RA 3130 – Air Traffic Management Equipment Safety Management

Rationale

There is a requirement to demonstrate that design solutions for new Air Traffic Management (ATM) Equipment or modifications to in-service ATM Equipment are procured using recognised safety practices and processes, and that ATM Equipment is safe to operate and is being operated safely.

Contents

Regulation 3130(1)

Project/Delivery Team Leader Responsibilities

3130(1) The Project/Delivery Team Leader (PTL/DTL) **shall** be responsible for delivering safe systems, services[1] and equipment.

Acceptable Means of Compliance 3130(1)

Project/Delivery Team Leader Responsibilities

1. The PTL/DTL **should** ensure throughout the life of the ATM systems, services, and equipment that:

   a. ATM Equipment is supported by an ATM Equipment Safety Case (SC) iaw RA 3132.

      (1) Safety targets and requirements are set and communicated in the ATM Equipment SC Part 1, System Requirements Documents (SRD) or other relevant safety documentation.

   b. Aviation Duty Holders (DH) are supported effectively in controlling risks to ensure that they are reduced ►so that they are As Low As Reasonably Practicable (ALARP) (see RA 1210) and Tolerable◄ through life.

   c. Appropriate through-life safety management arrangements are established for the ATM Equipment, including Safety Management Systems and plans (see RA 1200 and the Manual of Air safety).

   d. Maintenance and training procedures are detailed in technical documentation to ensure safe practises are adhered to.

   e. Support documentation and training documentation are maintained and their configuration controlled.

   f. Arrangements are in place for monitoring and recording safety performance, and regular reviews are carried out.

2. The PTL/DTL **should** ensure:

   a. Users (operators and/or maintainers) are provided with ATM Equipment user instructions, training, and maintenance procedures.

   b. All relevant documentation is subject to configuration control.

[1] In this regulation services refers to equipment engineering services, not an Air Traffic Service as defined in MAA 02.

Acceptable Means of Compliance 3130(1)

c. Users (operators and/or maintainers) understand the safety implications of any changes, such as PT/DT equipment modifications or operator procedural changes.

d. If users (operators and/or maintainers) are required to operate the systems outside of the defined safe maintenance and performance envelope due to operational reasons:

(1) Risk assessments and impact statements **should** be written.

(2) ,Permission **should** be sought from the local commander and/or Aviation DH as appropriate.

(3) The DTL/PTL **should** be informed.

Guidance Material 3130(1)

Project/Delivery Team Leader Responsibilities

3. The Project Oriented Safety Management System (POSMS) describes processes and procedures which are designed to assist with the identification and management of the safety risks of equipment and services throughout the acquisition process. The scope of POSMS is limited to acquisition projects for equipment and services

Regulation 3130(2)

User/Operator Responsibilities

3130(2) The Users (operators and/or maintainers) **shall** operate and maintain ATM Equipment in accordance with the ATM Equipment SC, user instructions and maintenance procedures.

Acceptable Means of Compliance 3130(2)

User/Operator Responsibilities

4. Through formalized agreements with the PT/DT where appropriate, users (operators and/or maintainers) **should**:

a. Confirm user instructions and maintenance procedures have been maintained and configuration controlled according to PT/DT changes.

b. Confirm ATM Equipments are being maintained and used in accordance with PT/DT procedures and safe performance envelopes.

c. Immediately report to the PT/DT, via the relevant FLC organization (e.g. RAF Engineering Role Office) concerns identified by users (operators and/or maintainers). Examples of concerns include unexpected performance or failures.

d. Report to the PT/DT all decisions taken to operate ATM Equipment and support outside defined performance and maintenance envelopes.

Guidance Material 3130(2)

User/Operator Responsibilities

5. Nil.

Regulation 3130(3)

Legislation Compliance

3130(3) The PTL/DTL **shall** ensure that a compliance assessment is undertaken for the ATM Equipment against all relevant legislation as appropriate during the Equipment's life cycle .

Acceptable Means of Compliance 3130(3)

Legislation Compliance

6. Compliance **should** be assessed in three stages as follows:

a. **Prior to contract award.** An initial compliance assessment **should** be made by the PT/DT to support Part 1 of the ATM Equipment SC. This broad assessment **should** identify the key items of legislation that could be applicable and any areas of potential non-compliance.

b. **During development and manufacture of equipment.** The PTL/DTL **should** ensure that a detailed compliance assessment is undertaken and that it includes all of the legislation for the ATM Equipment, managed through to compliance or to a justified position of non-compliance. The compliance assessment is an on-going process until the ATM Equipment is ready to be released into service in order that emergent legislation may be managed.

c. **Before Release into Service Process.** The PTL/DTL **should** ensure that the compliance assessment is completed in order to provide evidence into the Release into Service Process through the ATM Equipment SC.

Guidance Material 3130(3)

Legislation Compliance

7. The purpose of the compliance assessment is to:

a. Record all legislation deemed applicable to the ATM Equipment.

b. Apply scrutiny to its design features to ensure compliance.

c. Ensure that the correct process is followed where compliance cannot be achieved for operational reasons.

8. The PT/DT need to be aware that compliance status could change throughout the development and manufacture of the ATM Equipment and that justifiable non-compliances may become apparent up to release into service.

9. The detailed compliance assessment is usually provided by the supplier.

Regulation 3130(4)

Configuration Management

3130(4) The PTL/DTL **shall** be responsible for Configuration Management (CM) throughout the life of the ATM Equipment.

Acceptable Means of Compliance 3130(4)

Configuration Management

10. The PTL/DTL **should** develop and implement a Configuration Management Plan (CMP). The CMP **should** define how CM is to be carried out and detail the processes used to ensure that the ATM Equipment's functional and physical characteristics conform to the requirements throughout the life cycle of the ATM Equipment. As a minimum, a CMP **should**:

a. Be documented.

b. Show the configuration of an item at any time in its life cycle.

c. Provide a means for managing modifications.

d. Involve the principle CM activities of planning, documenting, controlling, accounting for and auditing the item's configuration.

11. JSP 886 provides details regarding the contents and structure of a typical CMP, as a minimum, the CMP **should** address:

(1) Purpose, scope and programme.

(2) Organization structures, committees and responsibilities.

(3) Configuration change management procedures.

(4) Change control of the CMP.

(5) Relationships with other plans.

Acceptable Means of Compliance 3130(4)

(6) Configuration audit.

12. The PTL/DTL **should**:

a. Review and take decisions on changes to ATM Equipment specification or design which could significantly affect project safety, performance, cost, timescales or delivery.

b. Agree project/ATM Equipment modification policy and the associated timescales.

c. Document all configuration changes and maintain an auditable trail of all proposals, reviews and decisions.

d. Ensure that the impact of individual modifications is assessed across the whole ATM Equipment range and that an annual review process maintains the agreed progress of embodiment.

e. Ensure that a focal point for the maintenance of CM is appointed and a statement included in staff terms of reference identifying individual authorities and responsibilities for CM within a PT/DT.

f. Ensure that, where items of ATM Equipment are shared across multiple PTs/DTs, CM is strictly maintained and duplicated activities are avoided.

g. Ensure that all modification procedures conform to the guidelines and procedures described in the MRP, single-Service APs and any subordinate Business Procedures.

13. For Service Modifications, the PT/DT must ensure that all relevant parties are made aware of the amendment and relevant documentation (incl. maintenance) is updated accordingly.

Guidance Material 3130(4)

Configuration Management

14. Configuration Management will need to be applied by the PT/DT in order to maintain effective control of the approved configuration. Configuration Management should also prevent unauthorized changes being made without the valid authorization via PT/DT Change Management Process. Change Management will need to be applied in order:

a. Ensure that change proposals are processed in a timely manner and are justified in terms of:

(1) Safety.

(2) Performance.

(3) Whole-life costs.

(4) Support.

(5) Project timescale.

b. Apply a classification, including:

(1) Applicability of change.

(2) Possible need for retrospective action.

(3) Degree of urgency.

c. Evaluate the impact of major deviations and modifications.

d. Enable the implementation of authorized changes and make use of configuration status accounting to track progress from concept through to completion.

15. Initial Configuration Control (CC) is vested in the Designer, who provides the Configuration Status Record (CSR). This contains the indexes to master sets of drawings, amendments, modifications, ancillary equipment and Service-supply items. It must be kept up-to-date throughout the life of the ATM Equipment, on behalf of the PT/DT, by the Designer. The CSR provides a baseline for defining the as-fitted and modification state throughout the life of the ATM Equipment.

Regulation 3130(5)

Safety Documentation Retention

3130(5) All safety documentation relating to ATM Equipment **shall** be retained for a minimum of 5 years beyond the equipment's out of Service date.

Acceptable Means of Compliance 3130(5)

Safety Documentation Retention

15. Documentation **should** be clearly marked and securely stored to avoid accidental destruction.

Guidance Material 3130(5)

Safety Documentation Retention

16. Scanned copies of documents are legally allowable under the "best evidence" principle.

17. Electronic storage can be used providing documents are protected to prevent accidental deletion.

Regulation 3130(6)

Independent Safety Auditor

3130(6) The PTL/DTL **shall** consider the appointment of an Independent Safety Auditor (ISA) at the outset of a project, in consultation with the Project Safety Panel (PSP).

Acceptable Means of Compliance 3130(6)

Independent Safety Auditor

18. The PTL/DTL **should** ensure that an auditable trail of the decision regarding the requirement for an ISA exists.

19. The ISA **should:**

a. Undertake the task of audits and other assessment activities to:

(1) Provide assurance that safety activities comply with planned arrangements.

(2) Provide assurance that safety activities are implemented effectively and are suitable to achieve objectives.

(3) Confirm whether related outputs are correct, valid and fit for purpose.

b. Have a well defined role that is documented and clearly understood by all parties.

c. Be independent of the organization being supported and have a good understanding of safety issues related to systems under review.

d. Sit as a full member of the PSP and their role and function **should** be defined in the Management Plan.

20. The ISA's independence **should** not be compromised by involving them in activities such as setting Safety Requirements, tender assessment or providing specific advice on engineering changes.

Guidance Material 3130(6)

Independent Safety Auditor

21. The use of an ISA can enhance a PT/DT's assurance arrangements, by assisting with the maintenance of safety integrity across large and/or high risk projects.

22. The ISA role may 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.

Guidance Material 3130(6)

23. The primary role of an ISA is assessment and validation of the ATM Equipment SC work. This is usually carried out through audit of the following:

a. The safety management arrangements set out in the Safety Management Plan (SMP) and ATM Equipment SC.

b. The safety activities set out in the contractor's Safety Programme Plan in response to the SMP.

Regulation 3130(7)

Air Traffic Management Equipment Risk Classification

3130(7) ATM risks involving ATM Equipment **shall** be classified and handled using the ATM Equipment Risk Classification Matrix.

Acceptable Means of Compliance 3130(7)

Air Traffic Management Equipment Risk Classification

24. This regulation **should** be read in conjunction with RA 1210 - Management of Operating Risk, Risk to Life (RtL) and Def Stan 00-56 Safety Management Requirements for Defence Systems.

25. This regulation **should** be used by PTs/DTs and users (operators and/or maintainers).

26. Annex A of this RA contains the ATM Equipment Risk Severity Classifications definitions (table 1) and Risk Classification Matrix (table 2). The information at Annex A **should** be used for ATM risks[2] that have an ATM Equipment element, but can also include people, procedure and environment elements, for example in the mitigations. For ATM risks that are unrelated to ATM Equipment RA 1210 **should** be used directly (see RA 3130(8)).

27. The ATM Equipment SC **should** set out and justify the process for making ALARP decisions.

28. Whenever there are changes to an ATM Equipment's design, role, operating environment and/or changes in legislation there **should** be a re-assessment of all risks falling within the scope of the changes.

Guidance Material 3130(7)

Air Traffic Management Equipment Risk Classification

29. EU Eurocontrol Safety Regulatory Requirement 4 (ESARR4) states that the Maximum Tolerability (of ATM direct contribution) to a Severity Class 1 Incident in the European Civil Aviation Conference (ECAC) Region, is 1.55 x 10^{-8} per flight hour (controlled). It is agreed that this is broadly suitable for use in a Military/Civil Joint and Integrated ATM environment.

30. It is important to note that 'tolerability' does not mean 'acceptability'. It refers to a willingness to live with a risk to secure certain benefits in the confidence that it is being properly controlled. To tolerate a risk means that it is not regarded as insignificant or something that could be ignored, but rather as something that needs to be kept under review and reduced further if possible

Risk Management Process

31. The aim of risk management is to ensure and demonstrate that all foreseeable risks have been identified and reduced ►so that they are ALARP and Tolerable.◄ It is an iterative process that will continue throughout the life of a system.

The essential steps required to manage Risks successfully can be found in the Guidance Material of RA 1210(2)&(3). All steps to manage risks must involve the PSP.

Risk Classification

32. A qualitative or quantitative approach can be used to determine the appropriate risk classification. Where possible, a quantitative approach must be used when a system poses significant risk.

[2] An ATM Risk is the risk resulting from a hazard caused by the provision of ATM. It should be considered by the service provider but will be held by the Aviation DH if it is a RtL, otherwise will be held by the PTL/DTL or the user, as appropriate.

Guidance Material 3130(7)

33. Annex A contains specific details for ATM Equipment risk classification. It has both quantitative figures and qualitative descriptions.

34. Whether a qualitative or quantitative approach is used, demonstration that a target has been achieved, or bettered, may not always be practicable. It may be used to indicate the level of performance/integrity expected from the system, and as a baseline against which to argue the ATM Equipment SC.

Regulation 3130(8)

Air Traffic Management Equipment Risk Management

3130(8) PTLs/DTLs or users (operators and/or maintainers) **shall** ensure that ATM Equipment hazards are articulated to Aviation DHs in a manner which enables DHs to assess any associated Risk to Life (RtL) appropriately.

Acceptable Means of Compliance 3130(8)

Air Traffic Management Equipment Risk Management

35. RtL **should** only be owned by Aviation DHs and therefore all factors affecting RtL must be articulated to the relevant Aviation DHs to allow them to consider the RtL appropriately.

36. Aviation DH responsibilities regarding RtL are laid down in RA 1210. Relevant ATM Equipment risks **should** be articulated to Aviation DHs with all the appropriate information and evidence to enable Aviation DHs to comply with RA 1210.

Guidance Material 3130(8)

Air Traffic Management Equipment Risk Management

37. Nil.

ANNEX A

ATM EQUIPMENT RISK CLASSIFICATION

1. ATM Equipment risks must have their severity classified using the information in table 1. The definitions in table 1 provide descriptions of possible outcomes.

Table 1. ATM Equipment Risk Severity Classifications.

Severity	Definitions[3]
Catastrophic 1	-One or more catastrophic accidents. -One or more mid-air collisions. -One or more collisions on the ground between two aircraft. -One or more Controlled Flight Into Terrain. -Total loss of flight control. (No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s)). -ATC issues instruction or information which can be expected to cause loss of one or more aircraft (no reasonable and reliable means exists for the aircrew to check the information or mitigate against the hazards). -Continued safe flight or landing prevented.
Hazardous 2	-Large reduction in separation (e.g., a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation. -One or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate). -The ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, completely unavailable. -Provision of instructions or information which may result in a critical near mid-air collision or a critical near collision with the ground. Many losses of Acceptable separation possible.
Major 3	-Large reduction (e.g., a separation of less than half the separation minima) in separation with crew or ATC controlling the situation and able to recover from the situation. -Minor reduction (e.g., a separation of more than half the separation minima) in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres). -The ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, severely degraded or compromised (e.g. contingency measures required or controller workload significantly increased such that the probability of human error is increased). -The ATC separation service provided to aircraft on the ground outside a runway protected area is suddenly, and for a significant period of time, completely unavailable. -Provision of instructions or information which may result in the separation between aircraft or aircraft and the ground being reduced below normal standards. -No ATS action possible to Support aircraft emergency.
Minor 4	-Increasing workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system. -Minor reduction (e.g., a separation of more than half the separation minima) in separation with crew or ATC controlling the situation and fully able to recover from the situation. -The ATC Separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, impaired. -The ATC separation service provided to aircraft on the ground outside a runway protected area is suddenly, and for a significant period of time, severely degraded. -ATS emergency support ability severely degraded.
Negligible 5	-No hazardous condition i.e. no immediate direct or indirect impact on the operations. -No effect on ATC separation service provided to aircraft. -Minimal effect on ATC separation service provided to aircraft on the ground outside a runway protected area. -Minimal effect on ATS emergency support ability.

[3] Definitions are taken from a combination of ESARR 4 and CAP 728.

Table 2. ATM Equipment Risk Classification Matrix.

ATM Probability			**ATM Severity**				
ATM Frequency	ATM Qualitative Description	Probability per controlled flying hour (CFg Hr[4])	1	2	3	4	5
			ATM Risk Class				
Frequent	Likely to occur often	>2.8x10^{-3}	**A**	**A**	**A**	**B**	**C**
Probable	Likely to occur many times	2.8x10^{-3} - 2.8x10^{-4}	**A**	**A**	**B**	**C**	**D**
Occasional	Likely to occur sometimes	2.8x10^{-4} - 2.8x10^{-5}	**A**	**B**	**C**	**D**	**D**
Remote	Unlikely to occur	2.8x10^{-5} - 2.8x10^{-6}	**A**	**C**	**D**	**D**	**D**
Improbable	Very unlikely to occur	2.8x10^{-6} - 1.55x10^{-8}	**A**	**D**	**D**	**D**	**D**
Incredible	Extremely unlikely to occur	<1.55x10^{-8}	**B**	**D**	**D**	**D**	**D**

2. ►All risks need to be reduced ALARP iaw the “Health and Safety at Work Act” and Health and Safety Executive.◄

[4] A controlled flying hour is an hour of an aircraft’s flight time for which an Air Traffic service is received.

Intentionally blank for print pagination