



Government of Bermuda DCA Airworthiness Management

Module 8

Software Criticality & Configuration

Control

Len Arnot-Perrett

AVISA



Software Criticality

- Certification standards addressing software certification have been in place for a considerable time – e.g. RTCA Doc. DO-178B/EUROCAE Doc.12b *Software Considerations in Airborne Systems & Equipment Certification*
- FAA Order 8110.49 *Software Approval Guidelines*
- Standards essentially address the design, production, modification of software and assign levels of criticality to software.
 - Criticality levels consistent with 25.1309 principles
 - ARINC Document addresses management of Field Loadable Software – *there are currently no specific standard requirements for operator in-service management of software!*



Software Criticality

ARINC

GUIDANCE FOR THE MANAGEMENT OF FIELD LOADABLE SOFTWARE

ARINC REPORT 667

PUBLISHED: MAY 17, 2002



Software Criticality

EUROPEAN ORGANISATION FOR THE SAFETY OF
AIR NAVIGATION



**Integrity of Aeronautical Information:
Principles - Data and Quality
Management**

CHAIN

*Controlled and Harmonised
Aeronautical Information Network*

CHAIN/0028

Edition	:	1.0
Edition Date	:	29th August 2007
Status	:	Released Issue
Class	:	General Public



Software criticality levels based on
25.1309 principles – hazard defined
at an airplane level

Level A - catastrophic

Level B - hazardous

Level C - major

Level D - minor



Software Criticality

Complex system architecture

sometimes makes it difficult to clearly understand in-service which system is at what level without reference to source documents produced by TC Holder

Partitioning of software systems difficult to achieve at design level and more difficult to understand at operator level without TC support *e.g. 'cabin*

environment includes JEE but also



- C of A issue: software criticality declaration (by TC Holder) for each aircraft undergoing C of A
- Software criticality relevant to
 - changes/modifications or classification changes
 - In-service airworthiness management procedures
 - Quality audit
 - Maintenance procedures
- C of A renewal: assess any software changes for criticality and continued airworthiness implications.

i.e. any changes relating to maintenance or serviceability assessment.



Field Loadable Software

- UK CAA published guidance material on the subject – CAP 562 – as yet no EASA equivalent.
- ARINC Report 667 refers – Guidance for the Management of Field Loadable Software
- Objective: to provide guidance to operators and maintenance organisations.
- Material is intended to be complimentary to Design requirements
- address software/database supplier, operator, maintenance provider responsibilities

Why worry?



Field Loadable Software

Why worry?

*Air New Zealand DC 10
accident – crash site
on Mount Erebus
Antarctica – 28
November 1979*





Field Loadable Software

Air New Zealand operate tourist
sightseeing flights over Antarctica using
DC 10 aircraft which requires aircraft to
descend to low altitude to improve pax
visibility <3000'

Flight navigation conducted using INS
coupled control



Field Loadable Software

- Route and procedure approved by NZ CAA – though not low altitude component
- Route coordinates in Air NZ Ground computer did not match approved route
 - Coordinates changed on morning of crash flight – *operating crew not informed!*
 - Coordinates fed into aircraft INS – no longer coincide with map mark up prepared by Captain prior to flight at crew briefing – *28 miles west of previous track!*



Field Loadable Software

- Aircraft track now coincides with Mt. Erebus – 12,000' plus
- Crew descend to 3000' – unaware of proximity of Mt. Erebus
- Aircraft destroyed – no survivors



Field Loadable Software





Field Loadable Software

Why worry?

Software is increasingly significant to the continuing airworthiness and safe flight of contemporary aircraft

Field Loadable changes are commonplace!

- *Electronic Flight Bag*
- *FADEC*
- *FMS*
- *TAWS*
- *NAV Data Bases*
- *Maintenance Test Equipment*

...and so on!



Field Loadable Software

Why worry?

Contemporary continuing airworthiness requirements in Europe and the USA do not adequately address the safety management issues associated with software management!



Field Loadable Software

OTAR 39.55(n) requires that

- (n) for any aircraft having systems utilising Field Loadable Software and Database Field Loadable Data, the operator has procedures acceptable to the Governor to ensure that:
 - (1) Field Loadable Software uploads are accomplished in accordance with the approval requirements of OTAR Part 21 Subpart C; and
 - (2) Database Field Loadable Data is controlled and transferred in accordance with the equipment manufacturer's instructions;



Field Loadable Software

No established requirements to set standards for operator management of software

As a minimum operators are advised to apply safety management principles – possible use of Arinc Doc. & UK CAA CAP 562 guidance as a start point.

Introduce management procedures and quality control/management processes



Field Loadable Software

Establish management procedures and introduce rigorous quality control and management processes

- *Internal distribution*
- *External suppliers*
- *Security*
- *Replication*
- *Adequate configuration records*
- *Training*

Complex management process using wide range of terms to describe software levels!



Field Loadable Software Definitions

- Field Loadable Software (FLS): Software, including data tables, which can be loaded without removing the system or equipment from its installation.
- Loadable Software Aircraft Part (LSAP): FLS that is considered to be part of the aircraft approved design and therefore an aircraft part requiring release documentation (EASA Form One, FAA 8130-3) or an equivalent agreed with EASA

Note: FAA guidance uses PMA approval and for FLS accepts F337 – could be unacceptable under EU Regulations – consult Part 21 DAH/EASA!



- Databases: LSAP in database form e.g. Navigational Data Base (NDB), Terrain/Airport Database (TDB), Model/Engine Database (MEDB) containing information such as navigation, route, engine performance and Terrain used by the Flight Management Computer (FMC), Terrain Awareness Warning System (TAWS)
- User Modifiable Software (UMS): Software declared by the aircraft Type Design Organisation as being intended for modification by the aircraft operator – *possibly not subject to Part 21 Change procedures*
- Electronic Distribution of Software (EDS): A process whereby FLS is moved from the producer or supplier to a remote site (generally the operator) without the use of a physical media.



Replication of Software

- If LSAP copies are to be made this should be accomplished using the aircraft type design organisation approved FLS Storage Media replication process. The copying should be recorded in an Aircraft Software Replication Register and be traceable to the original source from which copies were made - *to ensure traceability and facilitate audit*
- Operators should have appropriate procedures in place to ensure that it is possible to determine the equipment and software configuration of each aircraft in their fleet – *important continuing airworthiness management issues!*



- Operators/maintenance organisations procuring, modifying FLS should have documented procedures – CAME/MOE setting out management and quality processes - *It is expected that the procedure would cover the complete cycle from procurement specification, distribution methodology (e.g. EDS, media type etc.), receipt inspection/assessment through to embodiment, subsequent testing and release to service, including internal audit programme*
- There are instances when a change to UMS may modify aircraft performance information presented to the flight crew – *consult Part 21 DAH/EASA*
- Organisations need to ensure that competent staff are retained in order to ensure adequate management of processes



EURCAE/RTCA Documents

USA	Europe	Description
RTCA DO 178B	EUROCAE Doc. ED 12B	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO 201A	EUROCAE Doc. ED 77	Standards for Aeronautical Information
RTCA DO 200A	EUROCAE Doc. ED 76	Standards for Processing Aeronautical Information
RTCA DO 236A	EUROCAE Doc. ED 75A	Minimum Aviation System Performance Standards (MASPS): Required Navigation Performance (RNP) for Area Navigation



- **Electronic Distribution of Software (EDS): Document No. 666**
- **Field Loadable Software (FLS) Document No. 667**



- Let us not go back!