

2003 FAA National Software Conference

Software as a Single-Point-of-Failure

Software as Single Point-of-Failure *Brainstorm Session*

Barbara Lingberg, Jozef van Baal, Mike DeWalt
September 19, 2003

Agenda

- Session Overview
- Background
- Some Questions to Consider
- Open Discussion
- Wrap Up

2003 FAA National Software Conference

Software as a Single-Point-of-Failure

Session Overview

- Session Format
- Goals
- Expected Output



Background

- Basic Issues
- History
- Regulations and Guidance
 - *FAA, JAA*



2003 FAA National Software Conference

Software as a Single-Point-of-Failure

Some Questions to Consider

- What is our experience with single software failures?
- Do we have current systems with potential failures and, if so, what is their history?
- What are similarities or differences between other aircraft systems and what is our experience with their failures?
- What makes software unique from other systems or are the same standards already applied to other systems?



More Questions ...

- Is Level A assurance the same as “fail-safe”?
- Is Level A enough?
- If Level A is not sufficient, what criteria is used or should be used to make this determination?
- What types of solutions could be used to mitigate single software design faults?
- Are some solutions “better” than others?
- How do we determine what is alternately acceptable?



2003 FAA National Software Conference

Software as a Single-Point-of-Failure

... and More

- Where does engineering judgment fit in, or does it?
- What are issues with current guidance, e.g. uniform application, interpretation?
- What do we need to resolve these issues?



Open Discussion



2003 FAA National Software Conference

Software as a Single-Point-of-Failure

Wrap Up

- Summary of discussion
- Next steps



Thank you for participating!!

