

F.5.5 SOFTWARE REQUIREMENTS IDENTIFICATION AND MANAGEMENT

Objective:

Safety software functions, requirements, and their bases are defined, documented and managed throughout the safety software life-cycle.

Criteria:

1. The software requirements are documented and consistent with the system safety basis.
2. The functionality, performance, security including user access requirements, interface and safety requirements for the safety software are complete, correct, consistent, clear, testable, and feasible.
3. The documented software requirements are controlled and maintained. Changes to the software requirements are reflected in any and all documentation.
4. Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.

Approach:

Review appropriate safety basis documents, such as DSAs, safety analysis reports, TSRs, procurement specifications and any system documentation to determine if the safety software requirements document is consistent with the safety system design and safety basis. The software requirements may exist either as a standalone document, such as a software requirements specification, or embedded in other system or software level documents.

Determine whether the following types of requirements are addressed as appropriate.

- Verify that the software requirements address functionality, performance, security, safety design inputs, design constraints, installation considerations, operating systems (if applicable), and external interfaces necessary to design the software exist and are documented.
- If access to the system by only authorized users is a requirement, verify that use of software is controlled so that only personnel on authorized user lists apply or maintain safety software.
- Verify that the software requirements are correct, unambiguous, complete, consistent, verifiable, modifiable and traceable as appropriate.
- Verify that acceptance criteria are established in the software requirements for each of the identified requirements. Such criteria should be used for V&V planning and performance as defined in each related life-cycle phase.
- Verify that the software requirement documents are controlled under the configuration change control and document control processes. This may overlap with the SCM activity.

- Verify that software requirement documents are reviewed and updated as necessary. This may overlap with the software V&V work activity.