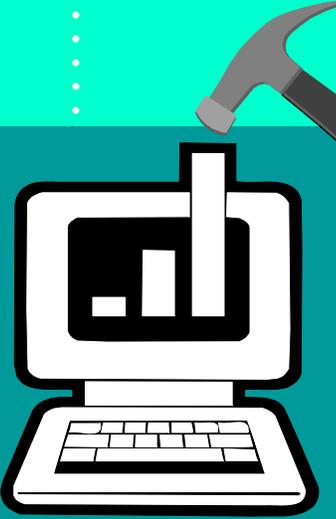


2003 FAA National Software Conference

Software Tool Qualification



Software
Tool
Qualification



Varun Khanna
FAA
Seattle ACO ANM-130S
Varun.Khanna@faa.gov

1

Relevant References

- **RTCA DO-178B/EUROCAE ED-12B**
 - Software Life Cycle Environment (4.1c., 4.1d., 4.2c., 4.4, 4.4.1, 4.4.2, 4.4.3, 6.4.1, 11.4b.(9) (control), 11.15 (CI))
 - Error Prevention/Detection (4.2c., 5.1.2b., 5.2.2f., 5.3.2d., 5.4.2c., 6.1, 6.2e., 6.3.1-6.3.4, 6.4)
 - Tool Identification (11.2c., 11.3d., 11.4a., 11.5a., 11.6c., 11.7d., 11.8e., 11.15(SECI), 11.16h.)
 - Tool Qualification (11.1g., 11.20g., 12.2)
- **FAA Order 8110.49, “Software Approval Guidelines” dated 6/3/03. Chapter 9, “Qualification of Software Tool using RTCA DO-178B**

2

2003 FAA National Software Conference

Software Tool Qualification

Purpose

- **Purpose of Chapter 9 of the ORDER:**
 - Provide Guidelines To ACO Engineers and DERs For Software Tool Qualification
 - Clarify Difference Between Development and Verification Tools
 - Clarify DO-178B Guidance On Tools Qualification

3

History

- **History of Order:**
 - Identified At Streamlining Software Aspects Of Certification (SSAC) Workshop #1 (Jan 1998) As Confusing Part of DO-178B
 - SSAC Workshop #2 (May 1998) - Began Work On Position
 - Draft Notice Routed For Comments - Sept 98
 - Original Notice Completed - April 1999
 - Order issued June '03

4

2003 FAA National Software Conference

Software Tool Qualification

What Is A Tool? 1/4



- **Dictionary**
 - An instrument
 - A Means To An End
 - Anything Used in Performing an Operation
 - Anything Regarded as Necessary to the Carrying Out of One's Occupation or Profession
 - One that is used or manipulated by another

5

What Is A Tool? 2/4

- **DO-178B Definition: Software Tool:**
 - A computer program used to develop, test, analyze, produce, or modify another program or its documentation.



6

2003 FAA National Software Conference

Software Tool Qualification

What Is A Tool? 3/4

- DO-178B Defines Two Software Tools:

Software Development Tools:
“Tools whose output is part of airborne software and thus can introduce errors.”

→ Tool that can inject an error into the software.

7

What Is A Tool? 4/4

– **Software Verification Tools:**
“Tools that cannot introduce errors, but may fail to detect them.”

→ Tool that may fail to detect an error in the software.

8

2003 FAA National Software Conference

Software Tool Qualification

Technical Info: Examples

Development	Verification
<ul style="list-style-type: none">• autocode generators• compilers• software libraries	<ul style="list-style-type: none">• simulators• emulators• test tools - coverage analyzers• test case generators

9

So .. What's Tool Qualification?

- **Process To Ensure That A Tool Provides Confidence At Least Equivalent To The Processes That Are Eliminated, Reduced, or Automated**
- **See DO-178B, Section 12.2**
- **Alternative: Verification of Tools Outputs per DO-178B Section 6**
- **Order 8110.49 Chapter 9 Provides Guidelines**

10

2003 FAA National Software Conference

Software Tool Qualification

Order Outline

- Section 9-1: General
- Section 9-2 Kinds of Tools
- Section 9-3 Determining if Qualification Needed
- Section 9-4 Which Criteria
- Section 9-5 Data Submittal
- Section 9-6 Evaluating Acceptability

11

Background

- Tools Are Developed to Eliminate, Reduce, or Automate Portions of the Process
- Obtain Confidence by Qualification
- DO-178B, Section 12.2 Addresses Tool Qualification

12

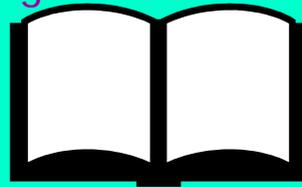
2003 FAA National Software Conference

Software Tool Qualification

When Is Tool Qualification Needed?

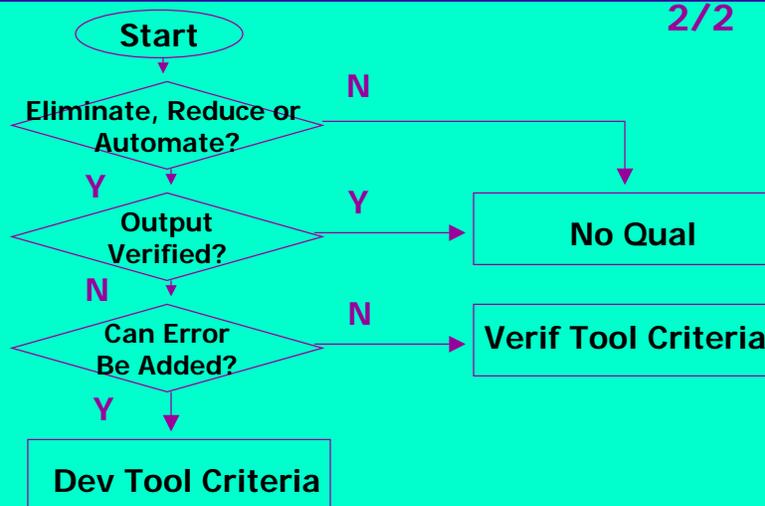
1/2

- DO-178B, 12.2 Tool Qualification states, "Qualification of a tool is needed when processes of this document are eliminated, reduced or automated by the use of a software tool without its output being verified as specified in section 6."



When Is Tool Qualification Needed?

2/2

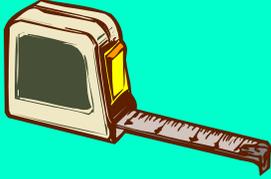


14

2003 FAA National Software Conference

Software Tool Qualification

Two Types of Tools

1. Verification 

 2. Development

15

Verification Tools 1/2

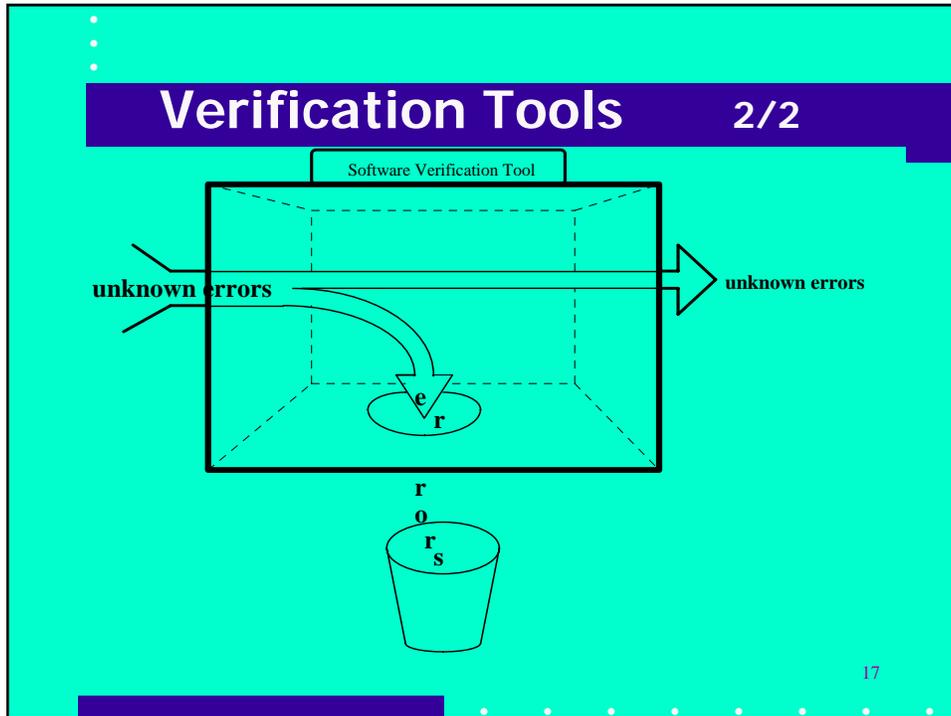
- Tools that cannot introduce errors, but may fail to detect them.
 - For example, a static analyzer, that automates a software verification process activity, should be qualified if the function that it performs is not verified by another activity. Type checkers, analysis tools and test tools are other examples.



16

2003 FAA National Software Conference

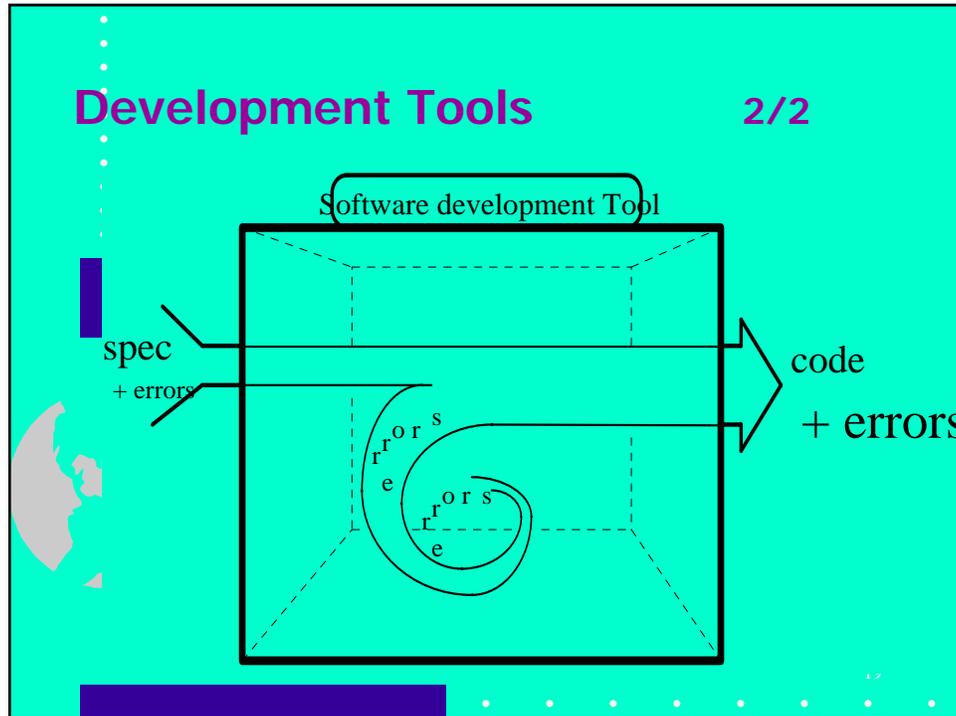
Software Tool Qualification



- Development Tools** 1/2
- Tools whose output is part of airborne software and thus can introduce errors.
 - For example, a tool which generates Source Code directly from low-level requirements would have to be qualified if the generated Source Code is not verified as specified in section 6.
- 18

2003 FAA National Software Conference

Software Tool Qualification



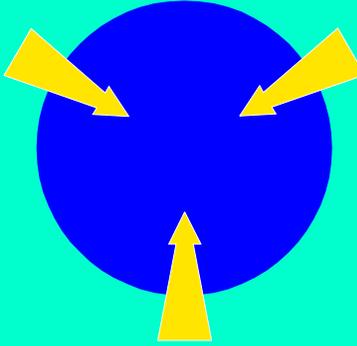
Guidelines

9.3 Determine if Tool Needs Qualification	9.6d Determining Determinism
9.4 Determine Which Tool Qual Criteria Applies	9.6e Qualify Combined Tools
9.5 Determine Data Submittals/Available	9.6f Configuration Mgt of Qualified Tools
9.6 Determine Tool Operational Req Acceptability	9.6g Verify Changes to Previously Qualified Tools
9.6c Determine Acceptable Testing of Tool Operational Req	9.6h DER Approval of Tool Qual Data
	9.6i Tools Prior to 178B

2003 FAA National Software Conference

Software Tool Qualification

Three Questions To Determine If Tool Qual Is Needed 1/2



1. Can tool insert error or allow an existing error to remain undetected?
2. Will tool's output not be verified per section 6 of DO-178B?
3. Are processes of DO-178B eliminated, reduced, or automated?

21

Three Questions To Determine If Tool Qual Is Needed 2/2



- **QUALIFY:** If answers to 3 questions are YES.

22

2003 FAA National Software Conference

Software Tool Qualification

Planning Data



- All Tools To Be Qualified Should Be Specified in the Plan for Software Aspects of Certification (PSAC, 11.1g.)

23

Sections 9.4 and 9.5

Section 9.4
What Criteria Applies to Each Tool Type?
- Ref Figure 9-1

Section 9.5
Data Submittal and Availability
- Ref Figure 9-2

24

2003 FAA National Software Conference

Software Tool Qualification

Data Submittals

- Development tool
- Plan for Software Aspects of Certification
- Tool Qualification Plan
- Tool Operational Requirements
- Tool Accomplishment Summary
- Software Accomplishment Summary
- Verification tool
- Plan for Software Aspects of Certification
- Tool Operational Requirements
- Software Accomplishment Summary

25

Tool Operational Requirements

- Development tool
- Functionality
- Operational Environment
- Installation or Operational Info
- Development Process Performed
- Expected Response Under Abnormal Conditions
- Verification tool
- Functionality
- Operational Environment
- Installation or Operational Info

26

2003 FAA National Software Conference

Software Tool Qualification

Tool Operational Requirements

- **Verification Tools**
 - Normal Operating Conditions
 - Only Test Used Portion
- **Development Tools**
 - Normal Operating Conditions
 - Abnormal Operating Conditions
 - See DO-178B Section 6.4.2 For “Normal” vs. “Abnormal”

27

Determinism of Tools

- **Ability to Establish Correctness of the Output from the Tool**
- **Given the Same Input, the Tool Should Generate the Correct Output Every Time**
 - All Possible Variations of the Output from Some Given Input Should Be Correct
 - Variations in Output Need to be Bounded; e.g., Case/Switch Construct in a Code Generator

28

2003 FAA National Software Conference

Software Tool Qualification

Combined Tools

- Output of Both are Used to satisfy a DO-178B Objective
- Tool Functions May Be Qualified Separately IF Partitioning Between Functions Can Be Demonstrated.

29

Configuration Management

Configuration Management Control of Qualified Tools:

DO-178B, paragraphs 7.2.9b and 12.2.3b

Tool Qualification Data for Software Development Tools should be controlled as CC1.

Tool Qualification Data for Software Verification Tools should be controlled as CC2.

30

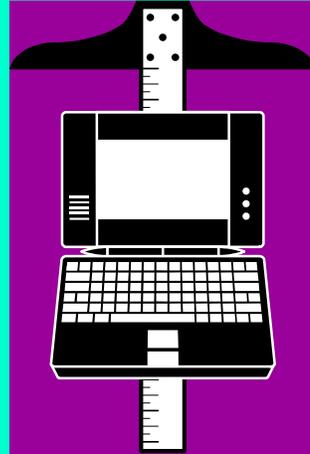
2003 FAA National Software Conference Software Tool Qualification

Section 9.6g, 9.6h, 9.6i

g: Changes to Qualified Tools Change Impact Analysis

h: DERs - Don't Delegate if Alternate Means or Policy Issues Exist

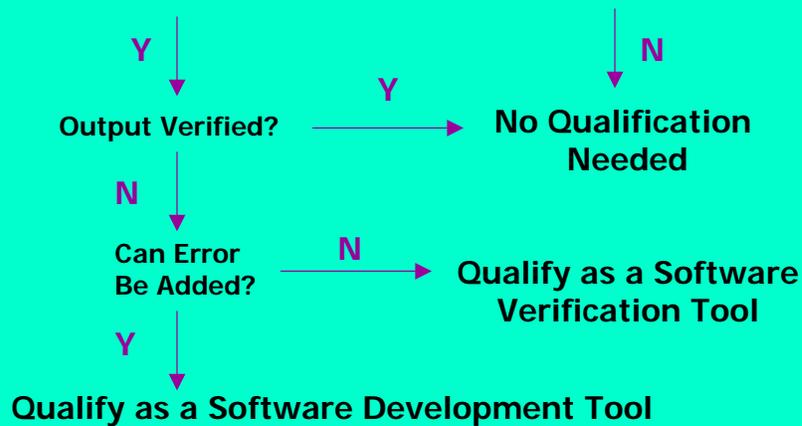
i: Tools prior to DO-178B



31

Summary

Process or Activity Eliminated, Reduced or Automated?



32