DEF STAN 00-970 NOTICE OF PROPOSED AMENDMENT (Def Stan 00-970-NPA)

TITLE OF PROPOSAL: Review and amendment of Part 13 Sections 1.7 and 1.8

Stage of Amendment: **Issue 1**

Def Stan 00-970 NPA Serial No:	**2015-002**		
Unsatisfactory Report Serial No:	***2015-001***		
MAA Originator:	Grade Redacted	Name Redacted	Post MAA-Cert-ADS1a

Affected Part: (including paragraphs)	**Part 13 Sections 1.7 and 1.8**
Cross-reference to other relevant amendment proposals or documents:	

ADS Point of Contact details		
Rank/Grade and Name:	As above	
Telephone Number mil/civ;	9679 35109	030 679 35109
Civilian Email address:	MAA-Cert-ADS1a@mod.uk	

Part 1 (for issue to User Community)

INTRODUCTION *(Not more than 250 words)*

Enter here a brief explanation of why NPA is being issued, i.e. what does the amendment hope to achieve, by when and how:

The interim issue of Def Stan 00-55 Issue 3, alongside the already issued Def Stan 00-56 Issue 5, now provides a clear requirement for the assurance of safety related Programmable Elements. It is therefore, now possible to update this clause in Def Stan 00-970 to remove Def Stan 00-56 Issue 4 which had formerly provided the safety related software requirement and to combine the clause with its sister clause (1.8 Complex Electronic Hardware). In addition to the changing development requirement, Def Stan 00-55 Issue 3 now also provides a clear and distinct requirement for the assurance of safety-related security. This is not dealt with by the existing acceptable means of compliance (since DO-178x and DO-254 do not explicitly cover security). From an airworthiness perspective, the increasing connectedness of airworthiness related

systems likewise increases the vulnerability of platforms to safety-related failures either through exposure to malicious or accidental cyber threats. This warrants explicit guidance, which has been included.

The new text will be clearly identifiable within Annex A.

SUMMARY OF PROPOSED AMENDMENT

Change: *See Annex A*

Impact Assessment:

Objective: Update and clarification of Software Requirements

Risk Assessment: The impact of not incorporating the recommended changes is the possibility of misinterpretation of the requirement

Courses of Action.

1. ***Do nothing: The standard currently refers to out of date standards for software development.***

2. Partial Amendment: N/A

3. Full Amendment: Reference to up to date standards for development including software security.

Preferred Course of Action. Full incorporation

Costs and Benefits:

1. ***Do nothing: Not recommended.***
2. ***Partial Amendment: N/A***
3. ***Full Amendment: Clarification of Software requirements***

Consultation period ends: 24/Apr/2015

The consultation period for this proposed amendment ends on the stated date. Please send your feedback via email to MAA-Cert-ADSGroup@mod.uk. Post 01 April 2015 to DSA-MAA-Cert-ADSGroup@mod.uk

Part 2 (for MAA internal use)

Log of Comments (to be completed once the consultation period has ended).

Comment reference	Date	From (name)	Post	Précis or Topic of Comment	MAA Response
				Comments and the MAA response are listed at Annex B	

Recap of Proposal: *A short summary of the proposal amendment including what changes were incorporated following the consultation period.*

Recommendation. *This section will be completed once all the comments have been received. The recommendation is for the relevant Head of Division to approve the proposal.*

Approval. *This section will detail exactly what has been approved and by whom, and confirm the date for the amendment to be incorporated as well as the date the NPA should be reviewed to determine what the effects of the amendment were in terms of meeting the objective of the change, if there were any unintended consequences and establishing whether the estimated costs were correct.*

Accepted changes will be authorised at the following levels:

- Changes requiring retrospective mandation: 2 * Director Technical
- Changes not requiring retrospective mandating, but introduce novel or contentious requirements or resulting in major changes to requirements: 1* Head of Reg & Cert
- Changes not requiring retrospective mandating but having a significant engineering impact: OF5/B1 Deputy Head of Reg & Cert
- Changes not requiring retrospective mandating but having a Minor engineering impact: OF4/B2 Head of ADS
- Changes deemed as administrational only: OF3/C1.

Approved by:

Signature:	Signed on Original
Name:	
Rank/Grade:	Redacted
Post:	MAA-Cert-S and ADS
Date signed:	4 Jun 2015
Date for amendment to be incorporated:	13 July 2015

Part 3 - NOTIFICATION OF AUTHORIZED AMENDMENT (Def Stan 00-970 NAA)

Document Part:	*Part 13*	Sub-Part:	***Section 1.7 and 1.8***

Unsatisfactory Report Reference:	*n/a*	NPA Reference:	***2015-002***

Originator:		Date:	***4 Jun 2015***

Amendment to be Incorporated on	**13/Jul/2015**

APPROVAL

This Def Stan 00-970 NAA has been approved by the 00-970 WG on behalf of D MAA

INCORPORATION

The amendment will be incorporated in issue 16

Signed on original

Signed (IAW with part 2).

for D MAA

Annex A

Current Text:

REQUIREMENT	COMPLIANCE	GUIDANCE
1.7 SAFETY RELATED SOFTWARE		
1.7.1 For the requirements, design, verification and validation of Safety Related Software (SRS) refer to Def Stan 00-56 Issue 4.	RTCA DO-178C and its appropriate supplements (DO-248C; DO-330; DO-331; DO-332; and DO-333), can be considered to be an acceptable means of compliance to provide design assurance of airborne SRS when supported by a robust, documented and auditable Safety Case as described within Def Stan 00-56 Issue 4 and a structured Safety Assessment Process. The Safety Assessment Process should define the top level safety requirements and design objectives of the software as detailed in the guidance contained within Aerospace Recommended Practices (ARPs) 4761 and 4754A. For legacy software which is intended to be used in a new application, or as a significant development of an existing system, the following principles apply: (a) For systems developed under Def Stan 00- 55 Issue 2, it may continue to be applied as an acceptable means of compliance provided the requirements of that standard continue to be met; and (b) For software developed using	RTCA DO-178C and its appropriate supplements (DO-248C; DO-330; DO-331; DO-332; and DO- 333), can be considered to be an acceptable means of compliance to provide design assurance of airborne SRS when supported by a robust, documented and auditable Safety Case as described within Def Stan 00-56 Issue 4 and a structured Safety Assessment Process. The Safety Assessment Process should define the top level safety requirements and design objectives of the software as detailed in the guidance contained within Aerospace Recommended Practices (ARPs) 4761 and 4754A. For legacy software which is intended to be used in a new application, or as a significant development of an existing system, the following principles apply: (a) For systems developed under Def Stan 00-55 Issue 2, it may continue to be applied as an acceptable means of compliance provided the requirements of that standard continue to be met; and (b) For software developed using RTCA DO-178B, it may continue to be used as an alternative means of compliance under the following circumstances: When considering the use of civil aviation standards (including RTCA DO-178C): civil

	RTCA DO- 178B, it may continue to be used as an alternative means of compliance under the following circumstances: (i) The new application does not require a higher level of software assurance; (ii) The development cycle is not updated to include technologies that have specific supplements in DO-178C; (iii) No new software criteria 1 or 2 (as defined in DO-178C) tool qualification is required. If this is the only differentiator then DO-178B can continue to be applied with the tool qualification objectives provided by DO-330 being used for the new tools; (iv) No new Parameter Data Item files (as defined in DO-178C) are introduced. Where this is the case, DO-178C should be applied to all affected areas of the software and an argument developed in the supporting safety case to show that the change has been contained. Where this is not feasible DO-178C should be applied; and	systems are designed so that there should be no catastrophic failure condition (e.g. loss of aircraft) from the failure of a critical function implemented in a Safety Related Software (SRS) component. If considered in a civil context of use, some SRS components applied in a Military Air Environment (MAE) would require additional mitigation to meet current civil aviations standards, e.g. additional functional, design or physical independence. Where the appropriate functional, design or physical independence cannot be obtained, an alternate military SRS system design should be sought with either a higher level of assurance chosen or the civil standard applied but with additional assurance methods in order to gain the necessary level of confidence to meet the requirements of Def Stan 00-56 issue 4. Civil systems developers utilise the Aerospace Recommended Practices (ARPs) to ensure that the system design is failure tolerant and that a catastrophic failure condition (e.g. loss of aircraft) should not result from the failure of a critical function implemented in a SRS component. The Safety Assessment Process should also ensure that the criticality of the SRS remains valid when used within the context of the MAE. The re-use of previously developed Def Stan 00-55 Issue 2 or DO-178B (and DO-178A) SRS within a new or existing military airborne system can only be considered to be acceptable to the authority on a case by case basis and should be supported by documented evidence and a full audit trail of the development history of the SRS. A robust Safety Case and safety argument should

	(v) All of the lifecycle processes and artefacts from prior certification have been maintained.	be made to support the re-use of the previously developed software within a new or existing military airborne system. The output from the Safety Assessment Process will allow the authority to judge the acceptability of previously developed software. Cognisance should be taken of the effect the introduction of the previously developed SRS has on the safety assessment of existing airborne systems. Any change in context from the previously developed software operating environment to the MAE should be taken fully into account within the Safety Case.
REQUIREMENT	COMPLIANCE	GUIDANCE
1.8 Safety Related Complex Electronic Hardware		
1.8.1	RTCA DO-254 / EUROCAE ED-80 can be considered to be an Acceptable Means of Compliance (AMC) to provide design assurance of airborne Safety Related Complex Electronic Hardware (CEH) when supported by a robust and auditable Safety Case (as required by DEF STAN 00-56) and a structured System Safety Assessment process. The System Safety Assessment process should define the top level safety requirements and design objectives of the CEH.	This requirement focuses on Complex Electronic Hardware (CEH), also known as complex custom micro-coded components. These include: Application Specific Integrated Circuits (ASIC); Programmable Logic Devices (PLD); Field Programmable Gate Arrays (FPGA); and other similar electronic components or devices. A hardware item is considered 'complex' if a comprehensive combination of deterministic tests and analyses cannot ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour. Meaning that, if the item is so complex that it is impossible or impractical to completely test and analyze it, one must rely on design assurance to give confidence in its correct operation. A System Safety Assessment, which is outside of the scope of DO-254 / ED-80, is required to assign a System Development Assurance Level to the CEH. Civil

		systems developers utilise the Aerospace Recommended Practices (ARPs) 4761 and 4754A as guidance for System Safety Assessments and design assurance. DEF STAN 00-56 applies to the requirements, design, verification and validation of Safety Related Complex Electronic Hardware (CEH). In addition to demonstrating compliance to DO-254 / ED-80, a Safety Case, produced in accordance with the requirements of DEF STAN 00-56, should ensure the Safety Assessment Process determines the criticality of the Safety Related CEH when used in the context of the Military Air Environment (MAE). Any contractor using Safety Related CEH that has been previously developed and does not use DO- 254 / ED-80 as its means of compliance is required to justify the alternative means to the authority. Justification for the use of the alternative means of compliance should show that those means meet the safety objectives of the regulations and be supported by documented evidence, including a full audit trail of the development history of the Safety Related CEH. Access to this documentation should be made available to the authority to establish sufficient confidence in the evidence. The System Safety Assessment process and Safety Case will allow the authority to judge the acceptability of previously developed CEH.

Proposed Text:

REQUIREMENT	COMPLIANCE	GUIDANCE
1.7 **SAFETY RELATED PROGRAMMABLE ELEMENTS**		
1.7.1 For the requirements, design, verification and validation of safety related Programmable Elements (PE) refer to Def Stan 00-55 Issue 3.	To meet the stated requirement, Compliance is provided in four sections: system level safety considerations; airworthiness related cyber security; Safety Related Software (SRS); and Complex Electronic Hardware (CEH). **(a) For the assurance of system level safety considerations:** At the system level, the Safety Assessment process should define the top level safety requirements and design objectives of the PE as detailed in the guidance contained within Aerospace Recommended Practices (ARPs) 4761 and 4754A. All aspects of the PE should be supported by a Safety Assessment Report as described within Def Stan 00-56 Issue 5.	Guidance for this requirement is provided in four sections mirroring those for compliance. **(a) Guidance for system level safety considerations:** Civil system developers apply ARPs to ensure that the system design is failure tolerant and that a catastrophic failure condition (e.g. loss of aircraft) should not result from the failure of a critical function implemented in a PE component. The associated Safety Assessment process should define the top level safety requirements and design objectives of the PE as detailed in the guidance contained within Aerospace Recommended Practices (ARPs) 4761 and 4754A. As required by Def Stan 00-56 Issue 5, the Safety Assessment Report should provide a complete, evidence-based, robust, compelling, documented and auditable argument for all aspects of the safety related PE including providing evidence that the criticality of any previously developed PE remains valid when used within the context of the Military Air Environment (MAE). Both the Safety Assessment process and resulting

		Safety Assessment Report activities should also be cognizant of security assessment requirement detailed below.
	(b) For airworthiness related cyber security assurance: RTCA DO-326A/EUROCAE ED-202A and associated RTCA DO-356/EUROCAE ED-203 combined with arguments made against JSP 440 should be used as an acceptable means of compliance with the cyber security requirements of Def Stan 00-55.	**(b) Guidance for airworthiness related cyber security:** It is necessary to ensure that platform cyber security vulnerabilities do not purposefully or accidentally threaten airworthiness. In keeping with threats to the continued safe operation of SRS and CEH, Def Stan 00-55 Issue 3 places a requirement to demonstrate that potential cyber security threats to safe operation are mitigated. Def Stan 00-55 highlights that JSP 440 provides guidance on security policy but the latter does not specifically provide AMC for design assurance of the security aspects of airworthiness, therefore a combined approach is required. It is recognised that DO-326A/ED-202A has been developed for use on large civil aircraft. As such, some tailoring of the guidance provided therein may be required for military aircraft and the military environment. As is the case for conventional software assurance, the level of airworthiness-related security assurance should be commensurate with the risk associated with failure. Usefully, some of the activities associated with safety assurance and airworthiness-related security overlap, it is therefore recommended that an integrated and coherent approach is taken to reduce unnecessary overheads. Due to the evolving nature of cyber security threats, where airworthiness-related security risks are

		identified, it would also be anticipated that a continuing airworthiness-related security strategy (for example, as described in RTCA DO-355/EUROCAE ED-204, Information Security Guidance for Continuing Airworthiness) would be implemented.
	(c) For Safety Related Software (SRS) assurance:	**(c) Guidance for Safety Related Software (SRS):**
	RTCA DO-178C and its appropriate supplements (DO-248C; DO-330; DO-331; DO-332; and DO-333), can be considered to be an acceptable means of compliance to provide design assurance of airborne SRS when supported by a robust, documented and auditable Safety Assessment as described within Def Stan 00-56 Issue 5.	The guidance in Def Stan 00-55 Issue 3 on the adoption of the DO-178 family identifies additional considerations relating to governance and shortfalls against the Def Stan 00-55 requirements; these should be addressed along with any 'military delta' particular to the application.
	For legacy software which is intended to be used in a new application, or as a significant development of an existing system, the following principles apply: (i) For systems developed under Def Stan 00- 55 Issue 2, it may continue to be applied as an acceptable means of compliance provided the requirements of that standard continue to be met; and (ii) For software developed using RTCA DO- 178B, it may continue to be used as an alternative means of compliance under the following circumstances:	For legacy software which is intended to be used in a new application, or as a significant development of an existing system the acceptability of remaining with the legacy means of compliance is based on the principle that switching development activities to a different standard may inherently increase the risk of introducing errors into the software due to applicants applying unfamiliar processes, methods or techniques. Should this not be an issue for the applicant, it is acceptable to switch to the current acceptable means of compliance (i.e. DO-178C) provided that a complete and coherent assurance argument can be maintained for all of the SRS. When considering the use of software previously developed for civilian applications using civil aviation

	a. The new application does not require a higher level of software assurance; b. The development cycle is not updated to include technologies that have specific supplements in DO-178C; c. No new software criteria 1 or 2 (as defined in DO-178C) tool qualification is required. If this is the only differentiator then DO-178B can continue to be applied with the tool qualification objectives provided by DO-330 being used for the new tools; d. No new Parameter Data Item files (as defined in DO-178C) are introduced. Where this is the case, DO-178C should be applied to all affected areas of the software and an argument developed in the supporting safety case to show that the change has been contained. Where this is not feasible DO-178C should be applied; and e. All of the lifecycle processes and artefacts from prior certification have been maintained.	standards, including RTCA DO-178C, the applicant should note that some SRS components applied in a MAE would require additional mitigation e.g. additional functional, design or physical independence. Where the appropriate functional, design or physical independence cannot be obtained, an alternate military SRS system design should be sought with either a higher level of assurance chosen or the civil standard applied but with additional assurance methods in order to gain the necessary level of confidence to meet the requirements of Def Stan 00-55 Issue 3. The re-use of previously developed Def Stan 00-55 Issue 2 or DO-178B (and DO-178A) SRS within a new or existing military airborne system can only be considered to be acceptable to the authority on a case by case basis and should be supported by documented evidence and a full audit trail of the development history of the SRS.
	(d) For safety related Complex Electronic Hardware (CEH) assurance: RTCA DO-254/EUROCAE ED-80 can be considered to be an Acceptable Means of	**(d) Guidance for safety related Complex Electronic Hardware (CEH):** This element of the requirement focuses on safety related Complex Electronic Hardware (CEH), also

	Compliance to provide design assurance of airborne safety related CEH when supported by a robust, documented and auditable Safety Assessment as described within Def Stan 00-56 Issue 5.	known as complex custom micro-coded components. These include: Application Specific Integrated Circuits (ASIC); Programmable Logic Devices (PLD); Field Programmable Gate Arrays (FPGA); and other similar electronic components or devices. In keeping with DO-254, this clause assumes that function allocations made during system level considerations are to either software or hardware. This part of the clause refers to those functions specifically allocated to hardware. A hardware item is considered 'complex' if a comprehensive combination of deterministic tests and analyses cannot ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour. Meaning that, if the item is so complex that it is impossible or impractical to completely test and analyze it, one must rely on design assurance to give confidence in its correct operation. Def Stan 00-55 Issue 3 provides guidance for the development of requirements, design, verification and validation of Safety Related Complex Electronic Hardware (CEH). Additional considerations relating to governance and shortfalls against the Def Stan 00-55 Issue 3 requirements should be addressed along with any 'military delta' particular to the application. Any contractor using Safety Related CEH that has been previously developed and does not use DO-254/ED-80 as its means of compliance is required to justify the alternative means to the authority. Justification for the use of the alternative means of compliance should show that those means meet the safety objectives of the regulations and be supported

		by documented evidence, including a full audit trail of the development history of the Safety Related CEH. Access to this documentation should be made available to the authority to establish sufficient confidence in the evidence. The System Safety Assessment process and Safety Assessment Report (or Air System Safety Case as appropriate) will allow the authority to judge the acceptability of previously developed CEH.

Annex B

Def Stan 00:970-NPA_2015-002 Comments

Reference Section	Comment	MAA Response	Recommendation
Introduction – line 9	I feel that this sentence should be reworded. From an airworthiness perspective, the increasing connectedness of airworthiness related systems, increases the vulnerability of platforms with respect to safety, either through exposure to malicious or accidental cyber threats.	This introduction does not form part of the amendment.	**No Change**
Introduction – line 9	I feel that it is not quite clear in the text, does the security vulnerability actually effect the safety related failures, or does the vulnerability just affect the overall safety of the platform?	This introduction does not form part of the amendment.	**No Change**
General - Format	It would be helpful for the purposes of tracking and data management, if this requirement was broken down into 4 discrete requirements e.g. 1.7.1 System Level Safety Assurance 1.7.2 Airworthiness related Cyber Security Assurance 1.7.3 Safety Related Software (SRS) Assurance 1.7.4 Safety Related Complex Electronic Hardware (CEH) Assurance	Agree, it is intended that the requirements are sub bulleted a., b., c. and d.	**Recommended Change as per text**
1.7.1 For airworthiness related cyber security assurance:	We believe that it is difficult to link a cyber security vulnerability to an unmanned airworthiness defence standard. This may already be covered through the existing security domain. Also, we can see the value in assessing an accidental threat to airworthiness, but not an assessment of a deliberate 'enemy' attempt.	That is true. From a software perspective DO-178C explicitly does not include security considerations. Intentional threats to airworthiness through cyber vulnerability does not only include "enemy action". In 'exposed' systems platform airworthiness may be compromised by any party with sufficient skill sets.	**No Change**

Reference Section	Comment	MAA Response	Recommendation
	00:55/3 makes the distinction between the PE being the unintentional cause of security integrity issues (Sec 7.2), and the effects from inappropriate intentional change (Sec 8.3.2); but does not go as far as requiring the assessment of deliberate cyber attack. The 970 guidance appears to go to that level through guiding towards (all) potential security threats.	This is not quite correct, Def Stan 00-55 is a goal based standard and does not attempt to provide explicit such requirements; however, in 7.2 it states that: "During PE Failure Assessment there may be potential for PE unintended behaviour to impact or be impacted by Security or Mission Integrity". This should be reading the context of para 0.8 which states: "PE is vulnerable to inappropriate intentional and unintentional change due to its ease of access and modification, particularly when in the supply chain and during maintenance".	
	It may be useful to draw the distinction between “Intentionally Negative Outcomes” and “Unintentionally Negative Outcomes”. Whether these arise from accidental or deliberate ‘Actions’ may be a red herring; protection against unintentional negative outcomes should be covered – the intentional negative actions should not. Having said that, the protection for either case is likely to be similar, although a persistent intent would be harder to mitigate than an accidental action, which would not be targetted to maintain an attack across diverse approaches.	The comment is correct in stating that it will probably not be possible to assure beyond doubt the invulnerability of a system from a determined intentional attack (much in the same way as it is probably not possible to demonstrate that a system is absolutely safe in all scenarios). Furthermore the comment is generally correct in stating that the mitigation is similar, therefore it is not proposed that it is useful to impose further burden on the TAA in demonstrating separately the safeguards against intentional and unintentional attack. The proposed text includes both intentional and unintentional outcomes so as not to inadvertently restrict the assessment.	

Reference Section	Comment	MAA Response	Recommendation
1.7.1 For airworthiness related cyber security assurance:	Neither DO-326A Airworthiness Security Process Specification (issued 6 Aug 14), nor DO 356 Airworthiness Security Methods and Considerations (issued 23 Sep 14) are mandated as AMC or GM in CS-25 Amdt 16 (issued 12 Mar 15) or FAR-25. So it seems premature for MOD to mandate a civil transport category aircraft standard in advance of it being adopted by the civil regulators. While it is helpful to signpost these publications as a source of guidance, the AMC for cyber security should be confined to the relevant objectives in 00-55.	Not at all, the MOD operate aircraft in differing environments from the civil sector and as such there are 'military deltas' that need to be considered. Security threats to safety have been part of the airworthiness requirement for some time (over a decade at least) but have been largely overlooked by the PTs. This specific inclusion into the Def Stan 00-970 is designed to assist PTs in demonstrating compliance. Although having particular relevance to Objective 4 of 00-55, the requirements as such are cross cutting, it is therefore not really appropriate to provide the direct link.	**No Change**
1.7.1 For airworthiness related cyber security assurance: Guidance on tailoring of DO-326	The current guidance recognises that DO-326 has been developed for large civil (piloted) aircraft, and that some tailoring may be required for military aspects.	Although developed for large aircraft, the standard provides general guidance that is deemed appropriate for a wider range of vehicles given the 'military delta' and the potentially hostile cyber environment the platform may need to operate in even during peace time and in friendly airspace. Therefore any tailoring must be conducted on a case by case basis and be informed by the risk to airworthiness from cyber threats. It would not be possible, at this stage to provide such guidance since there are no tailoring trends to work from.	**No Change**

Reference Section	Comment	MAA Response	Recommendation
	The guidance could be made clearer if the tailoring was also allowed due to unmanned aspects. There is a similarity with the classification and certification of UAS types, and some indication of this might be worth adding. Is there a guidance document for this tailoring from the MAA?	It is unlikely that there will be specific tailorings for an unmanned system. However, the Security Risk Analysis should identify the UAS specific hazards on a case by case basis. It is anticipated that as awareness increases these hazards will become more obvious and patterns may occur.	
Security	Accompanying Guidance: o The NPA states that "it is recognised that DO-326A/ED-202A has been developed for use on large civil aircraft. As such, some tailoring of the guidance provided therein may be required". Will there be any accompanying guidance on the level of tailoring that can be conducted? There is a risk that DO-326A/356 will be treated by ISAs and ITEs as an unofficial Appendix to Annex B of Def Stan 00-55 (i.e. it will be an accepted open standard for airworthiness related security and will be deemed to be have to be met in full). o Does the tailoring refer to fitting within the system procurement context so that some of the guideline aspects do not have to be considered? Or, does the tailoring refer to having to form an equivalence argument and therefore all elements within the guideline have to be met? There is a substantial difference in the level of evidence required for the two.	It is not intended at this stage to provide guidance on tailoring (just as there isn't for other standards such as DO-178C, which can be tailored). The concern reference the potential for an over zealous response from ITE/ISA is noted. This will be a matter for the individual PTs to manage. The contents of the standard has to be considered regardless of the system procurement context (e.g. it will also apply to COTS, GFA etc). Therefore in this consideration it should be treated the same as a more traditional software development standard such as DO-178C. The guidance in the standard recognises that it should work hand in hand with the safety processes, therefore it is not the intent of the standard to repeat work (e.g. hazard analyses should consider the cyber	**No Change**

Reference Section	Comment	MAA Response	Recommendation
		threats and if so then there is no need to provide a separate analysis). However, all aspects of the standard should be considered (again, as per a development standard).	
	o If the guideline can be tailored to fit the context of the system procurement then there needs to be advice on which elements are essential to the thrust of the guideline.	See clarification provided above.	
	Access to Supporting Evidence & Types of Evidence: o It is not uncommon for there to be issues with access to pertinent supporting evidence when conducting safety assurance (e.g. due to IPR and ITAR). There is a risk that these same access issues will be faced (and may potentially increase) due to requests to review relevant security evidence to support DO-326A/356 (e.g. Vulnerability Dossier). Also, any product evidence (that underpins the process evidence) could be viewed as exposing platform vulnerabilities etc.	Agree, however, this does not mean that the requirement should not exist. Indeed it can be helpful for the requirements to expose gaps in access to information and thus areas of increased risk.	
	o Will there be advice on the type of evidence (product, process etc) that would be acceptable to meet the guideline given the various procurement contexts that exist for MoD airborne platforms?	As is already the case, it is expected that the security aspects of airworthiness should for part of the platform safety case anyway. For such a safety case one would expect to see a diverse mix of process and product evidence. This is the same as per safety standards such as DO-178C.	

Reference Section	Comment	MAA Response	Recommendation
	Shortfalls in Evidence: o For potential shortfalls in compliance with 178C there are legitimate methods to use product service history (e.g. CAST-1) in order to meet the allocated DAL. However, within the security assurance domain a "service history" argument cannot be adopted as the nature of the threats and the environment will be dynamic. Will there be any guidance on how any DO-326A/356 shortfalls can be mitigated? This is especially pertinent for brown-field developments where a diverse evidence set maybe required. These comments aren't probably relevant for the NPA feedback but they are some thoughts:	This is good point, the AMC includes guidance for modification where there is no baseline security risk assessment. Additionally, whilst the point being made is to an extent true, there is a PSH element to DO-326A (albeit very weak).	
	The NPA states that "usefully, some of the activities associated with safety assurance and airworthiness-related security overlap, it is therefore recommended that an integrated and coherent approach is taken to reduce unnecessary overheads". This implies that there is a cross-over of the SQEP status of the assessor from the safety domain to security. Is this the position of the MAA?	Yes, there should be an overlap. It is no longer the position that a safety-related SME can be ignorant of security threats to safety. However, this does not mean that a 'single hat' can cover both roles, rather that the safety SME should be aware of the threats and ensure that appropriate assurance is in place.	
	That is The overlap with The amendments to include cyber security and The activities that will be conducted as part of any Information Assurance processes?	They should overlap but may not be completely covered. There may be safety-related security issues that are not of interest to the IA processes because they do not carry classified information. As an example, map data may not be of interest to the IA world but may be airworthiness related and as such its security may be required.	

Reference Section	Comment	MAA Response	Recommendation
	I believe it would be beneficial to have a workshop to discuss the changes and how in practical terms they are to be implemented. For example if an architecture solution for a sub-system is a closed system without any external interfaces and can be demonstrated that this is the case, do you really need to go down the DO- 326A approach. I do believe engineering judgement based upon competent SQEP approved staff would be one way forward.	The changes in the 00-970 should not require additional activities by the PT above what they should be doing already to provide defensible arguments in their safety case. Security has been a safety concern since issue 4 of def stan 00-56 (and this was strengthened in issue 5) as well as Def Stan 00-55 issue 2.	
1.7.1 For Safety Related Software (SRS) assurance:	The listed acceptable means of compliance (DO178C plus supplements) is fine as it flows through from STANAG-4703, however UK 00:55/3 allows a contractor to propose (any) Open Standard supported by RGP. The concern is that the singular reference to DO178 in 00:970 will actually act as a limitation as being the *only* acceptable means of compliance. Could it be more prudent to include an acknowledgement in the Guidance column that there are numerous open standards that may also be classed as alternative acceptable means of compliance, providing that they produce the evidence to still meet the Requirements of 00:55/3, and that this alternative evidence is acceptable to the MAA.	Agree, DS00-55 does permit the use of open (or indeed closed) standards. However, only DO-178C has been assessed as providing the level of software assurance required for airworthiness. No, there is an existing process for TAAs to propose AAMC contained in MAA03 Annex B.	**No Change**
1.7.1 For Safety Related Software (SRS) assurance: Legacy software guidance (Re-use of previously	The current guidance shows that the re-use of previously developed SRS (PE) can only be considered when supported by documented evidence and a 'full audit trail' of the development history. The requirement could be clearer if the description of 'full' could be expanded by some reference to an audit standard – or an explicit	Agree. This aspect of the requirement is unchanged from previous issues of Def Stan 00-970 Pt 13, as this	**No Change**

Reference Section	Comment	MAA Response	Recommendation
developed SRS)	citation that the audit should be against either the original development standard, or against 00:55, and therefore any 'Open' standard.	element falls into the guidance element and is commensurate with the guidance in the development standards (i.e. it is driven by the development standard applied), for example in DO-178C it states that "COTS software included in airborne systems or equipment should satisfy the objectives of this document.". It is not recommended that the text is changed.	
CEH GM	"*Justification for the use of the alternative means of compliance should show that those means meet the safety objectives of the regulations and be supported by documented evidence,* ***including a full audit trail of the development history of the Safety Related CEH****.* *Access to this documentation should be made available to the authority to establish sufficient confidence in the evidence. The System Safety Assessment process and Safety Assessment Report (or Air System Safety Case as appropriate) will allow the authority to judge the acceptability of previously developed CEH*." For OTS CEH, the requirement for a "full audit trial" will be unachievable in many cases and the requirement should be tempered against the risk that anomalous behaviour of the CEH might cause. The top level requirement in 00-55 is more pragmatic: 9.3.2 The Contractor shall ensure selection or implementation of PE is managed to identify, assess	It is agreed that the provision of evidence for OTS items (whether software or CEH) can be problematic. The level of evidence required in the audit trail is driven by the relevant standard. This is commensurate with the requirement shown in the comment: "If OTS PE forms all or part of the solution, then care will be needed to show that the pedigree and Design Integrity of the OTS PE is sufficient, or any shortfalls in integrity can be mitigated." Without a full audit trail, the PT would have to demonstrate mitigation for the evidence gap just as for any other gap in evidence. It is therefore not considered appropriate to add this to the text (since it could be argued that it would have to be added to every clause in the AMC for consistency).	**No Change**

Reference Section	Comment	MAA Response	Recommendation
	and mitigate the impact of PE unintended behaviour so far as is reasonably practicable and as defined by the design integrity framework of the chosen PE Open Standard, addressing the risks and uncertainty arising from: (Objectives 2, 4 and 5). Notes iii If OTS PE forms all or part of the solution, then care will be needed to show that the pedigree and Design Integrity of the OTS PE is sufficient, or any shortfalls in integrity can be mitigated.		