CHAPTER 7: VERIFICATION AND VALIDATION

(3hrs,12 marks) -Anuja Ghising

Syllabus

7.1 Planning Verification and validation

7.2 software inspections

7.3 Verification and formal methods

7.4 Critical system verification and validation

Verification

It is an act of reviewing, inspecting, testing, checking, auditing, or otherwiseestablishing and documenting whether items, processes, services ordocuments conform to specified requirements.

It can also be defined as 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 the phase.

Validation

Validation is the process of evaluating a system or component during or at the end of the developmentprocess to determine whether it satisfies specified requirements. Validationis, therefore, 'end-to-end' verification. Validation occurs through the utilization of various testing approaches.

Verification and Validation goals

a. Correctness

The extent to which the product is fault free.

b. Consistency

The extent to which the product is consistentwithin itself and with other products

c. Necessity

The extent to which everything in the product isnecessary.

d. Sufficiency

The extent to which the product is complete.

e. Performance

The extent to which the product satisfies its performance requirements.

7.1 Planning verification and validation

The development of a V &V plan is essential to the success of a project. The plan must be developed early in the project. Careful planning is required to get the most out of testing and inspection process. Effective V & V plan requires many considerations that are:

1. Identification of V&V Goals

   V&V goals must be identified from the requirements andspecifications. These goals must address those attributesof the product that correspond to its userexpectations.

2. Selection of V&V Techniques

   Specific techniques must be selected for each of the project'sevolving products.

3. Organizational Responsibilities

   The organizational structure of a project is a keyplanning consideration for project managers.Animportant aspect of this structure is delegation of V&V activities to various organizations

4. Integrating V&V Approaches

   Once a set of V&V objectives has been identified,an overall integrated V&V approach must be deter-mined. This approach involves integration of tech-niques applicable to the various life cycle phases asdelegation of these tasks amongthe project'sorganizations. The planning of this integrated V&Vapproach is very dependent upon the nature of theproduct and the process used to develop it. Traditional integrated V&V approaches have followed the"waterfall model".

5. Problem Tracking

Software V&V plandeveloping a mechanism for documenting problems

• when the problem occurred

• where the problem occurred

• evidence of the problem

•priority for solving problem

- The V model of development

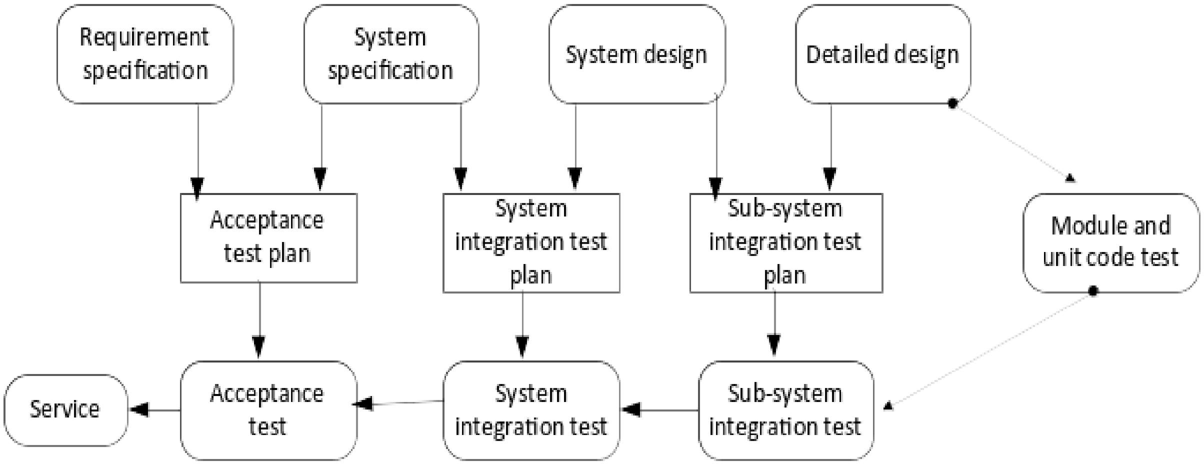
Requirement specification
System specification
System design
Detailed design
Acceptance test plan
System integration test plan
Sub-system integration test plan
Module and unit code test
Service
Acceptance test
System integration test
Sub-system integration test

Fig: V model of development

7.2 Software Inspections (static verifications)

Software inspections can be used for the detection of defects in detailed designs before coding, and in code before testing. They may also be used to verify system requirements, design models and even the proposed system tests. Software inspections are concerned with the analysis of the static system representation to discover problems (static verification).

λ Inspection is a manual, static technique that can be applied early in the development cycle.

λ Inspection is based on reading techniques.

- Advantages of inspection over testing
  1. During testing one error can hide other errors. As inspection is static process there is no interaction between errors,consequently an inspection can discover many errors.
  2. Incomplete versions of a system can be inspected without additional costs.
  3. Inspection considers inefficiencies, inappropriate algorithms and poor programming styles that could make system difficult.

- Inspection per conditions
  1. A precise specification must be available.
  2. Team members must be familiar with the organization standards.
  3. Syntactically correct code must be available.
  4. An error checklist must be present.
  5. Management must accept that inspection will increase costs early in the software process.

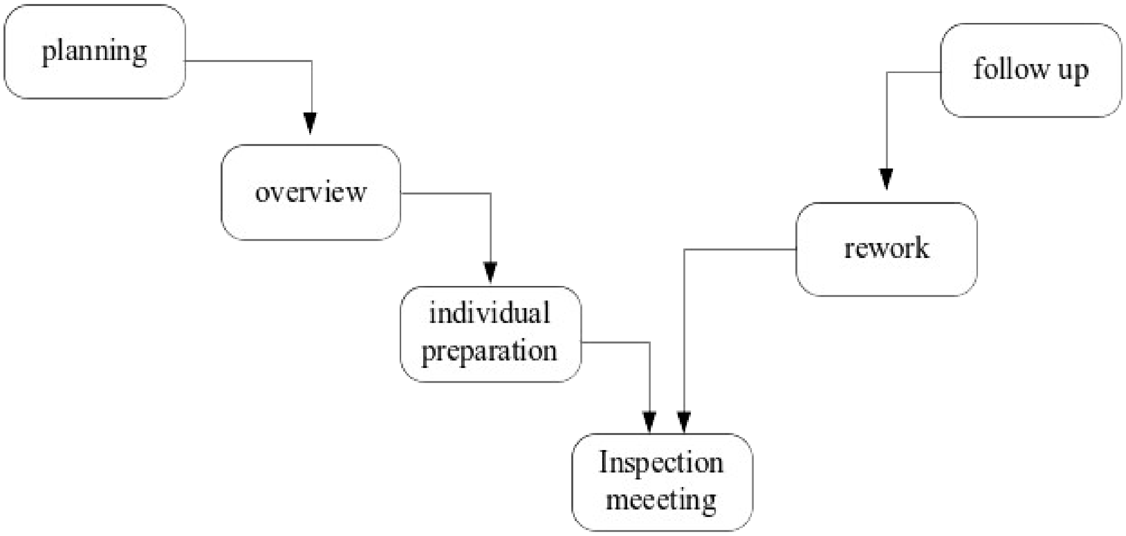

Fig: The inspection process

- Inspection procedure

  1. First of all, system overview is presented to the inspection team.
  2. Secondly, the required codes and documents are distributed to the inspection team in advance.
  3. Then, inspection takes place and errors are discovered. Pre inspection however may or may not be required.

- Inspection team and role

  1. Moderator:

     The moderator leads the inspection and chairs the inspection meeting. The person should have implementation skills, but not necessarily be knowledgeable about the item under inspection. He or she must be partial and objective. For this reason moderators are often drawn from staff outside the project. Ideally they should receive some training in inspection procedures.

2. Inspector:

   Inspectors identify and describe defects in the review items under inspection. They should be selected to represent a variety of viewpoints (e.g. designer, coder and tester).

3. Reader:

   The reader guides the inspection team through the review items during the inspection meetings.

4. Author:

   The author is the person who has produced the items under inspection. The author is present to answer questions about the items under inspection, and is responsible for all rework. A person may have one or more of the roles above. In the interests of objectivity, no person may share the author role with another role.

7.4 Verification and Formal Methods (FM)

FM can be used when a mathematical specification of the system is produced. They are the ultimate static verification techniques. They involve detailed mathematical analysis if the specifications and may develop format arguments that a program conforms to its mathematical specification.

- Arguments for FM

  Producing a mathematical specification requires a detailed analysis of the requirements and this is likely to uncover errors.

  They can detect implementation errors before testing, when program is analyzed alongside the specifications.

- Arguments against FM
    1. Requires specialized notations that are not understood by domain experts.
    2. It is very expensive to develop a specification and even more expensive to show that a program meets that specification.

7.4 Critical system Verification and Validation

- Verification and Validation cost

  V and V costs for critical system involves additional validation processes and analysis than for other system. The cost of failure is so high that it is cheaper to find and remove faults than to pay for system failure.

  Normally, verification and validation costs takeup more than 50% of the total system development costs which may be as follows:

    1. 33% - life sustaining medical devices or nuclear weapons
    2. 20-25% - telecommunications or financial systems
    3. 10-18% systems desiring software quality but not high-integrity.

- Critical system verification and validation includes:
    1. <u>Reliability Validation:</u>

       Exercising the programs to access whether or not it has reached the required level of reliability.
    2. <u>Safety assurance:</u>

       Concerned with establishing confidence labels in the system. However, quantitative measurements of safety is impossible.
    3. <u>Security assessment:</u>

Intended to demonstrate that the system can't enter some state rather than to demonstrate that the system can do something.

4. Safety and dependability cases:

   These are structured documents that set out detailed argument and evidence that a required level if safety or dependability has been achieved.

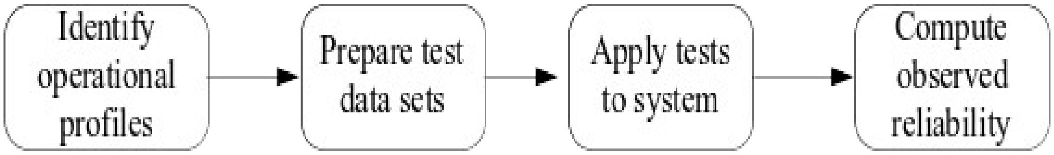

Fig :The reliability measurement process

- Process et al(1990) suggests five types of review for safety critical system:
  1. Review for correct intended function.
  2. Review for maintainable, understandable structure.
  3. Review to verify that the algorithm and data structure design are consistent with the specified behavior.
  4. Review the consistency of the code and the algorithm and the data structure design.
  5. Review the adequacy of the system test cases.

- Security assessment

  There are four complementary approaches for security checking:

  1. Experience-based validation
  2. Tool-based validation
  3. Tiger team
  4. Formal verification

PAST QUESTIONS

Qn. Distinguish between verification and validation. [066 Bhadra, 5 marks]

Qn. Explain why program inspection are an effective technique for discovering errors in program? What types of errors are unlikely to be discovered through inspections? [068 chaitra, 10 marks]