MINISTERO DELLA DIFESA

Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti

Direzione degli Armamenti Aeronautici e per l'Aeronavigabilità

AIRWORTHINESS RESIDUAL RISK IDENTIFICATION AND ACCEPTANCE

Edition 17th November 2023

LIST OF EFFECTIVE PAGES

NOTE: This standard is valid if it consists of the pages listed below, duly updated.

Copy of this Technical Publication may be found at the address:

http://www.difesa.it/SGD-DNA/Staff/DT/ARMAEREO/Biblioteca/Pagine/default_.aspx

The issue dates of the original and amended pages are:

Original…….. 0…….. 17th November 2023

This standard consists of a total of N° 16 pages as specified below:

Page N°	**Amendment N°**
Frontpage……..	0
A……..	0
i…… ……..	0
1 - 11……..	0
A1-A2	0

INDEX

1. INTRODUCTION

1.1. GENERAL

The airworthiness (AW) process follows the methodology defined in the DAAA norms AER(EP).P-2, AER(EP).P-16, AER(EP).P-21 and AER(EP).P-22.

In particular, for each of the AW requirements identified in the applicable Certification Basis, a compliance statement, and inherent supporting evidence, is provided by the System Design Responsible (SDR, as per DAAA AER(EP).00-00-5 norm) or Military Design Organization Approval (MDOA, as per DAAA AER(EP).P-21 norm) Company, in order to achieve the airworthiness certification of a Military Air System configuration.

In carrying this task, a few cases may be encountered, where the design maturity of the System does not consent a full compliance with the specific AW requirements. In such occurrences, an AW Risk (AWR) is identified in the form of a hazard, which needs to be adequately mitigated through System design changes, implementation of bespoke attention getters (warnings, safety switches, etc.), operational limitations or pilot workaround procedures.

The above-listed mitigations aim at downgrading the initial AW risk, hence resulting, for each non-compliance against the approved Certification Basis, into a set of AW Residual Risks (AWRR).

A similar approach, on a lower scale, is also applicable for the identification, mitigation and acceptance of any risks deriving from the continued/continuing AW tasks.

1.2. PURPOSE

The purpose of this Technical Publication (TP) is to define the process for AWRR identification and acceptance.

1.3. APPLICABILITY

The present TP is applicable to all Military/State aircrafts operating on the national territory. It is important to stress that the TP covers the airworthiness risks, from a technical perspective. Operational implications related to the employment of the specific System under scrutiny, along with additional operational mitigations, are evaluated under the responsibility of the Italian Military Aviation Authority and/or the End-User of the Air System.

The evaluation of AW risks applies at different stages of a certification lifecycle:

- Initial airworthiness – release of a Military Type Certificate (MTC,), Restricted MTC (R-MTC), Operational Military Permit to Fly (O-MPtF);
- Continued airworthiness – approval of configuration changes;
- Release of Permit to Fly in accordance with AER(EP).P-7 or AER(EP).P-21;
- Continuing airworthiness – approval of repairs or maintenance plans in accordance

with AER(EP).00-00-5 or AER(EP).P-21;

- Conversion of a Technical Operational Certification (TOC) into a regular Certification as per AER(EP).P-2, AER(EP).P-7, AER(EP).P-9, AER(EP).P-21.

1.4. VALIDITY

The present TP shall enter into force on the date of its approval.

1.5. DEFINITIONS AND GLOSSARY

- ***Airworthiness, Certification Basis:*** refer to AER(EP).P-2, AER(EP).P-21, AER(EP).P-22 norms.
- ***Company System Design Responsible:*** refer to the definitions reported in AER(EP).00-00-5 norm. For brevity, in the rest of this TP it may also be generically referred to as “the Company”.
- ***Company Design Military Organization/Production Approval:*** refer to the definitions reported in AER(EP).P-21 norm. For brevity, in the rest of this TP it may also be generically referred to as “the Company”.
- ***CONOPS*/*ORS:*** it is a programmatic document defining the scenario and the operational need which generate a particular set of high level technical and operational requirements, to be fulfilled through the achievement of a novel operational capability. It generally entails the information and indications about the aspired flight envelope, the mission planning, execution and reporting, the sustainability, maintainability, logistic support, etc.
- ***DAAA Certification Team:*** refer to AER(EP).P-16 norm.
- ***Hazard:*** refer to AER(EP).P-2 and AER(EP).P-6 norms.
- ***Hazard probability:*** refer to AER(EP).P-2 and AER(EP).P-6 norms.
- ***Hazard Risk Index:*** refer to AER(EP).P-2 and AER(EP).P-6 norms.
- ***Hazard severity:*** refer to AER(EP).P-2 and AER(EP).P-6 norms.
- ***Military aircraft, aircraft equivalent to a military aircraft or aircraft of military use:*** refer to definitions included in the Code of Aerial Navigation at reference [1], articles 744, 746 and 748. For brevity, in the rest of the document it will be generically referred to as "the System".
- ***Military Aviation Authority:*** it is identified with the AVIAM Office at the Italian Air Staff.
- ***Mishap:*** refer to AER(EP).P-2 and AER(EP).P-6 norms.
- ***Military Type Certificate:*** refer to AER(EP).-2, AER(EP).P-21 and AER(EP).P-22 norms.
- ***Operational Military Permit to Fly:*** refer to the definitions reported in AER(EP).P-7 and AER(EP).P-22 norms.
- ***Airworthiness risk:*** it refers to the risk acceptance matrix, interleaving the probability of occurrence of a particular hazard or failure condition versus the inherent severity, estimated after the application of the mitigations (procedural, technical, operational, etc.) captured in the documentation prepared in support of the clearance for a flight

mission. For further details about the general definitions of risk matrix, severity, etc. refer to AER(EP).P-2 and AER(EP).P-6 norms.

- ***Restricted Military Type Certificate:*** refer to AER(EP).P-2, AER(EP).P-21 and AER(EP).P-22 norms.
- ***Safety Case:*** Deliverable normally associated, but not precluded to, the RPAS certification category military specific, it represents a technical evaluation of the system safety and airworthiness features of the System under scrutiny. Tightly coupled with the flight mission and the specific scenario defined in the System CONOPS/ORS, it generates a set of recommendations and limitations with the scope of quantitatively calculating the AWRR's and their associated levels. More details can be found in AER(EP).P-22 norm.
- ***Software Criticality Index:*** refer to MIL-STD-882 for the classification of the level of rigour expected to the software.
- ***Technical Assessment:*** Deliverable normally associated, but not precluded to, the RPAS certification category military open, it represents a technical evaluation of the system safety and airworthiness features of the System under scrutiny. Tightly coupled with the flight mission and the specific scenario defined in the System CONOPS/ORS, it generates a set of recommendations and limitations with the scope of qualitatively estimating a generic AWRR level. More information can be found in AER(EP).P-22 norm.
- ***Technical Data Sheet:*** refer to AER(EP).P-2 and AER(EP).P-21 norms.
- ***Technical Operational Certification:*** refer to AER(EP).P-7 and AER(EP).P-9 norms.

1.6. ACRONYMS

AWR	Airworthiness Risk
AWRI	Airworthiness Risk Index
AWRL	Airworthiness Risk Level
AWRR	Airworthiness Residual Risk
AWRRI	Airworthiness Residual Risk Index
AWRRL	Airworthiness Residual Risk Level
CONOPS	Concept of Operations
CTR	Certification Technical Report
DAAA	Military Aiworthiness Authority
EASA	European Aviation and Safety Agency
EDA	European Defence Agency
FDAL	Functional Design Assurance Level
FH	Flight Hour
FMECA	Failure Mode, Effects, and Criticality Analysis

IAW	In Accordance With
IDAL	Item Design Assurance Level
MAA	Military Aviation Authority
MDOA	Military Design Organization Approval
MTC	Military Type Certificate
O-MPtF	Operational Military Permit to Fly
ORS	Operational Requirements Specification
R-MTC	Resctricted Military Type Certificate
RPAS	Remotely Piloted Aircraft System
SC	Safety Case
SDR	System Design Responsible
SwCI	Software Criticality Index
TA	Technical Assessment
TDS	Technical Data Sheet
TOC	Technical Operational Certification
TP	Technical Procedure

1.7. REFERENCE DOCUMENTS

[1] Code of Aerial Navigation, approved through R.D. 30 March 1942, n. 327 (and subsequent amendments)

[2] MIL-STD-882E Department of defense standard practice: System Safety

[3] ARP-4761 Guidelines and methods for conducting the safety assessment process on civil airborne and equipment

[4] ARP-4754 Guidelines for development of civil Aircrafts and Systems

1.8. CORRELATED DAAA NORMS

AER(EP).00-00-5	Configuration control processes for the preparation, evaluation and approval of amendments to material under GDAA responsibility
AER(EP).P-2	Military Type System Certification, Qualification and Fit-For-Installation
AER(EP).P-6	Instructions for the compilation of Technical Specifications for Military Aircrafts

AER(EP).P-7	Regulation for recording and maintaining the Military Aircraft Register
AER(EP).P-9	Technical Operational Certification and Homologation
AER(EP).P-16	Procedure for Military Type Certification
AER(EP).P-21	Certification of Military Aircraft and related Products, Parts and Appliances, and Design and Production Organizations
AER(EP).P-22	Certification of Military Remotely Piloted Aircraft Systems

2. PROCEDURE DESCRIPTION

2.1. GENERAL

The key aspects of the AWRR identification and acceptance process include:

- non-compliance with an applicable AW criterion (or requirement) indicates a potential hazard;
- the risk of an event of hazard is the combination of its severity and probability of occurrence. As it applies to AW, the probability of occurrence is defined as the probability of that event occurring either during a single flying hour (FH) or during a single sortie;
- for those hazards or failure conditions where the estimation of a probability of occurrence is not appropriate (for instance, those modelled by systematic errors or non-linear phenomena), an alternative method is established for the determination of the relevant AWR;
- the DAAA approve AW hazards and risk levels (i.e., severities and probabilities) prior to issue of a Military Type Certificate (MTC), a Restricted MTC or an Operational Military Permit to Fly (O-MPtF);
- a qualitative AWRR assessment is carried out by the DAAA also in the case where no certification artefacts are actually produced; for instance, in support of the release of a flight authorization for Remotely Piloted Aircraft Systems (RPAS) belonging to the certification category military open (in accordance with the AER(EP).P-22 norm), where a Certification Basis is not defined;
- each AWRR is assigned a risk level (AWRRL), ranging from High, Serious, Medium to Low;
- the required level of approval for each AWRR is proportional to its level.

The following paragraphs will present more details with regard to this approach, by making a clear distinction between the non-compliances which can be entirely and comprehensively modelled by a numerical probability of occurrence (for instance those associated to equipment failure rates as derived from an Failure Mode, Effects and Criticality Analysis), from those cases, more qualitative, where such practice is not valid.

It is important to highlight that each of the presented activities are allocated to the DAAA, supported by the Company.

It is also fundamental to remark that the individual tables shown in the following paragraphs are examples taken from the current DAAA norms and the applicable standards. However, each programme will define in its own System Safety Program Plan the safety rules, definitions and infrastrutture, which may differ from those excplicited in the DAAA norms. It will be DAAA duty and responsibility to evaluate, correlate and approve each individual safety System submitted by the SDR/MDOA.

2.2. AW RISKS MODELLED BY SEVERITY AND PROBABILITY

- Identify AW hazards and the associated mishaps that could reasonably occur. AW hazards are related to AW criteria and/or requirements and may be identified from sources including non-compliances with applicable AW criteria and/or requirements, non-standard AW assessments, fielded aircraft inspection findings or mishap investigations.
- Correlate AW hazards with those tracked by System Safety to prevent redundant risk assessments.

  A single risk assessment may be used to satisfy both the AW and the System Safety process if the identified hazard and risk are consistent. Multiple non-compliances with AW criteria and/or requirements may result in the same hazard. Each hazard may be associated with one or more risks.
- Determine the severity category of each event by using the definitions in accordance with (IAW) the AER(EP).P-6 Annex C norm[1].
- Determine the probability level associated with each event by using the quantitative thresholds IAW the AER(EP).P-2 and AER(EP).P-6 Annex C norms[2] . In this context, choose whether to evaluate probabilities per FH or per sortie and observe that such values may change over time. Efforts should be made, in this case, to identify an increasing (or decreasing) probability of occurrence. For weapon employment/jettison, use probability per weapon employment/jettison[3]. For events associated with emergency lifesaving system failures (e.g., escape systems, crashworthy seating, emergency slides, etc.), determine the probability of the event both per use of the System (assuming the System is needed) and/or per FH (or sortie), depending on the availability of information from the Company.

  If the available data do not consent a quantitative calculation of the hazard probability, identify the corresponding qualitative level and document the rationale; an example is reported on Table 1 (source MIL-SDT-882E).

[1] Or the safety table/level used for the specific programme.

[2] Or the specific probability levels defined for the programme.

[3] Aircraft may experience AW risks due to weapon carriage, employment or jettison. During weapon carriage, use probability determined “per FH” or “per sortie”. Upon employment or jettison, until the weapon achieves a safe separation, use probability determined “per weapon employment/jettison.” A weapon that has achieved safe separation from the delivery aircraft is no longer an aircraft AW issue, though the weapon may have its own system safety risks.

QUALITATIVE PROBABILITY LEVELS			
Description	**Level**	**Specific individual Item**	**Fleet or inventory**
Frequent	**A**	Likely to occur often in the life of an item	Continuously experienced
Probable	**B**	Will occur several times in the life of an item	Will occur frequently
Occasional	**C**	Likely to occur sometime in the life of an item	Will occur several times
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely but can reasonably be expected to occur
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item	Unlikely to occur, but possible
Eliminated	**F**	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated

Table 1: Example of qualitative probability levels

- Identify the numerical initial AWR Index (AWRI) and the corresponding AWRL (High, Serious, Medium or Low) at the intersection of the severity category column and probability level row. An example of AWRI, and of the corresponding AWRL, is shown in Table 2. This first assessment of the risk is the initial risk and establishes the fixed baseline for the hazard. (Non-constant probability levels may result in changes in AWRI during the lifecycle of a System).

AWRI		**Severity category**				
Probability level	**Probability per FH or Sortie**	**(1) CAT**	**(2) CRIT**	**(3) MAJOR**	**(4) MINOR**	**(5) NO SAFETY EFF.**
(A) FREQUENT	$1x10^{-3} \leq$ Prob	1A	2A	3A	4A	5A
(B) PROBABLE	$1x10^{-4} \leq$ Prob < $1x10^{-3}$	1B	2B	3B	4B	5B
(C) OCCASIONAL	$1x10^{-5} \leq$ Prob < $1x10^{-4}$	1C	2C	3C	4C	5C
(D) REMOTE	$1x10^{-6} \leq$ Prob < $1x10^{-5}$	1D	2D	3D	4D	5D
(E) IMPROBABLE	Prob < $1x10^{-6}$	1E	2E	3E	4E	5E
(F) ELIMINATED	Prob = 0	1F	2F	3F	4F	5F

HIGH | SERIOUS | MEDIUM | LOW | NO RISK

Table 2: Example of AWRI/AWRL for risks modelled by a probability

- Identify risk mitigation measures (both short-term and long-term), that will be implemented prior to risk acceptance, and estimate the associated event risk[4].
- Re-assess the AWRI and AWRL after the application of such measures, in order to determine the resulting mitigated AWRRI and AWRRL, by re-running the same table as per the initial risk assessment.
- Identify the proposed risk acceptance duration.
  If the proposed risk acceptance duration is the entire lifecycle, identify a process for periodic re-accomplishment of the AWRRL, which validates previous assumptions using accrued data and reassesses potential mitigations considering technological advances and process changes. Identify the date when re-accomplishment is required.

2.3. AW RISKS NOT MODELLED BY SEVERITY AND PROBABILITY

Software, Firmware

The increased level of complexity introduced by digital technologies such as software, complex electronic hardware, or Multicore Processors makes it difficult to examine the behaviors and properties of a system by direct inspection, analysis or test. The classical concept of deducing random failure rates, used in traditional System Safety methodologies, result in an incomplete safety assessment, as the failures of the digital technologies are mostly characterized by systematic failures, which are hard to predict and quantify.

One methodology to control systematic failures, and in particular those caused by design and implementation errors, is presented in the ARP-4754 (reference [4]) and consists into the achievement of an adequate level of rigor and assurance for the subsequent and inherent development process (Functional/Item Design Assurance Level, FDAL/IDAL). Another method is proposed in the MIL-STD-882 (reference [2]), with the introduction of the “software criticality index”.

Independent from the adopted methodology, a design shortfall/AW non-compliance detected on a software/firmware carries a different level of AW risk, depending on its expected IDAL/SwCI. An example is shown on Table 3.

SwCI / IDAL	AWRL	Notes
SwCI 1/ IDAL A	High	If the software tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH
SwCI 2/ IDAL B	Serious	If the software tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS
SwCI 3/ IDAL C	Medium	If the software tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM

[4] Using the same order of precedence as in MIL-STD-882/ARP-4671, in terms of design improvements, attention getters implementations, introduction of flight limitations or pilot compensation procedure. On this regard, it is important to highlight that the source of the mitigation, if any, may derive from different stakeholders (MAA, aircraft user, maintenance organization, etc.)

SwCI 4/ IDAL D	Low	If the software tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW
SwCI 5/ IDAL E	No Risk	No safety specific analyses or testing is required

Table 3: Example of AWRL and AWRRL for risks introduced by sw

Structures

Similar considerations as per software apply also to the evaluation of the risks associated to structural failures and shortfalls.

Depending on the significance of the structure in terms of airworthiness, any relevant non-compliance will have a different effect on the characterization of the initial and the residual risk.

For instance, a shortfall identified on a safety-of-flight structural element can bear remarkable consequences on the Air System, and normally leads to significant limitations and restrictions in the MTC accompanying Data Sheet. If unmitigated, such issues open to a potentially high residual risk, which needs to be formally acknowledged and accepted.

For more information about the categorization of an aircraft structure, refer to AER(EP).P-6 norm.

Establishment of the most suitable method

Similar considerations as per paragraphs 2.3.1 and 2.3.2 apply, for instance, to other disciplines like the ElectroMagnetic Compatibility and Interference.

Due to the vast range of subjects potentially falling into the category of AWR not modelled by severity and probability, this TP cannot be excessively prescriptive and granular. Nevertheless, the key message to extrapolate from this argumentation lies on the necessity, for the DAAA Certification Team, to establish the most suitable method to estimate the AWR for each individual topic.

2.4. AWR acceptance

After the identification and estimation respectively of the AWRI, AWRL, AWRRI and AWRRL as per previous paragraphs, the DAAA Certification Team will document the risk assessment and the adopted rationale.

The last step of the process consists into obtaining the approval of the associated initial and mitigated AWRI and AWRL. An example is illustrated in Table 4, which is expected to be included in the Technical Report in support of an MTC/R-MTC or the Safety Case in support of an O-MPtF. Such acceptance will be realized through the last signature placed on these documents.

It is anticipated that a particular Air System configuration, given the extent of the non-compliances and of the AWRRL's, may not achieve certification.

A bespoke module mapping AWRI, AWRL, applicable mitigations and resulting AWRRI and AWRRL is shown in attachment A. This module should accompany the produced deliverables in support of every clearance and signed by the certification Authority, IAW the applicable level of approval as per table 4.

Approval Level	High	Serious	Medium	Low	No Risk
DAAA Director	NO acceptance	X			N/A
DAAA Vice Technical Director	NO acceptance		X		N/A
Head of Airworthiness Office	NO acceptance			X	N/A

Table 4: AW Risk level of acceptance

2.5. INITIAL AIRWORTHINESS

For the initial airworthiness process, the AWR has to be established at the beginning of the programme, so to provide means and grounds for the application of the present TP.

2.6. CONTINUED/CONTINUING AIRWORTHINESS

For modifications to Air Systems, change to maintenance plans, major repairs to an approved configuration, a process similar to the one described at para 2.4 will be applied.

In these cases, the DAAA evaluates whether new AWRs are introduced by the changes, and/or whether any of the extant AWR (and relevant AWRRL) are affected by them, and update the matrix accordingly[5].

2.7. CONVERSION OF THE TOC

AWRs may also derive from the process of converting a TOC into a regular Certification as per AER(EP).P-2 and AER(EP).P-21 norms. This is due to the fact the TOC process generally accepts design and operational tradeoffs for the sake of achieving a capability in response to an urgent operational need.

The process described in the paragraph 2.4 will therefore be applied, with the scope of identifying such risks, and the relevant level of mitigation and acceptance.

[5] For instance, an AWR may be represented by the application of a waiver or a delay with respect to the application of the change.

2.8. UPDATING THE AWRRL

The AWRRL matrix can be updated/extended at the occurrence of any of the following cases:

- the Company propose a design change/improvement which affects the corresponding AW criteria and/or requirements (as described in paragraph 2.3);
- the deadline for reviewing the AWRRL matrix is expired;
- the Company propose a re-visitation of any of the AWRRL (based on new evidence, for instance).

3. LEGACY PROGRAMMES

For legacy programmes where a dedicated AWR acceptance table may not be present, the process described in this TP has to be tailored and an appropriate risk matrix be determined (for instance by adopting MIL-STD-882E), supported by an adequate rationale.

4. CONTRACTUAL AW PENALTIES

Although this TP aims at providing guidelines for the definition and acceptance of the AWRs, it should not be perceived as a workaround manoeuver to relax the certification and AW demands on a Company.

On this regard, it is important to stress that a Company should always aim at the resolution of every AW hazard before achieving a full, unrestricted MTC.

From this standpoint, the Certification Team is responsible to liaise with the procurement and contractual articulations of the DAAA, in order to stimulate the inclusion of specific AW penalties in the contracts.

Attachment A

AW Residual Risk Identification and Acceptance Module

Non Compliance	Hazard related to the Non-Compliance	AW Risk Level	Mitigations	AW Residual Risk Level	Required Approval Level	Approval Signature