

F.5.8 SOFTWARE VERIFICATION AND VALIDATION

Objective:

The V&V process and related documentation for software are defined and maintained to ensure that (1) the software correctly performs all its intended functions; and that (2) the software does not perform any adverse unintended function.

Criteria:

1. Safety software deliverables have been verified, and validated for correct operation using reviews, inspections, assessments, observation, and testing techniques.
2. Relevant abnormal conditions have been evaluated for mitigating unintended functions through testing, observation, or inspection techniques.
3. Traceability of safety software requirements to software design and acceptance testing has been performed.
4. New versions of the safety software are verified and validated to ensure that the safety software meets the requirements and does not perform any unintended functions.
5. V&V activities are performed by competent staff other than those who developed the item being verified or validated. This may overlap with the training work activity.

Approach:

Review appropriate documents, such as SQA plans, review plans, walkthrough records, peer review records, desk check records, inspection reports, test plans, test cases, test reports, system qualification plans and reports, and supplier qualification reports to determine whether—

- management process exists for performing V&V and management and independent technical reviews;
- reviews and inspections of the software requirement specifications, procurement documents, software design, code modules, test results, training materials, and user documentation have been performed by staff other than those who developed the item;
- software design was performed prior to the safety software being used in operations;
- for design V&V—
 - results of the safety software V&V are documented and controlled;
 - V&V methods include any one or a combination of design reviews, alternate calculations, and tests performed during program development; and
 - the extent of V&V methods chosen are a function of (1) the complexity of the software; (2) the degree of standardization; (3) the similarity with previously proved software; and (4) the importance to safety; and
- for test V&V—

- documentation for development, factory or acceptance testing, installation, and operations testing exists;
- documentation includes test guidelines, test procedures, test cases including test data, and expected results;
- results documentation demonstrates successful completion of all test cases or the resolution of unsuccessful test cases and proves direct traceability between the test results and specified software design;
- test V&V activities and their relationship with the software life-cycle are defined;
- software requirements and system requirements are satisfied by the execution of integration, system and acceptance testing;
- acceptable methods for evaluating the software test case results include (1) analysis without computer assistance, (2) other validated computer programs, (3) experiments and test, (4) standard problems with known solutions, and (5) confirmed published data and correlations;
- traceability exists from software requirements to design and testing, and if appropriate, to user documentation; and
- hardware and software configurations pertaining to the test V&V are specified.