United States Nuclear Regulatory Commission

Protecting People and the Environment

Expectations for Addressing U.S. EPR Non-Safety Control System Failure

Deanna Zhang

Wendell Morton

Kenneth Mott

Objective

- To discuss staff expectations regarding the resolution of non-safety control system failures in the U.S. EPR.

NOTE: This presentation provides response to questions and issues that were identified at the February I&C audit. The response is based on the staff’s present understanding of the EPR I&C system. Additional clarification will be provided as new questions and issues arise.

Background

- Within the U.S. EPR design, non-safety control systems have the capability to actuate and control both safety and non-safety related plant components.
- The non-safety control systems are software-based systems that are susceptible to a software failure. Such failures could spuriously actuate or cause malfunctions to multiple, redundant trains of safety or non-safety related components.
- Such failures should be protected against through design and/or analysis.
- Failure to do so may result in a condition that is not sufficiently protected against.

Contents of Guidance

- Criteria for credible failures that can lead to spurious actuation of safety equipment.
- Design features that can be used to reduce the likelihood of potential credible failures or to mitigate the effects of the potential credible failures.
- Acceptable analysis methods for evaluating the effects of the failures and the scope of such an analysis.

Criteria for Credible Failures

- Clause 5.6.3 of IEEE Std 603-1991 (as endorsed by 10 CFR 50.55a(h)) states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.
- Failure of redundant, fault-tolerant processors that results in spurious operation of affected safety and non-safety equipment is considered credible.

Mitigating Design Features

- Limitation functions or similarly implemented features (e.g. independent acknowledge functions, permissives, etc.) can be used to mitigate the impact of a potential hardware or software failures.
- Fault tolerance mechanisms should be implemented and well defined for both the Process Automation System (PAS) and Process Information and Control System (PICS). The ability of both systems to properly respond to faults originating in either hardware or software could help mitigate the effects of, or reduce the likelihood of, credible failures in either system.

Mitigating Design Features

- Segmentation of control functions can be used to reduce the likelihood of common cause failure. The segmentation analysis should address:
  - Any common inputs for each control function and the effects of these common inputs on inducing common triggers for latent software failures.
  - The effects from credible common cause failures are bounded by either the safety analysis or a best estimate analysis.
  - Acceptable operator response time if any manual actions are credited.
  - The level of independence between segments to demonstrate that single failures would not propagate to other segments.

Analysis Methods

- If analysis is used to address non-safety system spurious actuations, then:
  - The common cause spurious actuation of the control function should be bounded by the safety analysis as a credible failure.
  - An engineering evaluation should be performed to identify any concurrent control function failure (within the redundant, fault-tolerant processors) that could make the consequences of the spurious actuation worse.
  - If such conditions are identified in the engineering evaluation, they should be analyzed in the accident analysis (for those resulting from single failures) or a best-estimate analysis (for those resulting from software common-cause failures) to demonstrate adequate safety.

Design Information

- If limitation or segmentation design features are used, the design information should, at a minimum, address the types of diversity, independence, and fault-tolerant features utilized, taking into account common inputs, algorithms, equipment, etc.
- If segmentation is used, the safety analysis or best-estimate analysis should demonstrate adequate safety if a common-cause spurious actuation occurs.
- If analysis is used, the corresponding analyses as described in Slide 8 should be provided.

Summary

- Failures of redundant, fault-tolerant processors is considered credible.
- Limitation functions, segmentation, and analysis may be used to address common-cause spurious actuations by non-safety control systems.
- The type of design information to provide is dependent upon the approach taken.