From:	FREGONESE, Victor
To:	Alvarado, Rossnyev
Cc:	REMER, Jason; GEIER, Stephen; MUNDY, Dean
Subject:	[External_Sender] Follow up Item from July 11 Meeting
Date:	Friday, July 15, 2016 11:44:57 AM
Attachments:	Non-Concurrent Triggers (V0) 7-15.pdf

Hello Ross.

Thanks again for the very productive meeting we had this week.   I thought the dialogue between the staff and the attendees was very informative, and helped bring clarity to some key issues associated with CCF.   There were many good questions from the staff and we appreciated the open dialog. During our post meeting brief we identified one question in particular we felt necessitated a follow up response.

An excellent question was raised by Steve Arndt related to the concept of non-concurrent triggers.   We did not answer his question during the meeting as we felt some additional thought was needed. Our technical team has produced a draft which we believe responds to his question (attached). We felt it was important to share this information with you and your team for consideration.

We are not looking for a response at this time and are providing this information for potential discussion at the next workshop. We would intend to cover this and any other open questions or topics you may have from the July 11 CCF meeting. We would propose to discuss these as the first agenda item to close any lingering questions or discussion items from the previous workshop.

Thanks.

Vic Fregonese
Senior Project Manager
Nuclear Generation Division

Nuclear Energy Institute
1201 F Street, NW, Suite 1100
Washington, DC 20004
www.nei.org

M: 704-953-4544
E: vxf@nei.org

FOLLOW US ON

This electronic message transmission contains information from the Nuclear Energy Institute, Inc. The information is intended solely for the use of the addressee and its use by any other person is not authorized. If you are not the intended recipient, you have received this communication in error, and any review, use, disclosure, copying or distribution of the contents of this communication is strictly prohibited. If you have received this electronic transmission in error, please notify the sender immediately by telephone or by electronic mail and permanently delete the original message. IRS Circular 230 disclosure: To ensure compliance with requirements imposed by the IRS and other taxing authorities, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties that may be imposed on any taxpayer or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

Sent through www.intermedia.com

Non-Concurrent Triggers – Industry Notes for Discussion (DRAFT)

7-15-2016

In the July 11 CCF workshop, NRC Staff discussed with the industry team the concept of non-concurrent triggers due to different software execution trajectories and external signals for a running chiller and a standby chiller. The NRC Staff asked the following question: When the standby chiller is put into service after the defect is triggered in the first chiller, won't the standby chiller then see the same triggering conditions, resulting in a failure of both chillers, before the defect can be corrected (i.e., a CCF).

Since this is a complex issue that requires a comprehensive response, the industry team did not attempt to answer this question in the meeting. But since it is an important question that gets to the fundamental basis of non-concurrent triggers, we did want to provide the following thoughts for future discussion:

> As stated in NUREG-7007, "the IEC defines signal trajectory as the 'time histories of all equipment conditions, internal states, input signals and operator inputs which determine the outputs of a system'. Failures arising from latent faults activated by signal trajectory triggering conditions clearly correspond to conditions that either were not anticipated or properly addressed during system development and that were not exposed through testing."
>
> Systems with a structured development process, such as safety related chillers, have a rigorous assessment, design, verification and validation of signal trajectories. Therefore, it can be concluded that the signal trajectory that was not correctly considered during development and can cause a chiller failure (i.e., the design defect), is a trajectory initiated due to a rare combination of historical internal states, a rare occurrence of external inputs, or a combination of both. These are typically transient/intermittent conditions, such as an accumulation of transient memory errors, a sensor that may have recurrences of temporary out of range conditions, an unusual sequence/timing of manual or automatic state change or mode change demands that are associated with an external transient event, or a combination of completely unrelated transient internal and external conditions. The point is that, due to the comprehensive nature of a structured development process which includes a comprehensive assessment of unusual signal trajectories, the right combination of internal state histories and/or the right external inputs to trigger a software trajectory with a defect is a very rare and most often transient/intermittent condition.
>
> When the standby chiller is put into service it has a different set of internal state histories than the running chiller. This is because even though the logic/algorithm is the same in both chillers, the standby chiller has not been executing that logic as would be the case in a conventional hot-standby controller configuration, where the standby controller actually tracks the running controller to ensure a bumpless transfer. Due to divisional independence, the standby chiller also has completely different sensor inputs and manual/automatic state demand inputs. In addition, if the defect was ultimately triggered by an external transient event, that event is likely to be gone. It is unlikely for the internal state histories to accumulate in the same manner in both chillers, and also unlikely for the external transient event to occur again; having the recurrence of both internal and external conditions in combination is even more unlikely. Therefore, it is very unlikely that the same combination of internal state histories, and/or external inputs needed to trigger the defect will accumulate to occur at all, and even more unlikely that this would occur within a short time duration.

To cause a CCF, those rare and transient/intermittent internal and external states would need to accumulate in the same manner (or very similar) as they did in the running chiller. This is unlikely to occur before the original chiller failure can be diagnosed and corrected. Of course we can never claim 100% certainty of this. But the rarity of the design defect, together with the rarity of event combinations needed to trigger that defect, provides sufficient confidence to conclude that the CCF likelihood is at Level 2 (i.e., as unlikely as other sources of CCF that are not considered in deterministic safety analyses). Of course, even with the CCF likelihood at Level 2, a chiller CCF would still be considered in the PRA to the extent appropriate under risk informed guidance.

From the EPRI CCF research in 2008, there are three documented instances of digital design defects being triggered in one division or one controller, and being detected and corrected, before the same defect is triggered in an another controller to result in a CCF. That operating experience is summarized as follows:

> Operating Experience Event 1
> A plant reported a design defect in two PLCs, one in each division of hydrogen water chemistry equipment. Upon exiting a calibration procedure for a sensor connected to one PLC, the associated hydrogen water chemistry equipment tripped. It was discovered that a 60 second time delay was programmed into the PLC for allowing a controlled return to service upon completion of a calibration activity, but the calibration procedure did not describe the time delay, which timed out before the PLC was properly returned to service. The condition was detected and corrected before it could occur in both divisions of hydrogen water chemistry equipment. This is an example of a design defect common to two independent and redundant trains of equipment, but triggered in one train under the condition of calibrating one sensor. Plant procedures do not allow calibration activities to simultaneously occur on both divisions of hydrogen water chemistry equipment, thus making it very unlikely that the reported design defect would result in a CCF of both divisions.

> Operating Experience Event 2
> A plant reported a design defect in their feedwater control system. During startup testing, a tuning activity on one steam generator level control loop resulted in a loss of feedwater to that steam generator. It was discovered that a temporary high out-of-range flow condition during the tuning transient (5% step change in steam generator level setpoint at 95% power) resulted in a “bad value” assigned to the feedwater flow signal, which initiated a sequence of events that caused the control system to stop feedwater flow to the affected steam generator. The “bad value” setting was programmed into all steam generator level control loops. However, the condition was detected and corrected before it could occur in another steam generator level control loop. This is an example of a design defect common to multiple control loops, but triggered in one control loop under the condition of a temporary out of range signal in that loop. Multiple feedwater valve and/or feed pump turbine malfunctions would be required to initiate a high out-of-range flow condition on all steam generators, thus making it very unlikely that the reported design defect in the control system would result in a CCF of more than one steam generator.

Operating Experience Event 3

> A plant reported a design defect in 12 controllers, one of which was connected to MSR drain tank equipment. When a security setting was changed in the MSR drain tank controller, it locked up, resulting in loss of MRS drain tank control. Further investigation found that changing the security setting in any of the 12 controllers (all the same make, model, and firmware version) would cause a lockup condition. This is an example of a design defect common to multiple controllers, but triggered in one controller under the condition that its security setting is changed. The condition was detected and corrected before it could occur in additional control loops. It is very unlikely that security settings would be changed simultaneously in multiple controllers, thus making it very unlikely that the reported design defect could result in a CCF of more than one controller.

In each of the examples above a CCF was prevented for two reasons: (1) a trigger occurred in only one division, and (2) the trigger was of a rare and transient nature (i.e., a calibration activity, a tuning activity, and a setting change), so that it did not occur in the second division prior to corrective actions being implemented. LER 91-008-00 provides another example that illustrates the rare and transient nature of conditions that trigger design defects. This LER pertains to a design defect that momentarily delayed a reactor trip, because the reactor protection system did not correctly distinguish a rod slip transient from a controlled rod insertion. This trigger affected multiple safety divisions, because they were all in service concurrently. But due to the rare and transient nature of the event, it did not recur prior to corrective actions being implemented.