

Board Findings

Chemistry and Metallurgy Research Replacement Facility: Congressional Certification Review

Topic: Design Control

Finding Title: Documenting and Maintaining Preliminary Documented Safety Analysis Safety-Related Functions and Requirements

Finding: The overall approach to establishing and maintaining functional and operational requirements can be found in the following CMRR documents: (1) CMRR Program Requirements Document (PRD) (CMRR-PLAN-PM-0101, Rev. 0) January 2009, (2) CMRR Functional and Operational Requirements (F&OR) (CMRR-PLAN-ENG-2801, Rev. 0) January 2009, (3) CMRR Systems Engineering Management Plan (SEMP) (CMRR-PLAN-1905, Rev. 0) September 2007, (4) CMRR Configuration Management Plan (CMP) (CMRR-PLAN-ENG-0301, Rev. 0) December 2008, and (5) CMRR Facility Design Description (FDD) (CMRR-FDD-001, Rev. 0B) January 2009.

Review of these documents indicates that requirements generated through the safety basis development process are not adequately and explicitly integrated into the overall approach to Design Control.

The Preliminary Documented Safety Analysis (PDSA) is the fundamental document that identifies safety-class (SC) and safety-significant (SS) structures, systems, and components (SSCs). Once identified, the PDSA establishes an appropriate set of safety functions (see PDSA Table 3-37), and for each safety function a set of functional requirements and performance criteria are established (see PDSA Chapter 4). The safety envelope for CMRR depends on maintaining control of these functions, requirements, and criteria. Review of the PRD, F&OR, SEM, CMP, and FDD indicates that this control has not been established.

The PRD requires that CMRR develop a SEM, and that the SEM (1) establishes the hierarchy of technical documents and demonstrates how requirements are flowed down, (2) explains how requirements are allocated down to SSCs, and (3) that commits to crosswalk the safety case for SSCs with the design features. As noted above, the PDSA establishes the safety case. Review of the SEM indicates that the systems engineering process does not include information generated from the PDSA. The SEM describes an approach that can be labeled “a classic project management approach” (top-down derivation of functions and requirements), silent on the overall roll and preeminence of requirements generated from the PDSA.

The CMRR F&OR is consistent with the PRD, largely silent on requirements generated from the PDSA. The F&OR does include a requirement (R.0.7.m) that “Prior to Title I design of the CMRR, facility design features pertaining to meeting safety, security, and quality assurance criteria shall be identified and tracked as part of the project’s technical baseline.” It is not clear that the project has met this functional requirement.

The CMRR CMP establishes the overall approach to design control, using the CORE database to establish relationships between functions, requirements, and systems. The CMP indicates that requirements from the PDSA should be explicitly incorporated in the CORE database. However, review of the CMRR FDD suggests that key safety terms such as “safety functions” and “functional requirements” may not be consistent with how this terminology is intended in the PDSA. Review of the FDD design requirements indicates that the basis for these requirements is “code/standard” driven; the link and integration from the PDSA is missing. Given this, integration between the PDSA and System Design Descriptions (SDDs) is questioned.

The CMRR CMP also establishes the overall approach to change control. It is not clear how the change control process establishes appropriate change control of the PDSA safety envelope, specifically change control of SC and SS SSCs, and their safety functions and functional requirements. The change control process should include the appropriate level of control for critical safety-related decisions (note that the

