►This RA has been substantially re-written; for clarity no change marks are presented – please read RA in entirety◄

RA 1230 - Design Safety Targets

Rationale

It is important to provide a level of Assurance that an Air System's[1] Type Design can achieve specific Safety criteria. Design Safety Targets ensure that Air Systems are designed with Safety requirements considered from the outset and, once design activity is complete, provide a baseline for assuring that Safety levels are maintained through life. Failure to set design Safety Targets may lead to Air Systems entering service with design deficiencies which introduce unacceptable Hazards. This RA requires the Senior Responsible Owner (SRO)[2] to establish design Safety Targets early during Acquisition, and, for In-Service[3] Air Systems, the Type Airworthiness Authority (TAA)[4] to declare a design Safety baseline against which the Operating Duty Holder (ODH) / Accountable Manager Military Flying (AM(MF)), as Risk to Life (RtL) owners, can assess whether an Air System remains 'safe to operate' against As Low As Reasonably Practicable (ALARP) and Tolerability criteria through life.

Contents

Applicability

Applicability of this RA

1230(2)

1. Air Systems[1] destined for the UK Military Aircraft Register (MAR) in the Acquisition process, which are prior to submission of an Air System Safety Case[5] (ASSC) Strategy Report.

1230(3)

2. All Air Systems[1] on the UK MAR for which an ODH / AM(MF) owns the ASSC for In-Service Flying. For Air Systems to which sub-Regulation 1230(2) has applied, sub-Regulation 1230(3) becomes applicable at the point the end user ODH / AM(MF) accepts the RtL associated with operation of the Air System for In-Service Flying (but before such Risk is incurred).

Regulation 1230(1)

Design Safety Target Criteria

1230(1) Withdrawn – Incorporated into sub-Regulations 1230(2) and 1230(3) or no longer considered Regulatory material.

Acceptable Means of Compliance 1230(1)

Design Safety Target Criteria

3. Withdrawn – Incorporated into sub-Regulations 1230(2) and 1230(3) or no longer considered Regulatory material.

Guidance Material 1230(1)

Design Safety Target Criteria

4. Withdrawn – Incorporated into sub-Regulations 1230(2) and 1230(3) or no longer considered Regulatory material.

---

[1] For Remotely Piloted Air System (RPAS) this only includes those in the S2 sub-category or Certified category.
[2] Or Sponsor; refer to RA 1019 – Sponsor of Military Registered Civilian-Owned and Civilian Operated Air Systems - Air Safety Responsibilities.
[3] Refer to RA 1160 – The Defence Air Environment Operating Framework
[4] 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.
[5] Refer to RA 1205 – Air System Safety Cases.

Regulation 1230(2)

Establishing Design Safety Targets during Acquisition

1230(2) For Air Systems[1] destined for the UK MAR, the SRO **shall** establish suitable design Safety Targets.

Acceptable Means of Compliance 1230(2)

Establishing Design Safety Targets during Acquisition

Establishing Design Safety Targets

5. The SRO **should** establish design Safety Targets in agreement with the TAA, the MAA[6] and the end user ODH / AM(MF). Once established, design Safety Targets **should** form a baseline against which to maintain an acceptable level of design Safety through life in accordance with (iaw) sub-Regulation 1230(3).

6. The SRO **should** ensure that design Safety Targets are detailed in the appropriate Acquisition contract.

7. As part of the development of the ASSC:

   a. The SRO **should** ensure that the approach for delivering the agreed design Safety Targets is detailed as part of the ASSC Strategy and ASSC Acquisition Basis[5].

   b. In support of the argument that the Air System will be safe to operate, the end user ODH / AM(MF) **should** detail the use of design Safety Targets as part of the ASSC, transitioning to acceptance of a design Safety baseline iaw sub-Regulation 1230(3) before any RtL is incurred through In-Service operation of the Air System.

8. The TAA **should** include the proposed design Safety Targets in the Application for a Military Type Certificate[7] and detail their approach to the demonstration of achievement within the Type Airworthiness Strategy[8].

Design Safety Targets – General

9. Failure Conditions (FC) **should** be classified according to the severity of their effects as part of the design Safety Target definition noting that these will vary across Air System types.

10. The probability of a FC leading to death[9] or Aircraft loss **should** be Extremely Improbable (EI).

11. Quantitative design Safety Targets **should** be applied to aspects of the design that are subject to probabilistic failure modes.

12. For aspects of the design not subject to probabilistic failure modes, such as software and Structures, qualitative targets **should** be established based on adherence to good design practice as defined in the appropriate Certification Specification (CS)[10].

Guidance Material 1230(2)

Establishing Design Safety Targets during Acquisition

Design Safety Targets – General

13. In System design, a FC[11] is a condition that introduces a Hazard to the Air System, caused by one or a combination of lower-level System failures. The FC needs to be selected at the appropriate level to facilitate efficient System design, and for Systems which have been assigned a probability of failure, a reliability requirement can be allocated based upon consequences of failure. For FCs that can directly lead to death or Aircraft loss the probability of the FC materialising will be EI. Whilst 1230(2) focusses on early establishment of targets for these FC categories, it is

[6] Reviewed and agreed by MAA during ASSC Scrutiny, which may require additional engagement between MAA, TAA, SRO, ODH / AM(MF) as applicable throughout the Acquisition cycle.
[7] MAA Form 30: Application for Military Air System Certification Process (MACP).
[8] Refer to RA 5010 – Type Airworthiness Strategy.
[9] 1st and 2nd Party; refer to RA 1210 – Ownership and Management of Operating Risk (Risk to Life).
[10] Refer to RA 5810 – Military Type Certificate (MRP Part 21 Subpart B).
[11] Defined in Aerospace Recommended Practice (ARP) 4761A as "A condition having an effect on the Aircraft and / or its occupants, either direct or consequential, which is Caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events."

Guidance Material 1230(2)

expected that the design process will include identification of lower-level FC categories for which appropriate targets will need to be derived.

14. Accepted practice[12] is based on historical analysis of Accidents which found that the likelihood of crashes due to technical Causes was approximately 1 x 10^{-7} per Flying Hour and, for large commercial Air Systems with approximately 100 such FCs assumed, an acceptable EI probability of 1 x 10^{-9} per Flying Hour for each FC was established. For Military Air System design, this assumption of 100 approximate FCs may not always be suitable (ie a lower number of assumed FCs for some RPAS or simpler designs and a higher number for increasingly complex designs). As part of the MAA's agreement of a suitable design Safety Target, such assumptions will require validation.

15. Acceptable Occurrences per Flying Hour figures for EI are expected to vary for different Military Air System types to which this Regulation applies. In setting targets for specific Air System types, the benchmark figures detailed within Table 1 for individual FCs are based on widely accepted practice.

Table 1. Extremely Improbable Figures for Individual FCs (by Air System type)

Air System Type	**Maximum Extremely Improbable Figure (Occurrences per Flying Hour)**
Air Systems based on Civil-Certified Designs (EASA CS / Federal Aviation Administration (FAA) Federal Aviation Regulations (FAR) 23)	1 x 10^{-9} to 1 x 10^{-6} (13)
Air Systems based on Civil-Certified Designs (EASA CS / FAA FAR 25)	1 x 10^{-9}
Air Systems based on Civil-Certified Designs (EASA CS / FAA FAR 27)	1 x 10^{-9} to 1 x 10^{-6} (13)
Air Systems based on Civil-Certified Designs (EASA CS / FAA FAR 29)	1 x 10^{-9}
Military Air Systems (Part 1)	1 x 10^{-8}
Military Air Systems (Part 3)	1 x 10^{-8} to 1 x 10^{-6} (14)
Military Air Systems (Part 5)	1 x 10^{-8}
Military Air Systems (Part 7)	1 x 10^{-8} to 1 x 10^{-6} (14)
Certified RPAS (Maximum Take-Off Weight (MTOW) <= 5,670 kg)	1 x 10^{-7} to 1 x 10^{-6} (15)
Certified RPAS (MTOW > 5,670 kg)	1 x 10^{-8} to 1 x 10^{-7} (15)
S2 sub-Category RPAS	1 x 10^{-7} to 1 x 10^{-2} (16)

[12] For example, AMC to European Aviation Safety Agency (EASA) CS 25.1309.
[13] Safety Targets less stringent than 1 x 10^{-9} may be agreed with the MAA as appropriate based on the assigned Aircraft Class (I to IV) iaw CS / FAR 23 / 27 as applicable.
[14] Safety Targets less stringent than 1 x 10^{-8} may be agreed with the MAA as appropriate based on the intended usage, number of occupants, Air System complexity, and equivalent Aircraft Class (I to IV) iaw CS / FAR 23 / 27 as applicable.
[15] The lower bound Safety Target assumes no more than 10 Catastrophic FCs for the Air System. Higher Complexity Air Systems would be expected to use the more stringent Safety Target figure.
[16] The Agreed Safety Target (AST) for the uncontrolled Loss of Platform (LoP) of Specific Category RPAS will depend on the Specific Assurance and Integrity Level (SAIL) or equivalent, agreed with the MAA as part of the Letter of Endorsed Categorization (LEC). Typically for uncontrolled LoP, AST = 1 x 10^{-SAIL}.

Guidance Material 1230(2)

16. Calculation of a quantitative value[17] is only appropriate for airborne Systems which have a probabilistic failure mode. Other failures, eg software, lightning strike or structural failure, cannot be assigned a predicted failure probability. Safe design and qualitative assessment of these other aspects is reliant upon following appropriate CS which will deliver the required design integrity as agreed in the Type Certification Basis (TCB)[10].

17. It is expected that the agreed quantitative design Safety Target will inform the assignment of commensurate qualitative targets including Development Assurance Levels to establish the appropriate level of rigour for System Development[18]. Detailed System-specific requirements are detailed in the relevant Part of Defence Standard (Def Stan) 00-970 and Def Stan 00-055.

18. The purpose of setting a quantitative value for a FC probability as a design benchmark is to drive a safe design by allowing allocation of individual design budgets to each constituent System contributing to the appropriate FC based on the consequences of their failure. It is a one-way process to set the individual budgets, with specific achievement being argued at System level during the Development stages. For an Air System based on a design that has been Type Certified against a Civil CS the targets contained with the applicable CS can be used to support a declaration of design Safety Target achievement; there is no requirement to reverse back through the complete design to prove how each individual FC contributes to the declared cumulative value.

Non-Flying Hour Based Assessments

19. When assessing Air System design Safety Targets, the nature of some Systems, such as Aircraft Assisted Escape Systems (AAES), Aircraft Store release and jettison Systems, or fire suppression Systems, requires that they operate on an event basis rather than on a Flying Hour basis. Therefore, as well as being required to retain Safety through a designated life when flown in the Air System but not in operation, these Systems require additional consideration of high integrity and reliability on an 'event' basis when required to be operated.

20. For AAES[19], when quantifying design Safety Targets there is a need to consider the AAES separately from other System design (rather than incorporating the AAES into other Flying Hour-based targets) noting its use in tolerability arguments in the ASSC.

Regulation 1230(3)

Design Safety Baseline

1230(3) For In-Service[3] Air Systems[1] with a Live ASSC, the TAA **shall** declare the design Safety baseline for ODH / AM(MF) acceptance.

Acceptable Means of Compliance 1230(3)

Design Safety Baseline

21. The TAA **should** include their approach to maintaining the design Safety baseline within the Type Airworthiness Strategy[8].

22. The TAA **should** declare the Air System design Safety baseline within the Type Airworthiness Safety Assessment (TASA)[20] for acceptance by the ODH / AM(MF) as part of the ASSC:

a. For newly acquired Air Systems subject to sub-Regulation 1230(2), this declaration **should** be made when the end user ODH / AM(MF) accepts the RtL associated with operation of the Air System for In-Service Flying, and prior to commencement of such operation.

[17] Eg using the methodology detailed in EASA CS AMC XX.1309.
[18] ie Functional Development Assurance Levels (FDAL) and Item Development Assurance Levels (IDAL), the latter setting Programmable Elements (PE) Assurance levels.
[19] AAES has been used as a primary example however this guidance is equally applicable to other survivability equipment which may have been included within Air System design Safety calculations.
[20] Refer to RA 5012 – Type Airworthiness Safety Assessment.

Acceptable Means of Compliance 1230(3)

b. For all other In-Service Air Systems to which sub-Regulation 1230(2) has not applied, this declaration **should** articulate that the extant Type Design is acceptably safe.

23. The ODH / AM(MF) **should** articulate their acceptance of the design Safety baseline in the live ASSC.

24. The accepted design Safety baseline **should** form the basis / reference point against which future equipment Hazards, including those induced through Type Design changes[21], are assessed and justified in the TASA in support of the ASSC.

25. Changes which are not due to Type Design changes (eg different Aircrew Equipment Assemblies (AEA), conduct of new activities onboard the Air System) will not change the Air System design Safety baseline but their impact to equipment Hazards against the accepted design Safety baseline **should** be argued in the TASA.

26. Unsafe conditions reported iaw RA 5825[22] **should** be assessed for their impact against assumptions used to calculate a design Safety baseline and any change to the accepted baseline **should** be supported by an appropriate TASA Safety argument.

Guidance Material 1230(3)

Design Safety Baseline

General

27. Once the baseline has been declared by the TAA and accepted by the ODH / AM(MF), impacts to the baseline due to Type Design changes or new Hazard assessments will be identified and managed through established TAw Safety Management System[23] in conjunction with the ODH / AM(MF) Air Safety Management System.

Baseline Declaration - Acquired Air Systems Subject to RA 1230(2)

28. For Air Systems to which sub-Regulation 1230(2) has been applied, acceptance of the declared baseline within the ASSC then replaces the original design Safety Target articulated in earlier versions of the ASSC. Noting that 1230(2) requires establishment of targets at the System level, the expectation for these Air Systems in complying with 1230(3) is that the baseline is a declaration of the achieved 'position' of all System-level assessments.

Baseline Declaration - In-Service Air Systems (pre-RA 1230 Issue 7)

29. For In-Service Air Systems operating on the MAR prior to RA 1230 Issue 7 applying and / or which complied with previous versions of RA 1230 (Issue 6 and below) the declaration of the design Safety baseline provides an argument by the TAA that the existing Type Design is acceptably safe and provides a reference point or benchmark against which to assess changes. It is acknowledged that many platforms already have a declared cumulative (Air System level) design Safety Target derived iaw earlier issues of RA 1230; this may be used to form the baseline or else a baseline may be determined using the same methodology at System-level outlined above in 1230(2). Whatever methodology is used for these Air System types, the onus remains on the TAA to provide a compelling argument (to the satisfaction of the ODH / AM(MF)) within the TASA.

Ongoing Assessment of Impacts to the Baseline

30. Any impacts to the baseline as a result of Type Design change will be argued within the TASA. Additionally:

a. In cases of Type Design change where full evidence may be unavailable but, on balance of the available evidence and based on sound engineering judgement the design Safety baseline has not been breached there will need to be consideration of a Clearance with Limited Evidence (CLE)[24],[25];

[21] Refer to RA 5820 – Changes in Type Design (MRP Part 21 Subpart D).
[22] Refer to RA 5825 – Fault Reporting and Investigation.
[23] Refer to RA 5011 – Type Airworthiness Safety Management System.
[24] Refer to RA 1300 – Release To Service.
[25] Where the Release To Service (RTS) Regulation is referenced in this RA, this also includes Military Permit To Fly (MPTF) (In-Service) which is analogous to the RTS, as detailed in RA 1305 – Military Permit To Fly (In-Service), (Special Case Flying) and (Single Task).

Guidance Material 1230(3)

b. In cases of Type Design change where, on balance of available evidence and based on sound engineering judgement the design Safety baseline has been breached, there will need to be consideration of an Operational Emergency Clearance (OEC)[24].

31. Changes not associated with Type Design (eg introduction of new AEA) will not impact the baseline but may otherwise impact Safety. These will still be argued within the TASA and may also need to be considered for a CLE / OEC[24] if evidence is unavailable or there is an increased RtL.