F.5.3 SOFTWARE CONFIGURATION MANAGEMENT

Objective:

Software configuration is defined, maintained, and controlled until the software is retired.

Criteria:

1. Software configuration items are identified, baselined and controlled.
2. A baseline labeling system is established and implemented.
3. In addition, for Level A or Level B custom developed safety software, periodic configuration audits and reviews are conducted and documented.
4. Proposed software changes are documented, evaluated, and approved.
5. Only approved changes are implemented.

Approach:

Review appropriate documents, such as applicable procedures related to safety software change control to determine if an SCM process exists and is effective. This determination is made based on the following actions.

- Verify the existence of documented processes to control, uniquely identify, describe, and document the configuration of each version or update of safety software and its related documentation. This documented evidence may be in either SCM plan or embedded in another software or system level document.
- Verify that a configuration baseline is defined and that it is being adequately controlled. This baseline should include operating system components, any associated runtime libraries, acquired software executables, custom-developed source code files, users' documentation, the appropriate documents containing software requirements, software design, software V&V procedures, test plans and procedures, and any software development and quality planning documents.
- Verify a baseline labeling system has been created that uniquely identifies each configuration item, identifies changes to configuration items by revision, and provides the ability to uniquely identify each configuration.
- Review procedures governing change management for installing new versions of the software components, including new releases of acquired software.
- Review software change packages and work packages to ensure that (1) possible impacts of software modifications are evaluated before changes are made, (2) various software system products are examined for consistency and revised as necessary after changes are made and updated, (3) software is tested according to established standards after changes have been made, (4) changes are evaluated and approved for release by the responsible organization, and (5) software validation is performed as necessary to ensure that the

change does not adversely affect the performance of the software.

- Verify by sampling that documentation affected by software changes accurately reflects all safety-related changes that have been made to the software.
- Interview a sample of cognizant line, engineering, and QA managers, and other personnel to verify their understanding of the change control process and commitment to manage changes affecting design, safety basis, and software changes in a formal, disciplined, and auditable manner.
- For custom developed safety software, verify audits or reviews, such as functional configuration audit or physical configuration audit, have been performed.