

# 2003 FAA National Software Conference

## Is Level A Enough?



---

Is Level A Enough ?

Jozef B.J. van Baal

Is Level A Enough ?



---

**Objective:** to provide some background to discussions around:

*25.1309, requirements for preventing single catastrophic failures, criticality, Level A, common cause failures, development assurance, complexity, system architecture, .....*

19 September 2003      Is Level A Enough ?      2

# 2003 FAA National Software Conference

## Is Level A Enough?

### Overview



- Direct Trigger for Recent Discussions (2)
- Basic Architecture Proposed by Applicant (2)
- Technical Advice from JAA Avionics CSP (6)
- Results of Meeting 13 November 2001 (4)
- Some Additional Remarks (2)
- An Innocent Question (1)

19 September 2003

Is Level A Enough ?

3

### Direct Trigger for Current Discussion



- Airdata system proposed by one applicant
- 4 Identical integrated probes
- These probes are the only source on entire aircraft - with the exception of the power plant - Of:
  - Pressure Altitude
  - Airspeed
  - Angle of Attack
- JAA Team (Avionics Panel) expressed Major Concern: (see next slide)

19 September 2003

Is Level A Enough ?

4

# 2003 FAA National Software Conference

## Is Level A Enough?

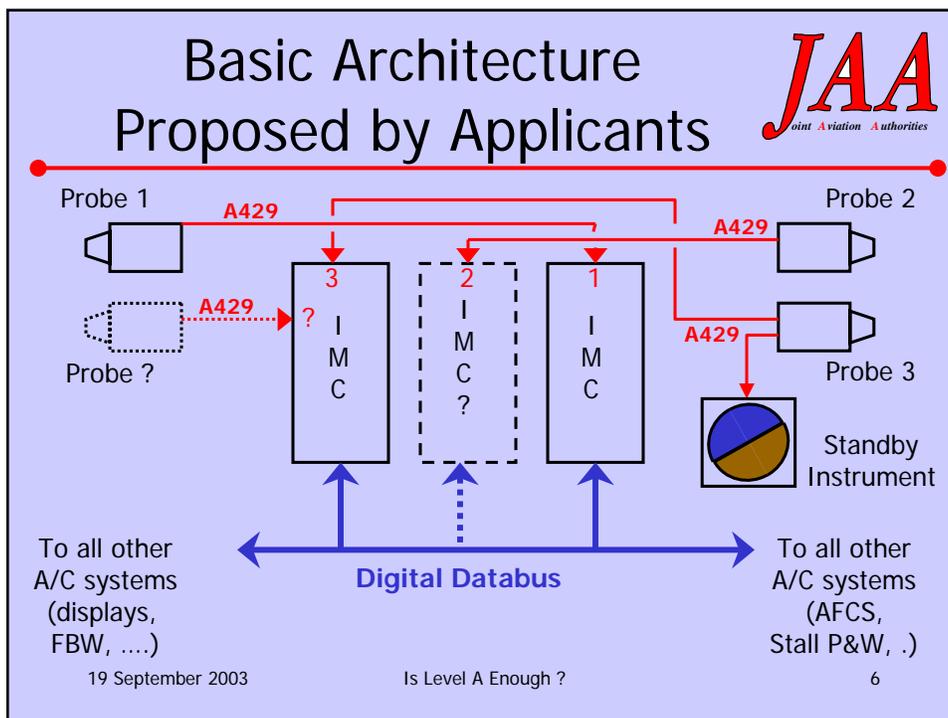
**JAA**  
Joint Aviation Authorities

### Why a "Major Concern" ?

---

- All airdata to primary, stand-by, FBW, stall warning and protection
- Loss or Malfunction of **all** probes **at same time** is **Catastrophic**
- Loss or Malfunction of all probes can be by **Common Cause** Failure
- Probes are considered a **Complex** Design
- Only protection offered against Common Cause is **Level A** for the Software

19 September 2003                      Is Level A Enough ?                      5



# 2003 FAA National Software Conference

## Is Level A Enough?

### Technical Advice from CSP (1/3)



#### **Question** put to Avionics CSP:

Advice is needed on how compliance with JAR 25.1309 requirements has to be shown when considering common mode software failures. The point is whether software, developed according to DO-178B, Level A is adequate or not to satisfy the fail-safe concept described in the advisory material to JAR 25.1309 (both current AMJ and NPA 25F-281) or if further mitigation means, such as dissimilarity, are required.

19 September 2003

Is Level A Enough ?

7

### Technical Advice from CSP (2/3)



#### **Technical Advice** provided by CSP:

(22 August 2001)

We believe that, while dissimilarity is one strategy for achieving an acceptable level of safety, it should not be a required strategy for the development of high integrity systems. We consider this position to be in line with the current requirements (25.1301, 25.1309, etc.), Industry Standards (ARP4754, DO-178B, ED-80, etc.) and the NPA on 25.1309 (NPA 25F-281).

19 September 2003

Is Level A Enough ?

8

# 2003 FAA National Software Conference

## Is Level A Enough?

### Key Words ... (1)



#### **Technical Advice** provided by CSP:

(22 August 2001)

We believe that, while dissimilarity is **one** strategy for achieving an acceptable level of safety, it should **not be a required** strategy for the development of high integrity systems. We consider this position to be in line with the current requirements (25.1301, 25.1309, etc.), Industry Standards (ARP4754, DO-178B, ED-80, etc.) and the NPA on 25.1309 (NPA 25F-281).

19 September 2003

Is Level A Enough ?

9

### Technical Advice from CSP (3/3)



#### **Explanation** provided by CSP:

The vulnerability to failures in similar components of the separate channels of an airdata system must be demonstrated to be reduced to an acceptable level. Dissimilarity, either at the system level or at the component level, is an acceptable mitigation strategy but should not be a required strategy. In the specific case of an airdata system, special attention should be on common causes for failures in both the primary and the stand-by system. It should also be considered that loss of, or incorrect, airdata, will effect other systems in addition to the airdata display to the crew.

19 September 2003

Is Level A Enough ?

10

# 2003 FAA National Software Conference

## Is Level A Enough?

### Key Words ... (2)



#### **Explanation** provided by CSP:

The **vulnerability** to failures in similar components of the separate channels of an airdata system must be demonstrated to be **reduced to an acceptable level**. **Dissimilarity**, either at the system level or at the component level, is **an acceptable** mitigation strategy but should not be a required strategy. In the specific case of an airdata system, **special attention** should be on common causes for failures in both the **primary and the stand-by** system. It should also be considered that loss of, or incorrect, airdata, will effect **other systems** in addition to the airdata display to the crew.

19 September 2003

Is Level A Enough ?

11

### LASCC Statement



#### **Agreement** by LASCC at meeting # 64:

The LASCC endorsed the advice from the Avionics CSP and agrees that Level A software, without dissimilarity, can be used for compliance with JAR 25.1309 in respect of satisfying there is no single common mode catastrophic failure.

19 September 2003

Is Level A Enough ?

12

# 2003 FAA National Software Conference

## Is Level A Enough?

13 November 2001 (1/4)



- Different interpretations of the CSP advice
- Meeting held at Central JAA, JAA specialists only
- Advice on approach:
  - Publish interim policy ASAP - see next 3 slides
  - Task an existing or new working group to determine the most suitable way to include this in the existing regulation
- A draft "TGL" was produced after the meeting
- The subject however proved far too controversial, so TGL was never published
- Possible working groups: SAE S-18 and EUROCAE WG 63; SD&A HWG; others?

19 September 2003

Is Level A Enough ?

13

13 November 2001 (2/4)



The current JAR 25 and advisory material could be interpreted such that a Level A development 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 have determined that the above interpretation is not appropriate as it is not sufficient to maintain the current safety level.

19 September 2003

Is Level A Enough ?

14

# 2003 FAA National Software Conference

## Is Level A Enough?

13 November 2001 (3/4)



The reasons are as follows:

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.

19 September 2003

Is Level A Enough ?

15

13 November 2001 (4/4)



The JAA has no wish to stipulate the exact mitigation means to be provided; however, they have agreed that development assurance alone is not sufficient. Further acceptable means of compliance can be found in NPA 25F-281.

19 September 2003

Is Level A Enough ?

16

# 2003 FAA National Software Conference

## Is Level A Enough?

### New Rulemaking ?



- We can not change our interpretation of the rules/advisory material/Industry documents without formal process
- Formal process should include Industry contribution and consultation
- Service Experience: There is not a significant number of accidents/incidents contributed to development problems with software or complex hardware
- But we want to keep it this way!
- So ??

19 September 2003

Is Level A Enough ?

17

### Similar Previous Designs Approved ?



- Engines
- FADEC
- Tail/Stabilizer
- IRS/ADC ← flawed example
- Airbus FBW
- Boeing FBW
- Modular units other generations

19 September 2003

Is Level A Enough ?

18

# 2003 FAA National Software Conference

## Is Level A Enough?

An Innocent Question:



---

Should we be guided by what is currently  
in 25.1309, ARP-4754, DO-178B, etc.;

Or should we be guided by our own  
engineering judgment, experience, even  
conscience maybe ?

19 September 2003

Is Level A Enough ?

19