RA 5890 – Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design

Rationale

Cyber vulnerabilities in Air Systems represent a significant threat to Type and Continuing Airworthiness and Air Safety. Cyber Security for Airworthiness (CSA) measures are required to identify and mitigate against inadvertent or malicious introduction of such cyber vulnerabilities, to maintain Airworthiness. This RA sets out the CSA requirements for Air System Type Design and Changes / Repairs to Type Design throughout the life of an Air System.

Contents

Regulation 5890(1)

Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design

5890(1) Type Airworthiness Authorities (TAA)[1] **shall** ensure Air System Type Design[2] and Changes / Repairs to Type Design[3] are assessed for cyber threats, which once identified are suitably mitigated to combat the potential negative impact on CSA and Air Safety; this applies to all Air Systems on, or destined for, the UK Military Aircraft Register (MAR).

Acceptable Means of Compliance 5890(1)

Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design

1. TAAs **should** use a recognized Cyber Security Risk Assessment and mitigation process[4], this can be as part of Air System Certification activity[2].

2. The fundamental requirements of any such process **should** identify:

   a. Cyber security threats (“Threat Conditions” in DO-326A).

   b. How cyber security threats can be caused (“Threat Scenarios” in DO-326A).

   c. The severity and likelihood (“Level of Threat” in DO-326A) covering each identified threat.

   d. Suitable mitigation (“Security Measure” in DO-326A) to manage the Level of Threat.

3. The TAA **should** provide appropriate Instructions for Sustaining Type Airworthiness (ISTA)[5] to the relevant Aviation Duty Holder (ADH) / Accountable Manager (Military Flying) (AM(MF)), including security event management procedures[6]. This is consistent with RTCA DO-355A / EUROCAE ED-204A, which refers to Instructions for Continuing Airworthiness (ICA)[7], the civil equivalent of ISTA.

[1] Where the Air System is ►not UK MOD owned, Type Airworthiness (TAw) management◄ regulatory responsibility by either the TAA or Type Airworthiness Manager (TAM) needs to be agreed within the Sponsor’s approved model ►◄ ; refer to RA 1162 – Air Safety Governance Arrangements for Civilian Operated (Development) and (In-Service) Air Systems or refer to RA 1163 – Air Safety Governance Arrangements for Special Case Flying Air Systems. Dependant on the agreed delegation of TAw responsibilities TAM may be read in place of TAA as appropriate throughout this RA.

[2] Refer to RA 5810 – Military Type Certificate (MRP Part 21 Subpart B).

[3] Refer to RA 5820 – Changes in Type Design (MRP Part 21 Subpart D), and RA 5865 – Repairs (MRP Part 21 Subpart M).

[4] Refer to Radio Technical Commission for Aeronautics (RTCA) DO-326A – Airworthiness Security Process Specification; or EUROCAE ED-202A – Airworthiness Security Process Specification. DO-326A / ED-202A is accompanied by associated DO-356A / ED-203A – Airworthiness Security Methods and Considerations.

[5] Refer to RA 5815 – Instructions for Sustaining Type Airworthiness.

[6] DO-392 / ED-206 – Guidance on Security Event Management are recognized standards.

[7] Refer to RTCA DO-355A / EUROCAE ED-204A – Information Security Guidance for Continuing Airworthiness (note that DO-355 is titled ‘Continued Airworthiness’, DO-355A still refers to Continuing Airworthiness throughout the standard despite title of document).

Acceptable Means of Compliance 5890(1)

4. Upon a change (ie Change / Repair to Type Design) to the Air System that affects the known cyber threats or generates new known threats[8], the TAA **should** inform the ADH / AM(MF), to gain acceptance of any increased Risk[9].

5. During the process used to identify cyber security threats, the security measures **should** be consistent with the principles of JSP 440[10].

Note:

> JSP 440 is aimed at all security threats, not only those necessary to preserve Air Safety and Airworthiness, but ensuring consistency helps to integrate CSA into the wider security arrangements. This is consistent with Defence Standard (Def Stan) 00-970[11] Guidance Material (Parts 1,3,5 and 7) Guidance for Cyber Security Airworthiness para b, which acknowledges that JSP 440 does not cover design Assurance.

Guidance Material 5890(1)

Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design

6. To harmonise the approach taken to address Risks to CSA, as in RTCA DO-326A / EUROCAE ED-202A and RTCA DO-356A / EUROCAE ED-203A, this RA captures the considerations for Air System Type Design and Changes / Repairs to Type Design. It is recognized that DO-326A / ED-202A has been developed for use on large civil Aircraft. As such, some tailoring of the guidance provided therein may be required for military Air Systems.

Note:

> RA 1202[12] sets out the CSA operational requirements for management of cyber threats throughout the life of an Air System, based on the principles of the MOD Cyber Compliance Framework[13].

7. **Supply Chain Risk Management.** Information for the Assurance of the supply chain may be found in Def Stan 05-138[14] and Def Stan 05-135[15] (eg counterfeit materiel may not meet the original manufacturer specifications, undermining protection assumptions, and compromised materiel could deliberately introduce vulnerabilities). The National Cyber Security Centre (NCSC) also provides guidance on Assurance of supply chains.

8. **Comparison to Air System Safety Assessment**. The similarity of security assessment to Safety Assessment is already acknowledged by Def Stan 00-970 (Parts 1,3,5 and 7) Guidance Material. This similarity can be exploited to utilize the two assessments during System development, as well as improve the understanding of security considerations (by comparing them to those for Safety). The following table suggests such a comparison:

Table 1 – Mapping Between Security and Safety Assessment Terminology

Security term	DO-326A section	Corresponding Safety term
Threat Condition (which "… arise [from] vulnerabilities")	3.2.1 para 1	Hazard (or "Failure Condition*" in Aerospace Recommended Practices (ARP)
Threat Scenario ("…lead[s] to threat conditions")	3.2.2 para 2	Cause

[8] RTCA DO-356A details both acceptable qualitative and quantitative methods of Risk Assessment.
[9] Refer to RA 1015 – Type Airworthiness Management – Roles and Responsibilities, and RA 1210 – Ownership and Management of Operating Risk (Risk to Life).
[10] Refer to JSP 440 – The Defence Manual of Security.
[11] Refer to Def Stan 00-970 – Design and Airworthiness Requirements for Service Aircraft.
[12] Refer to RA 1202 – Cyber Security for Airworthiness and Air Safety.
[13] A copy of the MOD Cyber Compliance Framework should be requested from the contracting organization.
[14] Refer to Def Stan 05-138 – Cyber Security for Defence Suppliers.
[15] Refer to Def Stan 05-135 – Avoidance of Counterfeit Materiel.

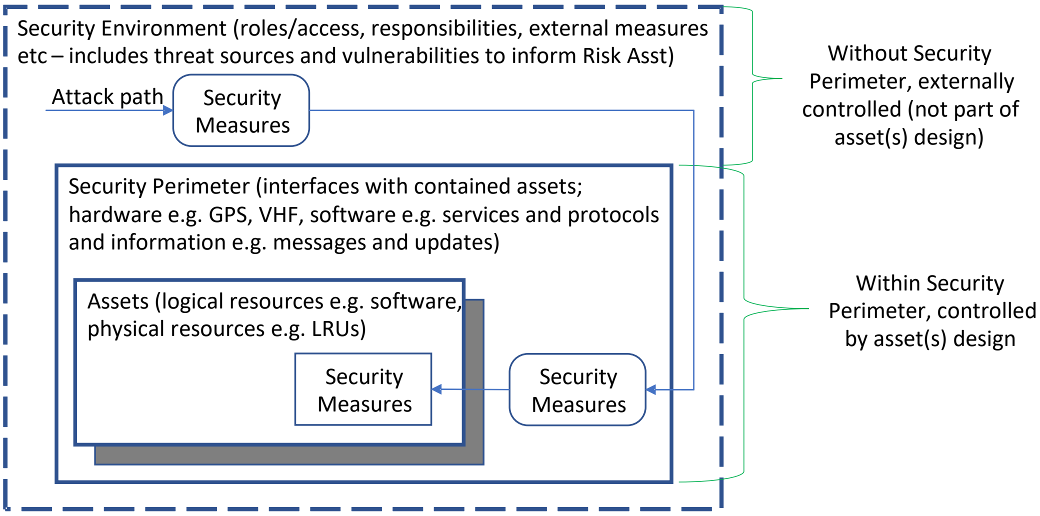
Guidance Material 5890(1)

Security Measure	3.2.3 (see also 3.4.2)	Mitigation / Control / Barrier
Security term	**DO-326A section**	**Corresponding Safety term**
Level of Threat ("the possibility that threat scenarios cause a threat condition")	3.2.4 para 1	Hazard probability (from combined causes)

** Failure Condition is a better mapping, as that has Safety effects and severity (which a Hazard would normally not have)*

9. **Security Risk Assessment**. Security Risk Assessment is performed on the Security Architecture (see Figure 1), as defined in DO-326A para 3.4.1, and identifies Security Risks. If these Risks are acceptable without further mitigation, the following sections (Security Effectiveness (DO-326A 3.3) and Security Development (DO-326A 3.4)) are not required.

Figure 1 – DO-326A Basic Concepts, Showing Scope of Security Assessment


Security Environment (roles/access, responsibilities, external measures etc – includes threat sources and vulnerabilities to inform Risk Asst)
Attack path
Security Measures
Without Security Perimeter, externally controlled (not part of asset(s) design)
Security Perimeter (interfaces with contained assets; hardware e.g. GPS, VHF, software e.g. services and protocols and information e.g. messages and updates)
Assets (logical resources e.g. software, physical resources e.g. LRUs)
Security Measures
Security Measures
Within Security Perimeter, controlled by asset(s) design

10. If further Security Measures are required to discharge the Security Effectiveness section (3.3) of DO-326A, this can be considered equivalent to Risk Reduction in the Safety Assessment process. The security process takes the Security Risk Assessment outputs and determines what level of Security Effectiveness is required. Security "Effectiveness" (DO-326A para 3.3.2.1) considers the combination of Threat Level (Probability) and Severity.

11. **Security Measures**. Security Measures (as defined in DO-326A para 3.2.3) are developed in two main parts:

a. Security Development (requirements, architecture); part of an Air System's development.

b. Security Assurance (vulnerability mitigation through Development Assurance Levels); part of integral (Safety) processes (eg Verification and Validation).

Note: DO-326A causes potential confusion by mixing the terms Security Development and Security Assurance in para 3.3.2.3.

12. **Security Effectiveness Requirements**. Security Effectiveness Requirements (DO-326A para 3.3.2.2) are equivalent to Derived Safety Requirements, in that they aim to reduce the Risk to a level that is acceptable. In this way, they are derived ("bottom-up"), as opposed to requirements which are "top-down" (flowed down from an Air System's requirements).

13. **Security Development**. Security Development is the final main part of the DO-326A process, described in its section 3.4. Its main purpose aims to develop and categorise the required Security Measures, developed as part of Security Development and Assurance (see above). Security Measures can be likened to any

Guidance Material 5890(1)

other functional requirements, and so can be developed using processes already in place to comply with ARP 4754A[16] or equivalent.

Note:

> DO-326A section 2 and Appendix A are closely tied to ARP 4754A, so its use within the MRP for CSA considerations is consistent with other military usage of ARP 4754A.

14. Security Measures are developed in two main categories:

    a. Technical (functions, systems).

    b. Procedural (including policies and human interactions).

15. **Verification of Security Measures**. Verification of Security Measures includes testing that would apply to any other requirement (ie correctness of implementation and robustness, as well as specific-to-security vulnerability testing and / or analysis[17]). It is important to note that with modern complex Air Systems, testing alone cannot give sufficient Assurance, and so analysis is almost always required in addition to testing.

16. **Cyber Security Artefacts**. Although the list is not exhaustive, the below artefacts are detailed in DO-326A, which is an AMC for Def Stan 00-970 alongside DO-356A:

    a. Plan for Security Aspects of Certification (PSecAC).

    b. Aircraft Security Scope Definition (ASSD).

    c. System Security Scope Definition (SSSD).

    d. Preliminary Aircraft Security Risk Assessment (PASRA).

    e. Preliminary System Security Risk Assessment (PSSRA).

    f. System Security Risk Assessment (SSRA).

    g. Aircraft Security Risk Assessment (ASRA).

    h. Plan for Security Aspects of Certification Summary (PSecAC Summary).

17. The PSecAC will describe how the intent of DO-326A will be met, with the content based on section A.1.1 of DO-326A. The ASSD and SSSD are used to determine the scope of the Air System for cyber / information security, as well as the interaction the Air System may have with external systems; this scope will be the foundation of a PASRA / PSSRA.

18. Undertaking a PASRA / PSSRA will identify threat conditions and threat scenarios, assessing an Air System’s security Risks at Aircraft / system level respectively. Security Assessment Criteria (SAC) and Airworthiness Security Risk Matrix are examples of tools used to facilitate a PASRA.

19. Completion of an ASRA and SSRA is used to identify threat conditions and threat scenarios and assess the Air System’s cyber security threats and vulnerabilities. Following this activity, Risk mitigation strategies are then developed and assured in accordance with DO-326A. The results of the analysis and subsequent assessments with associated mitigations are then summarised in the PSecAC Summary, before being communicated to the ADH / AM(MF), including any residual Risks or areas where there are gaps in analysis.

[16] Refer to ARP 4754A – Guidelines for Development of Civil Aircraft and Systems.

[17] A weakness of DO-326A is that analysis is limited to that of test results, as opposed to the more systematic approach (eg architectural analysis).