

FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

Implementation of RTCA DO-278/ED-109

Guidelines for CNS/ATM System Software
Integrity Assurance

Ron Stroup
Office of Information Services, AIO-200
Software Safety and Certification Lead
PH 202 493-4390
Ronald.L.Stroup@faa.gov
National Software Conference
Dallas, Texas
15 May 2002

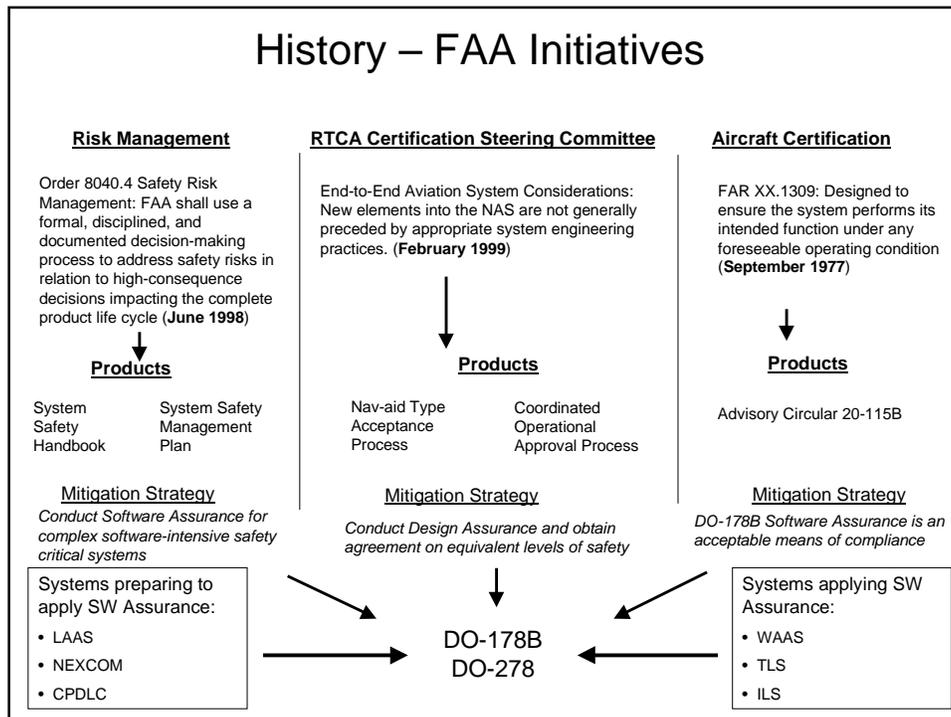
Agenda

- History
- Current status
- Common ground
- Community concerns
- Potential Benefits
- Proposed implementation strategy
- Summary

Premise – Software Assurance is a technically efficient and cost effective means to ensure complex software-intensive systems function as designed.

FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109



- Current Status of DO-278**
- Developed over past 3 years by RTCA/EUROCAE (SC-190/WG-52) Committee
 - Plenary approved April 2001
 - RTCA balloting process completed in August 2001
 - Comment resolution and editing
 - RTCA PMC approved in March 2002

FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

Common Ground

- Systems are becoming more complex?
- Testing alone is not sufficient nor efficient in complex systems?
- Finding errors late in the development and life cycle phases is:
 - Costly
 - Schedule prohibitive
 - Leads to compromise and trade-offs
 - Leads to acceptance of unnecessary risk
- Need for harmonization (airborne, CNS/ATM, Europe)
- System safety assessment is necessary to properly evaluate software-intensive complex systems
- Software assurance is different from software development

Community Concerns

- Too Costly
- Artificially High Assurance Levels
- Usability
 - 3 document into one?
- Constraining
 - “quasi-regulatory”
- RTCA’s Certification Processes
 - DO-249, DO-264, DO-278

FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

Benefit – New Guidance

- DO-278 is consistent with the last 20 years of software engineering best practices
- Exceptions are:
 - Modified Condition/Decision Coverage (MC/DC),
 - *Commercial-off-the-shelf (COTS),
 - *Adaptation Data, and
 - **Tool qualification

*DO-278 is the first document to provide specific information on COTS and Adaptation Data

**DO-178B provides specific information on tool qualification

Benefit – Graduated levels of Assurance

C,S/ATM SWAL Assignment Matrix

		LIKELIHOOD OF OCCURRENCE				
		No Safety Effect	Minor	Major	Hazardous	Catastrophic
SEVERITY	Probable (Note: 2)	AL 6/E	AL 5/D	AL 3/C	AL 2/B	AL 1/A
	Remote	AL 6	AL 5	AL 4	AL 3	AL 2
	Extremely Remote	AL 6	AL 5	AL 4	AL 4	AL 3
	Extremely Improbable	AL 6	AL 6	AL 5	AL 5	AL 4

•Software assurance is often used to control risk by mitigating anomalous software behavior.

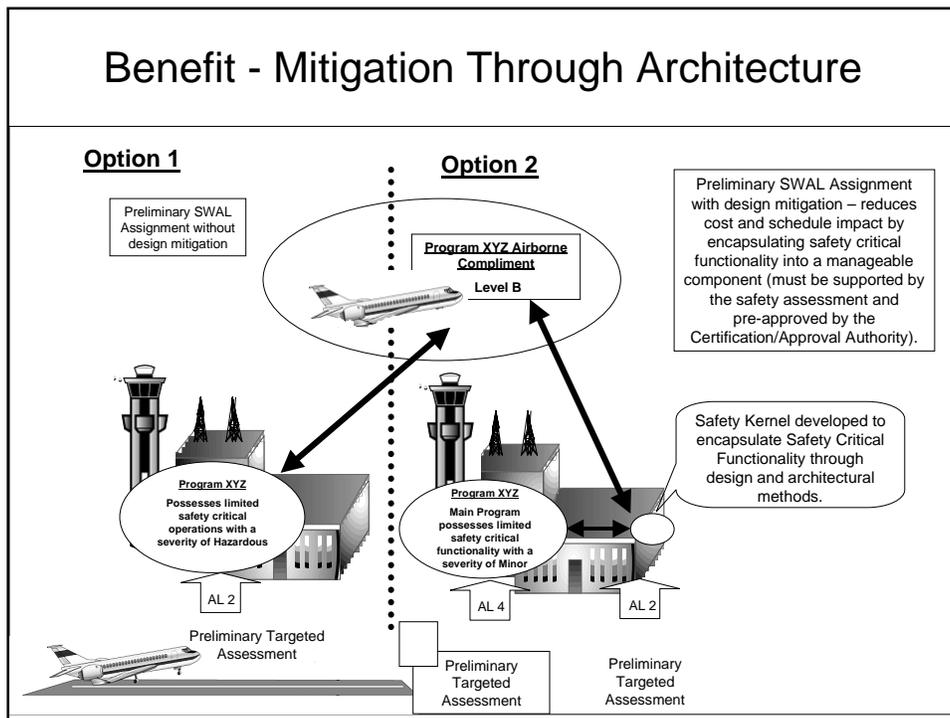
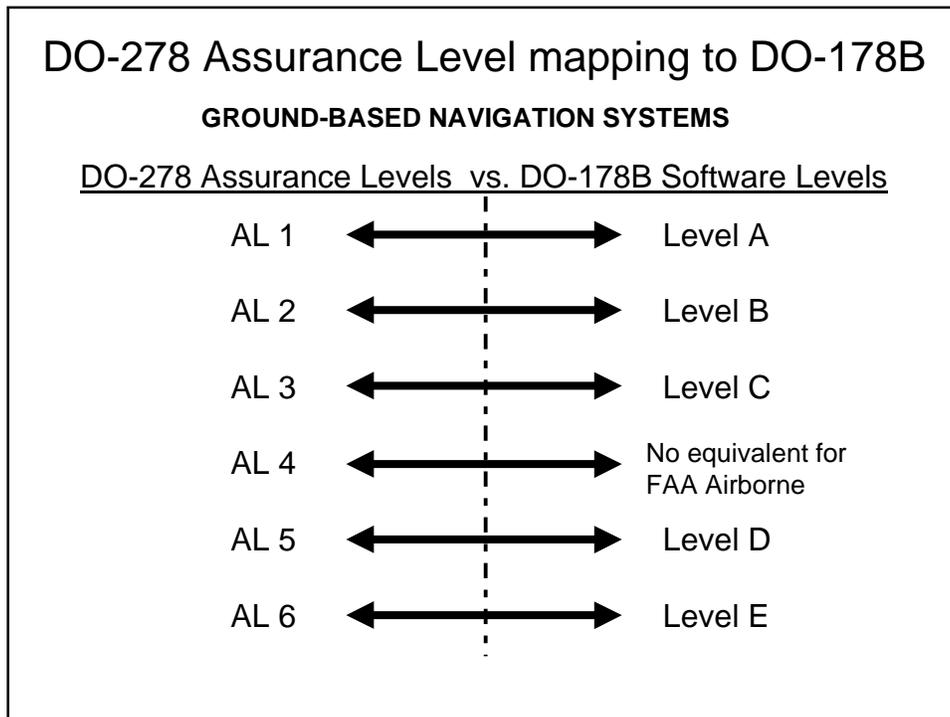
•Software assurance provides the confidence and artifacts to ensure the system safety requirements implemented in software function as designed.

Note:

1. Minimally recommended SW assurance levels based on system risk, any deviation must be pre-approved by the appropriate approval/certification authority.
2. DO-278 equates to DO-178B for SW whose functionality has a direct impact on aircraft operations (e.g., ILS, WAAS).

FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

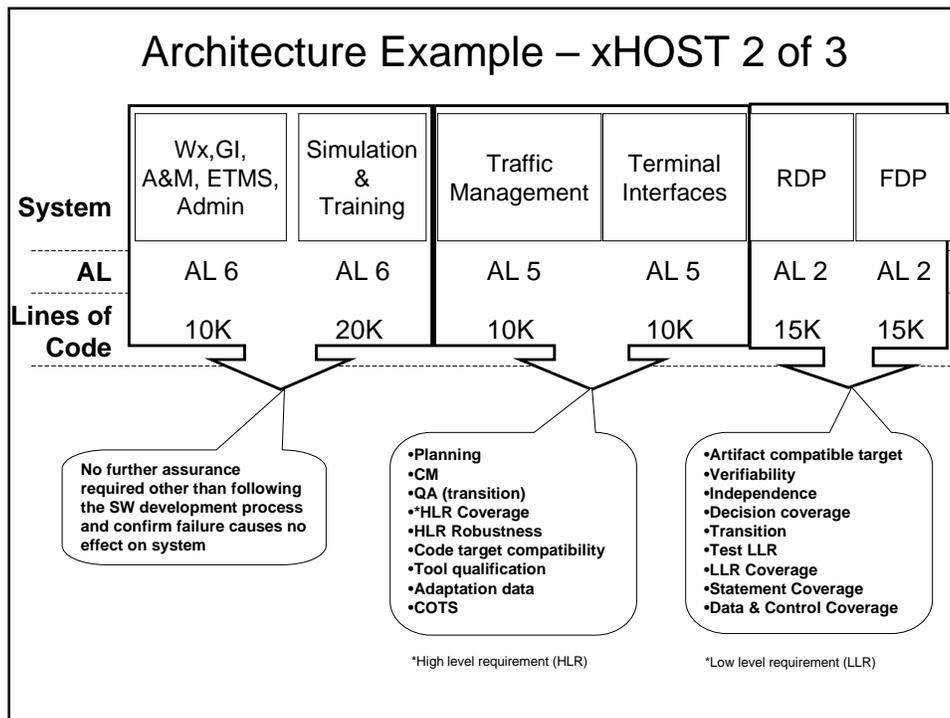


FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

Architecture Example – xHOST 1 of 3

System	Wx,GI, A&M, ETMS, Admin	Simulation & Training	Traffic Management	Terminal Interfaces	RDP	FDP
Evaluation of risk	Extremely Improbable	Remote	Remote	Extremely Improbable	Probable	Remote
	Minor	No Safety Effect	Minor	Hazardous	Hazardous	Catastrophic
Assurance Level	AL 6	AL 6	AL 5	AL 5	AL 2	AL 2
Lines of Code	10K	20K	10K	10K	15K	15K



FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

Architecture Example – xHOST 3 of 3

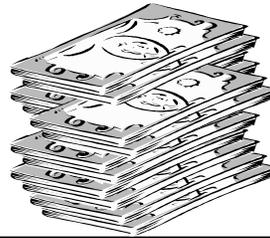
- Preliminary AL assignment with design mitigation

- 30K Lines of Code assessed as AL 2
- 20K Lines of Code assessed as AL 5
- 30K Lines of Code assessed as AL 6



- Preliminary AL without design mitigation

- 80K Lines of Code assessed as AL 2



Proposed Implementation Strategy

- Foundation
 - Acknowledge DO-278 as an acceptable means of compliance.
 - Implement as a tool for Program Office (Not to be imposed on contractor)
 - Update FAA-STD-026
 - Identify wording for RFP's and SOW
- New Systems
 - Select a date for all systems that have not had baseline established
- Legacy Systems
 - Grand-fathered pending review based on NAS Mission criticality
 - Perform Safety Analysis
 - Perform Gap Analysis (DO-278 Objectives)
 - Plan for upgrade as needed, based on program's existing schedule

Propose: Policy Memo, Job-aids and detailed Legacy Evaluation Plan

FAA National Software Conference, May 2002

Implementation of RTCA DO-278/ED-109

Summary

- Support end-to-end system safety of NAS
- Ensure CNS/ATM systems are built to consistent and documented levels of assurance
- Improved management of system SW cost throughout product lifecycle
- Consistency with the FAA's Best Practices (iCMM)