SUNSI Review Complete
Template = ADM-013
E-RIDS=ADM-03
ADD: Jordan Hoellman

COMMENT (3)
PUBLICATION DATE:
4/14/2020
CITATION 85 FR 20725

PUBLIC SUBMISSION

As of: 4/16/20 2:19 PM
Received: April 15, 2020
Status: Pending_Post
Tracking No. 1k4-9g5b-hbjd
Comments Due: June 29, 2020
Submission Type: Web

Docket: NRC-2020-0072
Design Review Guide for Instrumentation and Controls for Non-Light-Water Reactor Reviews

Comment On: NRC-2020-0072-0001
Draft Staff Guidance: Design Review Guide for Instrumentation and Controls for Non-Light-Water Reactor Reviews

Document: NRC-2020-0072-DRAFT-0004
Comment on FR Doc # 2020-07798

Submitter Information

Name: Mark Burzynski

General Comment

I was not able to participate in the April 2nd Periodic Advanced Reactor Stakeholder Meeting. I did get a change to review the presentation material and the Draft Design Review Guide for Instrumentation and Controls Reviews for Non-LWRs. I found the document to be well organized and easy to comprehend. I will give a hearty thanks to NRC on this effort. Overall, the I&C regulatory framework is becoming more predictable and practical. I have a few ideas where I think you could make a really good document even better.

Attachments

SunPort Comments on Design Review Guide - Instrumentation and Controls for Non-Light-Water Reactor Reviews

Comments on Design Review Guide: Instrumentation and Controls for Non-Light-Water Reactor Reviews

1. Section X.0.1.2, *Objectives of Review*, identifies two tasks not shown in Figure X-1: (1) the I&C system design includes the functions necessary to assure adequate safety during operation of a nuclear power plant under normal operation, transient, and accident conditions and (2) the instrumentation and control (I&C) system safety-related functions, systems, and equipment have been properly classified, and appropriate performance as well as special treatment measures have been established. It would be helpful to shown them in the figure to clarify whether they are within the scope of the I&C review or a prerequisite for the I&C review.

2. Section X.1.1, *Systematic Assessment Review Criteria*, specifies that credible hazards and failure modes of the design be identified and controlled. In practice, credible hazards and failure modes can be grouped in four categories that are treated in different ways.

    a. Abnormal Operating Occurrences and Postulated Accidents – These hazards are typically defined by deterministic means to provide safety margins for various categories of events. These events are analyzed by conservative methods (e.g., bounding parameters) with conservative assumptions (e.g., assumed single failures and no beneficial credit for non-safety related control system actions). The protective schemes developed from the formal safety analysis of these events form the basis for the safety-related functions implemented in I&C systems.

    b. External and Internal Plant Hazards - These hazards (e.g., seismic, flood, fire, etc.) are specified at the plant level and defined by deterministic or probabilistic means. These hazards form the basis for qualification, physical separation, and isolation requirements for the safety-related I&C systems.

    c. Beyond Design Basis Events – These hazards can be specified at the plant or system level by deterministic or probabilistic means. These hazards typically form the basis for alternate mitigation capabilities that are often implemented in a graded approach (i.e., less stringent design requirements than safety-related systems.

    d. Internal I&C System Hazards - These hazards have not been consistently defined and assessed. The methods for assessing hazards from assumed single failures in safety-related systems are well understood. The methods for assessing hazards from non-safety related system interfaces and associated circuits are also understood. Use of digital I&C equipment results in additional qualification requirements (i.e., electromagnetic compatibility).

    Consideration of digital common cause failure (CCF) in safety-related systems that result in a loss of safety-related functions are generally understood and have created a new set

of beyond design basis events to be considered. However, the criteria for use of diversity and defensive design measures to address the hazards are not well defined. A direct consequence of this weakness is that late regulatory rejection of these design features can lead to rework of plant and system level requirements.

The treatment of spurious operation of digital I&C systems are not well defined or universally understood. The spurious operation hazards can result in additional Abnormal Operating Occurrences that must be evaluated by formal safety analyses due to postulated failures in shared digital I&C resources or the assessment of additional Beyond Design Basis Events due to postulated software CCFs in I&C systems. Late identification of the spurious operation hazards to be considered can lead to rework of key inputs to the I&C system design.

Figure X-1 does not show how the assessment of the four hazard categories are integrated into the I&C system review framework and how the treatment of the Internal I&C System Hazards can affect the other three categories of hazards..

3. Section X.2.2.1, *Defense-in-Depth Measures*, specifies that the degree of defense-in-depth and qualification measures should be justified as being adequate to achieve the necessary robustness and reliability of the safety functions to be performed by the I&C systems. World Nuclear Association Report No. 2018/003, *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture*, outlines significant challenges in design, licensing and cost of nuclear power plants caused by inconsistent treatment of defense-in-depth. The regulatory reviews of defense-in-depth can be made more effective by having a defined framework for lines of defense. As an example, IAEA Safety Standards Series No. SSR-2/1, Revision 1, *Safety of Nuclear Power Plants: Design*, outlines five levels of defense:

   a. prevent deviations from normal operation and the failure of items important to safety (control system),
   b. detect and control deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions (reactor trip),
   c. prevent damage to the reactor core or radioactive releases requiring off-site protective actions from postulated accidents (engineered safeguards actuation),
   d. mitigate the consequences of accidents that result from failure of the third level (sever accident mitigation), and
   e. mitigate the radiological consequences of radioactive releases that could potentially result from accidents (emergency response).

   World Nuclear Association Report No. 2020/001, *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties*, outlines difficulties that have been encountered when developing and applying safety classification for I&C systems in nuclear power plants. Clear and consistent classification and design criteria should be defined for each level of defense.

4. Section X.2.2.1.3, *Diversity in Support of Defense-in-Depth to Address CCFs*, assesses the use of diversity in I&C systems to address CCF vulnerabilities. Timeliness of regulatory reviews has been impacted in other new plant reviews due to the subjective natures of both the definition of the digital CCF vulnerabilities to be solved and the acceptance criteria for diversity strategies. These factors have also influenced the degree of stability for the

regulatory decisions. For example, two popular guidance documents (i.e., NUREG/CR-6303 and the NUREG/CR-7007) focus on addressing a full set of potential diversity attributes with no regard to their relationship or usefulness in mitigating relevant or important digital CCF vulnerabilities. The trend has been towards lengthy and more difficult reviews of the treatment of digital CCF vulnerabilities and I&C system architectures. These reviews have required more specific and detailed information about the digital review systems to support regulatory decisions. The goals of timely reviews and approvals of I&C architectures early in the system development process cannot be realized with the current regulatory framework for treatment of digital CCF. The I&C architecture design and review process would be more predictable and efficient if the guidance focused on important CCF vulnerabilities and used appropriate diversity measures to address those vulnerabilities.