U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC TABLETOP EXERCISE
HVAC CHILLERS CONTROLS

August 22, 2016

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- Flowchart
- Tabletop exercise chillers controls replacement
- NRC feedback on NEI/EPRI methods

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

FLOWCHART

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital I&C

- BTP 7-19 Section A.3, definition of digital system
- SRM-SECY 93-087 requires a D3 analysis

Document the system

- BTP 7-19 Section 4.2
- System description
- Design basis
- Safety functions
- Tech Spec
- NUREG/CR-6303, Section 5

Construct a block diagram

- BTP 7-19 Section 4.1
- NUREG/CR-6303, Guideline 1

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Identify similar components

- NUREG/CR-6303, Guideline 2

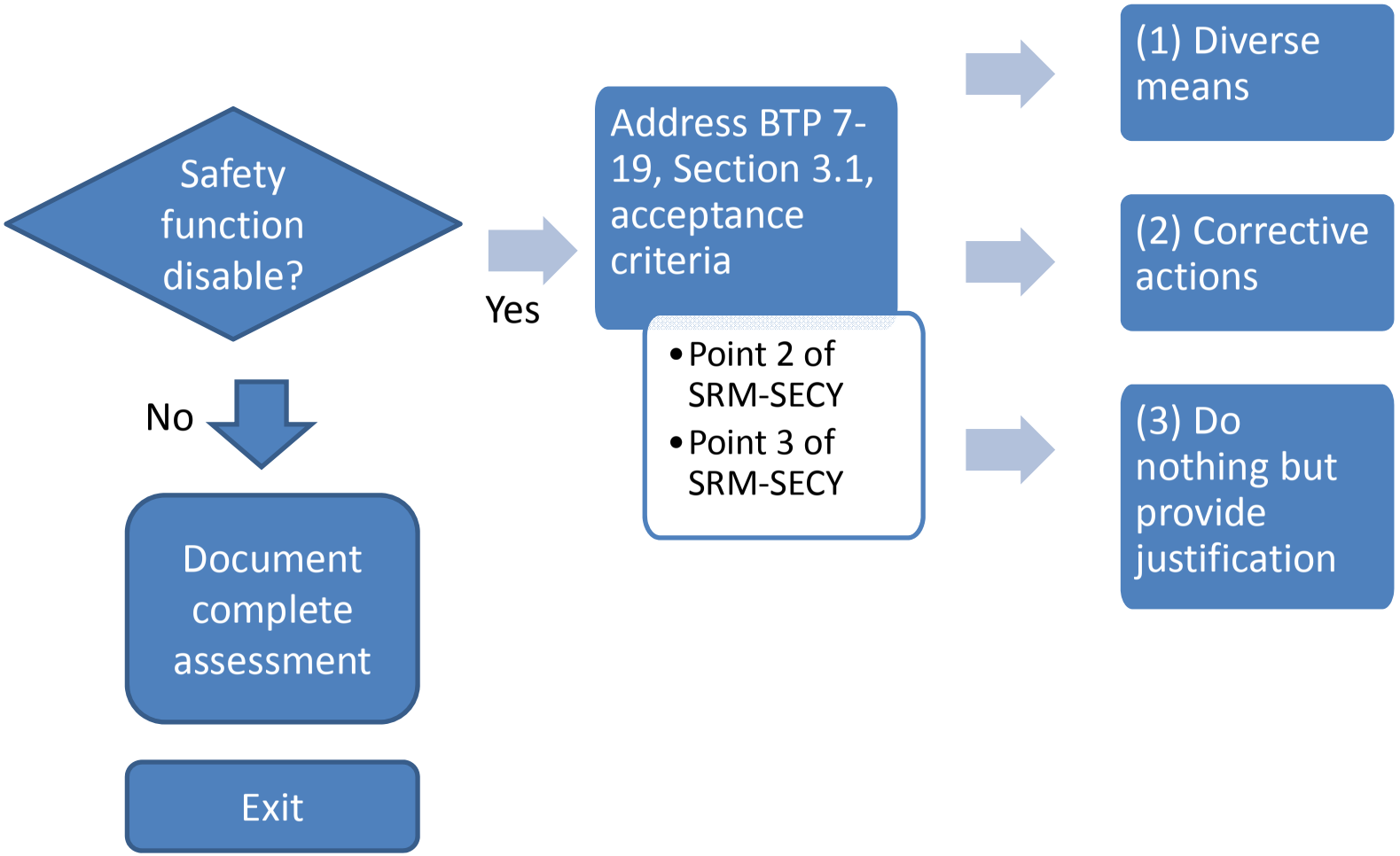
Identify CCF vulnerabilities

- NUREG/CR-6303, Guideline 6

Identify safety functions (FSAR)

- NUREG/CR-6303, Guideline 10, 11, 12

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

TABLETOP EXERCISE
CHILLERS CONTROLS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary

We believe a D3 analysis is required when installing a digital system.

How to perform this analysis is shown in the chillers control replacement described below.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Is the proposed modification using a digital equipment?

Criteria: BTP 7-19, Section A.3

- Replacement of chiller controls and chillers with digital technology
- HVAC air handling units not replaced
- Digital controls are independent from the HVAC fan controls

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Document the system - System Description

Criteria: BTP 7-19, Section 4.2, and NUREG/CR-6303, Section 5

- Consists of two independent and redundant trains that provide cooling and heating of control room air.
- Chillers are a safety related support system that maintains safety related equipment below the plant's 104°F mild environmental qualification limit.
- A single train will provide the required temperature control
- Same controls for the chillers (identical configuration)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Document the system - Safety Function

- Operations of the chiller subsystem of the Control Room HVAC
- Chillers are not modeled in new NUREG 1.200 PRA (low safety significance)
- Chillers are not an AOO or PA initiator
- A loss of both train chillers (i.e., CCF) results in continued circulation of outside air or re-circulated air for a MCR isolation
- Use of portable ventilation when chillers fail
- Heat up calculation that shows time delay to reach 104°F limit

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

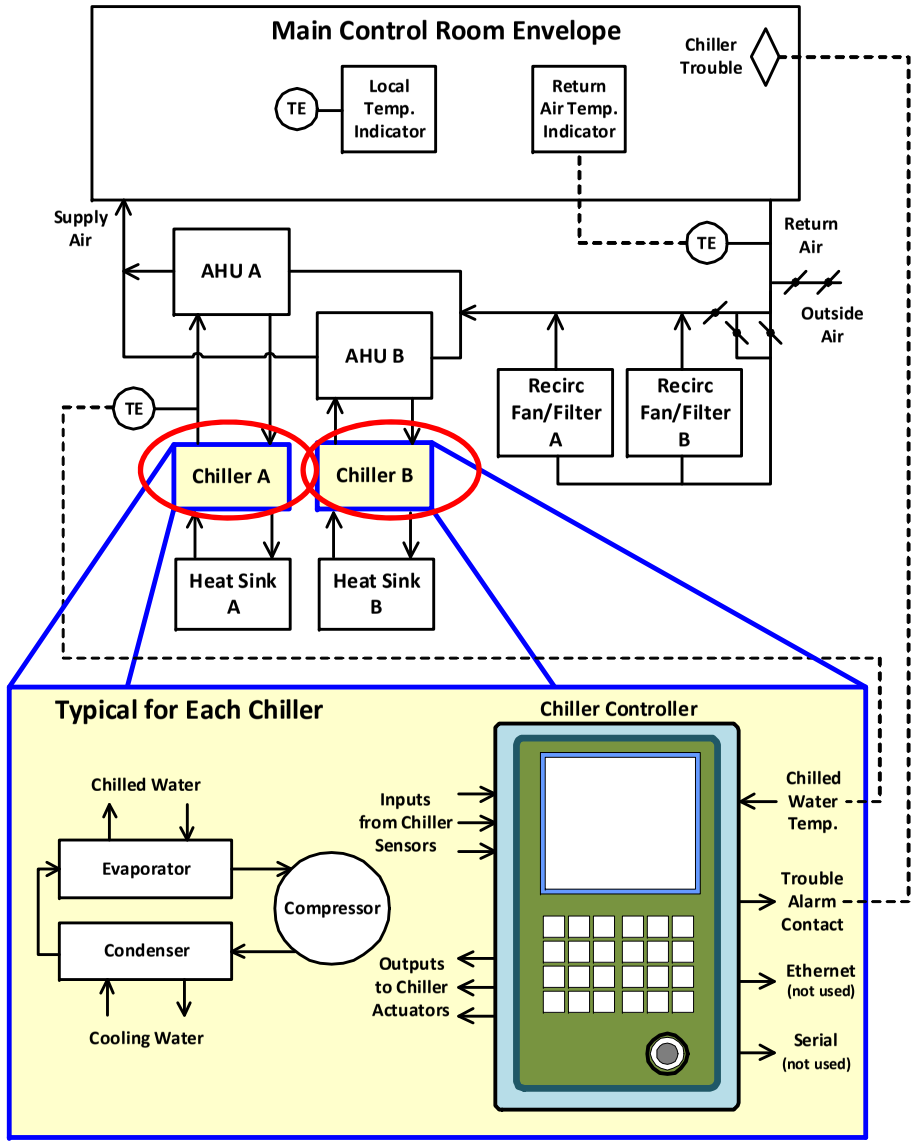
Document the system - Tech Spec

- LCO: Two independent and redundant trains of the CREATCS are required to be OPERABLE
- Action A1: With one CREATCS train inoperable, action must be taken to restore OPERABLE status within 30 days.
- Failure of both chillers (CCF) will require action B.1 (be in Mode 3).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Construct a block diagram

Criteria:
BTP 7-19 Section 4.1
NUREG/CR-6303,
Guidelines 1 and 2



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Identify CCF vulnerability

Criteria: NUREG/CR-6303, Guideline 6

- Identical controllers configuration. So design defects will affect both chillers

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Identify safety functions affected by CCF vulnerabilities

Criteria: Guideline 10, 11, and 12 of NUREG/CR-6303

- The chiller safety function is not credited in the accident analysis in Chapter 15 of FSAR
- Per analyzed event, failure of the chillers did not disable the credited safety functions of the Reactor Trip or ESFAS - (Assuming adequate indication of the chiller failure to and response by plant operators)
- Document evaluation
- Exit evaluation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC FEEDBACK ON NEI/EPRI CCF EVALUATION METHODS FOR THE CONTROL ROOM HVAC CHILLER CONTROLS TABLETOP EXERCISE

August 22, 2016

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Presentations 3 & 5: Chiller Controls Examples

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Presentation 3: Chiller Controls Example using EPRI CCF guide

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Stated Assumptions

- Chiller controls have robust design:
  - Multiple CGD methods
  - Use of EPRI TR-106439
  - SQA processes applied and documented
  - Critical Digital Review performed
  - Hazards Analysis performed
  - Significant operating experience
  - FAT performed
  - Qualification testing performed

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Stated Assumptions

- Control Room HVAC System Design
  - Uses 2- 100% Capacity Chiller Units—One Operating and One in Standby
  - Digital Chiller Controls are Independent from Control Room HVAC Air Handling Controls
  - MCR Chillers are a Safety Related Support System
  - Safety Function: Maintain Safety Related Control Room Equipment below 104 °F

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Stated Assumptions

- Failure Impact
  - Loss of Chillers not modeled in plant PRA (due to low safety significance)
  - System-level FMEA performed
  - Analysis shows significant time delay from loss of chiller to reaching 104°F
  - Loss of both Chillers triggers Tech Spec Actions to shut down both units within one hour
  - Chiller failure is not an AOO or PA initiator in Chapter 15 analyses
  - Outside air can be used as a backup, if below 100°F, and recirculation is not needed.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Problem Statement

- Plant modification placed on hold, due to:
  - "Uncertainty in technical and regulatory approach"
    - BTP 7-19 Applicability to "Inspection Guidance"
    - BTP 7-19 Only allows 2 design attributes to eliminate further consideration of software based CCFs:
      - Demonstrate it is Sufficiently Simple via 100% Testing, and
      - Demonstrate there is Sufficient Diversity

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC Staff Request

Background:

- BTP 7-19 states applicants should:
  - 1) determine sufficient diversity exists, or
  - 2) identify vulnerabilities found and corrective actions taken, or
  - **3) identify vulnerabilities and provide a documented basis justifying why it is OK to take no further action**
- Completion of a D3 Analysis would demonstrate the CCF is credible, but the consequences of a CCF can be shown to have minimal safety impact. (No new adverse safety impact.)

Clarify:

Why not complete the D3 analysis, and demonstrate the CCF can be tolerated using manual procedures and/or technical specification actions?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI-Worked
Chiller Controls Example

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Susceptibility Analysis

- Performed a susceptibility analysis. A CCF susceptibility analysis is a systematic assessment of all potential sources of CCF.
  - CCF Caused by a Single Random Hardware Failure in a Shared Resource
  - CCF Caused by an Environmental Disturbance
  - CCF Caused by an Activated Design Defect in the Operating System
  - CCF Caused by a Human Error

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Susceptibility Analysis

- CCF Caused by an Activated Design Defect in the Operating System
  - None of the (EPRI) P measures for an operating system defect are fully met
  - Use of CGD to determine quality of the OS
  - The likelihood of a CCF of both chillers due to an activated design defect is at Level 1 (EPRI methodology)
- Staff Question: What about a residual latent defect in the Application Software or its requirements?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Coping Analysis

Used best estimate methods to perform coping analysis for the CCF vulnerability identified

- The plant can cope with a loss of control room HVAC during postulated AOOs or PAs under best estimate conditions. Since there is no adverse impact to any systems credited for AOO/PA mitigation, this CCF is bounded by the events analyzed in the current deterministic safety analysis.

NRC Staff notes, however, the worked example did not really include all the details of a coping analysis (—assume this was for brevity.)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary

Industry participants stated that for this example (using coping analysis) they did not see a problem with the application of current NRC policy (defined in SRM-SECY 93-087) and guidance in BTP 7-19.

Staff agrees that the conceptual approach to the coping analysis appears adequate, (…noting that staff didn't have all the information needed to work through the details of any validation of assumptions or specific scenarios evaluated.)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC Staff View

The staff does not understand the reasons why, for this example, the control room HVAC chiller controls modification was placed “on hold.”

If the NRC I&C staff agrees that this approach is acceptable, provided a D3 analysis is adequately performed:

- What is the specific cause for any residual regulatory uncertainty?
- What specific guidance action(s) would still be needed to reduce that uncertainty?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Presentation 5: Chiller Controls Example using NEI 16-XX Guidance

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI 16-XX Example-Design Attributes

- Considered an implementation design defect
- Modified chillers configuration
- Used non-concurrent triggers argument
  - One chiller train is in operation at all times; the other train is in standby
  - The software execution trajectory in each chiller controller is different
  - Concurrent triggers is unlikely due to different configurations and external simulation
- LOOP consideration – bounded by SBO analysis

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Follow up
Non-concurrent Triggers

NRC Questions:

- 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)? Why, or why not?
- What about software failure mechanisms other than the accumulation of a set of internal states responding to external triggers?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Follow up
Non-concurrent Triggers

NEI Answer:

- Rare possibility of the right combination of internal state histories and/or the right external inputs to trigger a software trajectory with a defect
  - Different set of internal state histories for the standby chiller than the running chiller.
  - Different inputs for the standby chiller
- Therefore, 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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Follow up
Non-concurrent Triggers

NRC Staff Question:

- Staff understands this system was implemented using “Commercial Grade Dedication” processes, and the details of the software design are not fully known. There are many forms of software failure mechanisms besides internal states encountering the right triggers.
- Why is only this one mechanism addressed?
- What technical basis shows it is sufficient to demonstrate CCF can be eliminated from further consideration?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI Summary

- Industry representatives agreed that this is an area that requires further investigation
- Industry representatives stated that this example is consistent with current NRC policy (defined in SRM-SECY 93-087), but there are challenges associated with BTP 7-19

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC View

- The staff does not perceive a technical basis exists to support the non-concurrent trigger argument to eliminate software based or software logic based CCF from further consideration.
- However, in the longer term, the staff will consider proposals for technically supported analyses (other than sufficient simplicity and sufficient diversity) to eliminate CCF from further consideration.
- The staff needs more information about the industry's challenges associated with BTP 7-19, and how these challenges might be addressed in NEI 16-XX.
- The staff would like to explore the reasons why a D3 analysis for a modification like the Control Room HVAC Chiller example is considered overly burdensome.