

Criscione, Lawrence

From: Criscione, Lawrence
Sent: Tuesday, May 24, 2011 8:22 PM
To: Apostolakis, George
Cc: Lui, Christiana; Ostendorff, William; Borchardt, Bill; Zimmerman, Roy; Collins, Elmo
Subject: Feedback on SRA Discussion of Risk Informed Regulations
Attachments: Draft PROS article.pdf

Commissioner Apostolakis,

I enjoyed the discussion today you had with the SRA group. I am not a Senior Risk Analyst nor am I a qualified inspector so I know very little about how we regulate. However, from incidents I have been deeply involved in while working for the licensees, I am aware of some of the challenges mentioned by the SRAs.

Roy Zimmerman has told me that "There is more to Enforcement than violations". Only Roy can tell you what he meant by that, but what I took away from that statement is that we (the NRC) can effect great change in the behaviors of the licensees even when specific violations cannot be identified. One method is through writing an Information Notice. Another is through public statements and reports.

Roy's remarks were made to me during a discussion regarding an incident I was involved with at Callaway Plant. In 2003 the operators were shutting down the plant because of a broken piece of Tech Spec required equipment. By the time they reached 10% power (at 09:36) they were more than 2 hours ahead of schedule (the Tech Specs required them to be in MODE 3 by 13:21) and repairs were progressing on the broken equipment so they stopped reducing turbine loading. In accordance with their procedures, they cycled the turbine drains. When doing so, a few of the drains failed to cycle closed.

The failed drains caused no impact on the plant. However, they coincidentally corresponded with a 22°F/hr decrease in temperature which was being caused by the buildup of Xenon-135.

Prior to 09:36, the operators had been lowering reactor power at 10%/hour and the buildup of xenon was being masked by the positive reactivity being inserted by the lowering power defect. When the operators quit lowering steam demand at 09:36, xenon was still building up but there was no power defect to compensate for it so the plant responded by creating a temperature defect. The positive reactivity being inserted from the 22°F/hour uncontrolled cooldown was making up for the negative reactivity inserted by xenon and was maintaining the reactor critical. The crew failed to recognize this; they blamed the transient on the stuck open turbine drains.

Over the next 25 minutes, average coolant temperature fell 9°F resulting in a shrink in Pressurizer water level which caused the letdown system to automatically isolate at 10:00. The 9°F drop also caused temperature to fall below the Minimum Temperature for Criticality (551°F). The crew responded by lowering turbine load to 6% rated reactor power and manually tripping the turbine at 10:12:35.

The power mismatch caused by going to zero steam demand with the reactor at 6% power caused the average coolant temperature to rapidly rise to 557°F (the temperature at which the steam dumps were set to modulate open). The large amount of negative reactivity inserted as a result of this temperature spike caused the reactor to passively shut down.

The crew was in the midst of restoring letdown flow and failed to notice the reactor shutdown. Over the next 25 minutes reactor power lowered into the source range. During this time the crew was performing ancillary tasks (e.g. restoring cooling tower blowdown, raising RCS letdown flow, lowering flow at the intake) which in no way took precedence over monitoring and controlling reactivity.

By 10:39, the reactor was in the source range with: (1) its control rods still at their last critical rod heights, (2) no Source Range Nuclear Instruments energized because the subcritical multiplication afforded by the control rods being withdrawn prevented the SRNIs from automatically energizing, and (3) no formal calculation to show that Xenon-135 levels were large enough to prevent an inadvertent reactor restarted during postulated dilution or cooldown events. Note that none of this violated any licensing commitments.

Over the next forty-five minutes the crew performed routine surveillances on the Power Range Nuclear Instruments and alignment manipulations on secondary plant equipment. Over an hour after the passive reactor shutdown (at 11:25) enough xenon had built up that the first SRNI energized, alerting the crew that they were in the source range.

Anyone who has ever operated a reactor will tell you (ask Commissioner Ostendorff his opinion) that the crew's actions indicate they were unaware the reactor had passively shut down. No operator would ever allow his reactor to passively shut down and rely on xenon to keep it subcritical while the control rods were available. No operator would prioritize restoring cooling tower blowdown over actively controlling the fission reaction in the reactor core. Captain Ostendorff knows this. Bill Borchardt knows this. Elmo Collins knows this. Roy Zimmerman knows this. Yet, like me, none of these men can prove it. You cannot prove what was in someone's mind.

Following the alarm announcing the energizing of the Source Range Nuclear Instruments, the operators took another 40 minutes to insert the control rods. During this time they continued to perform ancillary tasks (e.g. the close-out of an off-normal procedure which had been awaiting a valve line-up, more surveillances on the PRNIs, commencement of containment mini-purge). Finally at 12:04 they began inserting the control banks. This coincided with the time the Outage Control Center was expecting the reactor to be shut down. Since the Outage Control Center was never informed of the passive reactor shutdown, when the control rods were inserted just after noon they assumed that the control rods were being used to shut down the reactor; why would anyone outside the control room assume that the control rods were in fact being inserted on a reactor which had passively shut down nearly two hours earlier?

The crew never documented the incident in the plant's corrective action process.

In early February 2007 I accidentally came across the incident while doing a data review of past reactor shutdowns in support of a revision to the Reactor Shutdown procedure. I documented the incident in the plant's corrective action program and it was assigned a significance level of 4 – meaning that no investigation was needed. After spending the remainder of February attempting to get the incident addressed by the plant (I met with my entire chain of command up through Adam Heflin, the site Vice President), I brought the issue to the NRC.

Following their 2007 investigation, Region IV issued two non-cited violations: for failing to write a condition report on the 9°F temperature transient which caused the letdown isolation and for failing to log the 15 minutes of operation below the Minimum Temperature for Criticality. That's it – two non-cited violations. No mention of taking 67 minutes to recognize the passive reactor shutdown. No mention of being in the source range for 45 minutes with the control rods at their last critical rod heights and no Source Range Nuclear Instruments energized. No mention of the 40 minute delay in inserting the control banks following the alarm at 11:25. No mention of the fact that no one outside the control room was informed of the passive reactor shutdown the day it occurred. No mention of the fact the event went undocumented in the corrective action program for 40 months. No mention of the fact that it was screened as insignificant when it was documented. None of these significant facts were documented because they fall outside of regulations for which we can cite the utility. But as Roy Zimmerman has noted, there is more to enforcement than violations. We can do something about these things.

One thing we can do is to write an Information Notice documenting the event. This was done, but in the review process Region IV weeded out many of the significant facts. I've attached an article I wrote on the event for the Professional Reactor Operator Society. You can compare that article to IN 2011-02 if you wish and see everything that was left out. By the way, per our Risk Informed processes Information Notice 2011-02 should have never included the Callaway Plant event – because Xenon-135 was building up, the Δ CDF for the Callaway passive reactor shutdown was below the threshold for being of great enough risk significance to even write an Information Notice.

Another thing that can be done is to honestly speak to the press when asked about the incident. We (the NRC) must stick to the facts. But the facts are often damning enough. It's a fact that the passive reactor shutdown was not reported to upper management by the operators. It's a fact that when the incident was brought to upper management's attention forty months later they discounted it as something not needing investigation. It's a fact that the NRC investigators believe the operators were not being honest when they claimed they were aware of the passive reactor shutdown as it was occurring. There is no law or regulation which prevents us from admitting facts like these to the public. Why are we afraid too? Doing so can have profound impacts on nuclear safety. Not doing so amounts to sticking our heads in the sand and shirking our public responsibility. *"If responsibility is rightfully yours, no evasion, or ignorance or passing the blame can shift the burden to someone else."*

Yet another thing we can do is to hold a public meeting to discuss the incident when asked to do so by local interveners. We need not fear interveners; although they are often our antagonists, they can be very useful in getting the licensees to address important vulnerabilities which were not identified during the initial deterministic licensing process. Nuclear safety is effected by the licensees. It is the utility, not the regulator, who prevents accidents. It is in the utility's interest to address vulnerabilities. Unfortunately, in today's deregulated electricity markets, sometimes the utilities do not recognize their own interests until they need to publically defend their position to interveners.

I share your frustration that deterministic licensing criteria continue to dominate our regulation decades after Probabilistic Risk Assessment has matured into a more reliable and efficient tool. However, Risk Informed Regulation must recognize its limitations. Risk Informed Regulation assumes honesty. It assumes competence. It assumes professionalism. Although these assumptions are valid for the overwhelming majority of licensees, there are individuals in high places who are still willing to lie to us. We need to have tools available to deal with those cases.

Today several of the SRA's gave you feedback that it is frustrating to them that safety significant issues cannot be documented if they fall outside of the licensing bases. I agree with anyone who states that we can only write VIOLATIONS to the licensing bases, but I strongly disagree that we should not document safety significant issues which fall outside the original deterministic licensing bases. We should internally document all concerns our inspectors/analysts come across and we should share those concerns with the public when asked. Transparency will result in safety; it will result in licensees taking action to correct vulnerabilities they cannot defend to the public. The "line" we draw for safety need not match the arbitrary "line" drawn for deterministic regulation; nature does not recognize our lines.

Thank you for coming to the meeting today to query the SRA's input.

V/r,

Larry

Lawrence S. Criscione
Reliability & Risk Engineer
RES/DRA/OEGIB
Church Street Building
Mail Stop 2A07
(301) 251-7603

Human experience shows that people, not organizations or management systems, get things done.