

RA 3132 - Air Traffic Management Equipment Safety Cases

Rationale

► *Air Traffic Management (ATM) Equipment types are complex and often have unique and emerging capabilities that present complicated developmental challenges; moreover, the operation of ATM Equipment presents a foreseeable and credible Risk to Life (RtL). A simple Risk Assessment will not be sufficient to assess the potential impact of these RtL, whereas the use of a Safety Case (SC) provides the ability to understand the cumulative and / or interrelated Risks from the use of the complex equipment. This Regulatory Article (RA) requires that all ATM Equipment has a robust SC that will demonstrate that the ATM equipment is, or will be capable of being, safe to operate and operated safely for a given application in a given operating environment.* ◀

Contents

- 3132(1): Air Traffic Management Equipment Safety Cases
- 3132(2): Responsibilities of Duty Holder-Facing Organizations
- 3132(3): Air Traffic Management Equipment Safety Case Management Process
- 3132(4): Air Traffic Management Equipment Safety Case Amendments
- 3132(5): Air Traffic Management Equipment Safety Case Reports
- 3132(6): Air Traffic Management Equipment Safety Case Independent Assessment
- 3132(7): Specific Site / Operating Area Safety

Regulation 3132(1)

Air Traffic Management Equipment Safety Cases

3132(1) The Delivery Team (DT) ►¹ ◀ **shall** be responsible for ensuring that a 4-part ATM Equipment SC is developed for all new and significantly² modified ATM Equipment.

Acceptable Means of Compliance 3132(1)

Air Traffic Management Equipment Safety Cases

1. The 4-part ATM Equipment SC³ **should** show that Risks are reduced so that they are As Low As Reasonably Practicable (ALARP) and Tolerable, through auditable and evidence-based arguments.
2. The approach described in Def Stan 00-56⁴ **should** be adopted for the auditable production of SCs.
3. The ATM Equipment SC **should** clearly describe the evidence and arguments used to justify the Safety of the equipment and its operation, so that agreement can be reached on the validity of the conclusions. It will be structured hierarchically, and the Safety justification summarized in a series of ATM Equipment SC Reports (SCRs).
4. An ATM Equipment SC **should** provide evidence that:
 - a. Safety requirements have been met.
 - b. Hazards have been adequately identified and analyzed, and associated Risks assessed in an appropriate manner.
 - c. All identified Hazards and Accidents have been addressed and controls applied, to ensure all residual Safety Risks have been reduced so that they are ALARP and Tolerable.

¹ ► Any reference to a DT within this RA also includes any organization responsible for delivering ATM Equipment, whether or not they are a Defence Equipment & Support (DE&S) DT; this includes Platform Authorities and other project teams with a similar remit. ◀

² See para 10.

³ Based on industry good practice.

⁴ Refer to Def Stan 00-56 – Safety Management Requirements for Defence Systems.

**Acceptable
Means of
Compliance
3132(1)**

- d. The system complies with all relevant Safety legislation, Regulations and standards.
 - e. All measures have been taken to ensure that Safety levels achieved can be sustained through life, both in operation of the system and through support.
 - f. The service can be terminated safely and the systems can be disposed of safely.
5. An ATM Equipment SC **should** demonstrate how Safety has been, is being and will be achieved and maintained.
 6. The 4 parts of the ATM Equipment SC **should** be:
 - a. Part 1 - Requirements. This part **should** establish and refine the Safety requirements for the system and the likely Safety Risks that the implementation of the User Requirement Document (URD) may present (eg a Preliminary Hazard Identification).
 - b. Part 2 - Design. This part provides the justification and evidence that a system is safe and suitable for its designed purpose (including demonstrating that the system complies with applicable Safety, operating and Maintenance Regulations). If more than one capability option is being explored the ATM Equipment SC Part 2 **should** be initiated during the Assessment phase, and when a solution is identified, the ATM Equipment SC Part 2 **should** be progressively refined and updated for the chosen solution alongside its Development and Manufacture.
 - c. Part 3 - Introduction to service. This part **should** provide evidence that the installation and transition will be safe and provide details of the proposed testing and commissioning plan, and any fallback options. Depending on the installation and transition arrangements this may have site specific elements within it.
 - d. Part 4 - In-Service. This part **should** provide details of how the equipment will be operated safely and includes any specific configuration issues or limitations from the Release into Service Process (RiSP)⁵. The ATM Equipment SC Part 4 will contain generic and site specific information. This could lead to one document for each site or annexes to a main document.
 7. The users requirements are instrumental to the ATM Equipment SC Part 1 and **should** include definitions of Risk tolerability and Safety budget apportionment.
 8. If other related SCs are already in existence they **should** be integrated as necessary, this may include integration with other ATM Equipment SCs or as input into Air Systems SCs and ship SCs.
 9. Any dependencies on other organizations **should** be recorded in the ATM Equipment SC.

**Guidance
Material
3132(1)**

Air Traffic Management Equipment Safety Cases

10. For the purposes of this Regulation modifications will be classed as significant when:
 - a. They change the way components of the functional system are used; or
 - b. The changes to equipment, either hardware or software, could affect the functional performance of the ATM equipment; or
 - c. The changes affect equipment configuration, excluding changes during Maintenance, repair and alternative operations that are already part of the accepted operational envelope; and

⁵ Refer to RA 3134 – Air Traffic Management Equipment Release into Service Process.

**Guidance
Material
3132(1)**

- d. They are not classified as minor in accordance with RA 3134(1)⁶.
11. A SC is defined as a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment⁴.
12. The degree of evidence required, and work involved in developing an ATM Equipment SC will be commensurate with the Risk posed by a particular system, its complexity and maturity.
13. The generation of an ATM Equipment SC is an iterative process and will start at the beginning of the system's / equipment's lifecycle.
14. The DE&S Project Orientated Safety Management System (POSMS) provides procedures and examples of good practice for developing SCs.
15. It is expected that the ATM Equipment SC Part 1 will contain the following information:
- a. Scope and assumptions.
 - b. User requirements or a reference to the URD.
 - c. Safety requirements and targets.
 - d. The equipment's operating context and environment.
 - e. Legislative and regulatory requirements.
 - f. Reference to appropriate MOD policy.
 - g. Military and civil standards to be complied with.
 - h. Any Safety Risks generated by the implementation of the URD.
 - i. Risk targets, tolerability criteria and the application of the ALARP principle.
 - j. Safety integrity requirements and derived Safety requirements.
 - k. Criteria against which the Safety performance will be measured.
16. It is expected that the ATM Equipment SC Part 2 will contain the following information:
- a. Details of the equipment design and function.
 - b. Demonstration that the equipment design meets the requirements set out in the ATM Equipment SC Part 1 and the System Requirements Document (SRD).
 - (1) This is to include demonstrating compliance with applicable legislation and Regulations, and more importantly where it does not comply.
 - c. Justification and evidence that the equipment is safe and suitable for its required purpose.
 - d. Evidence that there are no unsafe interactions with other equipment and that any required interactions / dependencies work correctly.
 - e. Evidence of how Risks have been mitigated through the design and details of remaining Risks that are mitigated through procedures.
 - f. The Hazard Log.
 - g. Demonstration that remaining Risks have been reduced so that they are ALARP and Tolerable.
17. It is expected that the ATM Equipment SC Part 3 will contain the following information:
- a. Confirmation that all Safety requirements have been met and Hazards are at a level where they can be agreed by the Aviation Duty Holder-Facing

⁶ Refer to 3134(1): Air Traffic Management Equipment Release into Service Process.

**Guidance
Material
3132(1)**

organization and highlighted to the relevant Duty Holder (DH) where appropriate.

- b. Details of the installation, testing and commissioning and transition plan / processes for the equipment and people, and where required platform integration.
- c. Evidence that the installation, testing and commissioning and transition processes are acceptably safe.
- d. Any dependencies on other equipment and how this will be managed and assured.

18. It is expected that the ATM Equipment SC Part 4 will contain the following information:

- a. How the equipment will be operated In-Service (including site specifics) which will include people, processes and equipment, eg Maintenance and training policies and operating procedures / documentation.
- b. Limitations of use and Safety related restrictions which have been imposed on the operation of the equipment. Limitations may come from the design, Risk mitigations or the RiSP.
- c. Any specific configurations for the site / operating area.
- d. Emergency and contingency arrangements and measures to ensure provision of adequate escape and / or emergency arrangements, if Accidents were to occur.
- e. Safety performance monitoring arrangements.
- f. The process for making changes to the In-Service operation and the associated ATM Equipment SC changes.

**Regulation
3132(2)**

Responsibilities of Duty Holder-Facing Organizations

3132(2) DH-Facing organizations involved in the provision of ATM **shall** be accountable to DHs for the provision of ATM Equipment SCs.

**Acceptable
Means of
Compliance
3132(2)**

Responsibilities of Duty Holder-Facing Organizations

19. Commanders and Accountable Managers in DH-Facing organizations **should** be individually accountable to DHs for the performance, Safety and integrity of those ATM Equipment SC elements for which they are responsible or the services that they provide. Their responsibilities **should** be laid down in an auditable manner.

**Guidance
Material
3132(2)**

Responsibilities of Duty Holder-Facing Organizations

20. Examples of DH-Facing organizations in the context of RA 3132(2) are Air Command Air Officer Battlespace Management, Fleet Capability Aviation Operations Support, Joint Helicopter Command Safety and Policy and the DE&S TEST DT.

**Regulation
3132(3)**

Air Traffic Management Equipment Safety Case Management Process

3132(3) The ATM Equipment SC **shall** be managed through the Project Safety Panel (PSP).

**Acceptable
Means of
Compliance
3132(3)**

Air Traffic Management Equipment Safety Case Management Process

21. Initially each part of the ATM Equipment SC **should** be authorized for release in order; however, development of the next part of the ATM Equipment SC can begin prior to the previous part being authorized for release.

**Acceptable
Means of
Compliance
3132(3)**

22. When a new project is being established the DT **should** contact the relevant DH-Facing organizations, Front Line Commands (FLC) and end users requesting they provide details of the nominated posts that will be PSP members and details of who will authorize the ATM Equipment SC (including accepting Risks where required).
23. Terms of Reference **should** exist for the PSP stating each member's role and responsibilities.
24. The PSP **should** be chaired by the Delivery Team Leader (DTL) or Delivery Manager. The minimum membership **should** be:
- DT staff, including the Safety staff / team.
 - Equipment designers / contractors.
 - Relevant DH-Facing organizations, FLC and end users (operators, maintainers etc).
 - The Independent Safety Auditor (ISA).
25. Staff from organizations that will be part of the RiSP **should** be invited to PSPs in the project's later stages.
26. The PSP minutes **should** provide an auditable trail of discussions, actions, and agreements.
27. All PSP members **should** be a Suitably Qualified and Experienced Person (SQEP). All members, replacements and representatives **should** complete SQEP forms at their first meeting. Completed SQEP forms **should** be held within the DT. If members details change (eg experience or qualifications) they **should** notify the chair and update their form.
- SQEP forms **should** clearly state the Area of Responsibility for each PSP member.
28. Each phase of the ATM Equipment SC **should** be owned by the appropriate organization:
- Part 1. Owned and written by the DT, however the content, ie requirements, **should** come from the relevant DH-Facing organizations, FLC and end users and stakeholders.
 - Part 2. Owned by the DT but predominantly written by the contractors responsible for designing the equipment or Safety consultants.
 - Part 3. Owned by the DT with input from contractors, relevant DH-Facing organizations, FLC, end users and stakeholders.
 - Part 4. Owned by the relevant DH-Facing organizations or FLCs, however on initial creation it will be predominantly written by the DT and contractors with input on procedures and processes from FLCs, end users and stakeholders.
 - (1) Once the equipment is In-Service it will be responsibility of the relevant DH-Facing organizations, FLCs and end users to maintain the ATM Equipment SC Part 4.
29. The ATM Equipment SC **should** be managed within current structures as a routine part of capability generation and employment.
30. When each part of the ATM Equipment SC and the associated reports are agreed by the PSP, all PSP members **should** recommend that it be authorized for release by the appropriate persons and their recommendations **should** be minuted.
31. Each part of the ATM Equipment SC **should** be authorized for release by the following:
- Part 1. DTL.
 - Part 2. DTL and relevant DH-Facing organizations / FLC. By authorizing this part the relevant DH-Facing organizations / FLC are confirming the procedural mitigations are acceptable and the residual Risks are at a level where they can be agreed by the DH-Facing organization, having highlighted

Acceptable Means of Compliance 3132(3)

- them to the relevant DH where appropriate. These Risks will be those that have not been designed out.
- c. Part 3. DTL and relevant DH-Facing organizations / FLC.
32. Part 4. DTL and relevant DH-Facing organizations / FLC.

Guidance Material 3132(3)

Air Traffic Management Equipment Safety Case Management Process

33. Where there is more than one relevant DH-Facing organizations, FLC or end user they may agree to empower one organization (eg have a lead service) to authorize the parts of the ATM Equipment SC on their behalf. If they elect not to empower a single organization, authorization would be required from all parties to proceed on to the next part.
34. Those required to authorize each part may send their Subject Matter Experts to PSP meetings to represent them, however authorization cannot be delegated.
35. For oversight and Assurance purposes, the MAA may be in attendance at PSP meetings.
36. The FLCs may delegate management of the ATM Equipment SC Part 4 to individual sites but not ownership.
37. Annex A summaries the ATM Equipment SC management process.

Regulation 3132(4)

Air Traffic Management Equipment Safety Case Amendments

3132(4) The ATM Equipment SC owner **shall** keep it current throughout the life of the equipment.

Acceptable Means of Compliance 3132(4)

Air Traffic Management Equipment Safety Case Amendments

38. When there is a change to the ATM Equipment, operating procedures, equipment use and configuration, or the environment is not covered by the existing ATM Equipment SC, the case **should** be revised as follows:
- a. For ► **significant** ◀ changes or changes with a large Safety impact, as a complete re-issue of the relevant part(s).
 - b. For minor changes with little Safety impact, a Safety statement **should** be produced as an annex to the relevant part(s).
 - c. Once the equipment is In-Service the ATM Equipment SC **should** be reviewed and amended on a regular basis, not exceeding 4 years.
39. If an Incident, Accident or failure occurs the ATM Equipment SC **should** be reviewed and updated with details to mitigate against reoccurrence. The review **should** also include a review of the Hazards and mitigations, to ensure they remain current.
40. Amendments **should** be published and publicized to the Regulated Community in a timely fashion.

Guidance Material 3132(4)

Air Traffic Management Equipment Safety Case Amendments

41. For the purposes of RA 3132(4) ► **the description of significant change is detailed in paragraph 10 of this RA.** ◀
- a. ►◀
 - b. ►◀
 - c. ►◀
 - d. ►◀
 - (1) ►◀
 - e. ►◀

**Regulation
3132(5)**

Air Traffic Management Equipment Safety Case Reports

3132(5) ATM Equipment SCs **shall** be summarized by a series of ATM Equipment SCRs.

**Acceptable
Means of
Compliance
3132(5)**

Air Traffic Management Equipment Safety Case Reports

42. ATM Equipment SCRs **should** summarize the arguments and evidence of the SC, and document progress against the Safety programme.

43. An ATM Equipment SCR **should** describe as a minimum the following:

- a. Capability or concept being assessed.
- b. Risk Assessment process.
- c. Requirements derived.
- d. Applicable Regulations.
- e. Potential Safety Risks.
- f. Measures to control them.
- g. Detail on assumptions made and shortcomings in knowledge and propose a strategy to deal with such issues.

44. ATM Equipment SCRs **should** be generated at key stages in the project as agreed by the PSP.

**Guidance
Material
3132(5)**

Air Traffic Management Equipment Safety Case Reports

45. A SCR is a key deliverable that summarizes the SC at a particular point in time. It provides Assurance that Safety is being managed effectively, highlights areas of Safety-related project Risk requiring management attention and gives stakeholders visibility of the status of the SC⁴.

**Regulation
3132(6)**

Air Traffic Management Equipment Safety Case Independent Assessment

3132(6) The ATM Equipment SC owner **shall** ensure the ATM Equipment SC is independently assessed.

**Acceptable
Means of
Compliance
3132(6)**

Air Traffic Management Equipment Safety Case Independent Assessment

46. During initial ATM Equipment SC development, or amendment due to **significant** changes, the ATM Equipment SC **should** be subjected to independent assessment.

**Guidance
Material
3132(6)**

Air Traffic Management Equipment Safety Case Independent Assessment

47. The primary role of an ISA is assessment and validation of the ATM Equipment SC work.

48. The ISA will have a well-defined role that is clearly understood by all parties. This role might include providing Assurance by auditing the Safety process being followed, or by doing some Safety Assessment independently to check the primary assessment. The role may change at different points through the life cycle, but the ISA's independence will not be compromised.

49. The ISA will be contracted exclusively by the DT to act on its behalf and not via the Prime Contractor and / or Designer; noting that if the MOD has the required competence, and based on the level of acceptable Risk, then this technical evaluation could be provided from within the DT.

**Guidance
Material
3132(6)**

50. It is acceptable for the ISA to be involved in the joint working environment between the DT and Designer. Duplication of effort will be avoided if the ISA works collaboratively with the MOD and Designer so that their assessments can be incorporated in the overall project schedule. It is important that the ISA work is conducted on behalf of the DTL and any advice they may have about the design and / or Safety will be directed to the DTL.

**Regulation
3132(7)**

Specific Site / Operating Area Safety

3132(7) The ATM Equipment SC Part 4s or the associated ATM Equipment SCR for all the equipment at a specific site / operating area **shall** be held on site and **shall** provide evidence that the site / operating area is safe.

**Acceptable
Means of
Compliance
3132(7)**

Specific Site / Operating Area Safety

51. The ATM Equipment SC Part 4 **should** contain the outcome of the ATM Equipment RiSP. This **should** include:

- a. A statement of outcome from the ATM Acceptance process.
- b. A statement of outcome from the relevant Site Specific Acceptance and Commissioning Board.

52. The ATM Equipment SC Part 4 (and ATM Equipment SCRs) for each site / operating area / equipment **should** contain sufficient information such that when combined for a site they make up the majority of what was previously termed a Terminal / Air Surveillance and Control System (ASACS) SC for ATM operations at that site. The remainder of the information required to provide the complete Safety argument (ie a Terminal / ASACS SC) **should** be written by the FLC.

53. Part 4 of the ATM Equipment SC (or ATM Equipment SCRs) **should** make reference to operating and engineering manuals and documents, training plans, staff qualifications and authorizations and site specific information, including interactions / dependencies with other equipment.

**Guidance
Material
3132(7)**

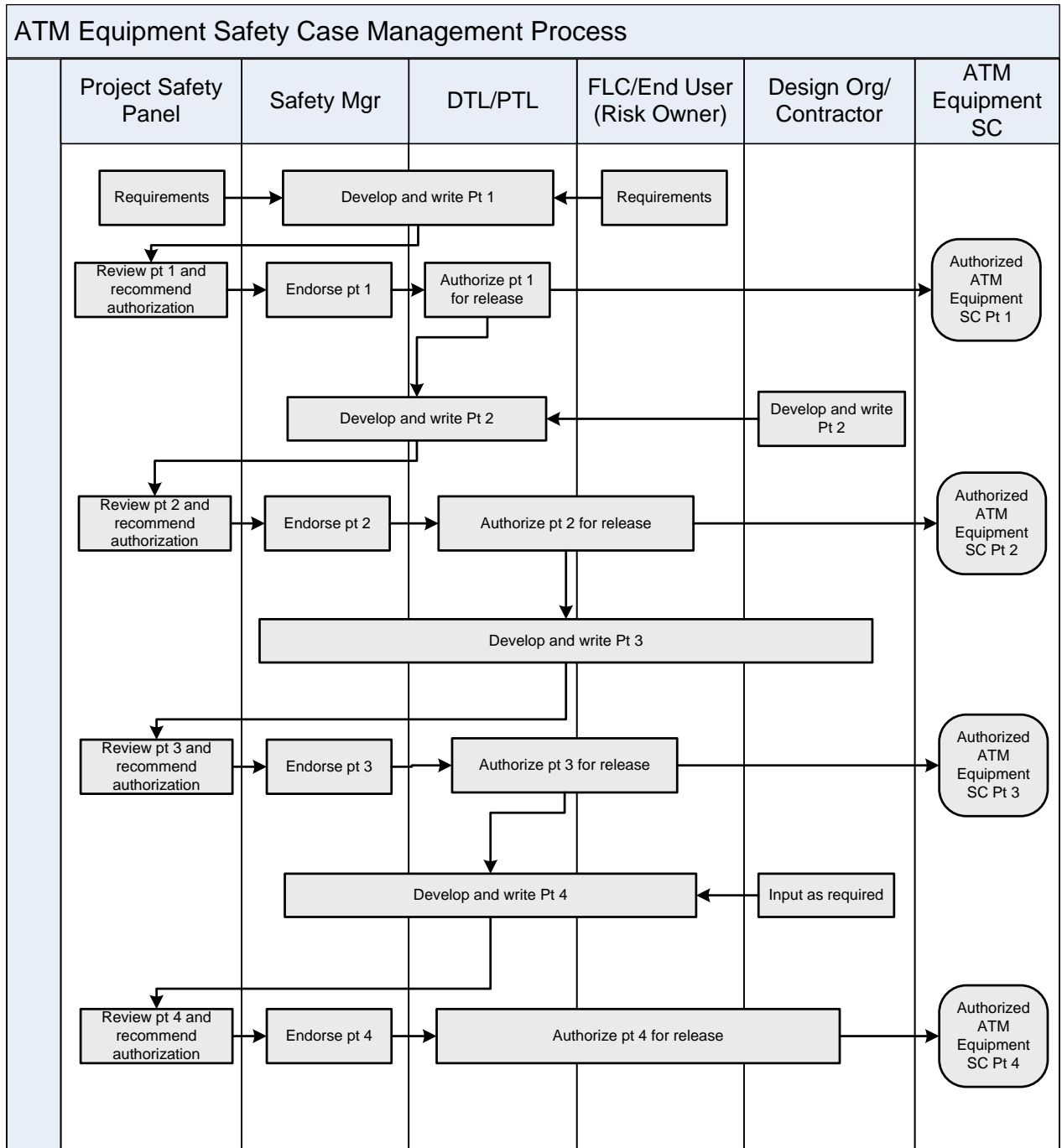
Specific Site / Operating Area Safety

54. The ATM Equipment SC Parts 1, 2 and 3 can be held centrally, there is no requirement for them to be held at each site.

ANNEX A

3132(3) ATM EQUIPMENT SAFETY CASE MANAGEMENT PROCESS

Figure 1. ATM Equipment SC Management Process.



Intentionally blank for print pagination