RulemakingComments Resource

From: Samuel Miranda <sm0973@gmail.com>
Sent: Sunday, March 20, 2016 2:09 PM
To: RulemakingComments Resource
Subject: [External_Sender] Docket No. PRM-50-112, NRC-2015-0213

Public Comments

10 CFR Part 50

Docket No. PRM-50-112, NRC-2015-0213

Federal Register, Volume 81, Number 3, Page 410 (January 6, 2016)

Re: Determining Which Structures, Systems, Components, and Functions are Important to Safety

I fully support Kurt T. Schaefer's petition for rulemaking to address issues in determining which structures, systems, components, and functions are important to safety. I believe that it's time to define the term, "important to safety", in 10 CFR Part 50, perhaps in Appendix A, and refer to this definition when specifying design and performance requirements for affected structures, systems, components, and functions. I also believe that rulemaking is the proper method to establish and implement this sort of key definition. The term, "important to safety", needs to be clarified, since it is widely-applied; but little-understood, especially when used with respect to new functions and equipment (e.g., some mitigation functions that were identified as a result of the Fukushima accident).

Design requirements for structures, systems, components, and functions that are intended to prevent accidents or mitigate their consequences are designated, "General Design Criteria", and defined in Appendix A of 10 CFR Part 50. They require very high levels of reliability for equipment and systems that must deal with relatively frequent events, i.e., "anticipated operational occurrences", and for events that are in the design basis. For example, General Design Criterion 29 requires that, "The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences." These systems are in the "safety-related" category. It follows that reliability requirements would not be as high for equipment that must deal with very rare events (i.e., for events that are not expected to occur during the plant's lifetime).

Equipment and systems that are used for normal operations (e.g., load follow or pressure control) are "commercial grade". Nuclear plants are designed to tolerate failures in commercial grade systems. There are

systems that must be more reliable than commercial grade; but not as reliable as “safety-related”. Unfortunately, this is a space that is ill-defined.

Equipment and systems could be categorized as “important to safety” if failures of such equipment or systems could cause:

1 Minor transients to develop into serious accidents, or

2 Serious accidents to occur, as a direct consequence, or

3 The performance safety functions, by “safety-related” systems, to be prevented or impeded

Additionally, equipment and systems that are designed to deal with very rare events that are outside the design basis (e.g., anticipated transients without scram (ATWS) or some severe accidents that are drawn from the Fukushima experience), could be designated as “important to safety”.

The General Design Criteria, specify strict limitations for the consequences of anticipated operational occurrences (e.g., no fuel clad damage or radiological releases), and allow more serious; but still limited consequences for occurrences that are not expected to be encountered during the lifetime of the nuclear plant (about 40 to 60 years). These are based upon the principle that events that are expected to occur must not result in serious consequences, whereas events that are not expected to occur may be allowed to result in more serious; but limited consequences.

Item (1), above, is particularly significant, since failures in equipment and systems, categorized as “important to safety”, that cause the development of minor, anticipated operational occurrences, into major accidents would violate this basic principle, since it would effectively create a new class of anticipated operational occurrences that produce the serious consequences of major accidents. Safety analysis reports do not include analyses of anticipated operational occurrences that become major accidents. Consequently, prevention and mitigation measures for such situations are not established, or even identified. Recognition of this possibility, through the use of a workable definition of “important to safety”, could yield a significant improvement to plant safety.

For example, power-operated relief valves (PORVs), mounted on top of the pressurizer are valves that are designed to relieve steam, and thereby control plant pressure during normal operations; but they’re not deemed to be reliable enough to be used as accident mitigation measures. If any of these PORVs stick open (e.g., after relieving water), then a new, more serious accident is created, since the stuck open PORV becomes a hole in the pressurizer. A minor event, the spurious opening of a PORV, develops into a loss of coolant accident.