U O W

Software Requirements, Specifications and Formal Methods

Dr. Shixun Huang

UNIVERSITY OF WOLLONGONG AUSTRALIA

Requirements Risk Management

Requirements Risk Management

Requirements can be inadequate in many ways including:

- Inaccurate or incomplete stakeholder identification
- Insufficient requirements validation
- Insufficient requirements verification
- Incomplete requirements
- Incorrect requirements
- Incorrectly ranked requirements
- Inconsistent requirements (Laplante 2010)

Requirements Validation and Verification

- It involves review, analysis, and testing to ensure that a system complies with its requirements.
- Compliance pertains to both functional and non-functional requirements.
- Boehm (1984) suggests the following to make the distinction between verification and validation:
  - Requirements validation: “am I building the right product?”
  - Requirements verification: “am I building the product right?”
  - In other words, validation involves fully understanding customer intent and verification involves satisfying the customer intent.

Requirements Validation and Verification

- There are great benefits of implementing a requirements verification and validation program. These include:
  - Early detection and correction of system anomalies
  - Enhanced management insight into process and product risk
  - Support for life cycle processes to ensure conformance to program performance and budget
  - Early assessment of software and system performance
  - Ability to obtain objective evidence of software and system conformance to support process
  - Improved system development and maintenance processes
  - Improved and integrated systems analysis model (IEEE Std 1012 2012)

Requirements Validation and Verification

Requirement verification (testing)

- checks the satisfaction of a number of desirable properties of the requirements
- Usually, we do both validation and verification (V&V) simultaneously
- The techniques used for one or the other are almost the same.

Techniques for Requirements V&V

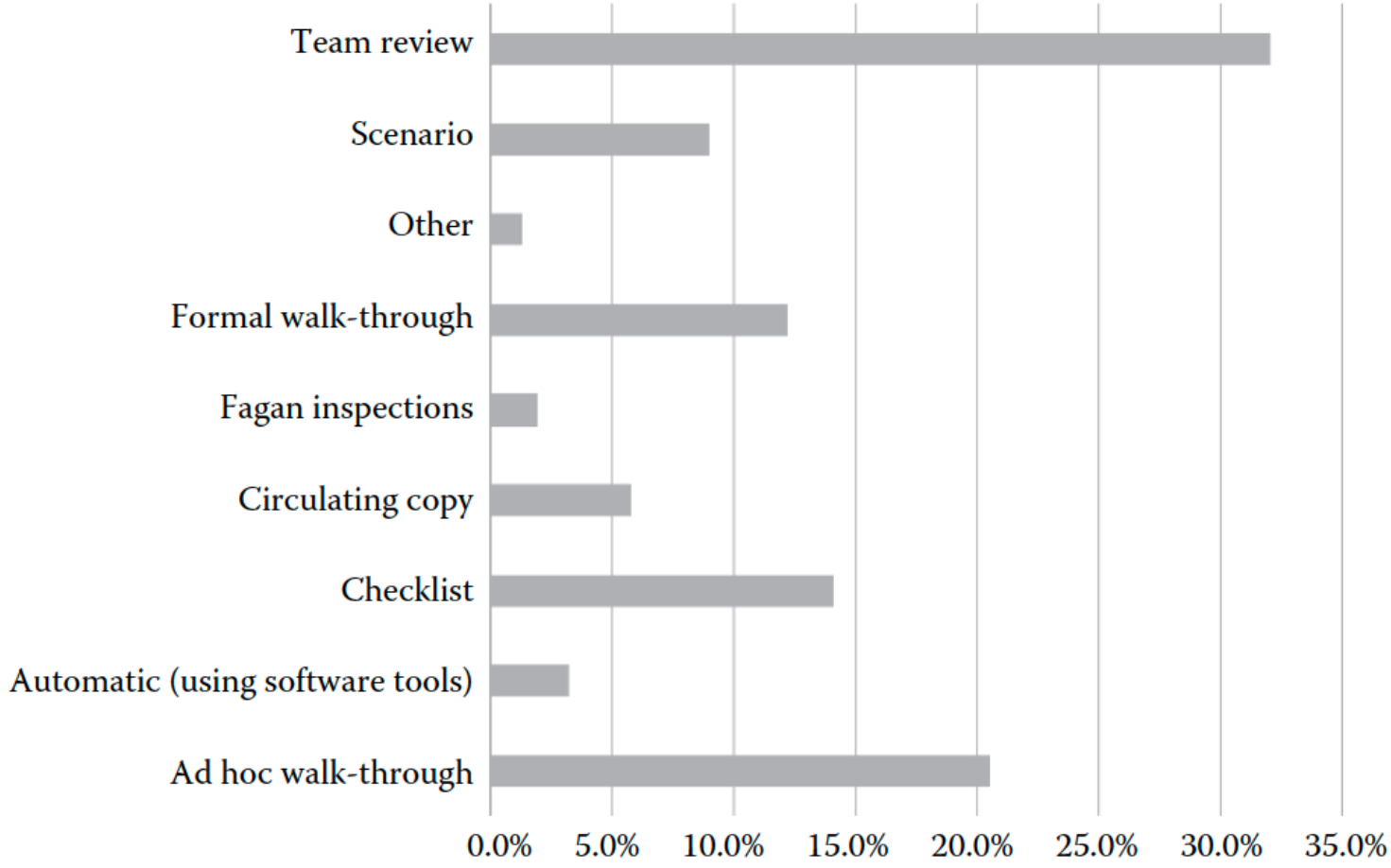
- V&V techniques may include some of the elicitation techniques introduced before, i.e., group review, focus groups, prototyping, viewpoint resolution, or task analysis.
- We can also use comparative product evaluations to uncover missing or unreasonable requirements.
- Walkthroughs or peer/team reviews are an informal methodology to detect errors and improve requirements quality.
- A typical walkthrough scenario involves requirements engineers, a supervisor, and peers participating in a semi-structured meeting to review the requirements prior to release.
- The goal is to identify ambiguities and inconsistencies, and to determine if the requirements can be tested.
- The IEEE 29148 rules can be used as a framework or checklist for the walkthrough.

Requirements Inspection

Inspections are a method of requirement quality control that can be informal or highly structured. Fagan inspections (1986) define the following:

- What can be inspected
- When the code can be inspected
- Who can inspect the code
- What preparation is needed for the inspection
- How the inspection is to be conducted
- The data to be collected
- The follow-up activities

Requirements Inspection



Comparison of Requirements Inspections Techniques

Requirements Understanding

- Stakeholders may have different understandings of requirements.
- One of the best ways to define a consistent requirement understanding is to specify the tests for accepting solutions along with the requirement statement.
- When the statement and test are listed together, most problems associated with misunderstanding requirements disappear.
- In particular, we want to derive requirements-based test situations and use them as a test of requirement understanding and validation.
- It is known as the test-driven development approach

Requirement V&V Matrices

- A requirements validation matrix is an artifact that associates high-level requirements with certain system attributes for the purposes of trade-off analysis and confirmation of requirement intent.
- Appropriate system attributes can include business need, safety, requirement volatility, and other factors.

Requirement Number	*Safety Impact (high=10)*	*Volatility (high=10)*	*Business Need (high=10)*
3.1	10	2	10
3.2	2	1	5
…	…	…	…
3.210	3	6	7
3.211	5	10	1

A requirement validation matrix

Requirement V&V Matrices

- A requirements verification matrix is used later after the validation matrix.
- The verification matrix associates requirements with test cases
- An easy mechanism to track the status of test-case design and implementation

Requirement	*Test Cases*	*Status*
9.13.1 System shall provide wireless support for driving any number of wall-mounted monitors for picture display.	T-1711 T-1712 T-1715	Passed Passed Passed
9.13.2 System shall provide Web-based interface for authenticated users to publish new photos for display on wall monitors.	T-1711 T-1715 T-1811	Passed Failed Passed
9.13.3 System shall allow users to configure which pictures get displayed.	T-1712 T-1715 T-1811 T-1812 T-1819	Passed Passed Passed Passed Not run
9.13.4 System shall allow users to configure which remote users can submit pictures to which wall monitor.	T-1712 T-1715 T-1716 T-1812	Passed Passed Passed Passed

A requirement verification matrix

Goal/Question/Metric Analysis

The goal/question/metric (GQM) paradigm is an analysis technique that helps in the selection of an appropriate metric.

- First, state the goals of the measurement, that is, “what is the organization trying to achieve?”
- Next, derive from each goal the questions that must be answered to determine if the goals are being met.
- Finally, decide what must be measured in order to be able to answer the questions

Goal/Question/Metric Analysis

An Example:

- Goal: The system shall be **easy to use (subjective)**
- One question: How many expert, intermediate, and novice users use the system?
- Reason: an easy-to-use system should be used by everyone
- Way to obtain the matric: provide the system in an open lab for a period of time and measure the number and percentage of each user type who uses the system
- Result: If a disproportionate number of users are expert, for example, then it may be concluded that the system is not easy to use. If an equal proportion of expert, intermediate, and novice users use the system, then it might be that the system is "easy to use."

Standards for V&V

The IEEE 29148 “describes recommended approaches for the specification of software requirements.” The standard attempts to help:

- 1. Software customers to accurately describe what they wish to obtain
- 2. Software suppliers to understand exactly what the customer wants
- 3. Individuals to accomplish the following goals:
  - a. Develop a standard software requirements specification (SRS) outline for their own organizations
  - b. Define the format and content of their specific SRSs
  - c. Develop additional local supporting items, such as an SRS quality checklist or an SRS writer’s handbook (ISO/IEC/IEEE Std 29148 2011)

Standards for V&V

1. Purpose
2. Referenced documents
3. Definitions
4. V&V overview
    - 4.1 Organization
    - 4.2 Master schedule
    - 4.3 Software integrity level scheme
    - 4.4 Resources summary
    - 4.5 Responsibilities
    - 4.6 Tools, techniques, and methods
5. V&V processes
    - 5.1 Process: Management
        - 5.1.1 Activity: Management of V&V
    - 5.2 Process: Acquisition
        - 5.2.1 Activity: Acquisition support V&V
    - 5.3 Process: Supply
        - 5.3.1 Activity: Planning V&V
    - 5.4 Process: Development
        - 5.4.1 Activity: Concept V&V
        - 5.4.2 Activity: Requirements V&V
        - 5.4.3 Activity: Design V&V
        - 5.4.4 Activity: Implementation V&V
        - 5.4.5 Activity: Test V&V
        - 5.4.6 Activity: Installation and checkout V&V
    - 5.5 Process: Operation
        - 5.5.1 Activity: Operation V&V
    - 5.6 Process: Maintenance
        - 5.6.1 Activity: Maintenance V&V
6. V&V reporting requirements
    - 6.1 Task reports
    - 6.2 Activity summary reports
    - 6.3 Anomaly reports
    - 6.4 V&V final report
    - 6.5 Special studies reports (optional)
    - 6.6 Other reports (optional)
7. V&V Administrative requirements
    - 7.1 Anomaly resolution and reporting
    - 7.2 Task iteration policy
    - 7.3 D eviation policy
    - 7.4 C ontrol procedures
    - 7.5 Standards, practices, and conventions
8. V&V test documentation requirements

IEEE standard V&V plan table of contents

Standards for V&V

The mandatory qualities for an individual requirement are:

- Singular
- Feasible
- Unambiguous
- Complete
- Consistent
- Verifiable
- Traceable

The set of all requirements should be:

- Complete
- Consistent
- Bounded
- Affordable

Standards for V&V

Singularity: a requirement specify a single behavior and have no conjunctions.

- Examples: The pump control unit shall start the submersible pump motors to prevent the wet well from running over and stop the pump motors before the wet well runs dry.

Actually, this requirement could be separated into two:

- The pump control unit shall start the submersible pump motors to prevent the wet well from running over.
- The pump control unit shall stop the pump motors before the wet well runs dry.

The problem with the conjunctions “and” and “or” is that they can introduce some ambiguity.

Standards for V&V

Feasibility: A requirement is feasible if it can be satisfied with current technology and cost constraints, that is, it is not a ridiculous requirement

- Various techniques can be used to assess feasibility including reviews, inspections, and competitive analysis.

Verifiability: An SRS is verifiable if satisfaction of each requirement can be established using measurement or some other unambiguous means.

- Verifiability can be explored through various reviews, through test-case design (design-driven development), and through viewpoint resolution.

Standards for V&V

Completeness: an SRS document is complete if there is no missing functionality, that is, all appropriate desirable and undesirable behaviors are specified.

- Completeness is a difficult quality to prove for a set of requirements. If a single requirement contains “to be defined” (TBD) or some variation of this phrase, then clearly the requirement is incomplete.
- If the requirement is missing measurable indicators of satisfaction, then that is a problem of incompleteness.
- But if those indicators are absent, how do you know when something is missing in a requirement specification?
- Typical techniques for reducing incompleteness include various reviews, viewpoint resolution, and the act of test-case generation.

Standards for V&V

Consistency: has two forms the internal consistency and the external consistency

- Internal consistency: satisfaction of one requirement does not preclude satisfaction of another
- External consistency: the SRS is in agreement with all other applicable documents and standards.

Examples: baggage handling system

- If the lever is in position 1, then valve 1 is opened.
- If the lever is in position 1, then valve 1 is closed.

The two requirements are inconsistent and therefore invalid

Standards for V&V

Traceability: An SRS is traceable if each requirement is clearly identifiable, and all linkages to other requirements (e.g., dependencies, subordinate, and predominant) are clearly noted.

- Traceability is an essential quality for effective communications about requirements, to facilitate easy modification, and even for legal considerations.
- For example, in the case of a dispute, it is helpful to show that responsible linking of related requirements was done.
- Traceability can be measured using network-like analyses. For example, we could count the efferent (inward) and afferent (outward) coupling as indicated by the key phrases “uses,” “is referenced by,” “references,” “is used by,” and so on.
- Group reviews and inspections and automated tools can also be used to check for traceability between requirements to/from tests.