From: Mark Burzynski <mjburzynski@newcleardayinc.com>
Sent: Thursday, May 24, 2018 9:16 AM
To: Holonich, Joseph
Cc: Thomas, Brian
Subject: [External_Sender] May 24 CCF Meeting
Attachments: SECY-91-292 w Comments.pdf; 304-20239, Impacts of CCF Regulatory Requirements on Protection System Architectures.pdf; SRM-SECY-93-087 w Comments.pdf; SRP 7 BTP HICB-19 R4 w Comments.pdf; BTP 7-19 R5 w Comments.pdf; BTP 7-19 R6 w Comments.pdf

ADAMSAccessionNumber: ML18145A005
ADAMSVersionSeriesId: {F224F0F8-2509-429E-895F-ABD6411A78D6}

Dear Joe,

I joined a few minutes late. I have some general comments to be considered in this effort.

I have highlighted portions of SECY-91-292 that I think describe the original underlying concerns with the use of digital technology in plant safety systems. The concerns stemmed from lack of experience in nuclear applications, evolving technology, absence of requirements and standards related to digital-specific design aspects, and lack of guidance and standards related to software development processes. As such, the preferred approach considered at the time was to bound the consequences of a digital CCF in a black box manner, since the black box was not well defined due to the issues described above.

I think the world has changed significantly since then. There is a vast body of operational data from the global deployment of digital I&C in nuclear plants. The safety-critical platforms developed for the global nuclear market have mature design features that provide for deterministic behaviors through the use modern IEC standards. The software development process standards (both IEEE and IEC) have matured and are now widely accepted by nuclear regulatory bodies.

It also clear that the application of system-level diversity as a panacea for the digital CCF concern has resulted in more complex system architectures with no clear connection between the application of the diversity to the most relevant or important CCF vulnerabilities (see attached ANS NPIC paper). The downsides to the added complexity are not really considered in the regulatory decisions.

As such, I think the mature technology (i.e., approved platforms and the IEEE and IC standards), the EPRI preventive and limitations methodology (summarized in NEI 16-16), and modern development and test tools reduce likelihood of design errors. These fundamental changes in the state of affairs in digital I&C warrants a reassessment of SRM-SECY-93-087, BTP 7-19, and the underlying concerns that drove the conservative treatment of digital CCF some 25 years ago.

I also took a look at SRM-SECY-93-087 and BTP 7-19 with respect to potential improvements. The comments in the attached documents suggest where I think updates to SRM-SECY-93-087 would be helpful to achieve the needed improvements. The notes for BTP 7-19 R6 point to the problem areas and suggest the changes that are needed. I have also included annotated copies of prior versions of BTP 7-19 to show how the current problem evolved.

Regards,

Mark J. Burzynski, President
NewClear Day, Inc.
Telephone - 423.834.4455

NewClear Day Inc.