[This is an example of a LAR addressing D.4 in which an NRC-approved process is not available. This example describes the Software Configuration Management Process. The intent of including the below information in the NRC tabletop is to show type of content and level of detail for a software configuration management process description to address ISG-06 R2 Section D.4.2.5.]

LAR Material to address ISG-06 R2 D.4.2.5 Software Configuration Management Processes

The vendor's software configuration management process (SCMP) meets the criteria described in ISG-06 R2 Section D.4.2.5. A summary description of the vendor's SCMP is below.

The vendor's SCMP is compliant with IEEE Std. 828-1990 as endorsed by RG 1.169.

The configuration management plan (SCMP) in Reference X describes the methods and tools to identify and control the system and programming throughout its development and use. Activities include: (1) the identification and establishment of baselines, (2) the review, approval, and control of changes, (3) the tracking and reporting of such changes, (4) the audits and reviews of the evolving products, and (5) the control of interface documentation. The SCMP describes the means through which the integrity and traceability of the system are recorded, communicated, and controlled during both development and maintenance. The SCMP includes an overview description of the development project and identifies the configuration items that are governed by the plan. The plan also identifies the organizations, both technical and managerial, that are responsible for implementing configuration management.

The SCMP defines the SCM roles and responsibilities for internal organizations and staff, identify the SCM tools, and describe the processes for SCM including item identification, configuration control activities, change control authority and request mechanisms, and change/error tracking and reporting. According to the SCMP, the Software Program Manager (SPM) has overall responsibility for SCM for the project and for the production and application of the SCMP; the Development and V&V teams perform technical SCM activities and create and identify configuration elements; and the Software Quality Assurance Manager (SQAM) verifies the application of requirements and conducts reviews and audits of SCM activities and software product configuration.

Reference configurations are created at various stages in the software development life cycle. In the configuration management (CM) tool, the reference configurations are created by baselines, which are a set of configuration elements under a given version.

Each SCM item is given a unique identification for control and tracking purposes. Items under the SCMP are identified with a major version number (incremented for each new version of the component) and a minor version number (incremented to keep track of intermediate steps). For file-type items, which are elements of standard components, the version numbers are identified by major version numbers only.

Among the items identified in the SCMP for configuration control are: the application program, the embedded software forming the basis of the platform, software forming an integrated development environment , the and verification tools), various application tools, and

documentation. Archival is performed at the end of the software version development, when all the software configuration elements are finished. An archive is a set of elements defined from an archive baseline and intended to be archived electronically. An archived baseline contains every version of every managed element regardless of its state.

The vendor archives configuration tracking by using the following elements:

- The List of Software Documents (LSD) which identifies a software version and contains the list of the documents related to this software. It is produced manually and its configuration is managed in the CM tool.
- The List of Tools and Libraries Used for Software development (LTLUS) identifies the versions of the tools and libraries used to develop the software.
- The Software Configuration Management Report (SCMR) which ensures the visibility of the software configuration. It is produced manually, and its configuration is managed in the CM tool with the other software documents. The SCMR identifies, for each software version, the changes taken into account as well as the corresponding baselines in order to ensure traceability in the CM tool. All the SCMRs for each managed component are referenced by a global SCMR.

One of the purposes of the CM tool is to manage access to the items. When a document or safety software source file is checked-out, the file is locked and no other user can check-out the file. When parallel check out is allowed (i.e., for non-safety software source files), the tool gives an alert at check-in when the item has been checked-out by multiple users. A merge function can be performed by the integrator with a merge tool provided by NOP CM.

Under the vendor's Configuration Management Process, the change control process is managed to ensure that unauthorized access and software changes of inadequate quality are prevented.

There are two types of change requests:

- Change Requests relating to changes in the client's requirements or in the purpose of the software development.

- Non-conformities in cases where the current production status has been found to deviate from the purpose of the software development.

The vendor uses the following tools to manage and track change requests and nonconformities:

- A system change management tool is used throughout the vendor organization. It is used in accordance with the vendor Procedure - Definition of Change Management Process.
- A product non-conformity management tool is used throughout the vendor organization. It is used in accordance with vendor Procedure - Nonconformities.
- A tool specific to the vendor Software group is used for change management (including change request management and software configuration management).

When a non-conformity is identified in software, a request is systematically created on the product. The request is created for the impacted software. The software anomaly resolution is identified and scheduled according to the impact of the problem and to the project status. If the non-conformity has been detected after the software validation (e.g., during interconnected tests, site tests, etc.), an analysis is also performed by the Software Method and Tools Manager in order to identify why and when the anomaly was introduced and why it has not been detected earlier. Following this analysis, improvement actions can be identified for the process, the methods, or the tools. The software improvement actions are managed in a global list. Each year, the Software Group Manager and the Software Method and Tools Manager identify the actions to be performed.

Non-conformities that represent a potential risk for safety will be handled in accordance with vendor procedure, Classified Non-Conformities, which will address the requirements in 10 CFR 21. In addition, the vendor will record equipment or parts returned to them in its [program] database.