11º Workshop em Engenharia e Tecnologia Espaciais
18, 19 e 20 de agosto de 2020

Definition of a Process to Minimize the Occurrence of Design Errors During the Development of Complex Systems for Small Satellites

Douglas Hiroyuki Washio[1], Marcelo Lopes de Oliveira e Souza[2]

Instituto Nacional de Pesquisas Espaciais, São José dos Campos, SP, Brasil

[1] Aluno de Mestrado do Curso de Engenharia e Tecnologia Espaciais/Opção Engenharia e Gerenciamento de Sistemas Espaciais – ETE/CSE

[2]Professor Doutor do Curso de Engenharia e Tecnologia Espaciais/Opção Engenharia e Gerenciamento de Sistemas Espaciais – ETE/CSE

douglas.washio@inpe.br

Abstract. *The increased level of complexity and integration of the systems in the aeropsace industry over the years increased also the potential of occurrence of errors during the development of such systems. The simple fact that those errors are not easily indentified, predicted and quantifiable (for example, the occurrence of such error may depend on a combination of factors like system operation and environmental conditions) turns it into an unfeasible or even impossible task to assure the complete coverage of all possible failure modes introduced in the system during its development phase: requirements definition, implementation and integration. In that sense, the present paper intends to propose a systematic process for mitigation of those design errors for complex systems of small satellites.*

Keywords: Process; Design Error; Complex Systems; Small Satellites.

1. Introduction

1.1 Complex and Highly Integrated Systems

Over the years, satellites and airplanes have been sharing the same challenge: the increased utilization of complex and highly integrated systems. The challenge does not reside in the fact that those systems became more complex and integrated over the years, turning the aerospace industry in the “state of the art” in terms of development of complex systems.

The increased computational capacity over the years allowed the development of systems that can acquire, process thousands of inputs and provide the correct response nearly on real time. This, with an availability and reliability that is only possible due to the employment of newer technologies in many areas like materials (with better electric properties) and electronic components manufacturing process.

1.2 Design Errors

However, all those benefits mentioned above come with a price. The price being paid by the aerospace industry is the fact that the introduction of those complex and highly integrated systems in its platforms "opened a door" to an uncountable number of errors that may be introduced in the system during its developments phases. And, in the end, those Design Errors will affect the system normal operation and may affect also its maintainability, availability, safety and integrity. Due to the inherent complexity and integration of those systems, it is not feasible (or even possible) to quantify all the possible failure modes that can be introduced in the system. In other words, it is not possible to create a finite number of tests that can reproduce all the possible combination of failures introduced during the development of the system.

1.3Airworthiness Regulation for Civil Aircrafts concerning Design Errors

Concerning the compliance with airworthiness requirements for Civil Aircraft Certification process, and as highlighted by [NETO, SOUSA, SOUZA 2009] the Federal Aviation Regulations (FAR) Chapter 25 (FAA and EASA) is dedicated to airworthiness standards for transport category airplanes. Included in this chapter, the § 25.1309 has the most important requirements regarding the safety aspects of a system design. The Advisory Circular (AC) of the § 25.1309, which describes the acceptable means for showing compliance with FAR § 25.1309, explicitly states in Section b of such AC that the airplane systems must be designed so that a catastrophic failure does not result from a single failure. To comply with this requirement the AC asks in Section 9b (1)(iii) to account for "the possibility of requirement, design and implementation errors".

1.3 Mitigation of Design Errors

[NETO, SOUSA, SOUZA 2009] developed a discussion applying hardware dissimilarity as one way to mitigate the occurrence of design errors for a flight controls system application.

Concerning requirements and software aspects, [REGINATO 2012] explained that around 13.1% of failures in a design may be attributed to incomplete requirements.

Establishing a development assurance process as presented in [SAE 2010] is another way to demonstrate that the development of a system is conducted aiming to limit the likelihood of development errors. Figure 1 outlines the relationships between the various development documents, which provide guidelines for safety assessment, electronic hardware and software life-cycle processes and the system development process.

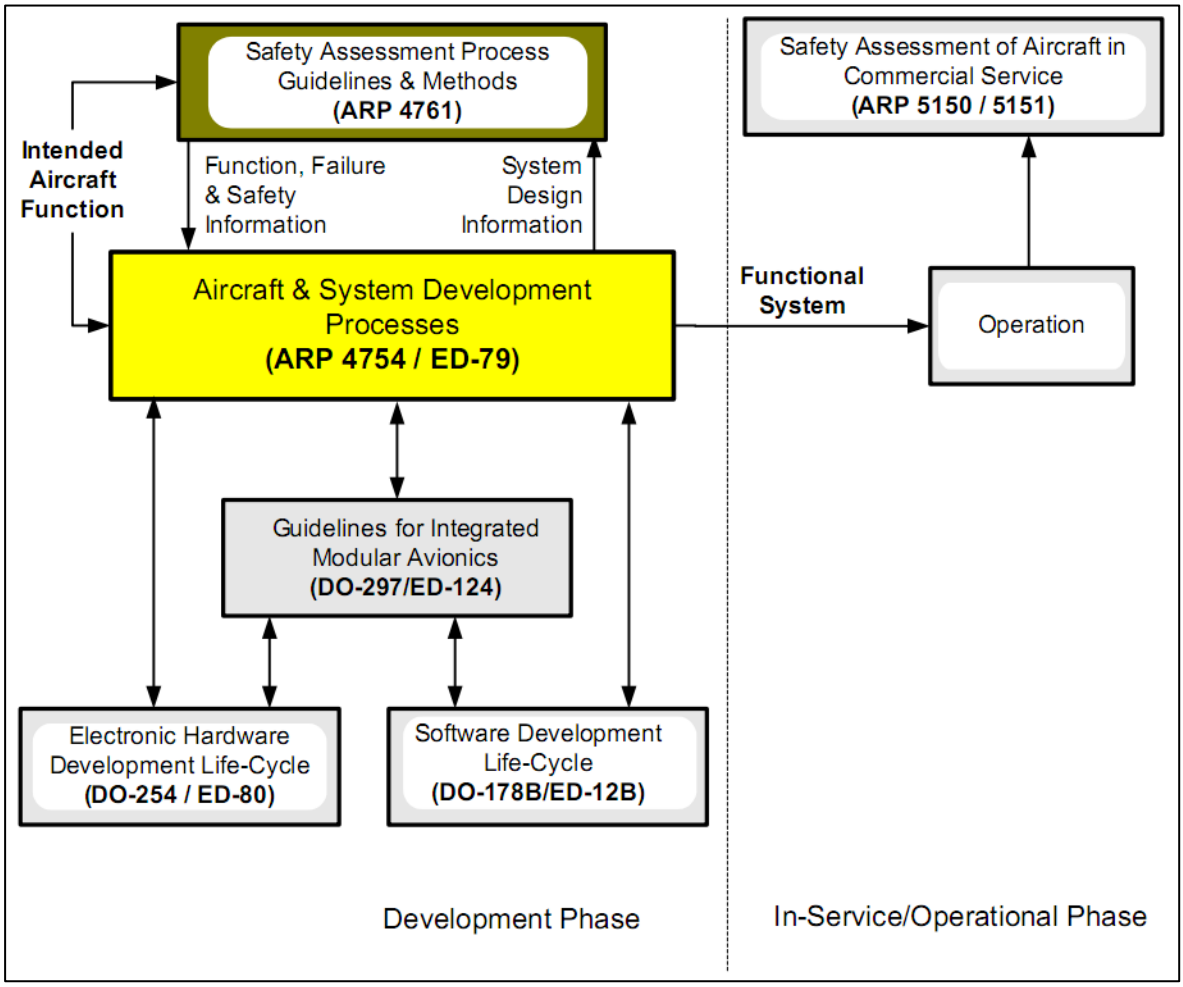

Figure 1 - Relationship between development documents used for development of system that implement aircraft functions [SAE 2010].

2. Methodology

This paper is part of the Dissertation under development from Author #1 under orientation of Author #2, which has the following objectives:

1) To present a revision of the references in the aerospace industry that focus on minimizing the occurrence of the design errors during the development of complex systems;

2) To compare the process already existent at INPE concerning the mitigation of Design Erros during the development of complex systems for small satellites;

3) To propose a systematic process to be applied during the development of complex systems of small satellites at INPE.

In this paper it is presented part of item 1.

3. Results and Discussion

Using the proposed methodology, the expected results for the Dissertation is to collect all the standard practices already used by the aerospace industry and propose a process that can be used by the INPE during the development of complex systems for small satellites with the objective to minimize the occurrence of design errors.

4. Conclusion

One way to bring the system to an acceptable level of safety, integrity and availability is to assure a process that would mitigate the introduction of errors during the development of the systems. Therefore, the intent of the Dissertation will be to gather what the aerospace industry has been doing so far and define a process to be followed during the development of complex systems of small sattelites at INPE.

References

Neto, H. M., Sousa, G. B., Souza, M. L. O. (2009) "Use of Dissimilar Hardware Architecture to Mitigate Design Errors in a Flight Control System Application"

Reginato, J. P. M. (2012) "Uma proposta de aperfeiçoamento de um processo de gerenciamento de requisitos de sistema e de software e sua aplicação a sistemas espaciais e aeronáuticos embarcados"

Federal aviation administration (FAA), Advisory circular 20-115d. USA, 1993

Federal aviation administration (FAA), Advisory circular 20-152. USA, 2005

Federal aviation administration (FAA), Advisory circular 20-174. USA, 2005

RTCA, Inc., Document No. RTCA/DO-178, Software Considerations in Airbone Systems and Equipment Certification. RTCA DO178, Washington, D.C., USA, 2011

RTCA, Inc., Document No. RTCA/DO-254/EUROCAE ED80, Design Assurance Guidance for Airborne Electronic Hardware. RTCA DO254, Washington, D.C., USA, 2000

RTCA, Inc., Document No. RTCA/DO-160/EUROCAE ED14G, Environmental Conditions and Test Procedures for Airbone Equipment. RTCA DO160, Washington, D.C., USA, 2010

SAE Aerospace, Document No. ARP4754 Revision A, 2010