

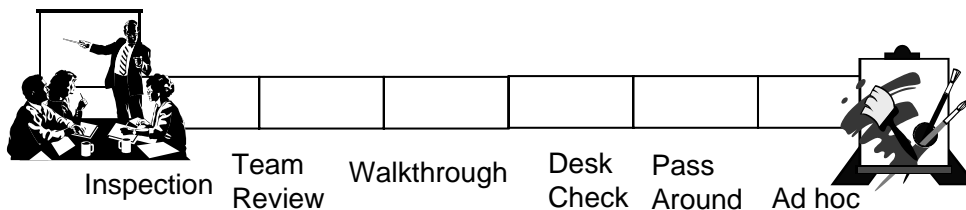


Reviews and Inspections

Systems Certification and Integrity
Directorate of Aviation Engineering
Directorate General Technical Airworthiness



Reviews and Inspections



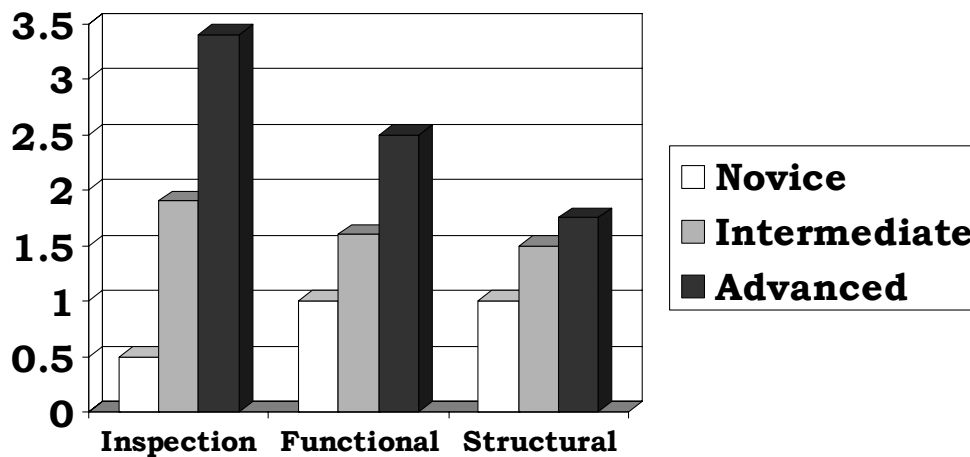
- Remove up to 95% of introduced errors (if done well).
- Effort up-front
 - cheaper to correct
 - correct errors at the current stage of the lifecycle
- Effectiveness varies with approach
- Check at 300 words per hour!
- **Techniques:** Peer Reviews, Team Reviews, Code Walkthroughs, Fagan Inspections





Effectiveness of Reviews vs. Testing

Number of Faults Detected per Hour



Inspections can detect more faults per hour than test, but only if the reviewer is suitably skilled.



What to review?

- Every element of the design
 - System Requirements, Software Requirements, Software Design, Software Architecture, Source Code, Object Code, Hardware.
 - Against higher and lower levels
 - For compliance, compatibility and traceability.
 - Against “goodness” criteria
 - Consistent, Accurate, Verifiable, Algorithms Accurate, Conformance to Standards.
 - Against the target hardware
 - For compatibility.
- All Verification Evidence
 - Test Evidence: for satisfaction of test objectives.
 - Review Evidence: for satisfaction of verification objectives.





What to review for?

- **Traceability.** Does each higher level element trace to at least one lower level element and does each lower level element trace to at least one higher level element?
- **Compliance.** Do the requirements/design/code satisfy the required system functional, performance and safety requirements?
- **Accuracy/Consistency.** Are the requirements/design elements accurate or is there ambiguity? Is there any conflict between requirements or design elements?
- **Conformance to Standards.** Has the defined requirements or design language been used? Have dangerous design and coding practices been avoided? Does the code comply with the approved language subset?
- **Compatible.** Are there any conflicts between the software requirements or design and the target hardware (e.g. 16-bit vs. 32-bit).
- **Verifiable.** Is it possible to prove through test that a requirement has been satisfied or design element correctly implemented?



Compliance vs. Traceability

- Software Requirement
 - The software shall not activate spoilers unless the aircraft is on the ground.
- Software Design

```
if (Wow & spoilers selected & wheels rolling)
    activate spoilers
else
    don't activate spoilers
```
- Does the design trace to the requirement?
 - Yes, this is the design element that implements that requirement.
- Is the design element compliant with the requirement?
 - No: where did the “wheels rolling” condition come from?
- Compliance and traceability are related, but not the same.



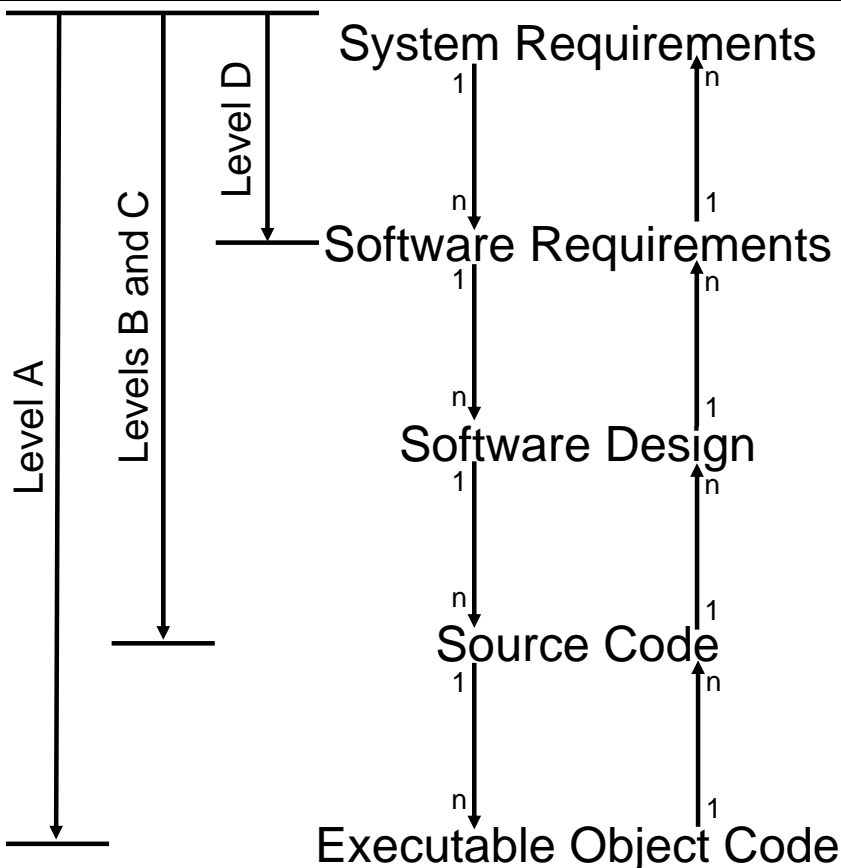


Verifiability Principles

- Criteria for verifiability:
 - Test Possible
 - Analysis Possible
 - Inspection Possible
- A successful test/analysis/inspection is sufficient evidence that a requirement or design is verifiable.
 - But, should check for verifiability at time of requirements or design development. Discovery during the verification phase may lead to a redesign.



Traceability



Note: 1:n is the minimum requirement, m:n is also acceptable.

Objective: Prove that all functions allocated to software have been implemented and that the software only implements allocated functions.

Can either perform a complete trace, or establish language subset for which traceability could be established.





Traceability (cont)

- Derived requirements are an exception to the traceability objectives.
- In DO-178B terms, derived requirements are those that are necessary, but cannot be traced to a parent requirement.
 - Generally only arise in aspects of the software necessary to make it work (e.g. memory management, scheduling, etc).
 - Derived requirements are functionality introduced by the software development process: care must be taken to assure that they are compatible with system objectives.
- Instead of establishing traceability, must demonstrate that:
 - derived requirements are clearly identified as derived, and
 - derived requirements are passed to the system safety program for assessment.
- Other objectives (accuracy, compatibility, etc) must still be met.



Evidence of Reviews

- The certifying authority will look to the evidence from reviews and inspections to verify whether software assurance objectives have been satisfied.
- The following is a pretty common review sheet, what does it tell the certifying authority?

<u>Review Sheet</u>	
Item Under Review: Module X	Version: 1.1.12
Reviewers: A. Smith M. Jones J. Smith	Date: 01 Feb 10
<u>Findings:</u> No issues found.	





Evidence of Reviews (cont)

- The certifying authority requires positive evidence that an item satisfies applicable criteria.
- Generally this requires:
 - A procedure that outlines the criteria that must be reviewed for.
 - Positive evidence from the review that the reviewed item satisfies each criteria.
- Checklists are a very common tool for obtaining good evidence from reviews.
- Can be very simple:

The reviewed source code correctly implements the relevant design element.

The reviewed source code conforms to the coding standard.



Independence

- Satisfaction of some DO-178B objectives requires independence.
 - Generally, AEO requirements for independence are more onerous than DO-178B.
- Independence in DO-178B means either:
 - Intellectual Independence
 - The reviewer was not involved in the development of the item under review.
 - Tool Independence
 - A tool is used to review an item that was developed manually, or vice versa.
- Example: Analysis of structural coverage.
 - Someone who didn't write the test cases may analyse the test cases for coverage.
 - The person who wrote the test cases may use a tool to analyse the coverage.
 - A person who used a tool to develop test cases may manually analyse the coverage provided by those test cases.





Summary

- Reviews and Inspections are an effective tool for identifying errors as early in the life cycle as possible.
 - Cost and schedule advantages.
- Reviews and Inspections are also required in order to comply with a software assurance standard.
- Reviews and Inspections are only as effective as the skills of the people who conduct them.
- To comply with standards, Reviews and Inspections must produce positive evidence of item compliance.



Questions

