Regulatory Notice

Military Aviation Authority
MAA

16 Nov 21

MAA/RN/2021/11 – MAA General Guidance for Cyber Security for Airworthiness

Issue

1. The Regulated Community (RC) requires clearer definitions for the intent and objectives of Cyber Security for Airworthiness (CSA), as outlined in Def Stan 00-970[1], and the term Cyber Vulnerability Assessment which has become confused with Cyber Vulnerability Analysis.

Scope

2. This Regulatory Notice (RN) is intended as an informative correspondence for the whole RC, differentiating CSA from conventional Cyber Security and clarifying the term Cyber Vulnerability Assessment.

Implementation

3. This guidance is effective immediately.

Background

4. CSA was included in Def Stan 00-970 in 2015 as an Airworthiness requirement and references the Civilian standards[2] RTCA DO-326[3], DO-355[4] and DO-356[5] alongside JSP440[6] as Acceptable Means of Compliance (AMC). The AMC was designed for large passenger Aircraft during development. Retrospective application of the standard requires the RC to identify and generate evidence for military deltas and differing Aircraft types. The AMC has a focus on rectifying software vulnerabilities and shortfalls during development which is often impractical on an in-service system.

5. Following the addition of CSA in Def Stan 00-970, no additional guidance was added to the Regulatory Articles (RA) to explicitly delegate the responsibilities of CSA on Air Systems. However, on 4 Jun 20, further to the MAA Risk Exposure Forum, a note[7] was drafted to Operational Duty Holders (ODH) directing that the RC begin to undertake Cyber Vulnerability Assessments, the outputs of which should form part of supporting evidence for Safety. However, further to the MAA note, the RC continues to express uncertainty with the application of CSA and Cyber Vulnerability Assessments.

6. The DE&S Airworthiness Team Software Centre of Excellence (DAT SCoE) are developing a framework that will provide guidance to the RC. It will detail how to undertake CSA baselining using existing management systems within the Delivery Team and Operator Area of Responsibility. However, with the publication of this work still pending, the RC are routinely translating CSA as a conventional Cyber Security function. This often involves confusing CSA with Accreditation

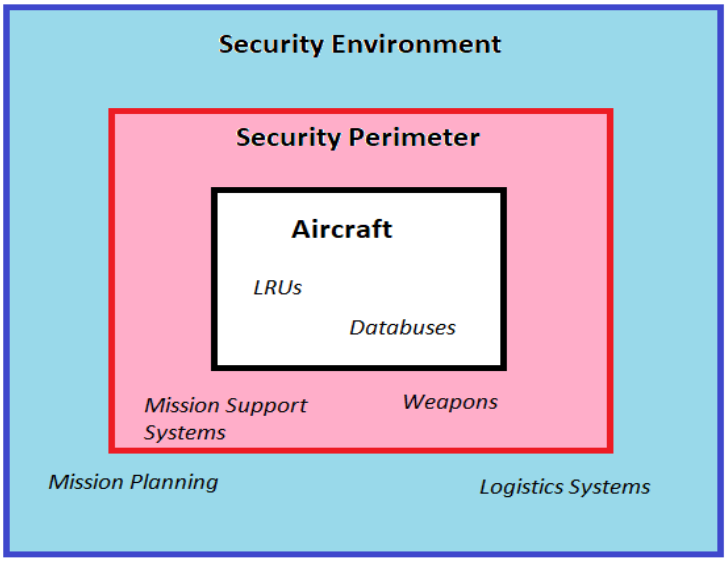
[1] Refer to Def Stan 00-970 'Design and Airworthiness Requirements for Service Aircraft'.
[2] Please note that standards are listed agnostic of version numbers. This notice is to cover the application of all versions of RTCA DO 326/355/356.
[3] Refer to RTCA DO 326 / ED-202 'Airworthiness Security Process Specification'.
[4] Refer to RTCA DO 355 / ED-204 'Information Security Guidance for Continuing Airworthiness'.
[5] Refer to RTCA DO 356 / ED-203 'Airworthiness Security Methods and Considerations'.
[6] Refer to JSP 440 'Defence Manual of Security and Resilience'.
[7] 20200604-DMAA_MOC_REF Letter 20.2-OS.

activity – the latter of which is focused around JSPs 440, 604[8] and 892[9]; policies that are not concerned with Safety or Airworthiness.

CSA

7. CSA is an activity focused around ensuring Safety and Airworthiness. It is the application of Cyber Security principles onto systems that have a direct or indirect interface to Safety Related Systems (SRS). Through mapping the SRS of an Air System and completion of a holistic risk assessment a CSA baseline is generated. Def Stan 00-970 references RTCA DO-326a as AMC. The AMC recommends separating the interface mapping exercise into 3 areas: Aircraft, a security perimeter, and a security environment. An illustrative example is shown in Figure 1. By completing a full mapping of information interfaces into SRS a baseline is generated.

Figure 1. Illustrative Example of RTCA DO-326A Holistic CSA Risk Assessment



8. Once baselining is complete, in line with AMC guidance, risk management activity can occur, implementing controls, mitigations or risk toleration as required. Management processes for the review, renewal and revision of baselines, sustainment of Type Airworthiness, risk management and system changes are also required; ensuring that a security risk management process doesn't introduce potential vulnerabilities to SRS and, thus, Risk to Life (RtL).

9. This activity will likely be informed by the security evidence that is generated from extant security processes, such as system accreditation. However, it cannot be accomplished without SRS baselining activity that is completed with an aim to secure the Safety and Airworthiness of the Air System. Similarly, thought must be given during risk management activity as to whether a given risk presents RtL.

Cyber Vulnerability Assessment

10. In the MAA correspondence issued to ODH[7], the term Cyber Vulnerability Assessment, abbreviated CVA, was used to encourage ODH to begin baselining Air Systems. Unfortunately, the term CVA is also used for a Cyber Vulnerability Analysis – a process that is conducted after a Cyber Vulnerability Investigation (CVI) has taken place. A CVI is a security investigatory process (sometimes involving penetration testing) that uses a DSTL developed framework to identify Cyber

[8] Refer to JSP 604 'Defence Manual for Information and Communications Technology (ICT).
[9] Refer to JSP 892 'Risk Management'.

Vulnerabilities, the final product of which is often a complex and technical breakdown of system design, architecture, vulnerabilities and proposed / possible remediation. These complex reports are analysed, producing a summary, known as a Cyber Vulnerability Analysis.

11. The term Cyber Vulnerability Assessment was used to describe the mapping of interfaces (described above under CSA), followed by a vulnerability analysis into SRS on the Air System and within the security perimeter / environment, that, if compromised, might undermine Air System Safety. By beginning the process of Assessment, the RC were requested to use outputs to support safety arguments. The body of this vulnerability assessment can be informed by existing security information (produced as part of system accreditation or comparable processes) but must place analysis of risk to Safety and Airworthiness at the core.

DAT SCoE CSA Framework for Retrospective Certification

12. The DAT SCoE Lead is developing a framework to enable the retrospective assessment and analysis of in-service Air Systems that meets the intent and objectives of CSA AMC. The ongoing work will include risk assessment templates and propose a methodology to integrate CSA activity into existing management structures to alleviate potential additional resource burdens on the RC. Currently, there are several templates in beta-testing which can be made accessible to those looking to begin the process of identifying and understanding CSA on their respective Air Systems.

MAA Regulatory Publication CSA Review

13. The MAA Cyber-Software Certification team are currently undertaking a review of the MAA Regulatory Publications (MRP) that will integrate Cyber Security within Airworthiness practices and Safety Culture. The aim of this work is to clearly define responsibilities within the delivery and operational space and enshrine Cyber Security Airworthiness and Programmable Elements Certification within existing vocabulary and terminology.

Summary

14. CSA, as mandated through Def Stan 00-970, is the baselining, vulnerability assessment and ongoing management of Cyber Security controls to protect the Safety and Airworthiness of an Air System. It is not covered through System Security Accreditation and requires explicit understanding of communication interfaces into SRS that allows for risk assessment to identify potential RtL. Guidance is in development by the DAT SCoE and the MAA are currently reviewing the MRP with an aim to make revisions that clearly outline roles and responsibilities for CSA implementation and ongoing management.

Queries

15. Any observations or requests for clarification on the content of this RN should be submitted by email to DSA-MAA-MRPEnquiries@mod.gov.uk.

16. Any requests for further guidance on the application of CSA should be submitted by email to DESDAT-Team@mod.gov.uk.

MAA Head of Regulation and Certification