A discussion of airworthiness in terms of safety and integrity

Jianbo Hu¹, Jun Li, Lei Zheng, Peng Wang and Zan Ma

Equipment Management and Unmanned Aerial Vehicle Engineering College, Air Force Engineering University, Xi’an, China

¹Email: jbhhu@iipc.zju.edu.cn

Abstract. System safety and integrity are regarded as two main aspects in aircraft airworthiness. Both are widely used in airworthiness design, verifying, and certifying. Firstly, a depth of understanding about the concept of airworthiness is given, and the total process of airworthiness based on safety standards and integrity ones is proposed. Secondly, airworthiness’ main aspects are discussed with the traditional safety assessment, current standards, STAMP and STPA. Lastly, the relationship between reliability, maintenance, safety, integrity and airworthiness is analysed.

1. Introduction

The airworthiness of military aircraft has also been carried out in some countries due to the important contribution of airworthiness to the improvement of civil aviation safety. For some years, military aircraft design and operation has been in accordance with system safety viewpoint and integrity requirement, and focused on fighting capacity such that there might be a tendency to mislead the implement of system safety engineering and integrity requirements due to airworthiness. This is a tendency to be noticed, because the ultimate goal of airworthiness is for system safety and its integrity. Is worthy of being studied the relationship between airworthiness and the traditional system safety viewpoint or integrity requirements to avoid the serious tendency of despising system safety and integrity. By now, there are little literatures on this aspect.

Airworthiness management and its technology are considered the effective way to improve civil and military aircraft’s safety. Military aircraft airworthiness is defined as the ability of a military aircraft to obtain, sustain, and terminate flight in accordance with prescribed usage requirements under the certain system configuration. This covers all phases of flight and focuses on the aircraft’s ability to fly [1]. Safety of Flight is defined as the property of an air system configuration to safely attain, sustain, and terminate flight within prescribed and accepted limits for airworthiness. For U.S. military aircraft the guidelines for airworthiness are defined in MIL-HDBK-516B. The fundamental difference between the military and civil airworthiness approaches is the amount of flexibility. The military airworthiness process is designed to be very flexible in order to accommodate large variation in aircraft designs and missions. A fighter jet is significantly different from a cargo aircraft such that no single set of airworthiness guidelines could appropriately cover both contexts. MIL-HDBK-516B defines a set of guidelines for tailoring a large set of airworthiness criteria to match the aircraft configuration being reviewed [1].

Practically, the main working in airworthiness process might be concluded as figure.1. The first part (requirement) should be criteria’s tailoring method based on SSA [2] (System Safety Assessment) and standards’ uniformity and integrity for IS [3] (Integrity Standards). The second part (design)
should be system design, safety design and failure alarm based on airworthiness requirement, and SSA, IS must be used step by step to obtain the adequate safety level and physical integrity according to airworthiness requirement. The third part (verify) should be compliance with airworthiness requirement by verification, SSA might be the most effective safety analysis method, and IS must be considered for the total system and the related sub-systems or equipments. The forth part (risk control) should be risk management and control the risk to an acceptable level, SSA must be used in constructing the risk control matrix, and IS must be used in compiling the related continued airworthiness files. It can be seen that, for aircraft airworthiness, whether military aircraft or civil aircraft, system safety and integrity should be mainly considered.

![Diagram of Airworthiness Working](image)

**Figure 1.** Airworthiness Working.

2. **Depth understanding about the concept of Airworthiness**

The airworthiness is defined as “For an aircraft, or aircraft’s component, airworthiness is the possession of the necessary requirement for flying in safe conditions, within allowable limits” (Filippo De Florio, [4], 2000). Airworthiness is the measure of an aircraft’s suitability for safe fight and is the requirement of an aircraft’s safety and integrity under the predicted operation environment and the authorized limits. The system safety assessment must be carried out in every airworthiness process to satisfy the safety’s requirement. The integrity standards for aircraft’s structure, engine and avionic equipment must be considered as soon as possible to get aircraft’s initial airworthiness and continued airworthiness.

In the view of control engineering, the inputs of airworthiness are the predicted operational environment and the authorized usage limits, and the outputs are the total performance and operational property of aircraft, including its components and subsystem. Airworthiness focuses on the main properties about aircraft’s safety and physical integrity. It is realized by conforming all along to the type design. It is continued by persisting all along in with conditions for safe operation. Obviously, the main aspects on airworthiness are safety, integrity associated with the proper analyzing, designing, verifying, and maintaining.

In fact, the process of airworthiness is based on system safety assessment and the related integrity standards. SSA is carried out in the total airworthiness process. IS should be used in design and verification to confirm the integrity of aircraft’s structure, engine, avionic systems, and equipments. Essentially, system safety is realized by the requirement of airworthiness as shown in figure 2.

Airworthiness requirements, which are used in designing and verifying, are obtained by tailoring the airworthiness standards (such as CAAR-25, [5]) or criterions (such as MIL-HDBK-516B, [1]), adding the additional rules associated with new technology, new material and new idea, and supplying the special rules with respect to the particular function to confront the existing safety risk source. While the professional standards should be used in verification and design to verify the compliance of airworthiness, some airworthiness requirements could not be realized or verified for the limitations in technology and verification capability such that risk of every un-airworthiness-item is assessed. Hence, the proper measurement should be taken to reduce the risk’s impact at an acceptable level or eliminate
the risk. Meanwhile, the related continued airworthiness items must be listed and deployed with the effective maintenance activity based on risk’s severity and likelihood.

Figure 2. Airworthiness process based on systems safety assessment and integrity standards.

3. System safety assessment

3.1. System safety assessment based on the traditional methods
System safety assessment is a series of methods used in the total processes through which safety, suitability, and effectiveness (OSS&E) [6] and airworthiness are implemented. The safety assessment process includes requirements generation and verification which supports the aircraft development activities and usage servicing, and provides a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazards have been properly addressed. It is noted that the risks in usage servicing should be identified and the proper measurement should be proposed by the risks control methodology based on system safety assessment.

Three main steps are necessary for system safety assessment, named by FHA (Function Hazards Assessment), PSSA (Predictive System Safety Assessment), SSA (System Safety Assessment), and the results from every step should be used in airworthiness compliance verification [2]. The main methods of system safety assessment are: FTA (Failure Tree Analysis), DD (Dependence Diagram), MA (Markov Analysis), FMEA (Failure Modes and Effects Analysis), FMES (Failure Modes and Effects Summary), CCA (Common Cause Analysis), ZSA (Zonal Safety Analysis), PRA (Particular Risks Analysis), and CMA (Common Modes Analysis) [2].

3.2. System safety assessment based on the current standards
For civil aircraft, many standards are proposed in aircraft’s safety engineering as shown in figure 3. These methods shown in figure 3 may be generalized to military aircraft with the adequate regulation or specification, where the top guideline program should be MIL-STD-882E [7] that gives the system safety standard practice, including management, analysis, evaluation and verification tasks.
ARP 4754 [8] is the guidelines for development of civil aircraft and systems, including to planning, processing, integrating and modifying of aircraft and systems development. ARP-4761 [4] is the guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. ARP 5150 [9] deals with safety assessment of transport airplanes in commercial service. ARP 5151 [10] is about the safety assessment of general aviation airplane and rotorcraft in commercial service. Do-297 [11] is the guidance and certification consideration about Integrated Modular Avionics (IMA) development. Do-178B [12] is software consideration in airborne and equipment certification. Do-254 [13] is the design assurance guidance for airborne electronic hardware.

System safety assessment methods described in ARP-4761 is widely used in ARP 4754. System function, failure and safety information based on ARP-4761 should be feedback to ARP 4754 to support the aircraft function development, allocation of aircraft functions to system, development of system architecture, allocation of system requirements to items, and system implement. System design information from ARP-4754 should be entered into ARP 4761 to support the FHA, PSSA, SSA and verification.

For the special airborne and systems, the airworthiness requirement associated with software in ARP 4754 should be considered with Do 178B, and the related software planning, process, verification, and management in the software development life-cycle as shown in Do 178B should be combined with aircraft and systems’ requirements from ARP 4754.

Meanwhile, it is noted for IMA that Do-297 should be used for complicated systems that is composite of software and hardware. The software should be complied with Do 178B and the hardware should be complied with Do 254. Finally, the integration for the hardware and software should be complied with Do 297.

3.3. The role of STAMP and STPA in system safety and integrity

Obviously, the various standards in figure 3 are based on the traditional safety models such as FTA, FMEA, which are used to find out the causes from the failures of components but the interaction among components. Recently, STAMP and STPA is proposed to identify UCAs (Unsafe Control Action) and its causal scenarios [14] such that system safety analysis is performed not only for the failure components but also for the components’ interaction.

STAMP (System-Theoretic Accident Model and Processes) and STPA (System-Theoretic Process Analysis) [15] [16] [17] is the model and method for complex technical system safety analysis to identify scenarios leading to hazards based on system theory. STAMP and STPA should be jointly used to identify a large set of systematic causes, many of them not involving failure or unreliability. These causes may be existed in the increasingly common component interactions such as software-intensive, multi modules transmit and man-machine interface systems. While each component should be considered and complied with its proper guideline program, respectively, the interaction must be considered, totally. As shown in figure 3, these interactions would be discovered in the closed control loops and among levels. Finally, it is possible for the obtained constraints and safety mitigations from STAMP and STPA to be a complement to the relative systems safety documents and integrity documents. In other words, UCAs and their causal scenarios will largely improve the system safety and integrity.

4. The relationship among reliability, maintenance, safety, integrity and airworthiness

4.1. Reliability and maintenance

Firstly, the products’ reliability must be high and may be described by the characteristics, such as mean life, MTBF (meaning time between failures), and failure rate. Some reliable measurements have been used to improve system’s reliability in some safety-critical systems, such as four channels fly-control computers based on redundancy technology. Of course, the products may fail for some reasons. Thus, it is very important for the failure components to be detected and isolated as soon as possible. Maintenance may be characterized by MFMT (meaning failure maintenance time) and maintenance
rate. Some maintenance measurements have been used to improve system’s maintenance, such as failure alarm, failure diagnosis, failure isolate and failure repair. Currently, based on the idea of RCM (Reliability Center Maintenance), reliability and maintenance are the integrity to measure the supporting capacity of the aircraft.

**Figure 3.** System Safety Assessment for Aircraft.

4.2. Safety and its engineering
Meanwhile, failure conditions may result in accidents, or may avoid from the accidents with the proper measures. In fact, the accidents may be deal with the typical “five efforts”, such as human, aircraft, regulation, material, and environment. Safety must be totally considered by safety engineering, which is a composite of compliance-safety and system-safety. Compliance-safety [18] is used to achieve safety by complying with the appropriate codes, standards, and regulations, such as military standards, airworthiness regulations, and some technical standards. It is noted that compliance safety is the result of compromise and represents minimum acceptable levels of performance. Compliance-safety is to be reactive, and most regulatory requirements were written in reaction to an accident or series of accidents. Thus, codes, standards, and regulations tend to lag behind rapidly changing technology so that a gap always exists between “compliance” safety and “practical” safety. Codes, standards, and regulations tend to be inadequate for new technologies, new materials, new battling ideas, and new functions in new-military developing and researching. Of course, system safety provides the effective ways to mitigate compliance-safety’s shortcomings. System safety effort attempts to exceed minimum standards and to provide the highest level of safety achievable, and strives to be proactive by very early identification, analysis and control of hazards, which may exist in new technologies, new materials, new operational concept, and new functions in new-military developing and researching, to produce first-time safe systems.

4.3. Integrity and its standards
As described in section 2, integrity is object to failure conditions too. The integrity requirement must be considered to achieve the safety opposite to the specified usage and operational environment. The integrity of aircraft structure, engine structure, Avionics/Electronics and mechanical equipment and
subsystems should be considered in their usage environment, material, criteria, strength, durability, damage tolerance, maintenance, and quality assurance [6] [19] [20] [21].

4.4. RMSI and MIL-HDBK-516B

In system theory, some accidents result from the dysfunctional interaction among systems components, external disturbance or Human error without any component failure. These interactions should be considered entirely with STAMP and STPA [14]. Thus, reliability, maintenance, safety, and integrity (RMSI) should be considered in the airworthiness process. The airworthiness requirement is presented in MIL-HDBK-516B and described in table 1.

| No. | Property   | Section in MIL-HDBK-516B                                      |
|-----|------------|----------------------------------------------------------------|
| 1   | System Safety | 13. System Safety                                              |
| 2   | Maintenance | 16. Maintenance;10. Diagnostics System                          |
| 3   | Reliability | 4. System Engineering                                          |
| 4   | Integrity   | 5. Structure;6. Flight Technology;7. Propulsion and Propulsion Installations;8. Air Vehicle Subsystem;9. Crew Systems;11. Avionics;12. Electrical system;13. Electromagnetic Environment;17. Armament/Stores Integration;19. Material |

4.5. Airworthiness and RMSI

The relationship among reliability, maintenance, safety, integrity, and airworthiness is shown in figure 4. It can be seen from figure 4:

- The problem of failure can be improved in terms of integrity, reliability and maintainability, and there are already a number of criteria to support such aspects in integrity and reliability.
Not all failures will result in accidents. If the measures are suitable and effective, safety can be guaranteed.

It is not without fault that it is safe, for there may be other complicated causals, such as human factors, environmental factors and interactions.

Traditional methods of safety analysis, control measures and related standards only analyse the causals of components. For the reasons for the interaction among system components, a systematic analysis method such as STAMP/STPA is needed to identify UCAs and its scenes.

Compliance Safety can be guaranteed by relevant standards.

It is necessary to use STAMP/STPA for UCAs and its scenes recognition to ensure effective coping strategies due to new technology and other factors.

5. Conclusions
This paper analyzes the theoretical principles and engineering methodology of airworthiness. An in-depth understanding of the concept of airworthiness is given, and system safety and integrity are regarded as the two main aspects. System safety standards and integrity standards are described to allow analysis of the relationships between reliability, maintenance, safety, integrity and airworthiness. The following are very important to undertake: (1) System Safety Assessment should be carried out for each component, subsystem and the total system. (2) Integrity should be covered in each component. (3) STAMP and STPA should be considered to identify UCAs and their scenarios due to the dysfunctional interaction among components, subsystems.

References
[1] Department Of Defense, MIL-HDBK-516B, Airworthiness Certification Criteria, 2005-2
[2] ARP 4761, Guidelines And Methods For Conduction the Safety Assessment Process On Civil Airborne Systems And Equipment, 1996-12
[3] MIL-HDBK-515, WEAPON SYSTEM INTEGRITY GUIDE (WSIG), 2002-12
[4] Filippo De Florio, Airworthiness, Second Edition: An Introduction to Aircraft Certification, 2011
[5] CCAR-25, Airworthiness Standards: Transport Category: Airplane, R4, 2011-11.
[6] Richard A. Stephans, PE, CSP, System safety for the 21st century, Wiley Inter Science, 2004-12
[7] Department Of Defense, MIL-STD-882E, Standard Practice, System Safety, 2012-5
[8] ARP 4754, Guidance For Development of Civil Aircraft And Systems, 2010-12
[9] ARP 5150, Safety Assessment of Transport Airplane In Commercial Service, 1996-12
[10] ARP 5151, Safety Assessment of General Aviation Airplanes And Rotorcraft In Commercial Service, 1996-12
[11] RTCA Do-297, Integrated Modular Avionics (IMA) Development Guidance And Certification Considerations, 2005-11
[12] RTCA Do-178B, Software Considerations In Airborne Systems And Equipment Certification, 1992-12
[13] RTCA Do-254, Design Assurance Guidance for Airborne Electronic Hardware, 2000-1
[14] Nancy G. Leveson, An STPA Primer, Version 1, MIT, 2013-8
[15] Hu J B, Li J and Zheng L 2017 STAMP Modeling and STPA Safety Analysis of Aviation Four Stations Gas Support Process Advances in Aeronautical Science and Engineering 8(4)
[16] Hu J B and Zheng L 2017. Safety analysis of wheel brake system based on STAMP/STPA Journal of Aeronautics 38(1) 241-251
[17] Zheng L, Hu J and Xu S 2017. Marine Search and Rescue of UAV in Long-Distance Security Modeling Simulation Polish Maritime Research 24(s1)
[18] MIL-STD-1798A, Mechanical Equipment and Subsystems Integrity Program, 2013-8
[19] MIL-HDBK-87244, Avionics/Electronics Integrity, 1995-1
[20] MIL-STD-1530C, Aircraft Structure Integrity Program (ASIP), 2005-11
[21] MIL-HDBK-1783B, Engine Structure Integrity Program (ENSIP), 2004-9