Verification/Validation/ Certification

18-849b Dependable Embedded Systems

Eushiuan Tran

February 2, 1999

Carnegie Mellon

Overview: V/V/C

- ◆ **Introduction**
  - Definition of verification/validation/certification
- ◆ **Key concepts**
  - Verification Techniques
  - Validation Techniques
  - Certification Process
- ◆ **Tools / techniques**
- ◆ **Relationship to other topics**
- ◆ **Conclusions & future work**

Description of Topic

- **Definitions from *IEEE Standard Glossary of Software Engineering Terminology***
    - **Verification:** *The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase.*
    - **Validation:** *The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.*
    - **Certification:** *A written guarantee that a system or component complies with its specified requirements and is acceptable for operational use.*
- **Verification simply demonstrates whether the output of a phase conforms to the input of a phase while validation demonstrates that the system is operational.**

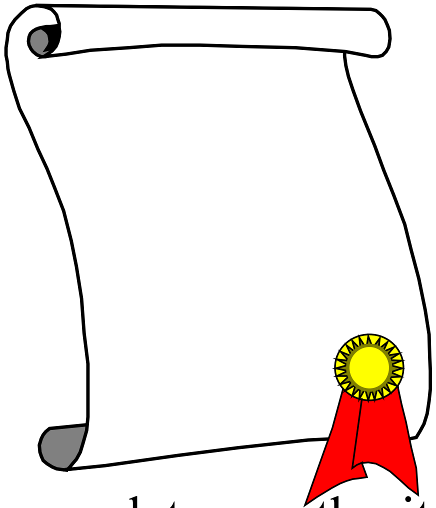
Verification Techniques

- **Dynamic Testing:** ***Testing that involves the execution of a system or component***
  - Functional testing
  - Structural testing
  - Random testing
- **Static Testing:** ***Testing that does not involve the operation of the system or component***
  - Consistency techniques
  - Measurement techniques
- **Sources for detailed descriptions**
  - *Software Engineer's Reference Book* (McDermid, 1992)
  - *Standard for Software Component Testing* (British Computer Society, 1995)
  - Standards including DO-178B and IEC 1508

Validation Techniques

- **Formal methods:** ***The use of mathematical and logical techniques to express, investigate, and analyze the specification, design, documentation, and behavior of computer hardware and software.***
- **Fault injection:** ***The intentional activation of faults by hardware or software means to observe the system operation under fault conditions.***
    - Hardware fault injection
    - Software fault injection
- **Dependability analysis -** ***Involves identifying hazards and then proposing methods that reduces the risk of the hazard occuring.***
    - Hazard analysis
    - Risk analysis

Certification



Forms of certification

- Certification of organizations or individuals
- Certification of tools or methods
- Certification of systems or products

Certification Process

- Certification liaison between parties established.
- Developer submit a verification plan for approval by the regulatory authority.
- Discussion between developer and regulatory body to resolve areas of misunderstanding and disagreement.
- Changes to methods used will be approved by the regulatory body to insure that certification will not be affected.
- Continued submission of documentation to show that certification plan is satisfied.
- The regulating authority will hold a series of reviews to discuss the submitted material.
- If terms of certification plan have been satisfied , a certificate or license is issued.

FAA Software Certification

- **In accordance with RTCA/DO-178B**
- **2 objectives**
  - To demonstrate that it satisfies requirements
  - To demonstrate that errors leading to unacceptable failure conditions are removed
- **Verification methods**
  - Hardware/software integration testing
  - Software integration testing
  - Low-level testing
  - Requirements-based test coverage analysis
  - Structural coverage analysis
- **Alternative verification methods**
  - Formal methods
  - Exhaustive input testing

Tools / Techniques

- **There is an abundance of verification and validation tools and techniques available. Some examples are ...**
  - Static analysis
    - walkthroughs
    - design reviews
    - checklists
    - formal proofs
  - Dynamic analysis
    - functional testing
    - boundary value analysis
    - structure-based testing
    - probabilistic testing

Relationship To Other Topic Areas

- **Fault injection** - Fault injection is a validation technique.
- **Requirements and specifications** - Validation is confirming that the specifications are consistent with the customer's requirements.
- **Standards -** Standards exist that define the software verification and validation process.
- **Software safety** - Can verification and validation prove that the software is "safe"?
- **Environment/EMC/EMI** - Environmental testing can be considered a verification technique.
- **Formal methods** - Formal methods is both a verification and validation technique.
- **Software testing** - Many software testing techniques are used for verification.
- **Safety critical systems analysis** - Hazard and risk analysis are validation techniques.
- **Social and legal concerns** - How does the certification process affect the legal responsibilities of a safety-critical systems developer?

Conclusions & Future Work

- **Verification and validation are crucial in the certification process**
- **How much testing is enough testing?**
- **Should artifacts be certified or the methodology certified?**
- **Certification does not remove any manufacturer's legal or moral obligations.**
- **Future Work**
  - Standardization of certification methods used in different industries
  - Use of formal methods in software certification

Required Reading

- ***Current Practice in Verification, Validation and Licensing of Safety Critical Systems - The Assessor's Point of View*** **by Gunter Gloe, Gerhard Rabe**
- **Outlines the verification/validation/certification procedure in Germany**
- **Type approval -** ***independent of any application; is targeted to certification of components***
- **Application dependent approval -** ***proof that system meets requirements related to a specific application***
- **Tools**
  - TASQUE - Tool for Assisting Software Quality Evaluation
  - SQUID
  - CATS
  - Commercially available tools