RA 1230 – Design Safety Targets

Rationale

►It is important to have design safety targets to provide a level of assurance that a design can achieve specific safety criteria. The design solutions for new Air Systems, modifications to new and in-service Air Systems, and associated equipment and software, are to be consistent with the acceptable design safety targets, unless overriding statements for Airworthiness are contained in the specification or contract, with the prior agreement of the MAA.◄

Contents

Regulation 1230(1)

Design Safety Target Criteria

1230(1) ►Air Systems,◄ associated equipment and software **shall** be ►designed[1] to acceptable design◄ safety targets.

Acceptable Means of Compliance 1230(1)

Design Safety Target Criteria

Military Aircraft

1. The cumulative probability of the loss of an aircraft due to a technical fault and the cumulative probability of a technical failure of the aircraft (inclusive of its systems, structure and stores) leading to ►a death[2]◄, **should** both be assessed to be ►no more frequent than◄ one in a million per flying hour (probability of occurrence $1x10^{-6}$ per flying hour) when operated within the conditions used for the ►Airworthiness◄ demonstration►[3]◄.

►Airworthiness Demonstration

2. The Airworthiness demonstration **should** be as specified in the contract including the operating conditions to be applied, and **should** be undertaken during the demonstration of the compliance with the Type Certification Basis (TCB)[4] and matured throughout the life of the platform. The demonstration of Airworthiness may include design analysis, application of specified standards (such as Def Stan 00-970), and historical evidence of successful use of design features, system tests, and ground and air tests to arrive at an overall assessment of Airworthiness.

Civil Aircraft Types

3. Civil certified aircraft types unmodified for military use, registered or operated by the MOD **should** meet the civil Type Certificate holder's design safety target. Where configurations specific to the needs of the military are embodied or the intended use of the aircraft has changed, MAA Certification Division **should** be consulted and a design safety target agreed in accordance with the TCB and prior to Main Gate approval or appropriate approval juncture.◄

Remotely Piloted Air Systems (RPAS)

4. ►◄ The operation of a RPAS **should** be no more likely to cause injury or fatality to personnel or the general public than the operation of a manned aircraft. ►The design safety target for the operation of RPAS **should** reflect the categorization found in RA 1600[5]◄.

Software/Complex Electronic Hardware (CEH)

5. It is recognized that it is not possible to set quantifiable design safety targets for software (including the software aspects of CEH). Therefore a qualitative design target **should** be set; how this is achieved will depend on the approach to compliance with the software/CEH aspects of Def Stan 00-970 Part 13. This **should** result in the

[1] ►It is acknowledged that some legacy Air Systems, equipment and software will not have direct correlation with the original design safety target. Therefore there will be a need to define an acceptable Design Safety Target.
[2] This is in reference to 1st, 2nd or 3rd parties, refer to RA 1210 – Ownership and Management of Operating Risk (Risk to Life).
[3] The primary mitigation for a technical design shortfall is to be through technical design changes; where this is not wholly possible, operator or maintenance procedures may be utilised, however this would require verification that the procedure has a reasonable expectation of being accomplished successfully and in a timely manner to provide acceptable mitigation.
[4] RA 5810 – Military Type Certificate (MRP 21 Subpart B).
[5] RA 1600 – Remotely Piloted Air Systems.◄

Acceptable Means of Compliance 1230(1)

assignment of design targets in the form of ►Design Assurance Levels◄ that are commensurate with the design target of the system in which the software/CEH operates.

►Weapon Release and Airborne Equipment◄

6. Weapon release►[6]◄ and Airborne Equipment (AE[7]) descent assessments **should** be made on an event basis, ►instead◄ of a target related to flying hours.

►Historic Aircraft[8]

7. When there is incomplete design, testing information, or when maintenance records are missing such that a numerical target cannot be reached, the TAA **should** carry out a Safety Assessment and in agreement with the Aviation Duty Holder (ADH) ensure the principles of As Low As Reasonably Practicable (ALARP) are adopted in authorizing any changes to design, maintenance policy or operating limits (see also RA 1325[9]). Any modification to the aircraft **should** as a minimum be Airworthiness safety-neutral and ideally be safety-positive. The TAA can accept a safety-neutral outcome where a reduction in risk would not be expected or where a positive outcome cannot be reasonably demonstrated.◄

Guidance Material 1230(1)

Design Safety Target Criteria

►◄

8. ►◄

9. ►◄

Aircraft Weapons, AE and Historic Aircraft

10. The ►safety◄ criteria given in this RA ►must include◄ the safe carriage, release/despatch, and jettison of armament, weapons and AE from the immediate vicinity of the aircraft.

Weapons and Armament

11. Following ►release or jettison of the weapon, the safety criteria of the subsequent trajectory◄ must be as defined in the relevant specification. However, the platform TAA must satisfy himself that the achieved Air Launched Weapon safety, from the immediate vicinity point to the arming point, meets the overall operating safety requirements for the complete weapon system. The ►ownership◄ of risks to safety associated with aircraft self-damage post weapon arming, and collateral damage, is the responsibility of the ►ADH, Accountable Managers (Military Flying)◄ and commanders.

AE

12. The safety criteria for the descent of the AE system must be as defined within the individual equipment's specification. In addition, the delivery aircraft TAA must satisfy himself that the AE safety meets the overall operating safety requirements for the delivery aircraft; during embarkation to the aircraft; airborne transit; despatch (until clear of the aircraft boundaries) and disembarkation.

Historic Aircraft

13. ►The same general principles apply to the management of the Airworthiness of historic aircraft as apply to other legacy aircraft on the military register. Where a design change is being considered under the terms of the AMC at paragraph 7, it is particularly important that when specialist advice or manufacture is required, it is sought from those with proven competence in the relevant design philosophy and techniques. In addition, historic aircraft are normally limited within the RTS to limits far below those for which they were designed, to ensure the Risk to Life is demonstrably maintained ALARP and Tolerable to the satisfaction of the ADH.◄

[6] ►Refer to Def Stan 07-085 – Design Requirements for Weapons and Associated Systems.◄
[7] AE encompasses Airborne Forces Equipment and Airborne Delivery Equipment.
[8] ►For the purposes of this RA, historic aircraft are flown by the Battle of Britain Memorial Flight and the Royal Navy Historic Flight.
[9] RA 1325 – Drafting of Limitations in the Release To Service (RTS).◄