AtkinsRéalis

Introduction to Software Safety & Cyber Security

Plan Design Enable

1

AtkinsRéalis

Session Objectives

- To explain how software (Programmable Elements) should be addressed to get a safe system
- What is software?
- Explain the particular problems of software?
- Describe how software safety is managed in the MOD
- Outline the methods of open standards
- Consideration of Cyber Threats

2

What Is Software?

"Intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system."

IEC 61508: 2010

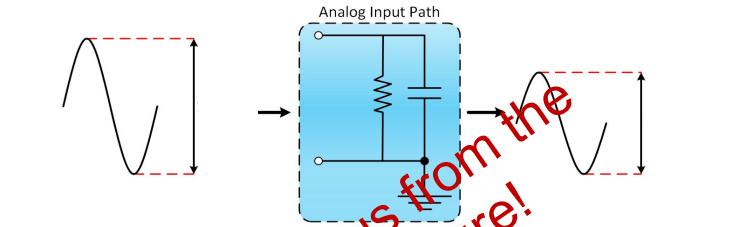
- ***Programmable Element (PE):*** **"PSS that is implemented in software or programmable hardware, which includes any device that can be customised"**

Def Stan 00-056 Issue 7

"Instructions given to hardware."

Kev

Digital – the benefits



Digital free us from the laws of nature!

Temporarily…

0010101010100111 → 1110011100001100

Therac 25: 1985-1987

- Development of earlier machines: Therac-6 and Therac-20 - AECL
- Intended for operation on tumours
  - Produces electron stream and X-rays
  - X-ray therapy needs 100 times more energy than electron therapy
  - If turntable in wrong position, wrong treatment given

Software ‘Features’ - Therac-25

- Additional functionality
  - Computer controlled and monitored from outset
  - Removal of mechanical control components: interlocks
- Cost – code re-use from Therac-6
  - Can replicate software component at no cost
  - Software does not wear out
- User Flexibility
  - Change to interface to enable quicker data entry
  - Treatment pause after error condition - could be restarted by single button press (up to 5 times)
- Precision
  - Electron stream and X-ray treatment in same machine

Software 'Features' - Therac-25

- BUT…
- Six known over-dosage accidents (1985 – 1987) resulting in deaths or very serious injuries
  - May have been many cases where ineffective treatment was given
- Cause(?):
- Software unable to handle certain different inputs at the same time or in the wrong order
- Made worse by inexperienced operators

Software 'Features' - Therac-25

- Additional functionality – removal of hardware
  - Adds software complexity – difficult to test
  - Faults not visible – reliance on error messages
  - Immediate failure – no warning
  - Flawed software may also control separate safety function – no backup
- Cost – code re-use from Therac-6
  - Over-confidence on component used for different purpose – skip analysis and testing
- User Flexibility – change to interface to enable quicker data entry
  - Because change is 'quick and easy' - lacked re-verification
  - User controls away from equipment – may not understand impact of actions
- Precision
  - Software fails systematically (same output for same input) but might seem random – complex failure modes
  - Systematic failure now being challenged with adoption of machine learning

Learning from Therac-25 – A Software Safety Process

- Software is a component in a system
  - Software safety requirements flow from system level requirements
  - Software components needs to be engineered
- Testing is difficult
  - Need other assurance methods
- Show that software has been correctly implemented
  - Is ‘correct’, therefore ‘safe’

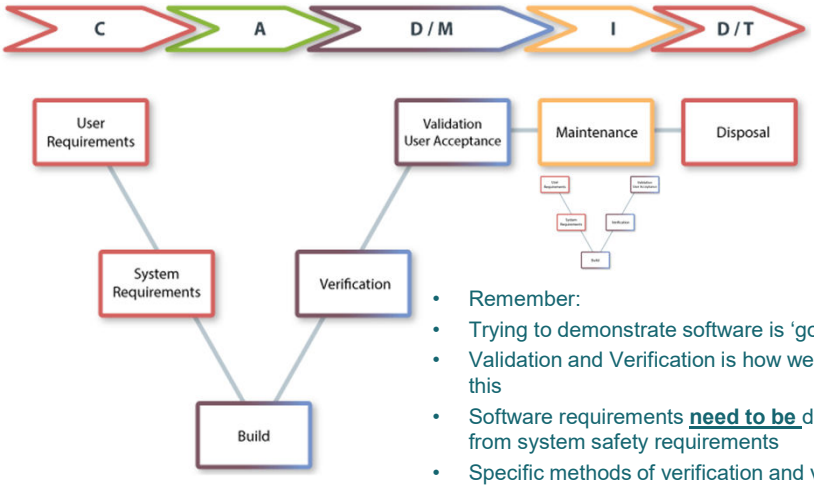
Software ‘Features’ - Ariane 5

- Maiden flight in June 1996
- 10 years in development
- Multi billion dollar investment
- Self destructing 37 seconds after launch because of a malfunction in the control software
- Cause was software error in Inertial Reference System (IRS): main and backup
- Systematic failure mode: common mode failure in main and backup IRS
- Software reuse: Software Safety Requirements specified under *assumptions* for Ariane 4 not applicable to Ariane 5

Software 'Features' - Airbus A400M

- May 2015
- Issue with Electronic Control Unit
- 3 of 4 engines did not respond properly to power setting adjustments
- Engines switched to flight idle mode – why?
- Could not be brought out of flight idle mode
- Incorrect Parameter Files – how to interpret input data from torque sensors
- Parameter Files deleted during installation? Human Factors?

Software Development Cycle



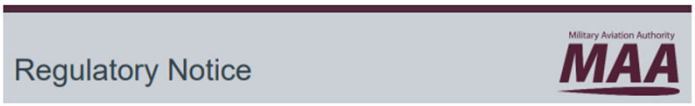
- Remember:
- Trying to demonstrate software is 'good'
- Validation and Verification is how we achieve this
- Software requirements **need to be** derived from system safety requirements
- Specific methods of verification and validation
- Requirements-Build-Verification-Validation cycle will happen often in maintenance

Software in the MOD - Standards

Def Stan 00-970 Pt 13 Req 1.7.1 refers to:

- Def Stan 00-055 Issue 5 (2021)
- Non prescriptive – use of an open standard to meet objectives
- Requirements around 5 objectives:
  - **Objective 1:** PE Safety Requirements shall be defined to manage the PE contribution to Product/Service/System (PSS) hazards
  - **Objective 2:** PE Safety Requirements shall be maintained throughout requirements decomposition
  - **Objective 3:** PE Safety Requirement satisfaction shall be demonstrated
  - **Objective 4:** Hazardous behaviour of the PE shall be identified and mitigated
  - **Objective 5:** The confidence established in addressing the (other) PE Safety Objectives shall be commensurate to the contribution of the PE to PSS risk
  - **New Objective 6 (coming Soon):** The safety-related consequences of adaptive PE behaviour ("*machine learning*") shall be addressed

Artificial Intelligence in Mil Air Systems



Regulatory Notice

Military Aviation Authority
MAA

8 February 2024

MAA/RN/2024/01 - Use of Artificial Intelligence within Safety Critical Systems operating on Military Air Systems

Issue

1. The proliferation of Artificial Intelligence[1] (AI) and Machine Learning[2] (ML) technologies used in digital control Systems and decision support tools has led to the requirement to clarify the position with respect to use of such technologies in Military Air Systems and Air-supporting Systems operated in the Defence Air Environment.

- The pace of technological growth has resulted in a lack of necessary specific standards of Safety critical systems utilizing AI / ML in aviation
- Where compliance cannot be demonstrated due to lack of suitable AI / ML standards, or by the unpredictability of the AI involved, it must be covered by the ASSC

Software in the MOD - Assurance

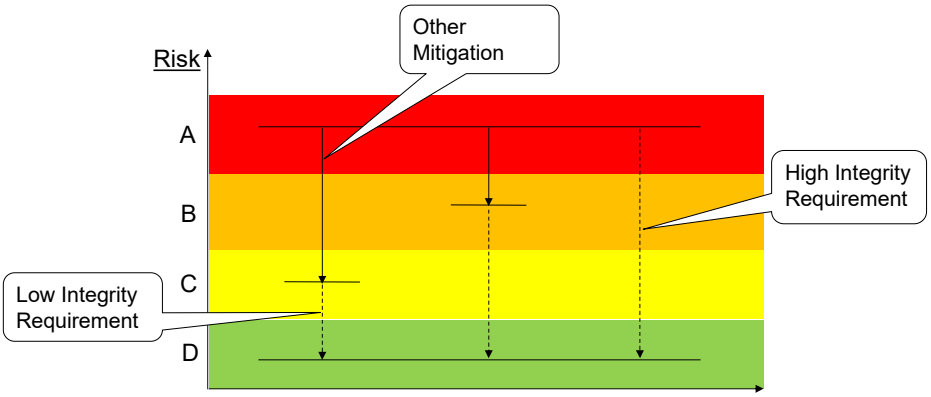
- Create Programmable Elements Safety Summary (PESS)
- Supports Safety Assessment Report (SAR)
- Supports Information Set Safety Summary (ISSS)
  - Sufficient information to enable system integrator or operator to discharge their safety responsibilities
  - Contains information on assumptions and limitations regarding the safe use of the PSS (including the PE within it)
  - May supplant PESS and/or SAR ***if*** system is simple
- Assured with a Programmable Elements Assurance Plan (PEAP) (AET SP4A)

Software in the MOD – Adopting Open Standards

- Use of Open Standards to meet Def Stan 00-055 requirements and objectives
  - "…application of Open Standards supported by Recognised Good Practice (RGP) as an acceptable means of managing compliance of the PE with its Safety Requirements"
- But need to manage military deltas
- Number of Open Standards which work together
  - (DO-178C, DO-254, DO-326A, etc)
  - Also involves use of ARP 4761 and ARP 4754A
- All work to similar principles - Levels

Adopting Open Standards - “Levels”

- How good should my software be?



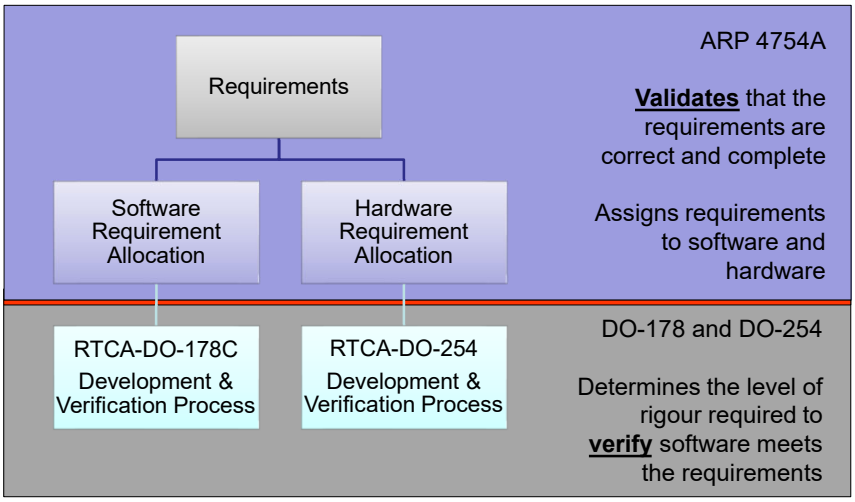
Development Assurance Levels - ARP 4761

Probability (Quantitative)	Per flight hour 1.0E-3	1.0E-5	1.0E-7	1.0E-9	
Probability (Descriptive)	FAA	Probable	Improbable		Extremely Improbable
Failure Condition Severity Classification	FAA	Minor	Major	Sever Major	Catastrophic
Failure Condition Effect	FAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants	- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects on occupants	- all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D	Level C	Level B	Level A

Rough Estimate of Levels

Failure Condition Classification	Development Assurance or Software Level	Example Systems
Catastrophic	A	FADEC, Air Data Computers, Radar Altimeters
Hazardous	B	Communication and Navigation radios
Major	C	Pressurisation System and Navigation Displays
Minor	D	Maintenance Systems
No Safety Effect	E	Entertainment System

Handling Levels



Source: FAA Presentation to 2011 SW & AEH Conference: SAE 4754A Linkage with DO-178 and DO254

The Burden of Higher Levels

Level	Failure condition	Objectives	With independence	Failure Rate
A	Catastrophic	66	25	10^{-9}/h
B	Hazardous	65	14	10^{-7}/h
C	Major	57	2	10^{-5}/h
D	Minor	28	2	10^{-3}/h
E	No Effect	0	0	n/a

Safety Audit & Review

- Def Stan 00-055 **mandates** contracted DOs to conduct internal PE safety auditing consistent with the 'software level' and PE standard used
- Common review gates include:
  - Software Specification Review (SSR)
  - Preliminary Design Review (PDR)
  - Critical Design Review (CDR)
  - Test Readiness Review (TRR)
  - Functional Configuration Audit (FCA)
  - Physical Configuration Audit (PCA)
- Def Stan 00-055 **mandates** the contractor to allow an ISA reasonable access to the information set.

Additional Guidance - Quality

- Remember, software is a product and as such the mandated requirements for quality apply, as detailed in JSP 940, including:
  - 3rd Party Accredited Certification (e.g. TickIT Plus)
  - Contracting – AQAP 2210
- Further information can be found at:
  https://www.aof.mod.uk/aofcontent/tactical/quality/content/4-2-2-2_sqm.htm

Cyber Security for Airworthiness (CSA)

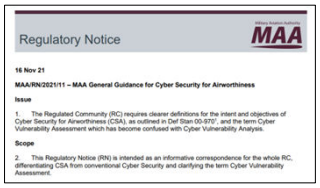
AtkinsRéalis

Background

2015
- Def Stan 00-970 requires CSA to be addressed
  - But not fully appreciated by the Regulated Community

2020
- Regulated Community directed to undertake Cyber Vulnerability Assessments (CVA), to inform CSA
  - Confusion with Cyber Vulnerability Investigation/Analysis undertaken for general cyber security aspects – Not Safety / Airworthiness

2021
- MAA issues guidance to address confusion


Regulatory Notice

MAA

16 Nov 21

MAA/RN2021/11 – MAA General Guidance for Cyber Security for Airworthiness

Issue

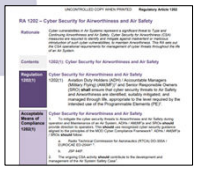
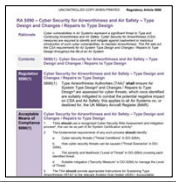
1. The Regulated Community (RC) requires clearer definitions for the intent and objectives of Cyber Security for Airworthiness (CSA), as outlined in Def Stan 00-970', and the term Cyber Vulnerability Assessment which has become confused with Cyber Vulnerability Analysis.

Scope

2. This Regulatory Notice (RN) is intended as an informative correspondence for the whole RC, differentiating CSA from conventional Cyber Security and clarifying the term Cyber Vulnerability Assessment.

2022
- DAT Software Centre of Excellence (DAT SCoE) are developing guidance (AET)

2023
- RA 1202 – Cyber Security for Airworthiness and Air Safety
- RA 5890 – CSA – Type Design and Changes / Repairs to Type Design

AtkinsRéalis

RA 1202

UNCONTROLLED COPY WHEN PRINTED **Regulatory Article 1202**

RA 1202 – Cyber Security for Airworthiness and Air Safety

Rationale

Cyber vulnerabilities in Air Systems represent a significant threat to Type and Continuing Airworthiness and Air Safety. Cyber Security for Airworthiness (CSA) measures are required to identify and mitigate against inadvertent or malicious introduction of such cyber vulnerabilities, to maintain Airworthiness. This RA sets out the CSA operational requirements for management of cyber threats throughout the life of an Air System.

Contents

1202(1): Cyber Security for Airworthiness and Air Safety

Regulation 1202(1)

Cyber Security for Airworthiness and Air Safety

1202(1) Aviation Duty Holders (ADH) / Accountable Managers (Military Flying) (AM(MF))[1] and Senior Responsible Owners (SRO) **shall** ensure that cyber security threats to Air Safety and Airworthiness are identified, suitably mitigated, and managed through life, appropriate to the level required by the intended use of the Programmable Elements (PE)[2].

Acceptable Means of Compliance 1202(1)

Cyber Security for Airworthiness and Air Safety

1. To mitigate the cyber security threats to Airworthiness and Air Safety during operation and Maintenance of an Air System, ADHs / AM(MF)s and SROs **should** provide direction to operators. This **should** use recognized cyber security guidance aligned to the principles of the MOD Cyber Compliance Framework[3]. ADHs / AM(MF)s / SROs **should** follow:

   a. Radio Technical Commission for Aeronautics (RTCA) DO-355A / EUROCAE ED-204A[4, 5].

   b. JSP 440[6].

2. The ongoing CSA activity **should** contribute to the development and management of the Air System Safety Case[7].

RA 5890

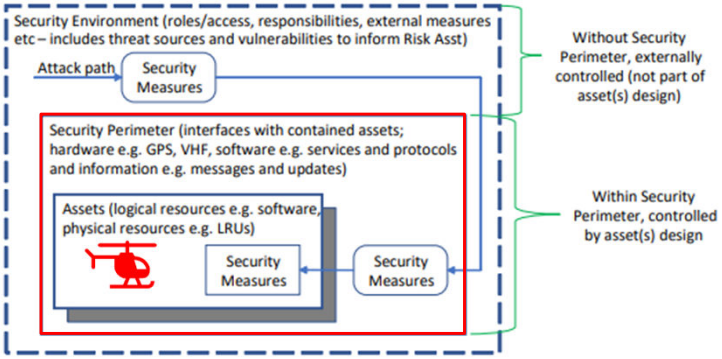
RA 5890 – Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design

Rationale	*Cyber vulnerabilities in Air Systems represent a significant threat to Type and Continuing Airworthiness and Air Safety. Cyber Security for Airworthiness (CSA) measures are required to identify and mitigate against inadvertent or malicious introduction of such cyber vulnerabilities, to maintain Airworthiness. This RA sets out the CSA requirements for Air System Type Design and Changes / Repairs to Type Design throughout the life of an Air System.*
Contents	**5890(1): Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design**
Regulation 5890(1)	**Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design** 5890(1) Type Airworthiness Authorities (TAA)[1] **shall** ensure Air System Type Design[2] and Changes / Repairs to Type Design[3] are assessed for cyber threats, which once identified are suitably mitigated to combat the potential negative impact on CSA and Air Safety; this applies to all Air Systems on, or destined for, the UK Military Aircraft Register (MAR).
Acceptable Means of Compliance 5890(1)	**Cyber Security for Airworthiness and Air Safety – Type Design and Changes / Repairs to Type Design** 1. TAAs **should** use a recognized Cyber Security Risk Assessment and mitigation process[4], this can be as part of Air System Certification activity[2]. 2. The fundamental requirements of any such process **should** identify: a. Cyber security threats ("Threat Conditions" in DO-326A). b. How cyber security threats can be caused ("Threat Scenarios" in DO-326A). c. The severity and likelihood ("Level of Threat" in DO-326A) covering each identified threat. d. Suitable mitigation ("Security Measure" in DO-326A) to manage the Level of Threat. 3. The TAA **should** provide appropriate Instructions for Sustaining Type Airworthiness (ISTA)[5] to the relevant Aviation Duty Holder (ADH) / Accountable

Refers to:
- DO-326A
- DO-355
- DO-356
- JSP440

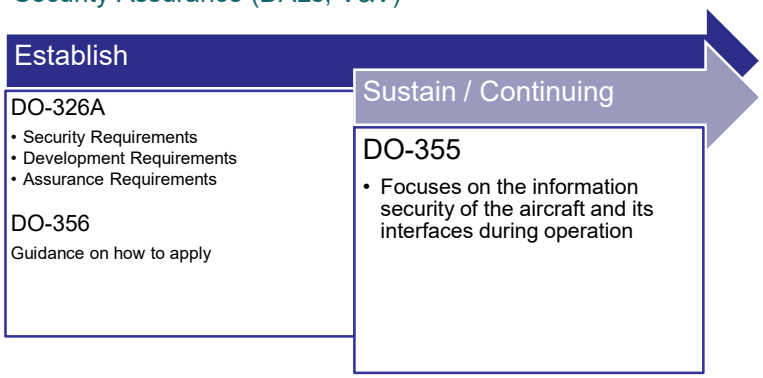
What is Cyber Security Airworthiness (CSA)

- CSA is the application of Cyber Security principles onto systems that have a direct or indirect interface to Safety Related Systems (SRS)

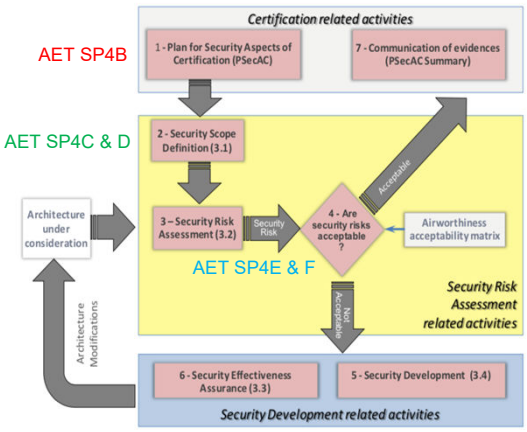


Security Measures

- Security Measures are developed in two main parts
  - Security Development (Requirements, Architecture)
  - Security Assurance (DALs, V&V)



DO-326A – Certification Activities



5 Main Activities

1. Plan for Security Aspects of Cerification (PSecAC) – How DO-326 will be met — AET SP4B
2. Preliminary Aircraft Security Risk Assessment (PASRA) – identify threat conditions and threat scenarios at aircraft and system level — AET SP4C & D
3. Aircraft / System Security Risk Assessments (ASRA / SSRA) determine acceptability of risks and whether further mitigation is required — AET SP4E & F
4. Based on the acceptability of the risk assessment, applicant conducts Security Development Related Activities (Security Development & Security Effectiveness Assurance)
5. Applicant details their accomplishment (PSecAC Summary), inc residual risks

Source: MAA MASG Brief Slidepack

DATIN 69

- Acknowledges all Air Systems on the MAR are required to carry out the CSA Risk Assessment
  - Includes legacy Air Systems on the MAR
  - But new Air Systems undergoing Type Certification can achieve this via compliance with Def Stan 00-970 CSA AMC
- Issues:
  - Full compliance may not be immediately achievable for legacy Air Systems. Latitude has been given in the Regulatory Instruction MAA/RI/2023/03:
    - 01 May 24 – Assessment iaw RA5890 to be completed (forecast)
    - 01 May 25 – Achieve full compliance iaw RA5890
  - Lack of Resource
    - DAT seeking an Air Environment level solution

DATIN 69

- Secure By Design – launched on 28 Jul 23
  - More dynamic continual assurance process
  - Phased transition:
    - Applies immediately to new platforms
    - 31 Dec 23 for all programmes in Concept phase
    - 31 Jul 24 for all programmes in Assessment / Demonstrate / Manufacture phases
    - In-Service capabilities whose traditional accreditation expires before 31 Jul 24 may apply for a maximum 12 months re-accreditation
    - 06 Jul 26 – Traditional accreditation will cease to exist

Conclusions

- Software is a specialised component in a larger system – PE
- Software has a number of attractive attributes: flexibility, precision
- These come at a cost: complexity, geekery
- Def Stan 00-055 has been helping MOD manage software in acquisition since 1991
- MOD software management emphasises use of Open Standards to manage Software ‘correctness’
- Open Standards require different design and assurance methods depending on the software criticality
- Cyber Security is of growing importance, must also be considered and follows similar principles

Questions