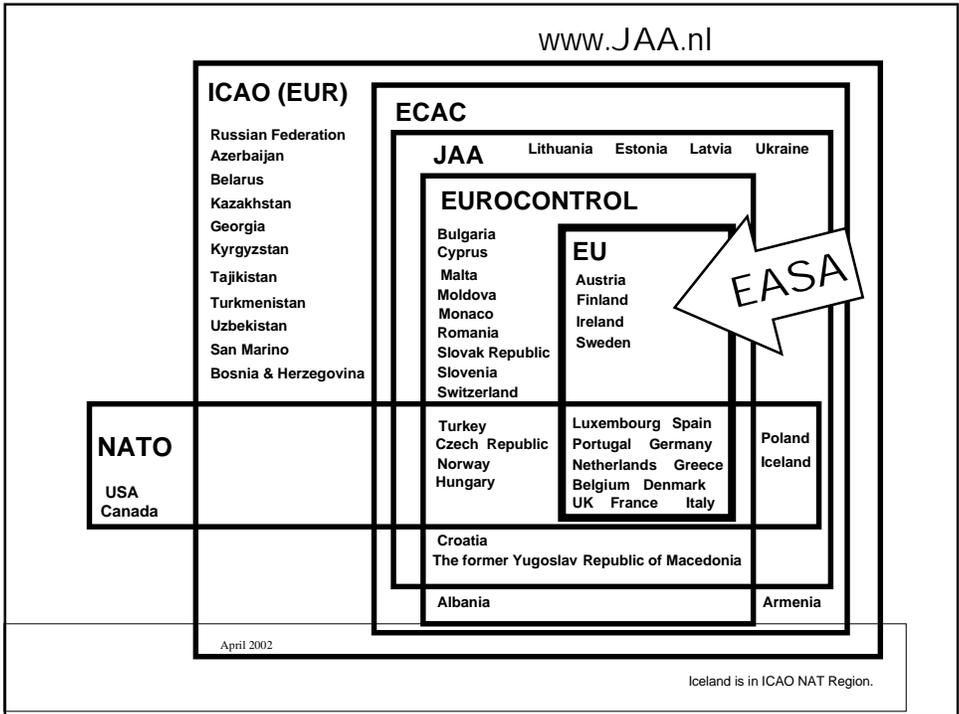


FAA National Software Conference, May 2002

International Activities - Report From Europe



FAA National Software Conference, May 2002

International Activities - Report From Europe

Contents

- DO-178B v 25.1309
- Approval of database suppliers
- Complex hardware
- Take questions.



Year 2002 FAA National Software Conference

3

DO-178B v 25.1309

- The JAA Avionics team investigating a new aircraft type had a major concern with the design of its air data system.
- Probes were of similar design and common to all aircraft dependent systems.
- Potential Common Cause failures were the **Level A** Software and complex hardware.
- Loss or Malfunction of **all** probes from a **Common Cause** would be **Catastrophic**

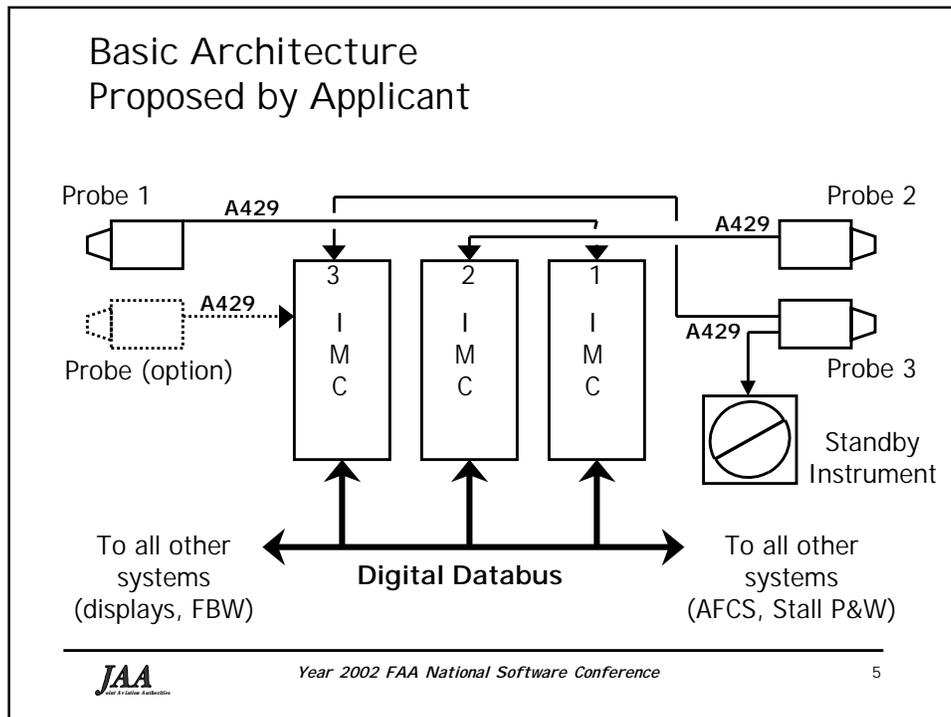


Year 2002 FAA National Software Conference

4

FAA National Software Conference, May 2002

International Activities - Report From Europe



Software Level plus "other measures" ?

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

FAA National Software Conference, May 2002

International Activities - Report From Europe

Note DO-178A
Paragraph 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".

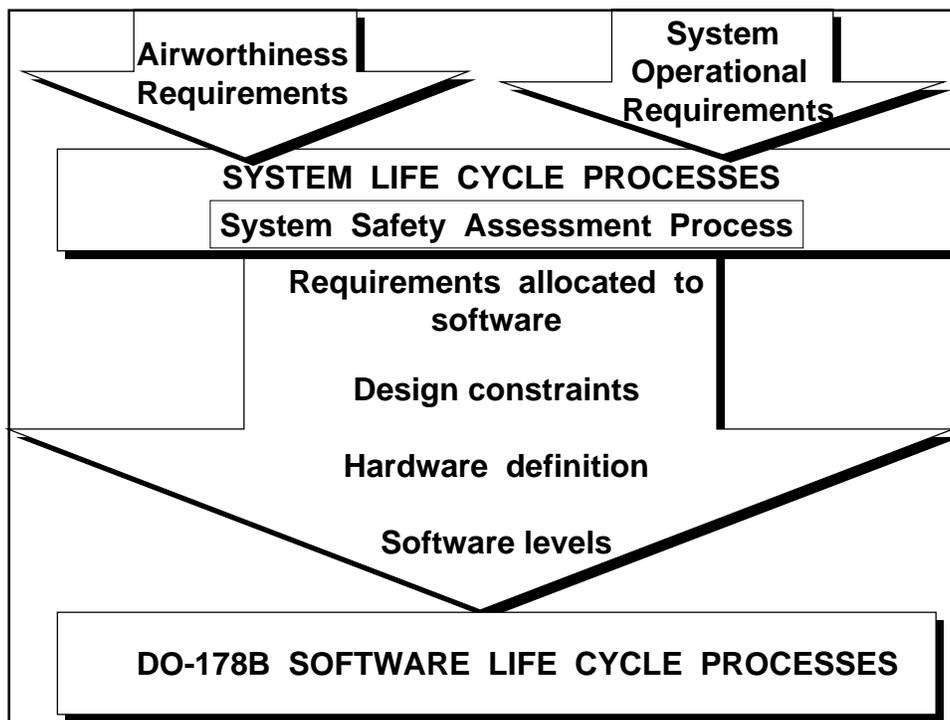
Software Levels:
a hot issue in 1990 !

- Is there a "Super Critical Level" beyond Level A ?
- Can software be developed that we would trust without additional mitigation where it could cause directly a Catastrophic Failure Condition ?

FAA National Software Conference, May 2002 International Activities - Report From Europe

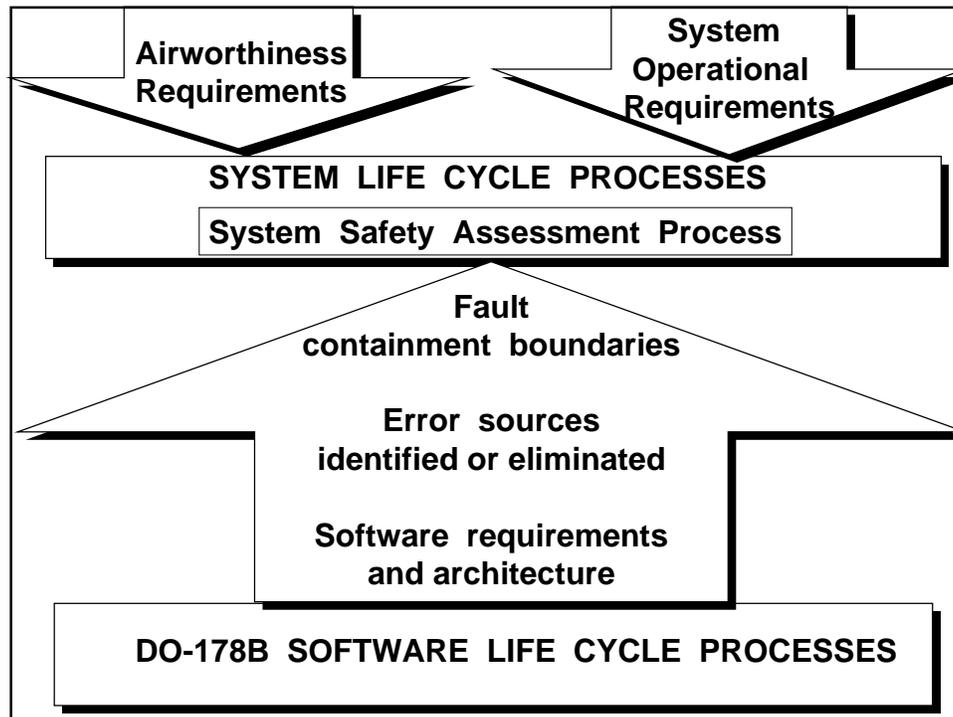
Position adopted for DO-178B

- A criticality beyond Level "A" was not defined.
- Text equivalent to the Note of paragraph 3.3 of DO-178A was not written into DO-178B.
- The interface between DO-178B and the system safety assessment process was described...



FAA National Software Conference, May 2002

International Activities - Report From Europe



The questions raised in 2001...

- Has software engineering advanced such that software developed to Level A can satisfy the fail-safe concept of the advisory material to JAR 25.1309 (both current AMJ and NPA 25F-281) without other measures as mitigation, such as dissimilarity ?
- How should compliance with JAR 25.1309 be shown considering failures where software was a common cause ?

FAA National Software Conference, May 2002

International Activities - Report From Europe

Response

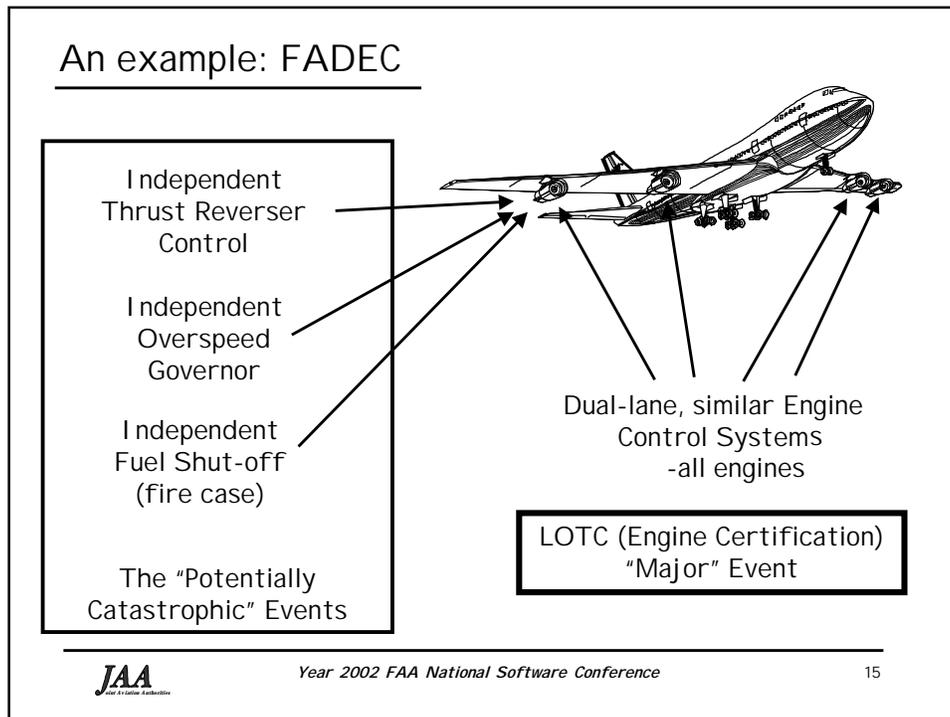
- There is a gap between requirements and current best practices for designing complex and critical systems.
- Redundant channels of similar design should be rejected, unless further mitigation is provided on how to reduce to an acceptable level the vulnerability of systems to development errors.

Dissimilarity?

- Dissimilarity is one strategy for achieving an acceptable level of safety, but it should not be a required strategy for the development of high integrity systems.
- The subject is a systems issue, not just software.

FAA National Software Conference, May 2002

International Activities - Report From Europe



- Proposed JAA Guidance
- Current JAR 25 and advisory material could be interpreted that a Level A development assurance process is acceptable as the only mitigation means against Catastrophic Failure Conditions resulting from a common cause development problem.
 - The JAA has assessed the architectures of currently certificated full-time flight critical systems and has determined that the above interpretation is generally not appropriate as it may not be sufficient to maintain the current safety level.
- At the bottom left is the JAA logo, at the bottom center is the text 'Year 2002 FAA National Software Conference', and at the bottom right is the number '16'.

FAA National Software Conference, May 2002

International Activities - Report From Europe

Reasons

- Means of compliance proposed to satisfy JAR 25.1309 requirements should include the analysis of common mode and single points of failure from any source, which includes development errors in hardware and/or software.
- This analysis is part of the system safety assessment process, and should identify the means to mitigate any Catastrophic Failure Conditions related to the system.
- This is an issue that needs to be addressed using safety engineering processes.

Other measures...

- The JAA has no wish to stipulate the exact mitigation means to be provided; however, it has been agreed that development assurance alone is generally not sufficient.
- Further acceptable means of compliance can be found in NPA 25F-281.
- The need for additional mitigation means (and also the definition of these means) should be discussed between the JAA and the applicant on a case-by-case basis.

FAA National Software Conference, May 2002

International Activities - Report From Europe

Next steps

- JAA to publish interim guidance.
- Issue presented to the JAA/FAA Systems Design and Analysis Harmonisation Working Group.
- Identified as a high priority activity.

Approval of database suppliers

FAA National Software Conference, May 2002

International Activities - Report From Europe

Database Integrity

- Studies in Europe have shown that data for navigation systems is not of acceptable quality for future high integrity and precision navigation.
- States Aeronautical Information Publications (AIP) are often inconsistent and erroneous.
- Database process needs improvement.

Improvements

- To reduce transcription errors, Europe is moving away from an AIP manually prepared by each state towards a centralised electronic AIP.
www.eurocontrol.int/aisagora
- An approval scheme is being devised by JAA for database suppliers.

FAA National Software Conference, May 2002

International Activities - Report From Europe

DO-200A/ED-76

- JAR-OPS 1.035 requires aircraft operators to apply a quality management process. For a database, the process will need to ensure that the data has an appropriate level of quality for its intended use.
- EUROCAE document ED-76 may be applied, as a means, but not the only means, of demonstrating that the processes applied to aeronautical data, intended for use in navigation or other databases, preserve a level of quality of the data commensurate with its intended use.

Complex hardware

FAA National Software Conference, May 2002

International Activities - Report From Europe

JAA adoption of DO-254/ED-80

- JAA has drafted a guidance leaflet calling attention to the EUROCAE document ED-80: *Design Assurance Guidance For Airborne Electronic Hardware*, April 2000.
 - It discusses how the document may be applied to the design of electronic hardware to provide the end user with the necessary confidence that the delivered hardware is of a standard commensurate with its intended use.
- But...

...DO-254/ED-80 has deficiencies

- The draft JAA leaflet supplements document ED-80 to provide further guidance applicable to complex digital devices such as Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs) which may be used in systems with safety implications for the aircraft.

FAA National Software Conference, May 2002

International Activities - Report From Europe

FAA AC DO 254 draft 5A



- The procedures and assurance provided by RTCA/DO-254 are recognized as appropriate techniques for the development of ASIC/PLD/FPGA devices incorporated in the design of avionics and electronic equipment.
- An applicant for TC, STC, TSO Authorization or PMA of type designs incorporating ASIC/PLD/FPGA devices which contribute to functions with failure effects assessed as Catastrophic (level A) or Severe Major/Hazardous (level B) shall utilize the procedures described in RTCA/DO-254, or equivalent procedures, to secure FAA approval.
- **DO-178 processes may be substituted for DO-254 for the devices listed above.**

FAA redefines "complex"



- designs which are considered complex according to DO-254 and which utilize a Hardware Description Language (HDL) for their specification. Designs implemented at the logic gate level, where the elements used and interconnections are explicitly controlled, are considered non-complex for the purpose of this AC.

FAA National Software Conference, May 2002

International Activities - Report From Europe

JAA clarifies "complex"

...digital devices whose logic is difficult to comprehend without the aid of analytical tools and whose compliance with its requirements cannot be demonstrated solely by testing.

The subject is Complex Hardware, but neither FAA nor JAA are comfortable with the DO-254/ED-80 usage of this fundamental term !

JAA additional considerations (1)

JAA attempts to be more consistent with DO-178B by adding criteria for:

- HDL coding standards;
- Modifiable aspects of embedded logic;
- Classification of each complex digital device within a certification plan;
- Validation of requirements; and....

FAA National Software Conference, May 2002

International Activities - Report From Europe

JAA additional considerations (2)

- Robustness testing;
- Appropriate test case selection;
- Validation and verification activities to be performed at the device level.
- Recording of verification test coverage; and
- Verification independence for Levels A and B.

What next ?

- JAA and FAA need to harmonise !
- Issues need to be reviewed with industry. ARAC process ?

FAA National Software Conference, May 2002

International Activities - Report From Europe

Questions ?

Some answers.....

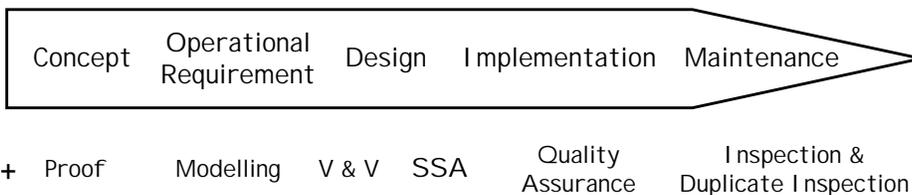
FAA National Software Conference, May 2002

International Activities - Report From Europe

Development Assurance

- You won't find in DO-178B the terms "Development Assurance" or "Design Assurance".
- They are *System* terms!

Airworthiness of a System



Robust system + Assurance = Airworthy

You can't "assure" the development, you can only assure people or bodies.

The aim is to provide confidence to satisfy all stakeholders that the system is safe.

FAA National Software Conference, May 2002

International Activities - Report From Europe

The bottom line...

- The more critical and complex the system then the more demanding is the process of development assurance.
- From experience, we know that today's development assurance processes are not perfect so don't be reluctant to ask for more. You need to be satisfied !

Is software safe?

- We have been successful in the past but the software in aircraft systems continues to increase in size and complexity so we can't relax.

“I shall stop taking the medication
because I'm not getting any worse”.

Pippa Moore

FAA National Software Conference, May 2002

International Activities - Report From Europe



Cautionary Note



- Any views expressed in this presentation, or references made to publications, should not be interpreted as being the current policies of any national authority. Readers are advised to consult the latest publications of national authorities for information on applicable policies, requirements and guidance material.
- Enquiries relating to the certification of aircraft systems, or to operational approvals, should be made to the applicant's own national authority.

JAA
Joint Aviation Authorities

Year 2002 FAA National Software Conference

39

