ICAS 2021 SHANGHAI
32nd Congress of the International Council of the Aeronautical Sciences

Research on Functional Hazard Assessment Technology of Military Aircraft

Quan Li[1], Yan An[1]

[1] AVIC XI'AN AIRCRAFT INDUSTRY GROUP COMPANY LTD.

Abstract

The process of analyzing the security of the military aircraft is studied using civil aviation security analysis method, based on military aircraft safety evaluation project as the background, the domestic as well as abroad existing research results for reference. Emphasis should be placed on the research of aircraft functional hazard assessment technology, including systematically and comprehensively inspecting aircraft functions, identifying functional failure states, evaluating the impact consequences of failure, determining the impact levels, establishing the safety design baseline, in order to provide guarantees for carrying out safety design verification.

Keywords: Safety; FHA; functional failure

1. Introduction

Safety is one of the important quality characteristics for aeronautical weapons and equipment to form sustainable combat effectiveness. Safety analysis and evaluation is an important process to realize the requirements of equipment safety indexes and to evaluate and control safety risks. Once the safety accident occurs in the mission, the loss caused is inestimable. Therefore, how to guarantee the safety of military aviation equipment is one of the key points in the research and development of military aviation equipment. GJB 900A General Requirements for Equipment Safety Work puts forward the goal of safety work is to "identify, eliminate or reduce risks by planning and implementing a series of management, design and analysis, verification and evaluation with engineering methods, techniques and professional knowledge". In order to achieve this goal, a series of safety analysis methods should be adopted in the design process of the aircraft to ensure the conformity of the product to the safety work objective.

In order to meet the safety requirements, the most fundamental way is to carry out safety engineering design and analysis comprehensively and systematically in the development process. Since the traditional safety analysis technology does not study the safety problem as a system engineering problem, there is a lack of systematic analysis method for the aircraft safety analysis from the aircraft to the system, and then to the hardware and software design. For safety design, analysis and evaluation, a theoretical system has been formed by developed countries composed of four modules: Aircraft/System Functional Hazard Assessment (AFHA/SFHA), Primary Aircraft/System Safety Assessment (PASA/PSSA), Aircraft/System Safety Assessment (ASA/SSA) and Common Cause Analysis (CCA). SAEARP4761, SAEARP4754 and a series of guidance is compiled. Based on the current military aircraft safety analysis and assessment project, this paper studies the safety analysis process of aviation equipment and focuses on the functional risk assessment technology of the whole aircraft by referring to the existing domestic and foreign research results and adopting the safety analysis method of civil aircraft.

Footers, except for the first page, contain the page number, centered.

2. Safety Assessment Procedure

Safety assessment is an indispensable part in the development of aircraft system, which runs through the whole development cycle. According to the process of aircraft design and implementation, it can be divided into two stages: from top to bottom, the top layer of aircraft safety requirements are allocated to systems, subsystems and equipment step by step. From bottom to top,

The safety level is predicted step by step and draw the conclusion that the compliance of the top safety requirements is obtained.

The entire aircraft safety analysis process includes aircraft level/system-level functional hazard assessment (AFHA/SFHA), preliminary aircraft/system safety assessment (PASA/PSSA), aircraft/system safety assessment (ASA/SSA), and common cause analysis (CCA), as shown in Figure 1.In the early stage of aircraft development, aircraft level functional hazard assessment (AFHA) is carried out according to the definition of aircraft level functions, which systematically and comprehensively inspects aircraft level functions, identifies the failure status of functions, evaluates the impact consequences of failure, determines the impact level, and establishes the baseline of aircraft safety design. The preliminary aircraft safety assessment (PASA) takes the analysis results of AFHA as input, distributes the safety requirements of each function to each system based on the aircraft architecture, and gives the system-level safety qualitative or quantitative requirements, independence requirements and safety maintenance requirements, etc. Each system takes the results of the assignment, performs a system-level functional hazard assessment (SFHA), and establishes a baseline for system safety design. Preliminary system security assessment (PSSA) is the first step of a systematic inspection of the system structure to ascertain how the fault causes danger, which is determined by SFHA and PASA, and assigning security requirements to the equipment. The safety requirements independence and security maintenance requirements of the equipment level is given qualitatively and quantitatively.

Common cause analysis (CCA) focuses on independence requirements in the process of system architecture, installation meet situation, by conducting zonal security analysis (ZSA), particular risk analysis (PRA) and common-mode analysis(CMA). Failure mode and effect analysis (FMEA) is a bottom-up list of a system, equipment, functions or a single component of possible failure modes. It determines the impact of these failure modes on the system, equipment, or function at the upper level. System safety assessment (SSA) and aircraft safety assessment (ASA) comprehensively analyses the results above to indicate the compliance of safety requirements at all levels.

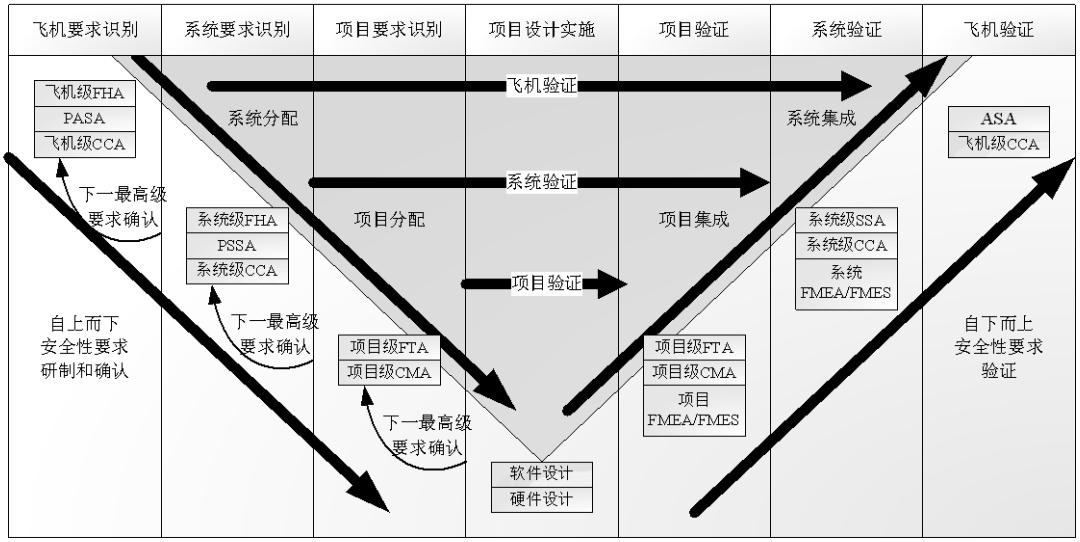

Figure 1 –Safety Analysis Process on Aircraft Development

3. Aircraft Functional Hazard Assessment Technology

3.1 Introduction of FHA

Functional hazard assessment is a systematic and comprehensive inspection of various functions of an aircraft, to clarify the failure status and impact of each function, and to classify the grades according to the severity of the impact. These grades are corresponding to certain safety requirements. It is a top-down assessment method which determines the critical system that affects the safety based on its failure impact level. Therefore, aircraft functional risk assessment is the first step for implementing safety assessment.

The input of aircraft functional risk assessment is to determine the function of the aircraft according to the aircraft architecture design documents and design requirements on the basis of obtaining the design requirements of the aircraft proposed by the user as well as the relevant regulations and

standards, and to determine the function failure state analysis results according to the functional risk analysis results by referring to the AFHA analysis of similar models. The input-output relationship is shown in Table 1.

Table 1–Aircraft Functional Hazard Assessment and Analysis

Input	Output
User proposed security design goals	Functional failure state
Aircraft top function list (e.g., lift, thrust, etc.)	Failure effect
Aircraft design objectives and user requirements (e.g. range, radius, etc.)	Effect level
	validation techniques
Preliminary design of the aircraft	Functional hazard
Regulations, standards and other systems	assessment analysis sheet

3.2 Failure State Requirements of Lower level

The depth of the subsequent preliminary aircraft safety analysis (PASA) analysis process varies as the complexity of the design and the level of functional failure status changes. The depth of PASA analysis is determined by AFHA (e.g., functional failure classification) and the design solution provided. The depth of analysis increases with the severity of functional failure states and the complexity of the design. After the completion of the aircraft functional risk assessment form, it is also imperative to provide qualitative design requirements and evaluate the feasibility of quantitative probability requirements for each functional failure state.

3.3 Establishment of Aircraft Functional Hazard Assessment Analysis

AFHA is adopted in the aircraft design process. The detailed contents include determining the aircraft function, analyzing the function failure, the influence of the failure state, determining the impact level, giving the method of verifying the conformance, and finally obtaining the result of the functional risk assessment and analysis by combining with the relevant supporting materials. As shown in Figure 2, the whole analysis process revolves around aircraft functions. After the safety design objective is determined, the functional failure of the aircraft is described and its impact is determined based on the operation condition, flight stage and external and environmental conditions of the aircraft, and the classification is made. Finally, based on the influence of the function failure state, the analysis results and the next level of safety requirements are output.

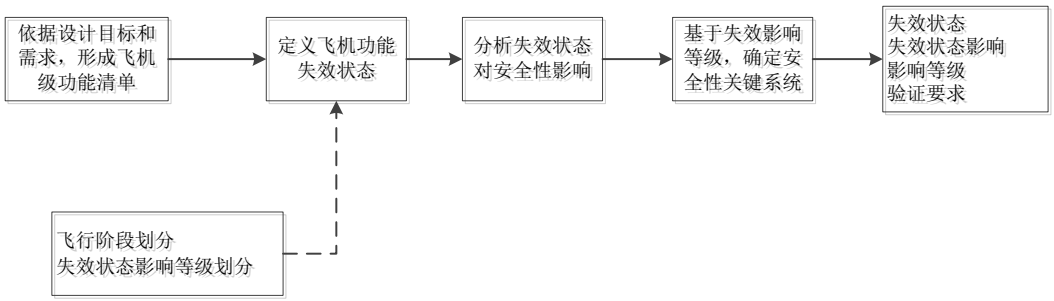

Figure 2 –Aircraft functional hazard assessment analysis process

3.3.1 Functional Definition of the Aircraft

Complete the analysis of aircraft functions (including internal functions and external functions)with a function list. The internal function refers to the function of the aircraft itself or the interface function between the systems; External functions also refer to interactive functions, aircraft functions that operate between other aircraft or in support of other systems (systems outside of other aircraft or ground systems). a functional list is established according to the structure complexity of the product and user requirements when it comes to aircraft design. In general, the following information should be collected:

1）The top level function list of the aircraft, which is the function extracted from the user during the designing process;

2）Aircraft design function decomposition scheme, which is aircraft preliminary design scheme, design framework, etc.

3.3.2 Definition of Aircraft Functional Failure State

[1] Flight Stage Division

According to the requirements of the functional hazard analysis, the flight stage division and the failure status influence grade should be defined first. The working state of each function of an aircraft is different in various flight stages, and the impact caused by function failure also differs. Therefore, the flight stage should be clarified while identifying the function failure state. The division of flight stages is based on the flight mission profile of the aircraft type being analyzed. The flight stage can be divided into taxiing, take-off, climbing, cruising, descending, approach and landing according to the flight mission profile of the object analyzed, which are shown in table 2.

Table 2 –Flight Stage Division

No.	Stage	Flight Stage Division
1	On the ground	G1 stationary on the ground
2		G2 ground taxiing
3	Takeoff	T1 take-off
4		RTO Rejected takeoff
5	Flying	F1 climbing
6		F2 cruising
7		F3 descending
8		F4 approach
9	Landing	L1 landing
10		L2 brake
11	All	ALL all

[2] Function Failure Status Identification

On the basis of considering different flight stages, environments and emergency configurations, the failure states of all aircraft functions are identified one by one, including single or multiple failures.

Single failure: check the confirmed function list one by one and list the single failure list. Common single function failures include: function loss, unannounced function loss, function error, etc. Multiple failures: A multiple failure list is determined based on the aircraft and system design architecture, taking into account the combined effects of systems within the aircraft and interactions with other external systems and ground systems. In particular, multiple failures due to other system functions must be considered. Common examples of multiple failures include: dysfunction of systems with multiple identical functions, loss of communication function and loss of navigation function at the same time, etc.

After the analysis of single and multiple failures on the basis of aircraft functions is completed, it can be compared with the AFHA of similar aircraft types to prevent the neglect of some uncommon failure states. In this process, the description of failure states must be concise, clear and accurate.

[3] Function Failure Status Impact Level

According to the definition of hazard severity grade in GJB900A, combined with the service characteristics of the aircraft, the definition of impact grade of the failure state of the aircraft is shown in Table 3. For the functional failure states with different impact levels, the safety quantitative requirements should be determined upon request of SAE ARP4761 and GJB 900A.

Table 3 –Identification of Failure State Effect Level

Severity grade	Failure state classification	Statement of accident consequence	Qualitative requirements	Quantitative requirements （/FH）
Ⅰ	Catastrophic	People killed or planes disabled, but no widespread environmental impact or serious harm to the public	Extremely improbable	＜10-8
Ⅱ	Hazardous	Serious personnel injury, serious occupational disease, serious damage to the aircraft, the crew greatly increase the workload, aircraft greatly reduce the safety margin	Extremely remote	＜10-6
Ⅲ	Major	Minor injury of personnel, mild occupational disease or system damage, the crew significantly increase the workload, the aircraft significantly reduce the safety margin	Remote	＜10-4
Ⅳ	Minor	Lesser than grade Ⅲ damage	Reasonably Probable	＜10-2
Ⅵ	No safety impact	No safety impact	no requirement	no requirement

3.3.3 The Effect of Aircraft Function Failure State

According to the definition of influence levels of failure states in Table 3, the influence levels of each failure state are analyzed and determined. Combined with the characteristics of the aircraft and the development stage, the failure state, flight stage, failure impact (to personnel, aircraft, environment) and failure impact level are analyzed. Taking "unordered landing gear drop" as an example, it can be known that this failure state will only cause safety impact in the cruise stage referring to the impact analysis on this failure state in other aircraft. Therefore, the event of "unordered landing gear drop" in this flight stage is analyzed considering the aircraft, personnel, environment etc. This failure state will increase the resistance during flight, and may also cause the landing gear door to fall off and hit the airframe due to the excessive load, resulting in the airframe damage. If the airframe is damaged, the crew members need to adjust the flight status of the aircraft in time, which seriously increases the workload of the crew and minor environmental impact. Therefore, the impact level of this functional failure is class Ⅲ.

3.3.4 Identification of Safety-critical Systems

The Ⅰ/Ⅱ level failure influence top event is screened out through the aircraft level functional hazard

analysis. According to the safety-critical system related to each failure state, the safety-critical system is obtained.

3.3.5 Methods for Verifying Compliance with Failure State Requirements

For the safety requirements determined by each failure state, in order to ensure that the design can meet the safety design objectives given and to confirm the probability of occurrence of the failure impact level determined, specific assessment methods should be selected in the design and subsequent safety analysis. Compliance verification methods used to show that aircraft design meets safety requirements include Failure Mode and Impact Analysis (FMEA), Fault Tree Analysis (FTA), Common Cause Analysis (CCA), etc., which can be selected to judge the functional failure state by referring to the method in Figure 3.

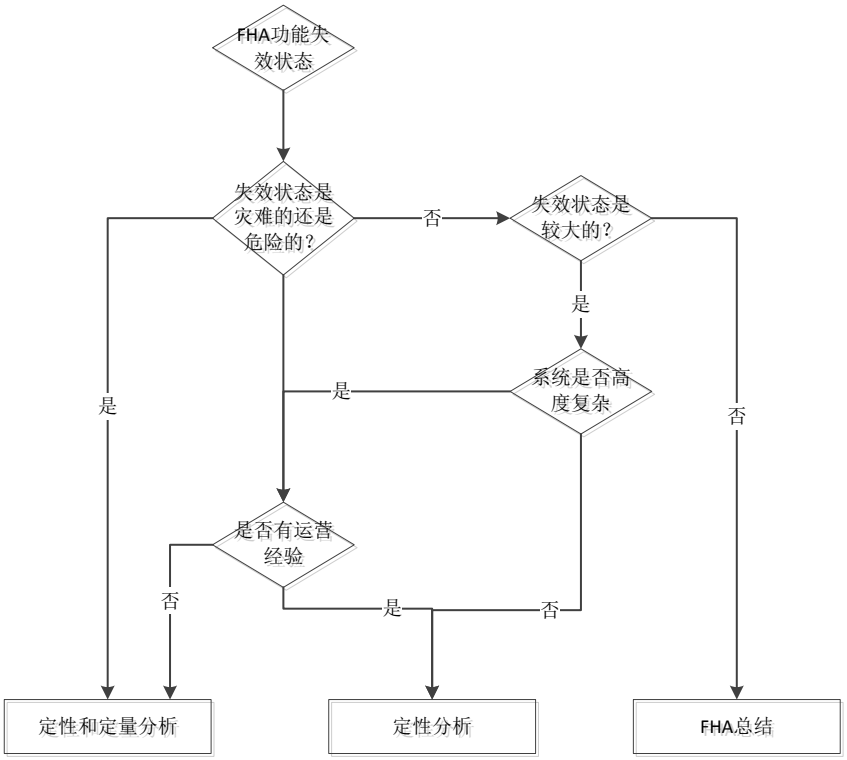

Figure 3 –Methods for Verifying Compliance

3.3.6 The results of aircraft functional hazard assessment are obtained, as detailed in Session 4.

4. Research on Functional Hazard Assessment Technology of An Aircraft

A certain aircraft was taken as an example to carry out the definition of aircraft level functions. There were 15 first-level aircraft level functions and 71 second-level aircraft level functions. An AFHA analysis was performed to evaluate the loss of all ground deceleration.

Table 5 –Function List of Aircraft Level(Excerpts)

Function Analysis of Aircraft Level				Corresponding to a level 1 function at the system level
No.	Primary function	No.	Secondary function	
F10	Provide and control ground movement of aircraft	F10.1	Provides and controls ground support and movement of the aircraft	Control landing gear retraction and retraction
		F10.2	Provide and control ground deceleration of aircraft	Provide and control ground deceleration of aircraft

		F10.3	Provide ground parking for aircraft	Provide ground parking for aircraft

4.1 Identification of Flight Phase

According to the typical mission profile of the aircraft, the safety analysis was carried out, which was determined in the flight stage according to Table 1.

4.2 Function Failure Status Impact Level

The classification of functional failure status is determined according to Table 2.

4.3 Hazard Probability Level

The possibility classification of function failure states and the safety quantitative requirements for different influence levels of function failure states are determined in accordance with Table 5.

4.4 Hazard Probability Level

For the function of "providing and controlling aircraft ground deceleration", take the failure state analysis result of the function of "losing all ground deceleration" as an example, as shown in Table 6.This function includes two failure states of Ⅰ function and one failure state of Ⅱ function.

4.5 Preliminary Aircraft Safety Analysis(PASA)

The input to the PASA analysis is the AFHA results, which include a description of the aircraft architecture, design principles, and a functional list of each system. The purpose of PASA is to establish safety requirements for the aircraft and to identify the desired system architecture to meet AFHA defined safety objectives. PASA is also an interactive process related to design definition, and in general PASA uses fault trees for analysis.

Based on the example of the result of the function risk assessment in Section 4.4, the function fault of "losing all ground deceleration" was analyzed as the top event. Examples of the results are as follows:

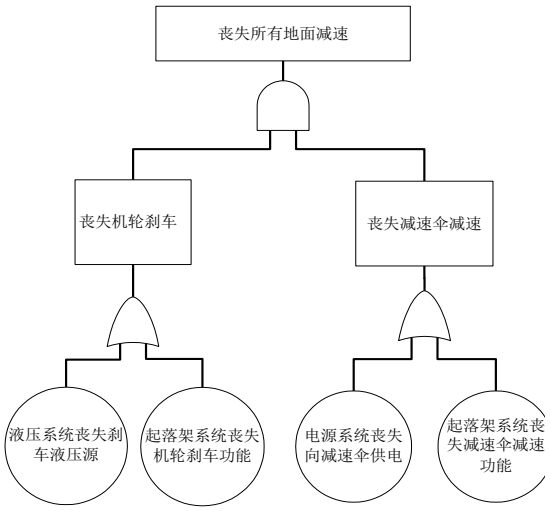

Figure 4 – An Example of Losing All Ground Deceleration(System Level)

Table 6 –Functional Hazard Assessment of Aircraft Level

Aircraft function	failure state No.	Function failure state	Flight Phase	Function Failure Status Impact(on aircraft, crew, environment)	Function Failure Status Impact Level	Methods for Verification
Deceleration on the ground	FC-10.1.1	Lose all ground deceleration (after reaching take-off speed)	take-off T1 landing & brake L1-L3	For aircraft: the aircraft overshot the runway at high speed, causing damage or scrapping of the aircraft To personnel: the crew is unable to slow the aircraft, causing injury or death to the crew Environment: No safety impact	I	quantitative FMEA FTA
	FC-10.1.2	Asymmetric loss of partial ground deceleration (high speed)	take-off T1 landing & brake L1-L3	For aircraft: The reduced deceleration function may cause the aircraft to overrun the runway sideways, causing damage or obsolescence of the aircraft. For personnel: the crew may be injured or injured due to damage to the aircraft, and may cause casualties on the ground. Environment: No security impact	I	quantitative FMEA FTA CCA
	FC-10.1.3	Unordered ground deceleration (after reaching take-off speed	take-off T1	For the aircraft: after V1, the engine of the aircraft still runs with large thrust, and the aircraft may rush out of the runway at high speed due to insufficient braking distance, resulting in serious damage to the aircraft. For personnel: may cause injury to the crew. Environment: No security impact	II	quantitative FMEA FTA CCA

4.6 An example of AFHA Provides Input for SFHA Analysis

The failure status of "Landing Gear System Loss of Wheel Braking Function" should be further analyzed

in the Landing Gear System SFHA, as shown in Table 7.

Table 7 –Landing Gear System Functional Hazard Assessment (Example)

System function	failure state No.	Function failure state	Flight Phase	Function Failure Status Impact(on aircraft, crew, environment)	Function Failure Status Impact Level	Methods for Verification
Wheel brake	FC.16.01.05	Lose all brake	landing & brake（L1～L3）	For aircraft: when the speed is less than 230KM/H, the deceleration parachute can be directly thrown to decelerate. but the long braking distance can cause the rush out at low speed, resulting in slight damage to the aircraft. For personnel: Before landing, the pilot checks whether the brake system is normal. If the wheel brake is lost, the pilot can take emergency fuel discharge, drop bombs and reduce and control the landing speed of the aircraft, and throw the deceleration parachute when the speed permits. The aircraft runs out of the runway at low speed, causing minor injury to the personnel. Environment: No environmental impact	Ⅱ	quantitative FMEA FTA CCA

5. Conclusion

The ICAS 2021 proceedings will receive an ISBN number and will be cataloged and archived by the German National Library. The research on aircraft function hazard assessment technology gives a picture of current practice of a military aircraft in meeting the requirements of GJB 900, and reach the target of safety analysis. This practice systematically and comprehensively checks the plane function, recognize all the failure states, assess failure consequences, determine the impact level, establish baseline. The results of AFHA analysis were used as input to conduct a system-level functional hazard assessment (SFHA) to establish a baseline for system safety design. It is therefore the first step in the process of assessing the safety of newly developed or modified aircraft. Then, the failure probability is assigned down step by step through system function hazard assessment (SFHA) and preliminary safety assessment (PSSA), and finally the safety requirements of the corresponding system and equipment are defined, and the hardware and software design work is carried out accordingly. After the state is solidified, the system safety assessment (SSA) and aircraft safety assessment (ASA) comprehensive analysis results are carried out to verify the compliance of safety requirements at all levels. The actual failure rate of each hardware is calculated through component failure mode and impact analysis (FMEA), and the fault tree (FTA) is established for qualitative and quantitative analysis of the design configuration, and the safety verification of the system and the whole machine is completed step by step.

References

[1] CCAR-25-R4, Airworthiness standards for transport aircraft. *CAAC*, 2011.

[2] SAE ARP 4761, Guidelines and Methods for conducting the safety assessment process on civil airborne systems and equipment.

[3] Gao.Z. Aircraft Design Manual volume 14. Beijing, *Aviation Industry Press*, Beijing, 2004.

[4] Lu J. Safety Evaluation and Analysis of Civil Aircraft Flight Control System. *Civil Aviation University of China*, 2009.

6. Contact Author Email Address

liquan528@qq.com

7. Copyright Statement