The platform architecture of systems safety design and management for Civil Aircrafts

Zhang Junyi

Beijing Aeronautical Science & Technology Research Institute of COMAC, Future Science and Technology Park, Beijing, China

hope_zhang@163.com

Keywords: Civil Aircrafts; Airworthiness Certification; Systems Safety;

Abstract: In order to meet CCAR/FAR/CS 25.1309 airworthiness requirements, commercial airplane safety design and management platform has been established, combined with the COMAC new plane development procedures. In areas of development processes management, life cycle configuration management and security quantitative analysis, this engineering method will provide aircraft systems security analysis and assessment, airworthiness work flow management and technical support and guarantee, to initiate research and development in this field in China, and to improve China's commercial airplane airworthiness certification work.

1. Introduction

The establishment of COMAC in 2008 indicates that the development of civil aircraft in China has entered a new era. China's civil aircraft industry has fully entered the global standard development system and will face competitions from international companies on the international market. Chinese civil aircraft design must meet the airworthiness regulations of American FAR and European CS requirements and their safety and reliability must be at or close to the international level. To be successful, airworthiness certifications are essential, and customer service and product support system of international standards must be established. Without their safety and reliability of high standards, it is impossible for the aircraft to survive and further develop on the market.

Therefore, on the top-level design stage of Chinese commercial airplanes, especially during the assessment stage of background model, it is needed to establish standard and general guidelines for civil aircraft systems safety work, to provide theoretical guidance and technical support for the follow-up safety work, in order to improve the design and safety of civil aircrafts. The system planning and management processes must be carried out in analysis and assessment of systems security design, and throughout the full aircraft development process. The relevant system security requirements will be put forward in the aircraft conceptual design stage and provide guidance and assessment of the design process, and then the aircraft design enters into re-design and re-assessment iterations till the improved design can finally meet the safety requirements. However, in the areas of the design and management of aircraft systems security, there is still a lack of systematic and engineering methods.

The prime commercial airplane manufacturers in Europe and America have built their own security analysis platform [1-2] on the basis of accumulating many years' experience. A practical and efficient security system has been established using the security analysis platform and it effectively solves the problems arised from complicated interfaces and intensive iterations in safety analysis work, greatly reduced manpower, time and cost, greatly improved the safety analysis. Therefore, the development of civil aircraft system safety design and assessment software platform, and proper management and guidance in relevant co-workers, are essential engineering methods to achive real-time sharing of civil aircraft safety related information and working process control.

Safety is the key and the most important requirement for civil aircrafts and it is the primary principle of civil aircraft for all aircraft manufacturers to follow. CCAR25.1309[3] is the airworthiness regulation for our country's transport type aircraft equipment, system and installation, mainly based on the relevant standards issued by FAA. In CCAR25.1309, systems, equipments, and installations in various expected operating conditions must perform their assigned functions, and the provisions of the probability of failure state should comply with the principle of the reverse relation with the degree of harm to the aircraft and passengers in the failure state. This is the minimum requirement for the safety of transport aircraft system / equipment. Among them, the CCAR25.1309 clause (a) is the overall requirement on the system. The provisions of CCAR2.1309 (b) are requirements on aircraft systems and related components design, further defining the permissible probability of failure in terms of security at various degrees of damage and failure. The CCAR2.1309 clause (c) provides requirements for aircraft monitoring and warning devices. In CCAR25.1309 (d), inverse relationships between the probability of each failure mode and the severity of the event are to be verified as reasonable and acceptable using analysis, and if necessary, by appropriate ground, flight or flight simulator tests. CCAR25.1309 terms (e), (f), (g) are requirements on systems, mainly involving systems and equipment energy requirements.

At the same time, in the development of international civil aviation industry, a series of guidelines has been established, such as: “Certification Considerations for Highly Integrated or Complex Aircraft Systems (SAE ARP4754A" (in [4]), " Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. (SAE ARP4761)" [5], derived from the Advisory circular AC 25.1309 of the guidance documents on airworthiness safety design, analysis and assessment.

In recent years of systems development, requirements and objectives for software development (Ref. [6]) and electronic hardware development (Ref. [7]) are airworthiness requirements that also must be met in the safety design and analysis of international civil aircraft softwares and airborne electronic hardwares. At present, SAE ARP4761, SAE ARP4754, RTCA DO-254, RTCA DO-178B, RTCA DO-297 (integrated avionics module design guidance and assurance considerations) have formed a standard system of safety analysis for modern civil aircraft systems, see figure 1.

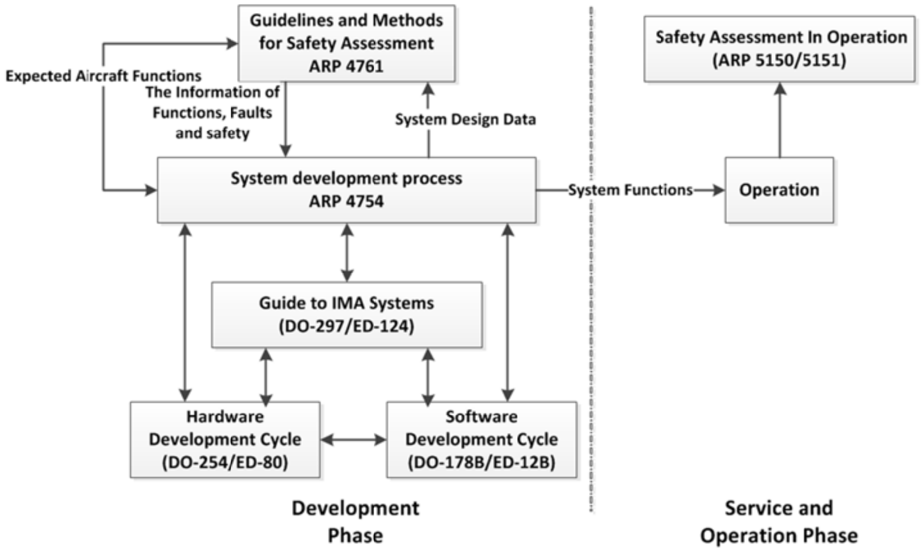
Guidelines and Methods for Safety Assessment ARP 4761
Safety Assessment In Operation (ARP 5150/5151)
Expected Aircraft Functions
The Information of Functions, Faults and safety
System Design Data
System development process ARP 4754
System Functions
Operation
Guide to IMA Systems (DO-297/ED-124)
Hardware Development Cycle (DO-254/ED-80)
Software Development Cycle (DO-178B/ED-12B)
Development Phase
Service and Operation Phase

Figure 1. The Standard of System Safety Analysis in Modern Civil Aircraft.

2. Requirements

2.1. Process management

Civil aircraft safety design assessments are carried out throughout the entire development cycle of civil aircraft. It is to ensure that systems design can meet the safety requirements, from the establishment of requirements and goals for the safety design in the stage of project demonstration and concept design, to the design verification stage including a number of iterations in the analysis and modification of preliminary and detailed designs. Corresponding overall to the development procedures of civil aircraft, safety design assessment procedures consist of three stages: functional hazard assessment (FHA), preliminary system safety assessment (PSSA), and system safety assessment (SSA) . In the entire development stage, the applicant must carry out safety assessments to ensure that systems and their functions meet their requirements, taking into consideration of all failure modes for all systems, in order to reach the goal to ensure an acceptable level of safety for the whole aircraft.

As shown in Figure 2, the safety platform takes process control as the core, and realizes the management of the whole safety design, analysis and assessment. It can flexibly customize safety related workflows in the software platform, including: data flow (submission of experimental data and documents), customization of control flow (approval processes, etc.) and interfaces, etc.

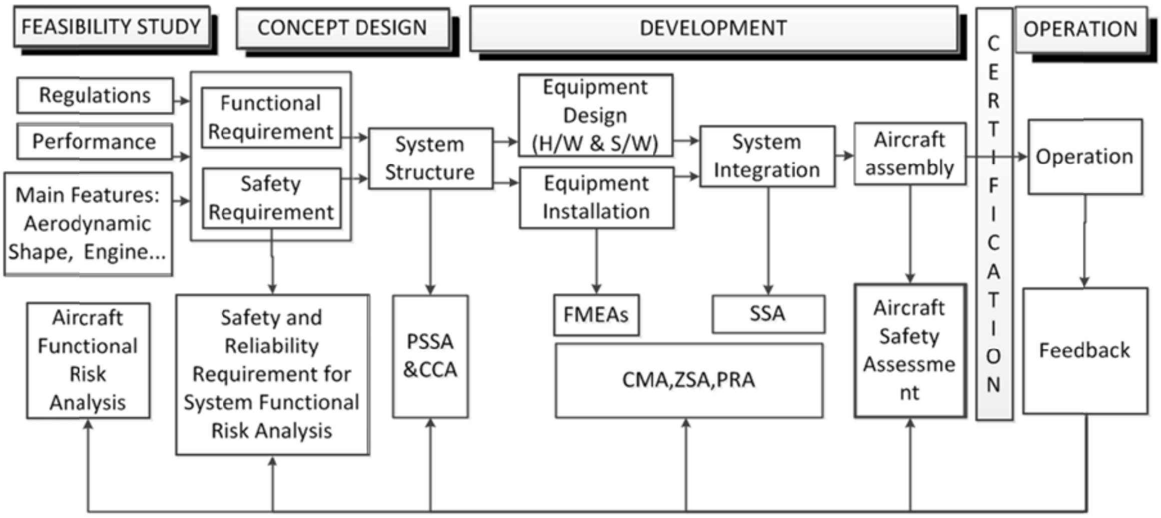

Figure 2. Safety Work Flow in Aircraft Development Phase.

2.1.1. Functional hazard assessment (FHA)

The FHA module features include:

1. Design and establishment of related database tables
2. FHA related data definition function
   - Definition of the system functions, including internal functions and cross-linking functions
   - Definition of targets of the aircraft and systems, and customer requirements
   - Definition of aircraft or system flight profile or task stage
   - Definition and management of failure probability
   - Definition of failure consequences, such as the impact on the aircraft, crew and passengers
   - Classification definition of failure state consequences, such as disaster, hazard, severe, mild, safe
3. FHA related data editing
   - The list of editing and management functions
   - The identification and description of the failure states of the system functions, including single failure and multiple failures
   - The list of editing and management of failure states
4. FHA related data cross-linking and mapping, document management of support materials, such as analysis, research, flight testing used in the determination of the impact and classification of failure states.

2.1.2. Preliminary system safety assessment PSSA& system safety assessment SSA

The development of the PSSA and SSA functional modules requires process control, specific planning as follows:

1. design and establishment of relative database tables
2. PSSA workflow control module

3. SSA workflow control module
4.cross-linking of PSSA, SSA data and other modules data

2.1.3. CCA

Common cause analysis (CCA) is composed of three software functional modules, namely regional safety analysis ZSA, specific risk analysis PRA and common mode analysis CMA.

1. regional safety analysis ZSA data tables
2. regional safety analysis ZSA modules
   - Definition of aircraft regions
   - Definition of the list of components in aircraft regions
   - Lead-in parts FMEA/FMES or equivalent results
   - Preparation of list of external failure modes of components
   - Preparation of design criteria and installation specifications
   - The failure effect analysis of region and cross linking system
   - The analysis of the regional conformity to design criteria
   - The analysis of the functional areas of the aircraft or the failure influence
   - The analysis of regional corrective measures
3. specific risk analysis PRA data sheet
4. specific risk analysis PRA module
   - Definition of aircraft specific risks
   - Definition of the failure model of specific risks
   - The analysis of specific risk regions
   - The analysis of specific risk affected systems / components
   - The analysis of the design in specific risks and installation of specific risk prevention measures
   - The assessment of consequences of specific risks to the affected components
   - The assessment of consequences of specific risks on the aircraft
   - The analysis of the specific risks to the airworthiness compliance
5. common mode analysis CMA data tables
6. common mode analysis CMA module
   - Definition of the Analysis objects
   - Definition of types of common modes
   - Definition of sources of common modes
   - The definition of common mode failure / error
   - The analysis and verification in accordance with the independence criterion
   - The determination of common mode failure / error data model
   - The calculation of common mode failure / error failure rates
   - The analysis of common mode failure on Airworthiness compliance

2.2. Configuration management

Configuration determines all the aircraft data through configuration control, including aircraft structural information, geometric information, process information, analysis results, technical specifications and test results, etc. Configuration management is the technical status management of engineering projects, that is, an engineering project contains multiple configurations. Each configuration is a technical state in the aircraft development phase, that is, sub engineering projects. For each configuration, including the aircraft's technical status, structural status and work status (for working condition monitoring), the safety platform for aircraft configuration management mainly includes:

1. grasp and establish the overall structure of aircraft from the macro perspective;
2. implement the aircraft configuration management rules, to enhance the aircraft configuration (TC configuration, single configuration, test subjects configuration) control methods, ensure the aircraft product data integrity and consistency, and record and report the progress of modification, record whole process of the implementation of modifications;

3. establish a complete history of modifications in the aircraft development phase, carry out effective version management and control, maintain all valid versions of the data, and ensure the complete technical description of the aircraft at all stages;
4. control, check, and adjust deviations between configurations at delivery and after the actual production.

2.3. Calculation and analysis

2.3.1. Safety probability computation

The method of fault tree analysis is a mature quantitative analysis method. But the safety probability calculation in safety system of civil aircraft and fault tree analysis in the classic calculation method are significantly different. The former in the treatment of concealed fault must be combined with the typical flight parameters and flight mission profile, and take into consideration of the aircraft maintenance time and task characteristics, otherwise it will get the results lower than those under actual situation and will show a "false" result that it meets the safety target. Therefore, it is necessary to establish specific analysis calculation models and convenient engineering means in order to solve problems in the safety probability calculation for safety analysis of civil aircraft systems.

The FTA module features include:

- The definition and editing of the top event, namely the aircraft level or system level failure state
- The definition and editing of intermediate events, namely fault tree logic gate
- Define and edit the bottom events, namely basic events or aircraft systems
- Define and edit the flight profile or task stage
- define and edit event risk time or exposure time
- The fault tree modelling
- The basic event failure rate calculation
- The minimum cut set calculation
- The top event failure rate
- Calculation of the important degree
- The sensitivity analysis

2.3.2. Failure modes and their impact analysis / summarization methods (FMEA/FMES)

It is necessary to establish general FMEA work tables for prime civil aircraft manufacturers and suppliers in China, combined with requirements on FMEA from system safety analysis of civil aircraft and airborne equipment, and maintenance work, as well as special requirements on FMEA from C919, together using ARJ21-700 FMEA/FMES experience. In them, FMEA work requirements will be defined for civil aircraft manufacturers and suppliers, as well as corresponding in-depth relationships between FMES and the relevant fault tree.

Failure mode impact analysis / aggregation FMEA/FMES module functions include:

- The establishment of aircraft level and system level unit components of the agreed level
- The definition of product function and function code
- The definition of function or component failure mode
- definition of failure rate of product at the lowest agreed level
- definition of function or component failure mode frequency ratio
- definition of function or component failure mode effect probability
- definition of product flight profile or working time of task stage
- analysis of causes of function or component failure
- analysis influence of function or component failure
- analysis detection method of function or component failure
- calculation of failure rate of the product or the failure mode
- calculation of severity of the product or the failure mode
- calculation of hazard of the product or the failure Mode

3. Software architecture requirements

The project management and data management framework need to be built on the software platform to facilitate subsequent functionality and data integration.

1. Project Management

The objects of project management include: engineering projects, configuration management, work flow, user authority, analysis tools and work interface.

The initial construction of project management, first of all, is to establish new projects, basic information editing, preservation and closing, at the same time, support for new construction, editing, and preservation of configurations.

2. Data Management

Data management in aircraft system safety analysis software platform is for use in the implementation of civil aircraft safety analysis system work to ensure the consistency of data, and data sharing, data storage and data management.

Aircraft system safety analysis software platform of data management should have the following functions:

- database management
- product tree management
- import data
- export data
- document management

A preliminary construction of data management is first implemented:

- establishment of database, realize the connection with the database platform;
- establishment of database tables for engineering projects and configuration management.

4. Conclusion

With China's ARJ21 project and C919 project started and combined with experience and lessons learnt in their safety design, it is proposed to establish a safety analysis software platform based on the safety analysis technology developed to effectively solve problems in areas of safety analysis, system development process management, safety work interface relations, etc., to improve China's civil aircraft airworthiness certification work.

References

[1] David A.Burke, Charles E.Hall Jr. System Level Airworthiness Tool (SLAT) [C].48th AIAA Aerospace Science Meeting Including the New Horizons Forum and Aerospace Exposition,2010.

[2] John C. Dalton. Advances in Safety Assessment in New Airplane Design [J]. American Institute of Aeronautics and Astronautics, Inc., 1998.

[3] Title 14 of the Code of Federal Regulations. Federal Aviation Regulations (FAR) Part 25.

[4] ARP 4754. Certification Considerations for Highly Integrated or Complex Aircraft Systems.

[5] ARP 4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

[6] RTCA DO-178B/EURO ED-12B. Software Considerations in Airborne Systems and Equipment Certification[S].Washington D C: RTCA Inc. 2003.

[7] RTCA DO-254/EUROCAE ED-80. Design Assurance Guidance for Airborne Electronic Hardware[S]. Washington D C：RTCA Inc. 2000.