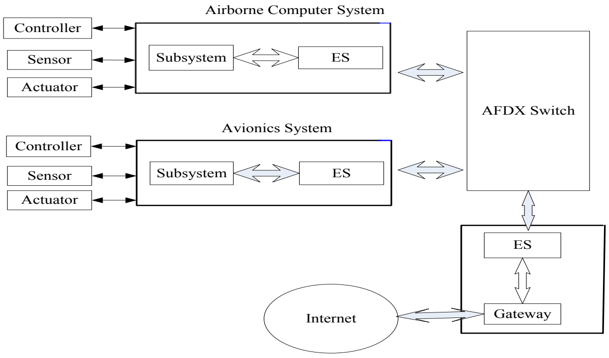

Figure 2 Structure of the AFDX network

Research on optimal design of virtual links in AFDX network was proposed in [9]. So long as the End Systems meet the requirement of availability, they could be separately connected to AFDX network via single switch. Every network channel is designed to contain all the failures probably taken placed between transmitting and receiving ports. The fault sealing property is realized by using complete algorithm that running in the End System. These will lead to higher availability in redundancy channels and ensure integrity not affected by the network.

C. The function of data conversion and Remote DataInterface Unite (RDIU)

RDIU is used to complete data conversion function in IMA primary processing system. Its main task is providing data interfaces via AFDX data bus for series of traditional sensors, effectors and main processing resources. It works as a data-to-data gateway among AFDX network, analog device, traditional ARINC 429 and linear CAN subnet. RDIU accumulates data from data bus in every buffer area and mapping these data to specially appointed ARINC 664-P7 ports which located in AFDX End System. In order to ensure the separation between function signals of I/O and avoid error propagation between interfaces, the partitioning method of I/O in RDIU is physical separation method.

The structure of RDIU is consisted of two different integrity areas, one is shared by all resources users and another is provided independently for dedicated users. The importance of this structure is to ensure that when failures exist in public resources, the failures will not lead to failures in dedicated resources or the function that is using the resources simultaneously. Output from each RDIU will be forced in a safe state when failures or not valid commands exist in output interface. A fault will be marked when it is detected and data in transmitting packets in a network will be regarded as invalid.

D. System composite structure

For the sake of forming a specified IMA primary processing system and achieving implementation in physical, the components can installed in varies of ways. These components can be assembled in the style of LRU, LRM or PCB, besides, the LRM and PCB can be combined in the cabinet of IMA to share public resources like power and refrigeration. As in Boeing 787 aircraft, its CCS is a specific physical implementation of IMA system. Many GPM and AFDX network switches are assembled in one cabinet. RDIU is made as RDC in CCS and other AFDX network switches are made in the style of LRM [10].

The scale of the IMA primary processing system is changed over the different security level of Hosted Function. Fig 3 describes one model structure of IMA primary processing system [11]. Each resource in module can be increased or decreased based on the requirement of Hosted Function in a given group. When the scale of these modules changed over time, the system operation and function structure will not be affected, as the resources allocation which linked to functions remain unchanged and have no effect on existing Hosted Function.

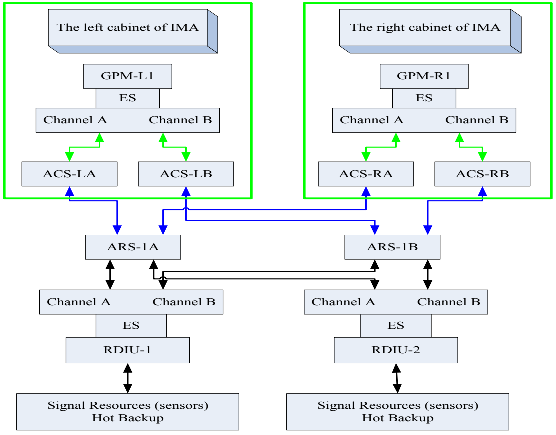

Figure 3 One model structure of IMA primary processing system

In Fig 3, GPM and part of network switches are placed separately in right/left cabinets and components can be mutual backup if they are in same types. Network switches are classified into two types: AFDX Cabinet Switch (ACS) and AFDX Remote Switch (ARS). AFDX is a full meshed network, every switch connected to another. The data transmitted in channel A is the same as channel B, integrity testing and the elimination of invalid frames can operated in the ES then redundant frames can be eliminated by redundancy management.

The resource module of IMA primary processing system can be configured. To make sure there will be enough processing time, memory capacity, I/O port and interface resource, each Hosted Function acquires required resources based on the safety level in the system. The distribution of these resources modules are realized by the specific configuration tables which loaded to every system component.

IV. ANALYSIS AND RESULTS

In order to ensure the security of IMA primary processing system, failure state should be put in the first place. By using the Function Hazard Assessment (FHA), failure state that caused by the potential hazard when system in failure or working state can be identified whilst classification on system failure state should be executed to match with the level that system expected to be. The FHA results are separately showed in Table I and Table II Table I is about the system availability and Table II the system integrity.

TABLE I THE FHA RESULTS ABOUT AVAILABILITY RELATED TO IMA SYSTEM

System Function	Failure State	Security Level
Providing General Processing Resources for Aircraft	Entirely lost the data transmission ability for a critical function.	Catastrophic
	Entirely lost the I/O interface for a critical function.	Catastrophic
	Lost the ability of providing general processing resource to a critical function.	Catastrophic
	Lost the ability to restart a critical Hosted Function.	Catastrophic
	Entirely lost the data transmission function to a high necessity function.	Hazardous
	Entirely lost the I/O interface for a high necessity function.	Hazardous
	Lost the ability of providing general processing resource to a high necessity function.	Hazardous
	Lost the configuration management function of system.	Hazardous
	Entirely lost the data transmission ability for a low necessity function.	Primary
	Entirely lost the I/O interface for a low necessity function.	Primary
	Lost the ability of providing general processing resource to a low necessity function.	Primary

Failures listed in Table I and Table II are matched with the function realized by IMA primary processing system, include data processing, data transmission, data conversion, and etc. Generally, undetected error data or action belongs to the domain of system integrity while lost ability or resource belongs to the domain of system availability. Only when the requirement of integrity and availability are fully met can system achieve the required security level.

TABLE II THE FHA RESULTS ABOUT INTEGRITY RELATED TO IMA SYSTEM

System Function	Failure State	Security Level
Providing General Processing Resources for Aircraft	Undetected error transmission in network data.	Catastrophic
	Providing undetected error I/O interface resource to a critical function.	Catastrophic
	Undetected error data processing in a processing component.	Catastrophic
	Undetected error behavior in IMA health management function.	Catastrophic
	Undetected error behavior in data loading function.	Catastrophic
	Undetected fault in system configuration management function.	Catastrophic
	Providing undetected error I/O interface resource to a high necessity function.	Hazardous
	Providing undetected error I/O interface resource to a low necessity function.	Primary

The classification of security level in failure state has a direct connection to the importance of Hosted Function, for example, the security level of failure state is catastrophic so as to the corresponded Hosted Function.

TABLE III RELATIONSHIP BETWEEN SECURITY LEVEL AND THE MAXIMUM PROBABILITY

Security Level	Hazard Class	The Maximum allowable probability(per Flight Hour)
Catastrophic	I	1.0×10^{-9}
Hazard	II	1.0×10^{-7}
Primary	III	1.0×10^{-5}
Secondary	IV	1.0×10^{-3}

The corresponding relationship between security level and the maximum probability is showed in Table III.

A. Fault tree modeling

Because of the dynamic characteristics of IMA primary processing system, dynamic logical gates are adopted to establish the dynamic fault tree with the help of conventional method.

Combined with possible failure states, the fault tree model of the integrity and the availability can be established. The dynamic fault tree analysis model is shown as Fig 4 and Fig 5. Fig 4 is integrity DFTA model, Fig 5 is availability DFTA model. UED is stand for Undetected Erroneous Data.

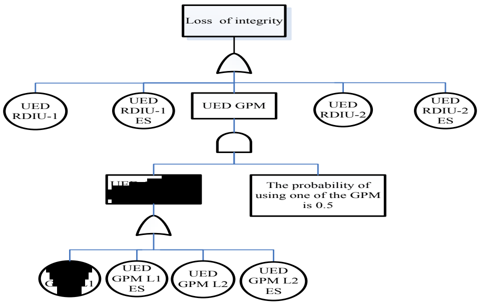

Figure 4 System integrity DFTA model

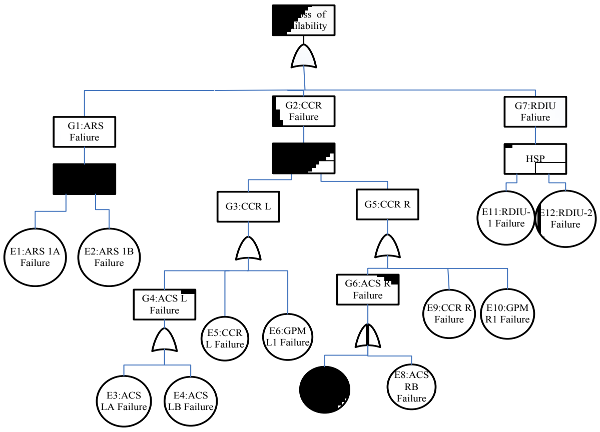

Figure 5 System availability DFTA model

B. Analysis based on DFTA

Modularization is an effective way to deal with DFTA. By decomposing the Dynamic Fault Tree into many independent modules, then, numerical combination or BDD can be used to analyze static module and Markov Model used to analyze dynamic module. There the DFTA model in Fig 5 is used to show the process of analysis.

Modular decomposition: according to the characters of DFTA, a search method based on linear DFLM is used to modular decomposition. Conducting DFLM search in fault tree module, the result is as TABLE IV.

TABLE IV DFLM RESULT

Event	R1	G1	G2	G3	G4	G5	G6	G7
#1	1	2	6	7	8	15	16	24
#2	28	5	23	14	11	22	19	27
Last	28	5	23	14	11	22	19	27
Min	2	3	7	8	9	16	17	25
Max	27	4	22	13	10	21	18	26
Mod	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Static/Dynamic	Dynamic	Dynamic	Dynamic	Static	Static	Static	Static	Dynamic

Results can be got form TABLE IV that the static modules include G3, G4, G5 and G6; dynamic modules include R, G1, G2 and G7.

Static modules analysis: BDD analysis method is used to analyze static modules: G3, G4 converted G3, G4 into BDD chart as Fig 6.

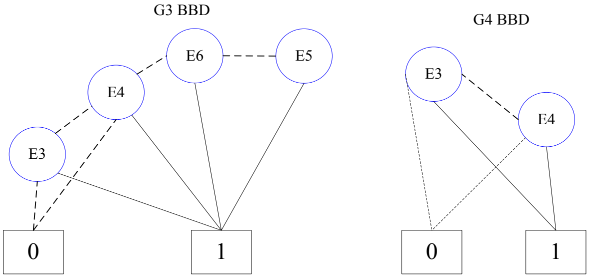

Figure 6 BDD chart

From the BDD chart, the cut-sets of G3 can be described as {E3}, {E4}, {E5} and {E6}. The probability of top event in G3 can be calculated as:

$$P(G\,3) = 1 - P(\overline{E3})P(\overline{E4})P(\overline{E5})P(\overline{E6}) \qquad (1)$$

$$P(G4) = 1 - P(\overline{E3})P(\overline{E4}) \quad (2)$$

Dynamic Modules Analysis: Markov state-transition method is used to analyze dynamic modules. G1, G2 and G7 contain HSP logic gate in their structures and the number of backup is one, the corresponded Markov state-transition figure is as Fig 7.

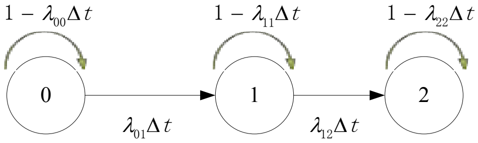

Figure 7 Markov state-transition diagram

The primary component in HSP logic gate has the same failure rate as backup in and the probability of dynamic module is:

$$PG_i(t) = 1 + e^{-2\lambda_i t} - 2e^{-\lambda_i t} \quad (3)$$

λ_i : the failure rate of the module under the HSP logic gate.

Comprehensive Analysis: R can be regarded as an independent sub-tree which takes independent sub-tree G1, G2 and G7 as bottom events. Then R can be treated as static module and converted used BDD method. Then the probability of R is:

$$P(R) = P(G1) + P(G2) + P(G7) \quad (4)$$

Calculation: with the probability of bottom events provide as TABLE V.

TABLE V PROBABILITY OF BOTTOM EVENTS

Bottom event	Probability(per hour)
Undetected error data in GPM	2.0×10^{-10}
Undetected error data in the ES of GPM	1.0×10^{-10}
Undetected error data in RDIU	1.0×10^{-6}
Undetected error data in the ES of RDIU	2.0×10^{-6}
ACS failure	1.1×10^{-5}
Cabinet failure	1.0×10^{-7}
GPM failure	3.0×10^{-5}
ARS failure	1.1×10^{-5}
RDIU failure	2.0×10^{-5}

The probability of losing integrity and availability can be gained as TABLE VI shows.

TABLE VI CALCULATION RESULTS

Loss integrity	Loss availability	Security Level	Suit to the degree of Hosted Function
6.01×10^{-6}	1.44×10^{-9}	Primary	Low necessity

Compared the results in TABLE VI with the security levels in TABLE III, it is clear that which structure is suit to the security level of Hosted Function and this will do benefits to the implementation of Hosted Function in IMA primary processing system. For example, the structure showed in this paper reaches the primary security level and it is applied to low necessity Hosted Function.

V. CONCLUSION

This paper has a deep study in IMA architecture especially the primary processing system of it. A clear structure and composition is showed. From the perspective of integrity and availability analyzed by DFTA, this paper analyses the security of IMA primary processing system, the results can be benefit to the implementation of Hosted Function in IMA primary processing system.

However, there are still lots of work should be done to expand the deeper study in the security of IMA architecture. One typical model of IMA primary processing system was enumerated in this paper, but it is not necessarily suitable for all avionics systems. The model should be changed with the system structure and the revised system should be re-analyzed. In addition, because of the restorability of system components and the software security level were discounted, the security analysis is limited in IMA primary processing system.

ACKNOWLEDGMENT

This work was supported by the project 973 (Grant No. 2014CB744904), the National Science Foundation of China (Grant No. 61179044), the Civil Aviation University of China (CAUC) Research Enabling Foundation (Grant No. 2012QD22X).

REFERENCES

[1] Christopher B Watkins, Smiths Aerospace LLC, Grand Rapids. Integrated modular avionics: Managing the allocation of shared intersystem resources [J]. 25th Digital Avionics System Conference, October 15, 2006.

[2] Jensen, David, 1 November 2005, B787 Cockpit: Boeing's Bold Move, Aviation Today.

[3] Rushby, John, December 2002, Modular Certification, NASA Contractor Report, CR-2002-212130, NASA Langley Research Center.

[4] Namjoshi, Kedar S., Richard J. Trefler, July2000, On the Completeness of Compositional Reasoning, Computer-Aided Verification, CAV 2000 Vol. 1855 of Lecture Notes in Computer Science, Chicago, IL, Springer-Verlag, pp. 139-153.

[5] Björn Annighöfer, Ernst Kleemann, Frank Thielecke. Automated Selection,Sizing ,and Mapping of Integrated Modular Avionics Modules [J]. 32nd Digital Avionics Systems Conference October 6-10, 2013, pages 2E2-1 – 2E2-14.

[6] Christopher B Watkins, Smiths Aerospace LLC, Grand Rapids. Modular Verification: Testing a Subset of Integrated Modular Avionics in Isolation [J]. 25th Digital Avionics System Conference, October 15, 2006.

[7] Zhengqiu Xie, Mingwang Wu. Analysis of Airborne Equipment and Its Key Technologies on Large Aircraft [J]. Aeronautical Manufacturing Technology, 2009(2): 48-51.

[8] Cary R.Spitzer. Digital Avionics Handbook: Avionics Development and Implementation [M].Beijing: Aviation Industry Press, 2010.

[9] Al Sheikh, Ahmad, Olivier Brun, Maxime Chéramy, and Pierre-Emmanuel Hladik, 2012. Optimal Design of Virtual Links in AFDX networks. Real-Time Systems, pages 1–29.

[10] Xiaozhe Sun, Song Han, Zongji Chen. Research on avionics system of and virtual prototype technology of civil aircraft [C]. Shanghai: Chinese Society of Aeronautics and Astronautics, 2007.

[11] Hongyan Zheng. Dynamic Fault Tree Analysis for the IMA Core Processing System of Civil Aircraft [D].Nanjing: Nanjing University of Aeronautics and Astronautics, 2013:18-48.