5.1 Introduction

Software verification and validation (V&V) is a technical discipline of systems engineering. The purpose of software V&V is to help the developer to build quality into the software during the software life cycle. The software V&V processes determine if development products of a given activity confirm to the requirements of that activity, and if the software satisfies the intended use and user needs. The determination includes assessment, analysis, evaluation, review, inspection and testing of software products and processes. The software V&V is performed in parallel with the software development, not at the end of the software development [5.1]. The complete framework of V&V procedure developed as part of research work encompassing artifacts, checklists, traceability matrix are detailed here. The V&V procedure evaluates on the following key concepts. They are software safety levels, V&V tasks for each software safety level, systems viewpoint and Compliance with International and IEEE standards. The V & V procedure is developed to

- Establish a common framework for V&V processes, activities, and tasks in support of all software life cycle processes.
- Define the V&V tasks, required inputs, and required outputs.
- Identify the minimum V&V tasks corresponding to software safety levels using a three-level scheme [5.2].

This V&V procedure shall use the following three-level software integrity scheme as a method to define the minimum V&V tasks that are assigned to each software criticality level as listed in Table 5.1 [5.3]
Table 5.1 Software Criticality Levels

<table>
<thead>
<tr>
<th>Criticality</th>
<th>Description</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Critical</td>
<td>Initiates the shutdown of the reactor when the signal crosses the safety limit.</td>
<td>1</td>
</tr>
<tr>
<td>Safety Related</td>
<td>Selected function affects important system performance.</td>
<td>2</td>
</tr>
<tr>
<td>Non Nuclear Safety</td>
<td>Systems not related to nuclear safety.</td>
<td>3</td>
</tr>
</tbody>
</table>

5.2. Verification procedure for Custom-Built Systems (CBS)

5.2.1 Documents submitted

The following design documents along with Traceability matrix have to be submitted by the designer / developer to the V&V committee as and when required as the verification process progresses. The documents are generated as per the standards [5.4]

Design Basis Document  System Requirements Specification (SyRS)
System Design Guidelines  System Architectural Design (SAD)
System Integration & Test Procedure(SysITP)Software Requirements Specification (SRS)
Software Design Description (SDD)  Software Integration & Test Procedure (SITP)
Programming Guidelines (PG)  Software Implementation (source and Object code)
User Documentation (UD)  System Build

During the process of V&V, all the documents are reviewed for clarity, completeness, correctness, consistency and compliance to standards. They are verified for complete traceability [5.5].
The following test reports have to be submitted to V&V Committee during system validation [5.6].

Software Unit Test Report (SUTR)    Software Integration and Test Report (SITR)
System Integration and Test Report (SyITR) System Acceptance Test Report
System Safety Analysis Report (SSAR)

5.2.2 Procedure for Verification

The procedure for verification has the following stages of review. They are System Requirements, System Architecture, Hardware / software specifications, Hardware / software Design, Hardware / software Implementation, System Integration and System Validation [5.7]. The V& V process is initiated once the SyRS for a particular system is submitted to the V&V Committee and the committee forms a review task force, which comprises the following members as minimum requirement as shown in Table 5.2.

Table 5.2 Review Taskforce Committee

<table>
<thead>
<tr>
<th>S.No</th>
<th>Responsibility</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Convenor</td>
<td>From V&amp;V</td>
</tr>
<tr>
<td>2</td>
<td>Co-convenor</td>
<td>From V&amp;V</td>
</tr>
<tr>
<td>3</td>
<td>Member</td>
<td>From V&amp;V</td>
</tr>
<tr>
<td>4</td>
<td>Subject Matter Expert (SME) / Domain Expert</td>
<td>Invitee</td>
</tr>
<tr>
<td>5</td>
<td>Inspectors / Peers</td>
<td>Invitee</td>
</tr>
<tr>
<td>6</td>
<td>Author</td>
<td>Designer / Developer</td>
</tr>
</tbody>
</table>
The task force reviews the document submitted / presented at various stages by the designer / developer and verifies for its compliance with the baselined documents and checks for the consistency of the document and produces verification report. In case of no anomaly, the document may be cleared and in case of any anomaly or controversy with the any document, a revision will be recommended to the designer. In that case, the designer has to re-submit the document again with the compliance report that states the reason for anomaly. After verification, the task force, issues verification report through V&V Committee. Once a document baseline, any change to that will initiate the review process to documents submitted thereafter [5.8].

5.2.3 System Requirements Specification (SyRS) Review

The Purpose of SyRS review is to verify that SyRS covers all of the I & C design requirements of the corresponding system as described in Design Basis and all the requirements are unambiguous, complete, consistent, traceable and verifiable. The documents to be submitted are Design Basis, System Requirements Specification as per IEEE standard 1233 [5.9] and other specific requirements, if any. The documents generated are Review comments along with Compliance Report and Traceability matrix report to track defect closure, which contains total defects, review efficiency and defect density. The System Requirements Specification document is base-lined after review.

When the review task force identifies any defect, it has to be recorded by Convener for the traceability purpose. The consolidated defects identified in the review process should be circulated to the review task force. The checklist for the system requirement review is detailed in Appendix-II. The review process may be repeated iteratively, once the defects
are fixed. The review process should ensure System consistency, safety, reliability and maintainability. The V&V effort shall perform, as appropriate for the selected system integrity level Traceability Analysis, System Requirements Evaluation, Interface Analysis, Criticality Analysis, System V&V Test Plan Generation and Verification, Acceptance V&V Test Plan Generation and Verification, Configuration Management Assessment and Safety Analysis.

5.2.4 System Architecture Review (SAR)

The documents to be submitted are baselined System Requirements Specification (SyRS), Software Design Guidelines, Software Integration Test Procedure and System Architecture Design. The documents generated are Review comments along with compliance report and traceability matrix report to track defect closure, which contains total defects and defect density. The System Architecture Design document is base-lined after review.

The baselined SyRS document forms the starting point for this review. This review is to ensure the completeness of the architecture design document. The review task force conduct the review process as per the given architecture review checklist and consolidate the defects in the compliance report. The same is communicated to the designer for the completeness of the document. This review process ensures the forward and backward traceability of the system. The checklist for system architecture review is provided in Appendix-III. The objectives of V&V are to demonstrate that the design is a correct, accurate, and complete transformation of the system requirements and no unintended features are introduced.
5.2.5 Software Requirement Specification (SRS) Review

The Purpose is to verify that the software requirements specification confirms to the system requirement specification, system architecture design and traceability. The documents submitted are baselined SyRS, SAD and SRS as per IEEE 830 [5.10], Traceability matrix with SyRS and SAD. The documents generated are Verification report of SRS, SRS document Check List and System V & V test plan. The V&V effort shall perform, as appropriate for the selected system integrity level. The checklist for the software requirement review is presented in Appendix-IV.

5.2.6 Software Design Description (SDD) Review

The purpose is to verify that the software design confirms to the software requirements and it is traceable. The documents submitted are baselined SRS with SDD as per IEEE 1012 [5.11] and Traceability matrix with SRS and SDD. The documents generated are Verification report of SDD and SDD checklist. The design V&V activity addresses software architectural design and software detailed design. The objectives of V&V are to demonstrate that the design is a correct, accurate, and complete transformation of the software requirements and that no unintended features exists. The checklist for the software design review is provided in Appendix-V.

5.2.7 Software Implementation Review

The documents submitted are software (both source code and object files), baselined Software Design Description (SDD), Traceability Matrix (SDD to Source Code), Observed Programming Guidelines, Software Unit Test Report (SUTR), Software Integration Test Report (SITR) and System Build Settings.
The documents generated include the code non-compliance report with respect to MISRA ‘C’ guidelines and to the observed programming guidelines [5.12], static and dynamic analysis report and the manual code walk-through report. The software coding, testing, and build settings are evaluated [5.13].

The code is subjected to static analysis to verify if the structure of code is as per the programming guidelines. For example, if Cyclomatic complexity of safety critical function software is defined to be within 10, and if the code does not meet this requirement then the code will be returned for correction. Only when the code passes the static analysis check, the software shall be taken for further verification process. The compliance of the source code to the observed standard is also checked before it is taken up for further verification process. Safety systems software will undergo manual code walk-through besides static analysis. V&V team shall evaluate the source code for correctness, consistency, completeness, accuracy, readability and testability [5.14].

5.2.8 System Integration Review

5.2.9 System Validation Review

The documents submitted are baselined System Requirement Specification, Traceability Matrix SyRS to Implementation (Software functions / Hardware) and System Acceptance Test Report [5.15]. The document generated is System Validation Report including the checklist for the system validation review as given in Appendix-VII.

5.3 Inferences

The framework of V&V procedure developed as part of research work encompassing artifacts, checklists, traceability matrix are applied on the I&C systems of nuclear power plant, resulted in phenomenal increase in quality, reliability and confidence on these systems.
REFERENCES


