Safety Assessment of an Unmanned Air Vehicle Flight Control System in accordance with SAE ARP 4761

Hanseong Son[1*], Changsun Yoo[2]

[1]*Division of Software Engineering, Joongbu University, 305, Dongheon-ro, Deogyang-gu, Goyang-si, Gyeonggi-do, 10279, Republic of Korea; E-mail: hsson@joongbu.ac.kr*

[2]*Korea Aerospace Research Institute, 169-84, Gwahak-ro, Yuseong-Gu Daejeon, 34133, Republic of Korea.*

Abstracts: Certification Technologies of Small Unmanned Aircraft System (CTsUAS) is an Unmanned Air Vehicle, which is on development based on KC-100. KC-100 is a four-seater civil aircraft developed by the Korea Aerospace Industries (KAI) with the type certification of the US Federal Aviation Administration (FAA). For the type certification of CTsUAS, system safety assessment and analysis have been conducted in accordance with SAE ARP 4761. This paper presents the partial results of safety assessment of the flight control system of CTsUAS, focusing on the fault detection and recovery functions. Through the lessons from the results, additional considerations needed to support safety assessment and safety compliance determination of an unmanned aircraft system have been derived.

Keywords: Safety Assessment, Unmanned Air Vehicle, Flight Control System, SAE ARP 4761.

1. INTRODUCTION

Aircrafts shall be developed under national regulations such as Code of Federal Regulation (CFR) 14 Aeronautics and Space, Part 23-Airworthiness standards and CFR 14 Part 25-Airworthiness standards. According to CFR 14 Part 23 and Part 25, for obtaining aircraft airworthiness certification, it is required to demonstrate the safety of the equipment, systems, and installation, therefore, to perform a safety assessment of the aircraft. Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761 offers the guidelines and methods for conducting the safety assessment [1]. In the United States, SAE ARP 4761, in conjunction with SAE ARP 4754, is used to determine if an airplane development comply with CFR 14 Part 25.1309. This compliance demonstration is harmonized with international airworthiness regulations such as European Aviation Safety Agency (EASA) CS-25.1309.

This paper presents the partial results of safety assessment of the flight control system of Certification Technologies of Small Unmanned Aircraft System (CTsUAS) [2], focusing on the fault detection and recovery functions. CTsUAS is an Unmanned Air Vehicle, which is on development based on KC-100. KC-100 is a four-seater civil aircraft developed by the Korea Aerospace Industries (KAI) with the type certification of the Federal Aviation Administration (FAA). For the type certification of CTsUAS, system safety assessment and analysis have been conducted in accordance with SAE ARP 4761. Although the intent of ARP 4761 is to support the safety assessment of civil manned aircraft systems, it may also support the safety assessment and safety compliance determination of unmanned aircraft systems. Due to the differences between manned aircraft systems and unmanned aircraft systems, the safety assessment and safety compliance determination of unmanned aircraft systems may require certain additional considerations to be addressed. This paper presents the additional considerations through the partial results of safety assessment of the flight control system of CTsUAS.

2. Safety Assessment Process

Figure 1 shows the safety assessment process of ARP 4761. This iterative process is composed of Aircraft FHA (Functional Hazard Assessment), System FHA, PSSA (Preliminary System Safety Assessment), SSA (System Safety Assessment) and CCA (Common Cause Analyses) first at Aircraft level, then at system level.

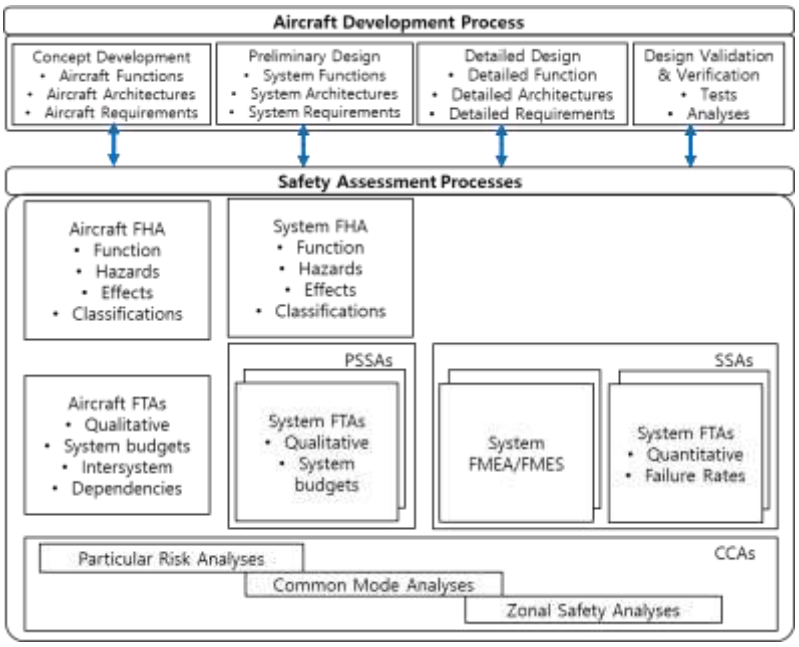


Figure 1. Safety assessment process of ARP 4761, quoted from [1]

The safety assessment of CTsUAS has been performed following this process. For the Aircraft FHA, Qualitative assessment of the basic functions of the CTsUAS has been performed to identify and classify the failure conditions leading to hazard, according to their severity. For the System FHA, Qualitative assessment has been performed to identify and classify the failures, or combination of system failures, that affect an aircraft function leading to hazard, according to their severity. For the PSSA, the analysis to complete the failure conditions list and the corresponding safety requirements from FHA has been performed. It is also used to demonstrate how the system meets the qualitative and quantitative requirements for the various hazards identified. For the SSA, Quantitative analyses of critical failures conditions, defined in System PSSA, have been performed to show that relevant safety requirements are met and to verify that the implemented design meets both the qualitative and quantitative safety requirements, as defined in the FHA and PSSA. CCA identifies individual failure modes or external events which can lead to a catastrophic or hazardous/severe-major failure condition. It consists of three separated analyses: 1) The Particular Risk Analysis (PRA) looks for external events which can create a hazard 2) The Zonal Safety Analysis (ZSA) looks at each compartment on the aircraft and looks for hazards that can affect every component in that compartment. 3) The Common Mode Analysis (CMA) looks at the redundant critical components to find failure modes which can cause all to fail at about the same time.

3. Safety Assessment Results of CTsUAS FCS

CTsUAS has Flight Control System (FCS), where the flight control computer connects electrical wires to the entire system of the aircraft, controlling it instead of the pilot and implementing the fly-by-wire design. To present the other partial results of safety assessment of the flight control system of CTsUAS, several Reliability Block Diagrams (RBDs) are offered with the corresponding results in this paper. Figure 2 shows the RBD of FCS. All the blocks in the RBD are linked in a serial manner.

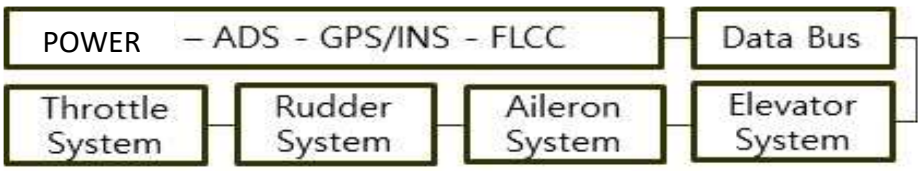


Figure 2. Reliability Block Diagram of FCS

Figure 3 shows the RBD of POWER, ADS, GPS/INS, FLCC, and Data Bus subsystems, which corresponds to the upper part of Figure 2.

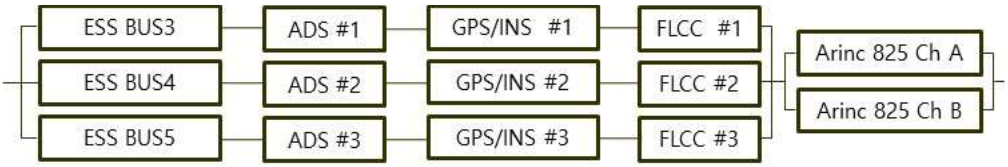


Figure 3. Reliability Block Diagram of POWER, ADS, GPS/INS, FLCC, Data Bus Subsystems

In PHA, the safety objective for the failure condition “Total Loss of Primary Flight Control” is set to be 1.4E-6 /flight hour. To meet this safety objective, fault detection capabilities such as sensor voting of FLCC, CRC of Arinc 825 are adopted. FDAL/IDAL Level B is also required.

Figure 4 shows the RBD of actuator (sub) systems, which corresponds to the lower part of Figure 2.

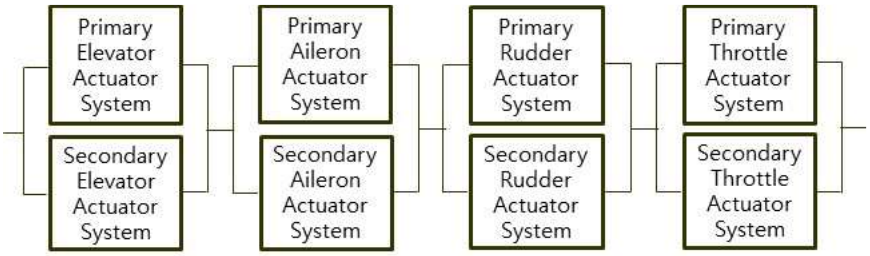


Figure 4. Reliability Block Diagram of Actuator Systems

In PHA, the safety objective for the failure condition “Total loss of control” is set to be 4.8E-7 / flight hour. To meet this safety objective, built-in test (BIT) of FLCC as fault detection capability is adopted. FDAL/IDAL Level B is also required.

As mentioned above, for ensuring the safety and reliability of FCS, FCS adopts redundancy design and fault detection capability. These are as shown in Figure 5. However, redundancy design and fault detection capability make it difficult to model and quantify the Fault Tree (FT), which are essential for PSSA and SSA.

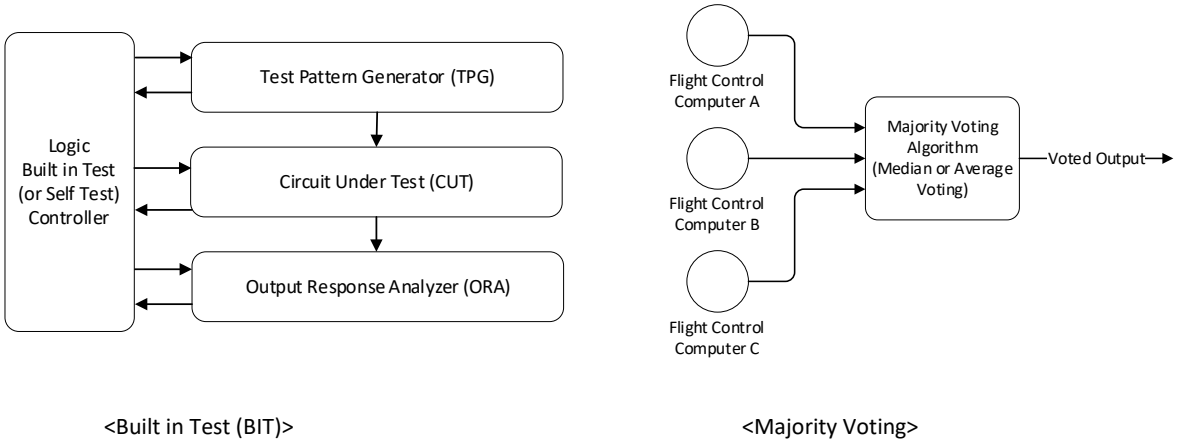


Figure 5. Fault detection capability and redundancy design of FCS [3]

A built-in test (BIT) or built-in self-test (BIST) is a mechanism that permits a machine to test itself. It has the advantages like lower cost due to elimination of external tester, in-system, at-system, high-quality testing, faster fault detection, and ease of diagnosis. It also reduces maintenance and repair costs at system level. According to ARP 4761, fault detection can be carried out using a dedicated hardware circuit, software code, or various test methods, which is referred to as a “monitor” in this paper. For the FT modelling, a subtle assumption is typically made that the monitor provides 100% failure detection coverage of the item performing the function. Figure 6 shows an example of FT model with a monitor. Depending on the ratio of fault detection (90% in this model), the failure rate of Function ‘X’ can be simply applied. However, this simplified FT provides a conservative result because the left branch of the tree does not consider the required failure order between monitor and function failures in the same flight.

Majority voting in Figure 5 describes the voting algorithm technique in a triplex system [4]. In a triple redundancy system, if more than 2 channels of 3 channels cannot be used, fault detection fails. Therefore, if more than 2 channels cannot be used, it is critical failure combination [5]. In this case, however, it is difficult to simply calculate the fault detection ratio and modeling of voting logic using FT is impossible.

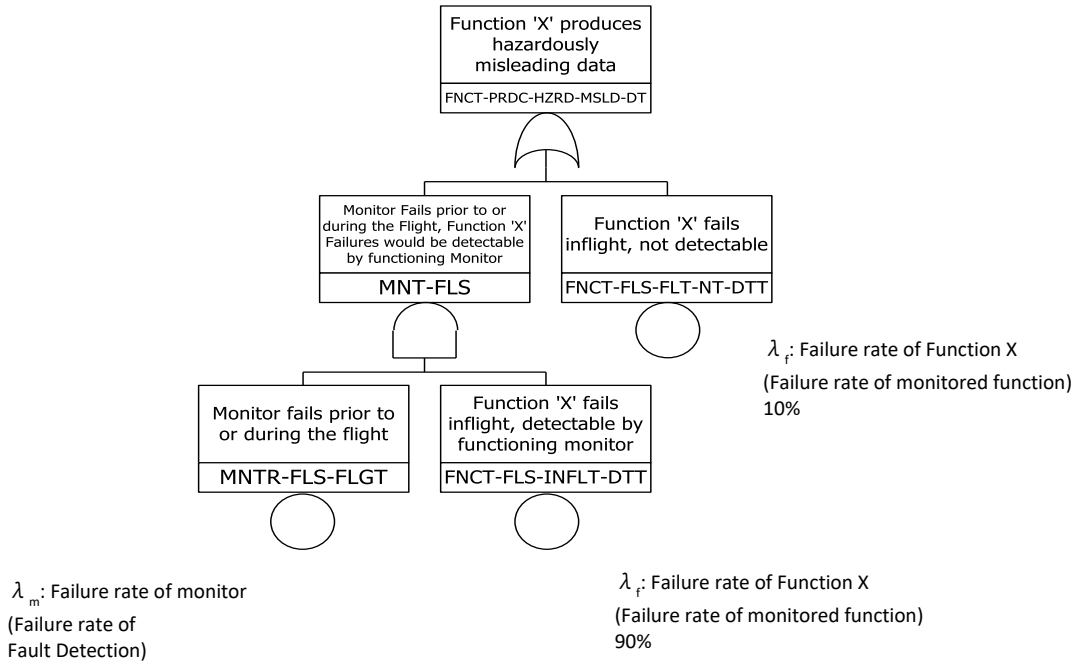
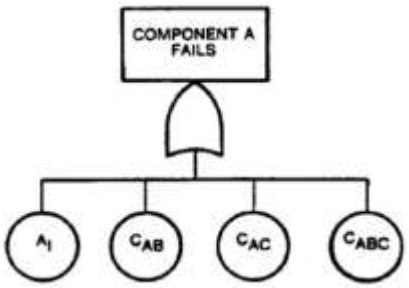


Figure 6. An example of FT model with a monitor, quoted from [1]

To deal with this issue effectively, the Common Cause Failure (CCF) modeling technique, which is popularly used in the nuclear power plant safety analysis, is applied [6]. CCF is an event in which one or more components fail at the same time or at a similar time due to a common cause. With the CCF method, it is possible to estimate probability parameters and perform modeling using the estimated parameter probability. For the parameter estimation, Basic Parameter, Beta-factor, Alpha-factor, C-factor, Multiple Greek Letter (MGL), Binominal Failure Rate (BFR), Multinomial Failure Rate (MFR) methods are used. As for the CCF FT modeling, when there are the same type of components A, B, C in a system, independent failures, common cause failures involving two component, and common cause failures involving all three component failures are modeled as shown in Figure 7.



*A_I: Independent Failure

C_{AB}: CCF of Component A, B

C_{AC}: CCF of Component A, C

C_{ABC}: CCF of Component A, B, C

Component A fails: $A_I + C_{AB} + C_{AC} + C_{ABC}$

Figure 7. An example of CCF FT model, quoted from [6]

Considering all the above-mentioned issues as well as the design of FCS, PSSA and SSA are performed using various FT models. Figure 8 shows one model of them, which corresponds to the failure condition “Total Loss of Flight Control Computer Channel”. The left branch of the tree is the tree applying CCF modeling and the middle branch of the tree is the tree for BIT.

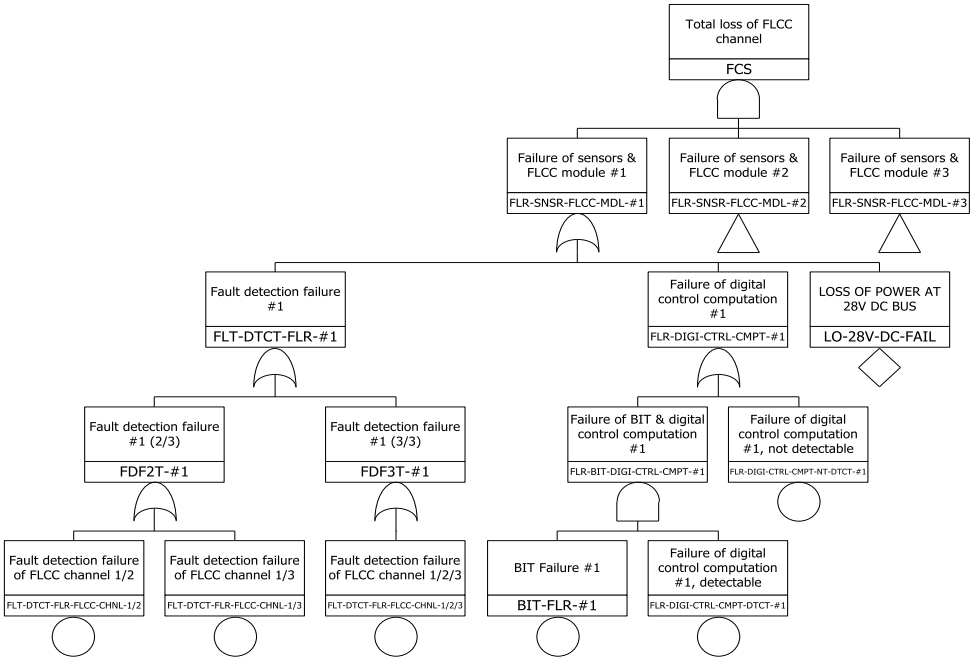


Figure 8. FT for the failure condition “Total Loss of Flight Control Computer Channel”

From the safety assessment of FCS, various recommendations for design improvement have been derived. Some of the recommendations are as follows:

– Dissimilar redundancy for sensors and Flight Control Computer (FLCC)

– Data Bus between sensors and FLCC

– Improved sensor Mean Time Between Failures (MTBF)

– Improved BIT capability

– Dual control surfaces

– Jamming factor minimization and control actuator hard-over minimization

CONCLUSIONS

This paper presents the partial results of safety assessment of the flight control system of CTsUAS. The safety assessment of CTsUAS has been performed following the process recommended by SAE ARP 4761. Through the lessons from the safety assessment results, additional considerations needed for SAE ARP 4761 to equally support safety assessment and safety compliance determination of an unmanned aircraft system have been derived as follows:

– Different criteria definition for safety objectives,

– Different emergency conditions,

– Failure condition effects on mission, third parties on the ground or on other systems in the air or on the ground,

– Complexity of the system due to redundancy design and fault detection capability, etc.

ACKNOWLEDGEMENT

This work was supported by ‘Development of Certification Technology for Small Unmanned Aerial Vehicle Systems (RS2019-KA151724)’ Program through the Korea Agency for Infrastructure Technology Advancement (KAIA), funded by the Ministry of Land, Infrastructure and Transport (MOLIT).

REFERENCES

[1] SAE ARP 4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE; 2010.

[2] Korea Aerospace Research Institute (KARI). CTsUA Operate Requirement Document (ORD). CTsUA-KARI-DS-004v1.3; 2010.

[3] Mohammad MM, Arash K. Software-Based Self-Testing for AES Crypto-chips. [January 2014]: Available from: https://www.researchgate.net/publication/262933308

[4] Jongmin A. Comparative Analysis of Voting Algorithm for Redundant Flight Control System. J KS Aero Space Sci November 2006; p.321-24.

[5] Weiting H, Xueyun W, Kun Q, Jie Z, Wenjun H, Architecture design and safety research of a double-triple-channel redundant and fault-tolerant system, J Loss Prev Proc Ind November 2016; 44; p. 495-502.

[6] Kang HG, Jang SC, Eom HS, Ha JJ. The Common Cause Failure Probability Analysis on the Hardware of the Digital Protection System in Korean Standard Nuclear Power Plant, KAERI/TR-2908; 2005.

[7] Jam, F. A., Singh, S. K. G., Ng, B., & Aziz, N. (2016). Interactive effects of Gender and Leadership Styles on Open Service Innovation: A Study of Malaysian Doctors, International Journal of Economics Research, 13(3), 1287-1304.

[8] Jam, F. A., Haq, I. U., & Fatima, T. (2012). Phychological contract and job outcomes: Mediating role of affective commitment. Journal of Educational and Social Research, 2(4), 79-79.

[9] Kahn, M.R., Ziaulldin, K., Jam, F.A., Ramay, M.I. (2010). The Impacts of Organizational Commitment on Employee Job Performance, European Journal of Social Sciences – Volume 15, Number 3 (pp. 292-298).

DOI: https://doi.org/10.15379/ijmst.v10i3.1638