ICAS 2021 SHANGHAI
International Council of the Aeronautical Sciences
32nd Congress of the International Council of the Aeronautical Sciences
September 6-10, 2021
Pudong Shangri-La, Shanghai, China

Research on Certification Management of Aircraft Engine Based on Risk Analysis

Wang Chunxiao[1], Zhu Qin[1], Wang Xiaokun[3], Tang Xinhao[4]

[1,2,3,4] AECC Commercial Aircraft Engine Co. Ltd, Shanghai, China

Abstract

With the increasing number of airworthiness certification projects, the shortage of airworthiness certification personnel and the increasing complexity of civil aviation products, the traditional airworthiness certification mode has been difficult to be followed up. China's civil aviation industry manufacturing enterprises own research and development system is becoming more and more perfect and improved, and it is possible to gradually rely on the self-regulatory of the industry enterprise’s system to reduce the involvement of the airworthiness authority in the process of conformity verification. However, how to ensure that the products meet the airworthiness requirements through system supervision, and reduce the depth of involvement of airworthiness authority with satisfying the airworthiness and safety requirements, is a subject worthy of study.

This paper takes the development of a newly developed civil aero-engine as an example to study how to carry out risk-based management of certification. Civil aviation engine product development process should follow the systems engineering process, using a structured process and the hierarchical files and specification, guide and control the design, integration and validation process, in pursuit of close to the optimal way to complete the development of aircraft engine products, and meet the needs of all stakeholders, including airworthiness requirements. General risk management process which are collaborated with authority and risk identification methods are given in this paper, include potential risk in process of airworthiness requirements capture, analysis, architecture design, verification and validation, and design assurance for complex system. This paper also discusses how to match the authority's risk-based certification procedures and policies in the future.

Through carrying out risk management of airworthiness certification in the whole process of product development, and forming a hierarchical management mechanism in coordination with the authority, potential certification risks can be effectively identified and controlled. More importantly, it can strengthen the authority's confidence in the applicant's airworthiness ability, gradually shift from focusing on products compliance evidence to controlling risks, moderately reduce the involvement of the authority, and improve the efficiency of certification, so as to meet the internal needs of the development of civil aviation enterprises in China and promote the vigorous development of the aviation industry.

Keywords: Certification, Aircraft Engine, Risk Management, Process Assurance

1. Introduction

With the vigorous development of civil aviation industry, the number of type certificate for civil aviation products increases year by year. According to the 2019 annual report issued by Civil Aviation Administration of China in 2020, the amount of new certificate of Type certification (TC), Supplementary type certification (STC), Modification design approval (MDA), Validation of type certificate (VTC), Validation of supplementary type certification (VSTC), Validation of design approval (VDA) and other types is more than 200, among which TC certificate is 7 [1]. The number of accepted application for new TC/VTC is 13. At the same time, the number of professional personnel engaged in engine type certification has been insufficient according with the increase in the number of new TC/VTC project and system complexity. The concept of "risk-based certificate" has emerged as the industry continues to improve the ability of airworthiness and strengthen its own system to assure product development. In the Guiding Opinions on Strengthening the Capacity Construction of Airworthiness Certification System issued by Civil Aviation Administration of China [2], risk-based certificate is regarded as one of the main tasks to strengthen the ability of airworthiness certification. Risk-based airworthiness certification project management will focus on the risks in process of type certificate, and solve the key issues affecting safety with as few certifications human resources as possible [3,4]. How to accurately identify the risks in the process of type certificate, dynamically manage and monitor these risks, and effectively allocate resources to improve the efficiency of certification is a topic that the authority and the industry applicant need to explore together. European Union Aviation Safety Agency (EASA) published a certification memorandum [5] in 2017 on the level of involvement in product certification, which provides guidance on how to determine the depth and scope of intervention based on risk. However, this Certification Memorandum is only applicable to DOA (Design Organization Approval) holders. For non-DOA holders, especially new aviation manufacturing enterprises, there is still a lack of corresponding guidance materials on how to carry out the identification, analysis and management of certification risk.

This paper discusses how to analyze the technical airworthiness risks based on a structured product development process, and the design assurance risks according to SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems development (ARP 4754A) [6], for a new developed civil aircraft engine. In addition, taking a certain airworthiness requirement and a complex system as examples, the focus of risk identification and common risks in product development activities are presented respectively. Finally, the prospect of how to match the risk-based level of involvement for authority is given.

2. Overview of Risk Management of Type Certification Project

2.1 Type Certification Project

Type certification project refers to the process in which aircraft, engines, propellers, and other civil aviation products complete type certification and obtain certificate in accordance with relevant procedures [7,8]. This process includes not only the product development process for the industry to design and verify a product that meets the requirements of airworthiness regulations, but also the validation process for the authority to confirm that the product meets the requirements of airworthiness regulations which is related to technical and management factors. Therefore, the process of industry and authority need to be taken into consideration when carrying out risk management of type certification project. According to Aircraft Type Certification Procedure, type certification project can be divided into five phases, including conceptual design phase, requirements determination phase, compliance planning phase, implementation phase and post-certification activities phase. Based on the milestone objectives of each phase, the risk management include the following work in each phase:

Phase I Conceptual Design

Phase Objectives. The authority responds to the potential applicant’s questions about the procedural and technical requirements that may arise after the applicant’s process orientation. Potential applicants give the authority an initial familiarization briefing and submit a certification plan which will be kept throughout the project.

Risk management objectives. The potential applicants formulate risk management plan, understand the authority's principles of risk-based level of involvement for certification project and carry out risk management for the certification risks identified in the familiarity phase.

Phase II Requirements Definition

Phase Objectives. Applicant TC. The authority establishes the certification basis, defining the applicable requirements of CCAR (China Civil Aviation Regulation) for the issuance of the TC. The authority and applicant finish the preliminary Project Specific Certification Plan.

Risk management objectives. The applicant carries out risk management, focusing on identifying risks that are inconsistent with the authority 's understanding in terms of airworthiness requirements and compliance methods.

Phase III Compliance Planning

Phase Objectives. Complete the Certification Plan and Certification Project Plan, or the Project Specific Certification Plan.

Risk management objectives. The applicant carries out risk management, focusing on identifying risks associated with the development and implementation of compliance plans. Based on the results of risk assessment, the level of involvement was determined with the authority.

Phase IV Implementation

Phase Objectives. Compliance Data Generation, Compliance Substantiation, and Compliance Finding, corresponding to Certification Plan and Certification Project Plan, or the Project Specific Certification Plan.

Risk management objectives. The applicant carries out risk management, focusing on identifying risks in the development assurance process, and dynamically adjust the risk assessment results and the level of involvement of the authority.

Phase V Post-Certification Activities

Phase Objectives. Finish the final work of the certification project, such as certification summary report. Carry out the Post-Certification management work and continued airworthiness.

Risk management objectives. Complete the risk management final report and update the risk database. Transferred to risk management in the continuous airworthiness.

2.2 General Certification Risk Management

Risk in certification project is associated to a non-compliance with the certification basis. For derived serialized engines, the risks are mostly related to the new/novel/unusual design feature, the development process of complex systems, and the operation of Design Organization Approval [5]. For a newly developed engine, it is not possible to reuse a large amount of compliance data as a serialized derivative model. The process of type certification has the characteristics of long period, high complexity and deep involvement of the authorities, and it is more necessary to carry out risk management to minimize the possible adverse effects caused by the risks. In Phase II and Phase III of certification, potential risks need to be fully and accurately identified in conjunction with the authority along with the process of establishing certification basis and certification plans. When analyze and evaluate the risk, the applicant need evaluate the severity of the consequences of risk occurrence and the probability level of risk occurrence, forming a risk evaluation matrix, thus providing input for the development of graded risk response work plan, as shown in Table 1 and 2.

Table 1 Risk assessment matrix

		Likelihood				
		1 Very low	2 Low	3 Medium	4 High	5 Very high
severity level	5 Very high	5	10	15	20	25
	4 High	4	8	12	16	20
	3 Medium	3	6	9	12	15
	2 Low	2	4	6	8	10
	1 Very low	1	2	3	4	5
High Risk		Take corrective/improvement action immediately until the risk is reduced to a low risk level.				
Medium Risk		Take corrective/improvement actions to mitigate/control the risk within a certain period of time until the risk is reduced to a low risk level.				
Low Risk		Correction/improvement actions to mitigate/control risks are not required and must be documented.				

Table 2 Risk occurrence consequence severity level

severity level	Score	Description of consequence
Very high	5	Certification project will be significantly affected, and huge time and economic costs will be paid to eliminate this risk, and even the project will fail.

severity level	Score	Description of consequence
High	4	Certification project will be seriously adversely affected, and it will take a large amount of time and economic cost to eliminate this risk.
Medium	3	Certification project is negatively affected to a certain extent.
Low	2	Certification project is temporarily negatively affected, but the impact is very low.
Very low	1	No effect on certification project, or the effect is negligible.

Generally, the main process of risk management includes risk identification, risk analysis, risk evaluation and risk response [9-11]. There has been a lot of literature on risk management processes, which will not be described in depth in this article. Two points should be paid special attention to when dealing with the risk of airworthiness certification. First, there are needs to be corresponding airworthiness engineer and organization to carry out risk management. For example, the airworthiness engineer who is owner of airworthiness requirement is responsible for the risk management process activities related to this requirement, including the identification and analysis of potential risks together with the authority, coordination of different management, design and manufacturing team to develop the risk response work plan and tracking the status. At the same time, it is recommended to set up a certification risk management committee to regularly review the situation of risk management and make decisions on risk downgrade or closure. Second, in the early stage of the certification project, the risk monitoring strategy should be agreed with the authority, which level of risk should be reported to the authority, or even be given technical advice on whether to recommend closure. For the red high risk in Table 1, it is strongly recommended that the applicant report to the authority immediately when identify, and report the progress of risk response regularly. For the red high risk items to be closed, it is recommended that the applicant obtain confirmation from the authority through formal forms such as meetings, and record the discussion process and closing conclusion in the meeting minutes. The process of continuous tracking of airworthiness certification risk and risk closure is shown in Figure 1.

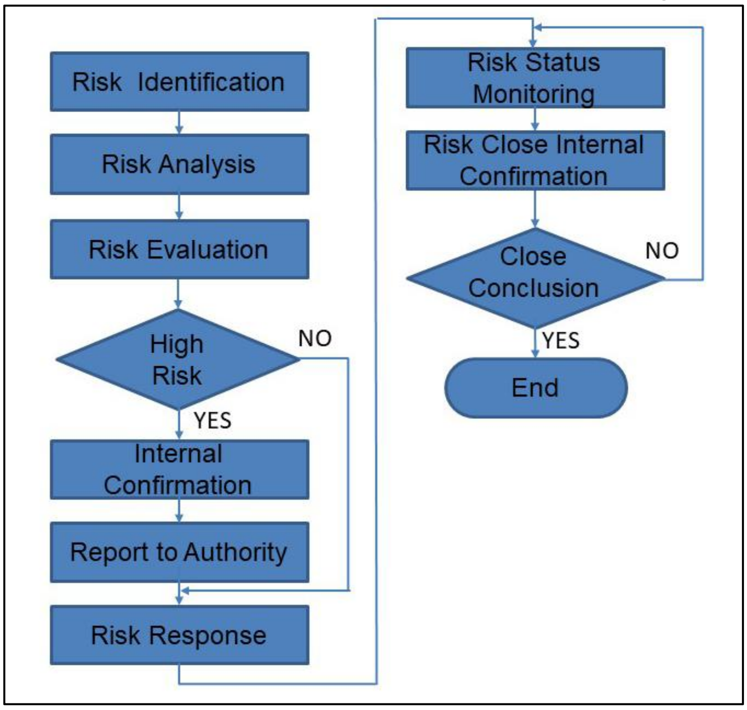

Figure 1 – Risk Management Collaborative Process

3. Risk Identification Methods

3.1 Risk identification based on system engineering method

For the identification of airworthiness certification risks, the whole life cycle process of product development needs to be considered, and it depends on the system engineering process of structured product development. As a highly complex product [12], aeroengines must be developed in accordance with system engineering methods. System engineering emphasizes the determination of the overall logical framework of the system in the early stage of product development, followed by the construction of structured system engineering processes and the transmission link of hierarchical documents, specifications and models to guide and control the design, synthesis and verification of various professional fields. It is to complete the development of aeroengine products in a way that is close to the optimum, and to meet the needs of all stakeholders. Airworthiness regulations with compulsory and statutory force, as one of the requirements for aeroengine products, also need to rely on system engineering methods to be assigned by design, achieved by manufacturing, and complied by verification during product development, and continuously satisfied by repairing during in-service life.

Therefore, airworthiness regulations need to be regarded as the original needs of stakeholders, and the entire process of their requirements, design, manufacturing, verification and validation needs to be identified, and the iterative and recursive process between systems and subsystems needs to be considered. If this regulation has a supporting reference relationship with other regulations, it is also necessary to focus on identifying the risk of the interface with other regulations. When conducting risk management, based on a structured development process, different types of development activities should be targeted to identify their airworthiness certification risks. If aviation manufacturing companies have richer development and certification experience, they can also form specific risk identification checklists for each airworthiness regulation.

Based on the product development process, the identification of airworthiness risk points for various development activities such as requirements, design, and verification have different point of focus. For requirement-related development activities, more attention needs to be paid to the completeness of requirements and whether there are risks in requirements confirmation. Examples of common risks are as follows:

Table 3 Risk Identification for Requirement

Main Concerns for Requirement	Example for CCAR 33.17[13]
• Have the requirements of the regulations been understood?	The requirements and essential meanings of CCAR 33.17(d)(3) for anti-corrosion are not fully understood.
• Have the requirements of the relevant airworthiness regulations of the aircraft been considered?	The requirements for nacelle drainage do not consider that flammable fluid discharged cannot enter other compartments or contact aircraft components to avoid fire in unexpected areas in CCAR 25.863 [14] Flammable fluid fire protection.
• Have the requirements of the interface of the aircraft been considered?	The requirement for drainage from the pylon of the aircraft is not considered.
• Have the Federal Aviation Administration amendment, advisory circular and policy been referred?	Draft AC 25.863 [15] is not considered
• Have the requirements of EASA regulations, Acceptable Means of Compliance (AMC) and certification memorandum been referred?	AMC E130 [16] is not considered.
• Has the future revision trend of this regulation been considered?	The revision of the standard for kerosene-type flame burners by "AS6826 Powerplant Fire Test Standard Top Level and Scope-Draft" [17] was not considered.
• How to understand the smallest granularity of regulations?	Not sure how to understand the CCAR 33.17, based on 33.17(d) or 33.17(d)(2).
• Can the definition of key terms be	There is no quantitative standard for the

quantified?	"hazardous quantity" of flammable fluid mentioned in CCAR 33.17(f).
• Are the safety intent and substantive requirements of the regulations clear?	It is not clear how to satisfy "minimize the possibility" in CCAR 33.17(a).
• Are there any supporting documents for the understanding of regulations?	CCAR 33.17(g) does not have a clear advisory circular to support compliance methods.

For design-related development activities, more attention needs to be paid on whether airworthiness requirements are implemented in the design, and there are no unsafe design features. Examples of common risks are as follows:

Table 4 Risk Identification for Design

Main Concerns for Design	**Example for CCAR 33.17**
• Have the airworthiness requirements at the system/subsystem level been considered in the design with verification evidence?	There is no verification evidence for electrical bonding/grounding related requirements
• Has it avoided the unsafe design of similar product?	When the stators and rotors use titanium alloy at the same time, there is a possibility of internal titanium fire.
• Are there novel and unique design features?	The fuel nozzle uses additive manufacturing, which may affect the compliance of the combustor case burn-through.
• Are there any potential special conditions, equivalent safety, or exemptions?	The current CCAR33 regulations [18] cannot cover the entire engine electrical bonding compared to CS-E 135 [19] electrical bonding requirement, which may impose potential special conditions.

For verification-related development activities, focus on the completeness of the airworthiness verification plan and the adequacy and feasibility of verification implementation. Examples of common risks are as follows:

Table 5 Risk Identification for Verification

Main Concerns for Verification	**Example for CCAR 33.17**
• Have the method tools been verified with verification documents?	The analysis tools for the burn-through and burn-through path of the combustor case have not been verified.
• Have the instructions on which the verification process is based been verified with verification documents?	The fire protection analysis process of the mounting system has not been verified by tests.
• Is the chain of compliance evidence complete?	Only through the compliance verification tests and the engine fire protection design description to show that the design and construction minimize the possibility of the occurrence and spread of fire in the external and internal engine.
• Is the compliance verification arrangement executable?	Accessory Gear Box (AGB) fire test is still uncertain about the flame impingement position.
• Can the test resources meet the requirements of the test and are these resources available?	Insufficient resources for concentratedly conduct multiple firewalls and flammable fluid lines fireproof/fire resistance tests.

• Is it sufficient to substantiate by non-test compliance methods?	The verification of the burn-through of the combustor case just by analysis is not sufficient for the first product certification program.
• Is there any internal process supervision for compliance verification related to process assurance?	The control system is a complex system and requires process assurance, but internal supervision of its development process is not carried out.

3.2 Design assurance risk identification for Complex system

For simple system, it can be only used the above method to identify risk, for highly integrated and complex system it is not enough. This is because can't rely on the traditional test method to verify all possible failure situation, also can't get by on only analysis each process activities related to each airworthiness requirement to identify all potential certification risks. The complex system needs to be developed according to SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems. At the same time, the compliance method of Design Assurance (DA) should also be used when highly integrated and complex systems such as the engine control system show compliance to CCAR25.1309 [20], CCAR33.28 [21], etc. Therefore, compared with simple systems, certification risk identification of complex systems should not only consider the requirements of airworthiness regulations, but also consider all system requirements. The development process to be evaluated should include requirement, design, verification, validation, safety, configuration management, assurance process and certification process.

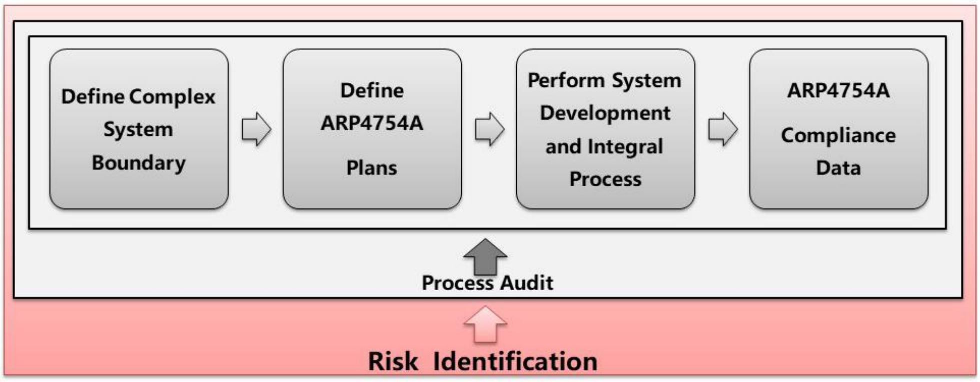

Figure 2 – Risk identification model for Complex system

Once the boundary of the complex system is defined, a series of plans are developed to define the development process requirements for the product. The plans include system/sub-system level development plan, safety project plan, validation plan, verification plan, configuration management plan, process assurance plan, and certification plan. The product development team shall carry out development activities according to the planning documents and form the corresponding evidence of airworthiness compliance. Process assurance engineer shall monitor the entire process of the development team's ARP 4754A life cycle activities in accordance with process assurance plan to ensure compliance with the corresponding planning and development assurance process requirements. Process assurance engineer shall approve all deviations to ensure that they have no negative impact on the completion of the safety objectives of system and sub-system. Process assurance engineer shall participate in the review or audit of the whole life cycle process. The review or audit results shall be recorded. As shown in the model in Figure 3, the scope of risk identification should include all of the above, and special attention should be paid to the risks caused by boundary changes or uncertainties of complex systems.

Table 6– The main concerns of airworthiness risk identification of complex systems

Activity Type	Risk Identification main Concerns (Example)
system enables	Whether the existing development system forms a top-down unified document framework.

Activity Type	Risk Identification main Concerns (Example)
system enables	Whether there are sufficient resources to carry out the 4754A planning work.
system enables	Whether to establish a set of independent supervision mechanism, to ensure that in the process of implement ARP 4754A lifecycle activities, strictly follow the approved plan and development assurance system files, for any does not conform to and deviation from, must be approved by the designated role?
Product development	For specific technical points, due to lack of experience, the implementation of existing processes/standards/plans may still be difficult, including but not limited to: 1. Requirements capture 2. Identification, confirmation and verification of safety requirements 3. Use simulation/modeling as a method of validation or verification 4. Interface management 5. Verification technology (fault injection, response to abnormal situation, etc.) 6. Change impact analysis 7. Relationship between system activities and safety activities 8. Relationship between system activities and hardware and software activities
Product development	Whether the consistency and traceability of the ARP 4754A lifecycle data can be ensured to meet the relevant objectives of the Transition Criteria for process data as required in the ARP 4754A.
Certification	As it was the first time for the applicant and the authority to conduct the ARP 4754A certification compliance, they lacked relevant practical experience and had inconsistent understanding of the requirements.

4. Risk based level of involvement of the Authority

The authority and the applicant should determine the principle of risk-based intervention in the early phase of system development to determine the future level of involvement (LOI) of the authority. LOI can be divided into four types: none, low, medium, and high, as shown in Table 7. The factors determining LOI include two dimensions, certification risk and failure status impact level. Certification risk assessment should be based on the applicant's assessment of the identified risk and the authority's confidence score.

The confidence score by authority should be considered comprehensively: 1) The result of spot check on the risk management of the applicant to confirm whether the risk management of the applicant is controllable and reasonable; 2) the construction of the applicant's design assurance system, especially the ability of the airworthiness; 3) the applicant's performance in the past design approval process; 4) The novel design characteristics and complexity of civil aviation products.

The authority can dynamically manage and evaluate the risk assessment scores, and dynamically implement different level of intervention. However, for specific topics such as impact analysis of system requirements change, safety evaluation, and supplier supervision, it is not recommended to adopt risk-based intervention assessment, but to carry out strict special review activities.

Table 7– Activities of different levels of intervention

LOI	Activities By Authority
High	• Conduct a review of all evidence of compliance, including compliance report reviews and test witness, and a detailed review of analysis reports of test results. • For novel and unique technologies, the scope of review should include supporting data in addition to evidence of direct compliance, and even extend to requirements. • For complex systems, on-site review should be carried out primarily, supplemented by a small amount of document review.
Medium	• Review most compliance reports and witness most tests and other verification activities. • For complex systems, some development and validation processes need to be reviewed on site, while others are mainly reviewed by documents.
Low	• Review a small number of compliance reports, witness few or no witness tests and other verification activities. • For complex systems, it mainly focuses on document review.
None	• Review the submission of a declaration of conformity report by the applicant requires no process review. • For complex systems, only review the stage review reports.

5. Conclusion

With the increasing of development and airworthiness capability of China's civil aviation manufacturing enterprises, risk-based certification has gradually had the implementing conditions. In this paper, from the perspective of TC applicant, a civil aero-engine developed in accordance with systems engineering is taken as an example to explore how to implement risk-based airworthiness certification management. At the same time, considering the complexity of civil aero-engine system, the risk management in the process of complex system design assurance is also studied. Most importantly, it shows how the applicant's risk-based airworthiness certification management should be matched and coordinated with the authority's risk-based model.

Risk-based airworthiness certification is the future development trend of airworthiness field and must-go road for civil aviation manufacturing industry. Research on airworthiness risk management and coordination mechanism with authority for the whole process of product development can help to build a more reasonable and effective processes to identify and control the potential risks, to establish a new cooperation partnership in the future, so as to promote the vigorous development of the civil aviation industry in China.

6. Contact Author Email Address

Mail to: wangchunxiao@gmail.com; qinzhu_amy@163.com; kun910218@gmail.com; txh0926@sina.com

7. Copyright Statement

References

[1] Civil Aviation Administration of China, Annual report of airworthiness certification department (2019). 2020.

[2] Guiding Opinions on Strengthening the Capacity Construction of Airworthiness Certification System, Civil Aviation Administration of China, 2019.

[3] Xu Xin, Wang Xiaoquan, Dong Lijie. Preliminary Exploration of Project Management of Airworthiness Certification Based of Risk. Civil Aviation Management, Vol 2, 104-106, 2020.

[4] Yin, Shijun. Study on Resources Allocation between Airworthiness Authority and Aviation Industry. Procedia Engineering, Vol80, 668-676, 2014.

[5] European Aviation Safety Agency, Certification Memorandum: Criteria for the determination of EASA level of involvement in product certification, Proposed CM-21.A/21.B-001 Issue 01, 2017.

[6] SAE ARP 4754A. Guidelines for Development of Civil Aircraft and Systems. Warrendale, PA. SAE International, 2010.

[7] Civil Aviation Administration of China, AP-21-AA-2011-03-R4 Aircraft Type Certification Procedure, 2011.

[8] Federal Aviation Administration, Order 8110.4C: Type Certification, 2017.

[9] ISO 31000:2018, Risk management - Guidelines. Switzerland: ISO, 2018.

[10] ISO/IEC 31010-2009, Risk management - Risk assessment techniques. Switzerland: ISO, 2009.

[11] Giannakis M， Papadopoulos T . Supply chain sustainability: A risk management approach. International Journal of Production Economics, Vol171,455-470, 2016.

[12] DOT/FAA/TC-17/26. Definition and Measurement of Complexity in the Context of Safety Assurance. William J. Hughes Technical Center Aviation Research Division Atlantic City International Airport. FAA, 2017.

[13] CCAR 33.17 Fire Protection. Airworthiness Standards: Aircraft Engines. Civil Aviation Administration of China, 2016.

[14] CCAR 25.863 Flammable Fluid Fire Protection. Airworthiness Standards: Transport Category Airplanes. 2016.

[15] Federal Aviation Administration. Flammable Fluid Fire Protection: AC 25.863 Draft [S]. US: Department of Transportation, 2002.

[16] AMC E130 Fire Protection, European Union Aviation Safety Agency, 2020.

[17] AS 6826 Powerplant Fire Test Standard Top Level and Scope-Draft, Society of Automotive Engineers, 2019.

[18] CCAR 33. Airworthiness Standards: Aircraft Engines. Civil Aviation Administration of China, 2016.

[19] CS-E 135 Electrical Bonding, European Union Aviation Safety Agency, 2020.

[20] CCAR25.1309 Equipment, systems, installations. Airworthiness Standards: Transport Category Airplanes, 2016.

[21] CCAR 33.28 Control System. Airworthiness Standards: Aircraft Engines. Civil Aviation Administration of China, 2016.