

Implementation of RTCA DO-XXX/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

13 November 2001

Brief:ARA-1/2, ATS-2, AIO-1/2, AND-1/2, AUA-1/200, AOS-1

Agenda

- History
- Current status
- Community concerns
- Proposed implementation strategy
- Potential Benefits – What does this mean to you?
- Benefits Realization – What can you do for us?
- Summary

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

History – FAA Initiatives

Risk Management

Order 8040.4 Safety Risk Management: FAA shall use a formal, disciplined, and documented decision-making process to address safety risks in relation to high-consequence decisions impacting the complete product life cycle (**June 1998**)

Products

System Safety Handbook	System Safety Management Plan
------------------------	-------------------------------

Mitigation Strategy

Conduct Software Assurance for complex software-intensive safety critical systems

Systems preparing to apply SW Assurance:

- LAAS
- NEXCOM
- CPDLC

RTCA Certification Steering Committee

End-to-End Aviation System Considerations: New elements into the NAS are not generally preceded by appropriate system engineering practices. (**February 1999**)

Products

Nav-aid Type Acceptance Process	Coordinated Operational Approval Process
---------------------------------	--

Mitigation Strategy

Conduct Design Assurance and obtain agreement on equivalent levels of safety

Aircraft Certification

FAR XX.1309: Designed to ensure the system performs its intended function under any foreseeable operating condition (**September 1977**)

Products

Advisory Circular 20-115B

Mitigation Strategy

DO-178B Software Assurance is an acceptable means of compliance

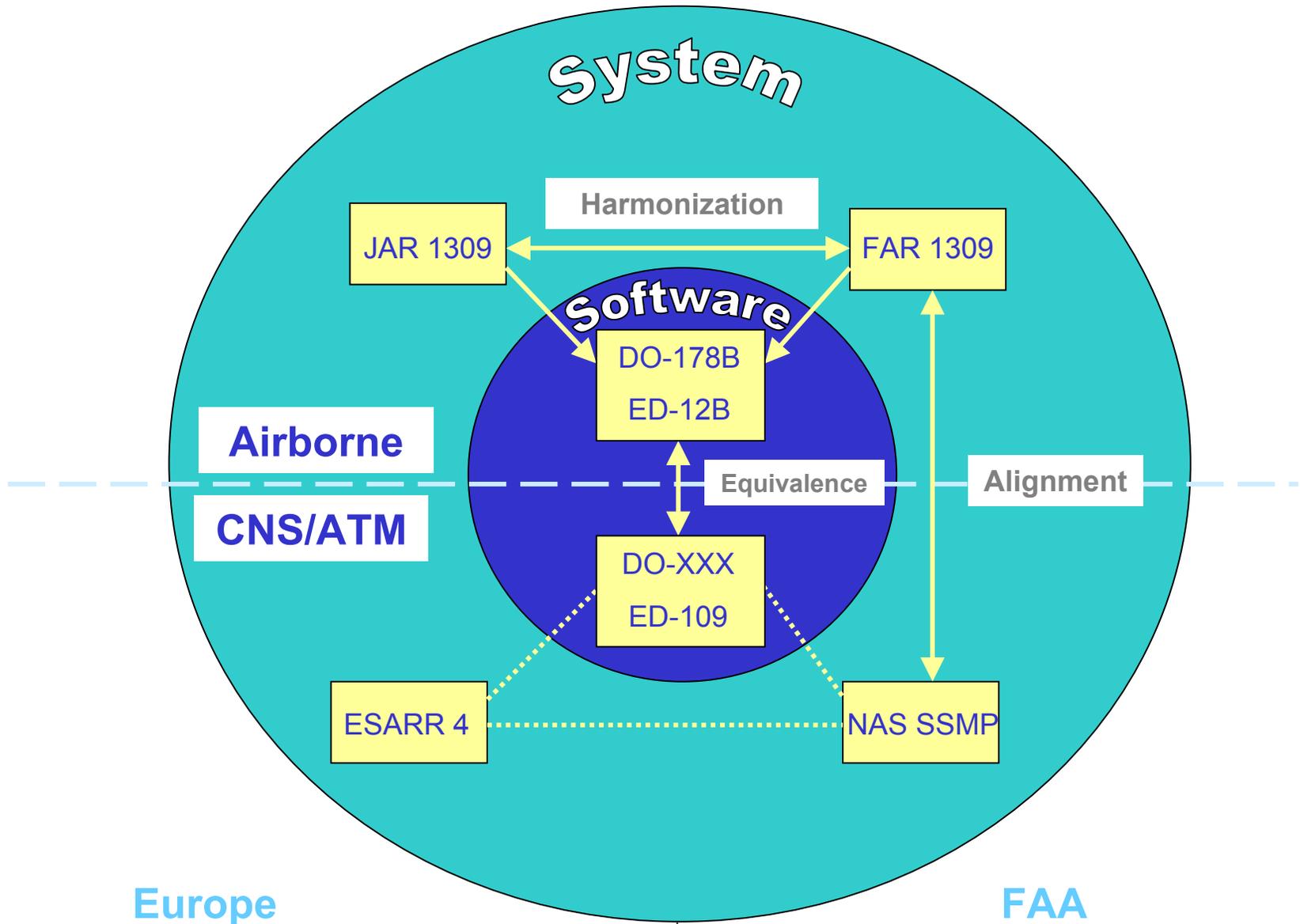
Systems applying SW Assurance:

- WAAS
- TLS
- ILS

DO-178B
DO-XXX



History – International Harmonization



Current Status of DO-XXX

- 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 approval expected in January 2002

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-XXX

Benefit - Business Case

*Data provided by:

13 Organizations (Commercial and Government)
(Boeing, Hughes, IBM, Motorola, NASA, and Raytheon)

• **Implementation**

- Achievable in 2 to 5 years
- Initial investment of 20% to 40% of software development costs
 - Modification of work instructions.
 - Decision path coverage
 - Qualification of tools
 - Learning curve of supplier and FAA
 - Compliance threshold

• **Benefits** (follow-on projects)

- \$ of SW development reduced 35%
- \$ of SW rework reduced 30%
- On-time delivery of software increased by 40%
- Decreased SW development cycle time by 30%
- Post release SW defects reduced by 15%

Benefit – New Guidance

- DO-XXX 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-XXX 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

CNS/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.

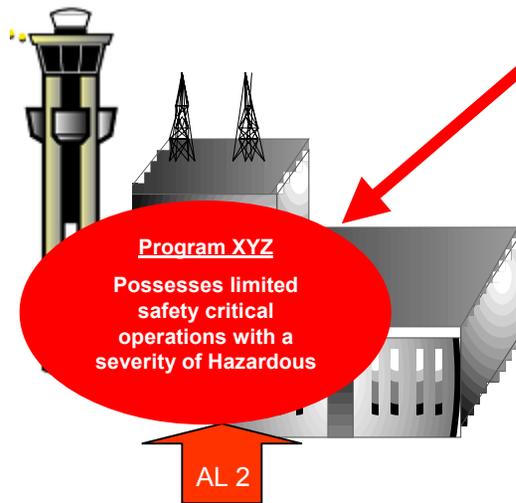
Note:

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

Benefit - Mitigation Through Architecture

Option 1

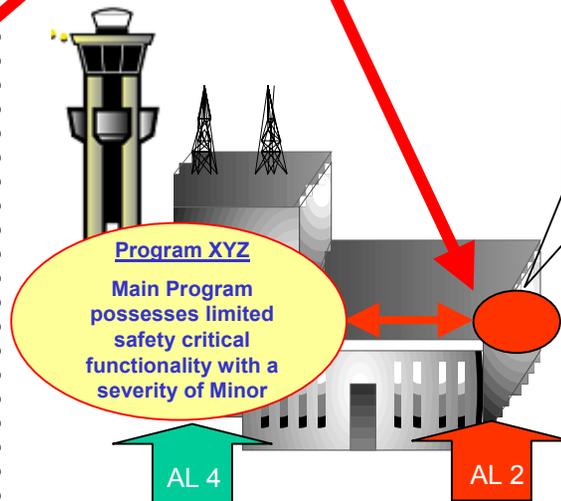
Preliminary SWAL Assignment without design mitigation



Option 2

Program XYZ Airborne Compliment

Level B



Preliminary SWAL Assignment with design mitigation – reduces cost and schedule impact by encapsulating safety critical functionality into a manageable component (must be supported by the safety assessment and pre-approved by the Certification/Approval Authority).

Safety Kernel developed to encapsulate Safety Critical Functionality through design and architectural methods.

Preliminary Targeted Assessment

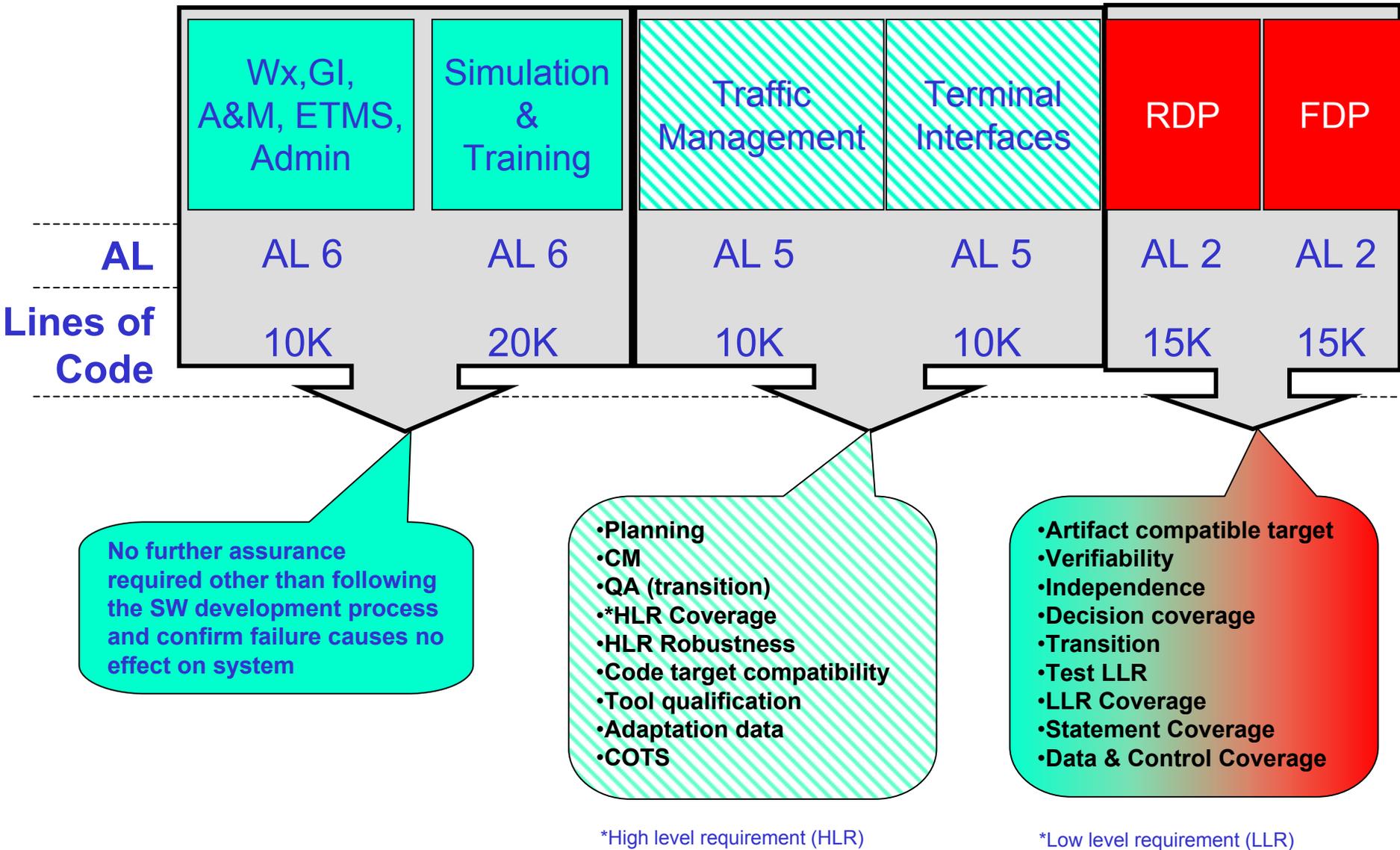
Preliminary Targeted Assessment

Architecture Example – xHOST 1 of 3



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

Architecture Example – xHOST 2 of 3



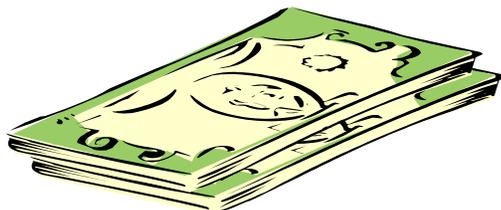
Architecture Example – xHOST 3 of 3

- 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-XXX 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-XXX Objectives)
 - Plan for upgrade as needed, based on program's existing schedule

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

Benefit Realization – How Can you help?

- Champion assurance for your organization
 - Host information meeting with sw stakeholders
- Provide a point of contact for implementation team
 - Policy
 - Job aids
 - Legacy Evaluation Plan

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)

Back-up Slides

Development vs. Assurance

- Development

- Ensures and orderly and repeatable software development process

- Planning
- Requirements
- Design
- Code
- Test

- Assurance

- Provides a means to establish that certain attributes are present in a development.

- Correct
- Reliable
- Verifiable
- Maintainable

Typically one would apply a software development standard and then use a software assurance standard to make sure all the needed visibility and characteristics have been captured by the specific instantiation of the chosen software development standard.

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

Safety Risk Management

Perform safety analyses

Identify hazards

Assess risks

Identify mitigation strategy

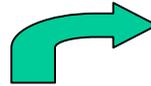
Recommend safety requirements
(Software assurance)

Verify requirements

Risk Index

Likelihood

Probable	<p>Qualitative: Anticipated to occur one or more times during the entire system/operational life of an item.</p> <p>Quantitative: Probability of occurrence per operational hour is greater than 1×10^{-5}</p>
Remote	<p>Qualitative: Unlikely to occur to each item during its total life. May occur several times during the life on an entire system or fleet.</p> <p>Quantitative: Probability of occurrence per operational hour is greater than 1×10^{-7}</p>
Extremely Remote	<p>Qualitative: Not anticipated to occur to each item during its entire life. May occur few times during the life on an entire system or fleet.</p> <p>Quantitative: Probability of occurrence per operational hour is greater than 1×10^{-9}</p>
Extremely Improbable	<p>Qualitative: So unlikely that is not expected to occur during the entire life of an entire system or fleet.</p> <p>Quantitative: Probability of occurrence per operational hour is greater than 1×10^{-9}</p>



Severity Likelihood	No Effect	Minor	Major	Hazardous	Catastrophic
Probable	Green	Yellow	Red	Red	Red
Remote	Green	Green	Yellow	Red	Red
Extremely Remote	Green	Green	Green	Yellow	Red
Extremely Improbable	Green	Green	Green	Green	Yellow

Diagonal labels in the matrix:
 - Low Risk: Green cells (Major/Minor, Major/Remote, Major/Extremely Remote, Major/Extremely Improbable)
 - Medium Risk: Yellow cells (Major/Probable, Major/Remote, Major/Extremely Remote, Major/Extremely Improbable)
 - High Risk: Red cells (Major/Probable, Major/Remote, Major/Extremely Remote, Major/Extremely Improbable)



Consequences

	Technical	Schedule	Cost
Catastrophic	Unacceptable – results in fatalities and/or system loss	No known way to meet program milestones	Development or acquisition costs increase > 10%
Hazardous	Large reduction in safety margin or functional capability	Program critical path impact with workaround available	Development or acquisition costs increase .GT. 5% & .LTEQ. 10 %
Major	Significant reduction in safety margin or functional capability	Minor schedule slip, will miss need date without workaround	Development or acquisition costs increase .GT. 1% & .LTEQ. 5%
Minor	Slight reduction in safety margin or functional capability	Additional tasks required, able to meet key milestones	Development or acquisition costs increase .LTEQ. 1%
No Effect	No effect on safety	Minimal impact	Minimal impact

Current NAS Architecture

Ground

Airborne

Equipment

Human

Equipment

Equipment

Human

Equipment

Surveillance Radar

Data-Link

Traffic Management

Communications

Navigation

Equipment

Equipment

Equipment

Human

Equipment

Future NAS Architecture

Ground

Airborne

Equipment

Human

Equipment

Equipment

Human

Equipment

Weather Radar

Surveillance Radar

Traffic Management

Equipment

Equipment

Equipment

Equipment

Navigation interfaced to autopilot/autoland

Implementation

Process Mission Need Investment Analysis Solution Implementation In-Service Management

Analyses OSA CSA PHA SSHA SHA O&SHA HHA HTRR

Functional requirements Performance requirements
Operational requirements Safety requirements
Security requirements

FAA MNS IAR RFP SOW Operation & Maintenance

Contractor Development Maintenance

Oversight

Safety Analyses

- OSA
- CSA
- PHA
- SSHA

Software Development Standards

- 12207
- 498
- 2167

Desk Review

- Artifacts
- Interviews

Software Development Process

Artifacts

Combination

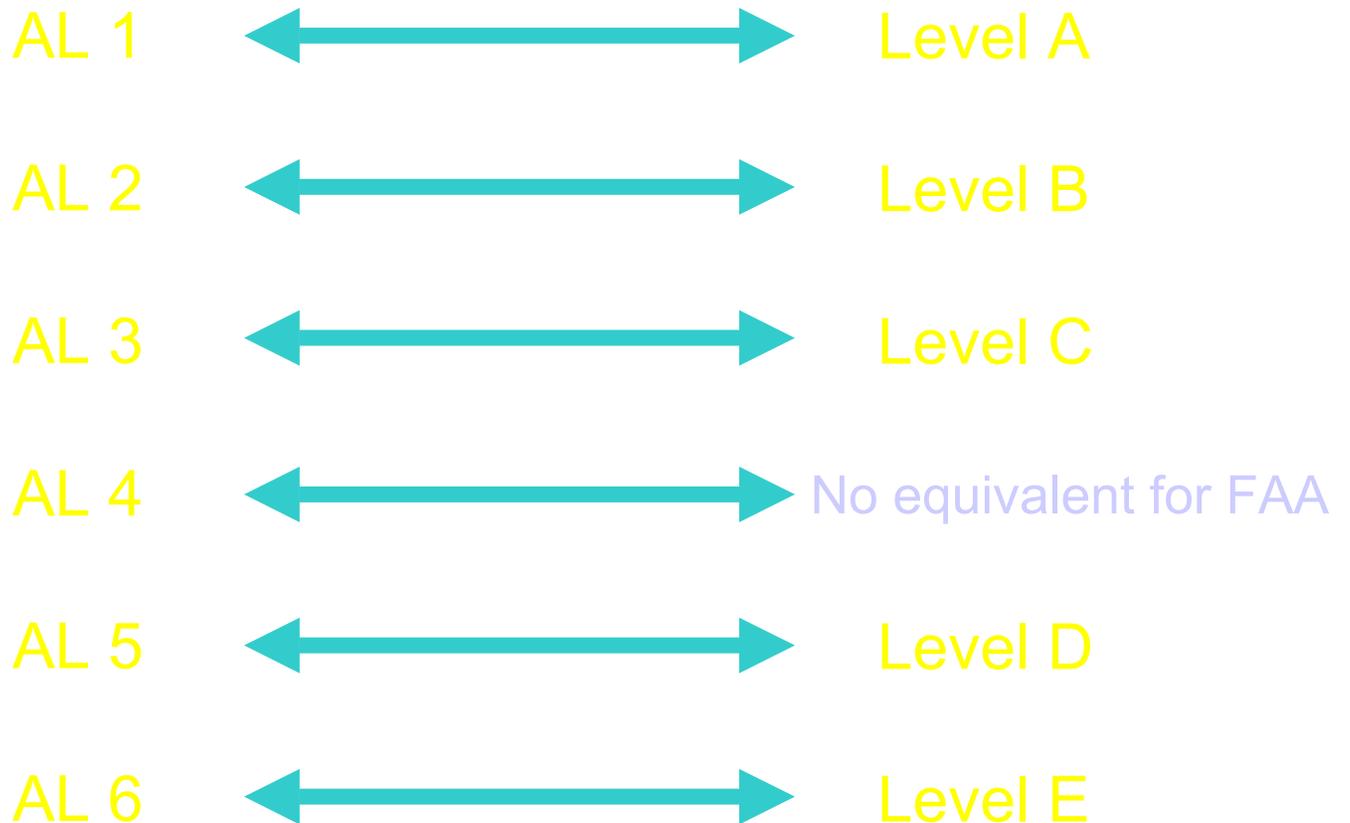
Software Development Assurance

In-site Review

- Artifacts
- Interview
- Witness

DO-XXX Assurance Level mapping to DO-178B

DO-XXX Assurance Levels vs. DO-178B Software Levels



Architecture Example - xHOST

