



Software Regulations

Systems Certification and Integrity
Directorate of Aviation Engineering
Directorate General Technical Airworthiness

1

Directorate General Technical Airworthiness (DGTA-ADF)



Overview

- Background
- Stepping Through the Regulations
 - What do they actually mean?
 - Reg 2.2.12 Software Compliance Findings
 - Reg 3.5.3 Software Integrity Management
- This is a very dry presentation:
 - No way to avoid this when discussing regulations.

2

Directorate General Technical Airworthiness (DGTA-ADF)





Background

- Motivation for the software regulations:
 - Emerging trend the in the management and acceptance of aviation software.
 - Risks retained by OAA because airworthiness requirements not properly imposed.
 - Software possibly suitable, but the PO was unable to prove it.
 - Particular Issues
 - Access to data.
 - Load control (LRUs were returning from repair venues with the same part number, but different software).

3

Directorate General Technical Airworthiness (DGTA-ADF)



Why regulate aviation software?

- Aside from some administrative issues (how to document compliance), the software regulations do not introduce any new requirements for aviation software.
- Previous regulations contained sufficient requirements for aviation software.
 - i.e. define airworthiness requirements and then prove that you meet them
- But, they weren't being applied well:
 - Attitude: "What is the minimum I have to do to satisfy the regulations?" rather than "How do I assure that the aviation software is safe and fit for purpose?"
- Regulations were being applied by practitioners in a strict sense so DGTA updated the regulations to strictly define aviation software airworthiness requirements.

4

Directorate General Technical Airworthiness (DGTA-ADF)





What do the regulations cover?

- Reg 2.2.12 Software Compliance Findings
 - Applicable to the conduct of software compliance findings by Commonwealth personnel in support of Design Acceptance.
- Reg 3.5.3 Software Integrity Management
 - Applicable to all AEOs that manage software or items containing software.
 - Even if this responsibility has been subcontracted, still need to satisfy Reg 3.5.3.



Regulation 2.2.12 Software Compliance Findings





Reg 2.2.12.a

The DAR shall ensure that a Software Compliance Finding Plan is documented to support the Design Acceptance of new or modified aviation software, where aviation software is defined in accordance with Regulation 3.5.3.a.

- Reasonably straightforward.
- If a Software Compliance Finding is required, the plan for the Software Compliance Finding must be documented.
- What the plan needs to cover is described later in Regulation 2.2.12.



Reg 2.2.12.b

The DAR shall ensure that the software compliance finding is conducted in accordance with the Software Compliance Finding Plan.

- Very straightforward.
- Follow documented plans and procedures.





Reg 2.2.12.c

The DAR shall obtain TAR approval of the Software Compliance Finding Plan if the worst credible failure condition of the new or modified aviation software is more severe than Minor (as defined in FAA AC 25.1309) or Marginal (as defined in MIL-STD-882C).

- Reasonably straightforward.
- TAR approval of the Software Compliance Finding Plan is required if the consequences of failure or partial performance of the software are severe.
- Note that MIL-STD-882C reference does not include a consideration of the control category.
 - This is by design.
- When to seek approval:
 - Prior to contract signature (so DGTA can make sure the contract and the plan are consistent).



Reg 2.2.12.d

Where TAR approval of the Software Compliance Finding Plan is required in accordance with Regulation 2.2.12.c, that TAR approval shall be in the form of either:

- (1) approval of the Software Compliance Finding Plan for a specification acquisition, or
- (2) a standing approval of the Software Compliance Finding Plan for on-going software compliance findings for in-service changes to previously design accepted aviation software.

- Possible to get standing TAR approval for in-service changes.
- Candidates: MPSP0 for DMS changes, TFSP0 for TFWSSF developed changes, ARH, MRH and AEW&C eventually.





B-2 Guam Accident



Water in some air data sensors during calibration evaporated prior to take off. The calibration bias in these sensors confused the flight control computer and the aircraft crashed on take off. Both pilots ejected but the \$2 billion airframe was lost.



Reg 2.2.12.e.(1)

In order to obtain TAR approval of the Software Compliance Finding Plan, the DAR shall submit to the TAR, a Software Compliance Finding Plan that:

(1) was prepared in accordance with AAP 7001.054
Section 2 Chapter 7 Annex A.

- .054 S2 C7 Annex A provides a template for software compliance finding plans.





Software Compliance Finding Plan Template

- Scope
- Referenced Documents
- Basis of Assessment
- Recognition of Prior Acceptance
 - Evidence of Prior Certification
 - Risks Retained or Treated by the NAA
 - Configuration, Role and Environment Differences
 - Level of Rigour
 - Focus of Compliance Finding
 - Planning Objectives
 - Requirements Objectives
 - Design Objectives
 - Code Objectives
 - Test Objectives
 - CM Objectives
 - QA Objectives
 - Non-Interference
- Compliance Finding Process
- Classification of Findings
- Contractual Requirements
- Compliance Finding Agency Competency
- Schedule
- Resource Requirements
- Approval



Reg 2.2.12.e.(2)

In order to obtain TAR approval of the Software Compliance Finding Plan, the DAR shall submit to the TAR, a Software Compliance Finding Plan that:

(2) defines software safety and assurance benchmarks commensurate with the worst credible failure condition of the new or modified software through either application of TAR recognised software safety and assurance standards in AAP 7001.054 Section 2 Chapter 7, or alternative standards approved by the TAR;

- The plan must identify the software safety and software assurance benchmarks against which the software will be assessed.
- You can use the TAR recognised standard, or propose an alternative (which will be assessed for equivalency).





Reg 2.2.12.e.(3)

In order to obtain TAR approval of the Software Compliance Finding Plan, the DAR shall submit to the TAR, a Software Compliance Finding Plan that:

(3) nominates a competent compliance finding agency to undertake the software compliance finding, or includes details of arrangements to resolve the limitations to compliance finding agency competency using technical specialists approved by the TAR;

- Software compliance findings should only be performed by competent agencies.
- Specific competency requirements for all technologies is available in the paper 'Compliance Finding Agency Competency' available through the DGTA website.
- If competent staff are not available to the project, the plan should describe how the required competencies will be obtained (training or outside assistance).



Reg 2.2.12.e.(4)

In order to obtain TAR approval of the Software Compliance Finding Plan, the DAR shall submit to the TAR, a Software Compliance Finding Plan that:

(4) to the extent that the compliance finding uses Commonwealth oversight:

- (i) identifies software life cycle data...
- (ii) identifies arrangements for software compliance finding agency access...
- (iii) identifies the method of evaluation of the software life cycle data...

- For aspects of the software where RPA will not be relied upon, the plan must identify:
 - what data is required to demonstrate compliance
 - how the Commonwealth will get access to that data
 - e.g. contractual clauses, TAA, FMS line items, etc
 - what the Commonwealth will do with that data
- All of these have contractual implications: important to at least draft the plan prior to contract signature.





Reg 2.2.12.e.(5)

In order to obtain TAR approval of the Software Compliance Finding Plan, the DAR shall submit to the TAR, a Software Compliance Finding Plan that:

(5) to the extent that the compliance finding relies on prior acceptance by a recognised civil or military airworthiness authority, includes evidence relating to prior acceptance of the software and any additional supporting information required by *Regulation 2.2.7 Recognition of Prior Acceptance*.

- Should identify evidence of prior certification up front.
 - Failure of RPA arguments is a huge issue for projects.
 - If the intent is to rely on RPA, may not have sufficient airworthiness requirements in the contract, no access to data, etc.
- DGTA wants to have some confidence that RPA will be successful.



Air Inter ITF148 - A320 Strasbourg



The HMI for descent rate was confusing. -3,300 feet per minute and -3.3° were displayed as -33 and -3.3 respectively. A mode switch located away from the display also indicated the mode. Aircrew failed to notice the difference and crashed into a hill on final approach. 87 of 96 people on board died.





Regulation 3.5.3 Software Integrity Management



Reg 3.5.3.a

Each applicant responsible for the Configuration Item management of aviation software or aviation systems containing software shall establish and maintain a Software Integrity Management System, where aviation software is inclusive of:

- (1) on-aircraft software, off-aircraft software with aircraft interface, and off-aircraft software with no interface but which has airworthiness or safety implications; and
- (2) technologies that resemble software development such as Field Programmable Gate Arrays (FPGAs) and firmware.

- Need to establish a system to manage software integrity
 - The rest of Reg 3.5.3 describes what that system should be.
- Defines aviation software:
 - Any software on or interfacing with the aircraft and any software that could affect the safety of the aircraft.
 - Clears up ambiguity regarding firmware: may be manufactured differently, but designed and verified the same as software, so treated like software.





Reg 3.5.3.b

The Software Integrity Management System shall include:

- (1) a Software Management Plan;
- (2) procedures to assure software integrity of new or modified software; and
- (3) procedures to provide continuing assurance of the software integrity of accepted software.

- Need to:
 - assure that new or modified software is acceptable,
 - assure that nothing can happen to the software during use that would affect acceptability, and
 - tell DGTA how you will do it.
- Sub-point (2) is further expanded in Reg 3.5.3.d
- Sub-point (3) is further expanded in Reg 3.5.3.e



Reg 3.5.3.c.(1) and (2)

The Software Integrity Management System shall ensure that:

- (1) the SMP is issued by the SDE and approved by the TAR;
- (2) any amendment to the SMP:
 - (i) has been approved by the DAR; and
 - (ii) where there are additions to the Configuration Items listed in the SMP, or a reduction to the assurance of software integrity, has been approved by the TAR.

- Every SMP must be issued by the SDE and approved by a member of the Commonwealth (TAR or DAR).
- TAR approval is required for initial issue.
- If the scope of software being managed is increased, TAR approval is required.
- If a reduction in assurance is proposed (e.g. less testing), TAR approval is required.
- Otherwise, the DAR can approve amendments.





Reg 3.5.3.c.(3)

The Software Integrity Management System shall ensure that:

(3) all aviation software Configuration Items being managed by the applicant, including the associated software assurance level, and worst credible failure condition are identified in the SMP;

- The SMP needs to list the software being managed and whether the software is safety related.
- Why?
 - Some AEOs did not know what software they were “managing”.
 - Particularly legacy aircraft and non-aircraft SPOs.
 - Some AEOs state that they do not manage safety related software, but had no justification.
- The software list also provides the context for determining whether software integrity management system is sufficient.
 - i.e. are there support arrangements in place for all managed software items?



Reg 3.5.3.c.(4)

The Software Integrity Management System shall ensure that:

(4) all software tools being used by the applicant, including the tool categorisation and qualification, are identified in the SMP;

- Similar justification to the above, some AEOs not aware of the tools that were in use.
- Some had no control and no qualification.





Reg 3.5.3.c.(5)

The Software Integrity Management System shall ensure that:

(5) the SMP is reviewed at an interval not exceeding two years.

- Very straightforward.



Air France 296 - A320 Paris Air Show



During the Paris Air Show, the A320 flying display included a low altitude, low speed, high alpha fly past. Software controlled throttle (allegedly) did not respond to pilot inputs. 3 of 136 people on board died.





Making off with the evidence...



Useless Statistics

- In large, modern aircraft, you have an 82.5% chance of surviving an accident.
 - 77% of accidents have no fatalities at all.
 - If there are fatalities, there is a 24% chance that it won't be you.
- Even if we only look at accidents severe enough to cause the loss of the airframe, your chance of survival is 72%.





Reg 3.5.3.d.(1)

The procedures to assure software integrity of new or modified software shall:

(1) ensure software development of safety-related software is conducted to satisfy the objectives of either a TAR recognised software assurance standard, or a Software Assurance Matrix approved by the TAR;

- Software must be developed to an appropriate level of assurance.
 - See earlier presentations.
- Can use either a recognised standard (e.g. DO-178B) or develop your own.
 - A Software Assurance Matrix effectively defines the outcomes or pass marks for each phase of software development.
 - Further guidance is available in AAP 7001.054 Section 2 Chapter 7.



Reg 3.5.3.d.(2)

The procedures to assure software integrity of new or modified software shall:

(2) require a software safety program be established for the development of all software that is safety related;

- It is not enough for the software to be built well, it must have been built to do the right things.
 - Software safety is how you prove that the software has been told to do the right things.
- Software safety is not assignment of software assurance levels.
 - That is software in system safety.
- Software safety is a set of analyses to identify software vulnerabilities and software safety requirements.





Reg 3.5.3.d.(3)

The procedures to assure software integrity of new or modified software shall:

(3) to the extent that Commonwealth oversight applies:

- (i) ensure a Plan for Software Aspects of Certification, or equivalent document, is submitted to and approved by the TAR prior to the commencement of development if the worst credible failure condition of the new or modified aviation software is more severe than Minor (as defined in FAA AC 25.1309) or Marginal (as defined in MIL-STD-882C);
- (ii) provide for Commonwealth oversight of software for safety-related systems to permit the Commonwealth to make software compliance findings;

- Prior to development for safety related software with severe consequences of failure, must obtain TAR approval that development activities will be sufficient.
 - Note: abridged PSAC can be developed for in-service changes.
- The Commonwealth must have sufficient access if Commonwealth oversight is to be provided.



Reg 3.5.3.d.(4)

The procedures to assure software integrity of new or modified software shall:

(4) to the extent that recognised civil or military Airworthiness Authority oversight applies:

- (i) ensure that certification requirements are agreed by the recognised civil or military Airworthiness Authority prior to commencement of development if the worst credible failure condition of the new or modified aviation software is more severe than Minor (as defined in FAA AC 25.1309) or Marginal (as defined in MIL-STD-882C);
- (ii) provide for oversight by the recognised civil or military Airworthiness Authority of safety-related systems to permit the recognised civil or military Airworthiness Authority to issue their certification to the Commonwealth;

- As per Reg 3.5.3.d.(3), but this time the agreement is with an airworthiness authority other than the ADF.





Reg 3.5.3.d.(5)

The procedures to assure software integrity of new or modified software shall:

(5) implement acceptable software load control as required by Regulation 3.5.

- System must assure that the version of software used is the same as the version that was certified.
- May be a simple task:
 - Prior to use, check version number against procedure.
 - After loading, check version number procedure.
- May be more complicated:
 - Software in LRUs that are sent to repair venues: the ADF may not be responsible for assuring the version loaded is correct.
 - May need:
 - agreement with repair venue regarding software to load
 - identification of software version on outside of LRU



V-22 Jacksonville, NC



A flight control hydraulic line burst (due to chaffing) during transition from fixed to rotary wing operation. The Flight Control Computer reset button was pressed by aircrew (standard procedure) to restore the system to a safe state. The reset coupled with the failed line confused the Flight Control Computer which started giving grossly incorrect commands (so aircrew kept pushing reset). Four marines were killed in the accident.





Reg 3.5.3.e.(1)

The procedures to provide continuing assurance of the software integrity of accepted software shall:

- (1) implement a framework for software problem reporting, problem assessment, tracking of problem reports and corrective action to ensure that safety-related errors, faults and failures are identified and resolved within a timely manner as per Regulation 3.5.2;

- Regulation of the Key Issue in AAP 7001.054 Section 2 Chapter 17.
- A standard problem reporting system (that is already in place for most aircraft) will satisfy this regulation.
- Note: even if there is no intention and no contractual mechanism for changes to be made to a software item, a problem reporting system must still be in place.



Reg 3.5.3.e.(2)

The procedures to provide continuing assurance of the software integrity of accepted software shall:

- (2) ensure the DAR and TAR are notified of any errors, faults or failures of aviation software which potentially result in a large reduction in safety margins;

- Notify the DAR and TAR of any safety-related problem reports in software that is Level B or above.
 - “Large reduction in safety margins” is the FAA definition for Hazardous/Severe Major failure conditions.
- No need to notify the TAR if a non-safety-related problem report is raised in Level B or above software.
 - e.g. minor HMI issues
- If you cannot determine whether the problem report is safety-related or not, notify the TAR.





Reg 3.5.3.e.(3)

The procedures to provide continuing assurance of the software integrity of accepted software shall:

(3) describe configuration management processes of all aircraft software as required by Regulation 3.5.

- A very broad requirement.
 - Compliance requires good software CM.
- Focus (two things historically done poorly):
 - Configuration Status Accounting
 - What version of software is loaded to which aircraft/LRU?
 - Control of Changes
 - In particular, items returned from repair venues.



Notes on Compliance with Reg 3.5.3

- Acquirers (e.g. SPOs)
 - The SMP should identify how the integrity of contractor developed software will be managed.
 - i.e. what are the requirements for the contractor to develop safe software and how are they enforced?
 - Little or no information on software development will be required.
 - SMP Template: AAP 7001.054 Section 2 Chapter 7 Annex C
- Developers
 - Need to describe how the software will be developed to meet airworthiness requirements (i.e. requires detail on or reference to development and verification procedures).
 - SMP Template: AAP 7001.054 Section 2 Chapter 7 Annex B Appendix 1





Summary

- Software regulations were introduced in response to an emerging trend of poor management of aviation software.
- The new software regulations are consistent with the previous regulations: just more explicit.
- If an organisation was doing a good job managing software, there will be an administrative burden to demonstrate compliance, but that's all.
- If an organisation was not doing a good job, there may be significant effort required to comply with the regulations.
- Compliance with Reg 3.5.3 for existing AEOs is required by 17 Dec 10.



Questions

