

2003 FAA National Software Conference

History of the Dissimilarity Discussion



History of the Dissimilarity Discussion

*As remembered/reconstructed by
Jozef B.J. van Baal, CAA-NL*

19 September 2003

History of the Discussion.

1

DO-178 and DO-178A



- WRT “additional activities”:
 - DO-178: Contains only a Note that declares out of scope the providing of guidance on additional activities that the authorities may require for full flight regime critical systems, e.g. FBW
 - DO-178A: Contains a Note that “other measures”, usually within the system, may be necessary in addition to a high software Level

19 September 2003

History of the Discussion.

2

2003 FAA National Software Conference

History of the Dissimilarity Discussion

Note DO-178A Par. 3.3



It is appreciated that, with the current state of knowledge, the software disciplines described in this document may not, in themselves, be sufficient to ensure that the overall system safety and reliability targets have been achieved. This is particularly true for certain critical systems, such as fly-by-wire. In such cases it is accepted that other measures, usually within the system, in addition to a high level of software discipline may be necessary to achieve these safety objectives and demonstrate that they have been met.

19 September 2003

History of the Discussion.

3

WG12/SC167 – 1/3



- Software Levels hot issue in 1990
 - How many Levels ?
 - JAA had already split "2" in "2A" and "2B"
 - Note suggested that there was a Level "zero"
 - Is there a "Super Critical Level" that needs additional protection ?
 - Can, with current software development techniques, software be developed that we trust in architectures where it can directly cause a Catastrophic Failure Condition ?

19 September 2003

History of the Discussion.

4

2003 FAA National Software Conference

History of the Dissimilarity Discussion

WG12/SC167 – 2/3



- Note in Section 3.3 was heavily debated
- SG 2 of WG 12 in April 1990 decided:
 - Five Levels
 - No direct translation Levels between 178A and 178B
 - Keep Note
- However, Draft 1 of January 1991 does not have the Note, and neither do any later drafts

19 September 2003

History of the Discussion.

5

WG12/SC167 – 3/3



- Note was deliberately deleted
 - However, arguments not documented...
- Discussion centered on number of software Levels
- Consensus was that application of the guidance for Level A provides sufficient confidence in safety to use the software in full flight regime critical systems
 - Without additional protections !

19 September 2003

History of the Discussion.

6

2003 FAA National Software Conference

History of the Dissimilarity Discussion

WG52/SC190



- Discussion started again (?) in June 2000 at an EPIC co-ordination meeting
- Subject discussed at CAST, and with several industry representatives since then
- Avionics Panel for the JAA Validation of an JAR/FAR 25 Aircraft expressed a major concern, asked for CSP advice
- CSP provided advice to LASCC

19 September 2003

History of the Discussion.

7

The Rules ?? (1/3)



- CAR 4-B in 1945: no requirement really
- Changed end 1940-ies to include 4b.606(b):
All equipment, systems and installations shall be designed to safeguard against hazards to the airplane in the event of their malfunctioning or failure.
- JAR 25 Change 15 contains .1309(b):
The aeroplane systems <> must be designed so that
 - any failure condition preventing continued safe flight and landing: extremely improbable;
 - any failure condition that would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions: improbable.
- Single Failures only discussed in AMJ 25.1309

19 September 2003

History of the Discussion.

8

2003 FAA National Software Conference

History of the Dissimilarity Discussion

The Rules ?? (2/3)



- DO-178B consciously introduced 5 Levels
 - New Level E: no safety effect
 - New Level A: if software can directly cause (or contribute to) a Catastrophic Failure Condition
 - Although not documented, consensus in WG/SC that there is no more critical software exists then Level "A"
- ARP-4754 (system level development assurance) followed this approach

19 September 2003

History of the Discussion.

9

The Rules ?? (3/3)



- AMJ 25.1309 modified by NPA 25F-281:
 - Explains that probabilities not useful for Development Assurance
 - Confirms five Criticality categories
 - Confirms value of ARP-4754, DO-178B, and equivalent hardware document (now ED-80)
 - Adds explanation on relation between ARP-4754 and DO-178B
- ED-80/DO-254 on hardware Development Assurance published, using same principles

19 September 2003

History of the Discussion.

10

2003 FAA National Software Conference

History of the Dissimilarity Discussion

Link JAR/FAR 25 to Development Assurance



- 25.1309 requires inverse relation between severity and probability of failures
- Consensus exists that no probabilities can be attached to Development Errors
- Advisory Material wrt Development Errors:
 - Explains that compliance with 25.1309(b) can be demonstrated by Development Assurance
 - Points to ARP-4754, DO-178B and ED-80 to cover Development Assurance

19 September 2003

History of the Discussion.

11

How about Single Failures?



- JAR 25 at Change 15:
 - Not in 25.1309 rule, mentioned in AMJ
 - Fail Safe Principle in AMJ includes objective that no single failure should prevent continued safe flight and landing
 - AMJ Discussion explains that MoC in AMJ not applicable to software assessments
- NPA 25F-281:
 - 25.1309(b)(1)(i): any catastrophic failure condition <> does not result from a single failure
 - AMJ details that for complex systems development assurance methods is acceptable MoC

19 September 2003

History of the Discussion.

12