AREVA

Presentation Topics

- Meeting Purpose and Objectives
- U.S. EPR™ Licensing Background
- I&C Analysis of Common Cause Failures
- (D3) Analysis Methodology
- Conclusion
- Path Forward

Purpose and Objectives

- Present Proposed D3 Quantitative Analysis Methodology for the U.S. EPR, submittal scheduled for November 2009
  - Present I&C analysis of common cause failures
  - Present Key Initial Conditions and Assumptions to be used in the U.S. EPR™ (D3) Quantitative Analysis Methodology
- Obtain feedback from the NRC staff on the proposed approach

Licensing Background

- June 2007.....Submittal of D3 Topical report for NRC review
- August 2007.....NRC Acceptance of D3 Topical for Review
- November 2007 .....NRC Request for Additional Information (17 questions)
- January 2008 .....AREVA Response to RAIs
- May 2008 .....NRC Second Set of RAIs (10 questions)
- June 2008 .....AREVA Response to Second RAI Request
- January 2009 .....NRC Letter – D3 Findings
- January 2009 .....AREVA/NRC Public Meeting to Discuss D3 Findings
- March 2009 .....AREVA Letter to NRC – Proposed Path Forward for D3
- April 2009 .....AREVA/NRC Public Meeting to Discuss D3 Path forward
- May 2009 .....AREVA Letter to NRC, Changed D3 Topical Report to a Technical Report, Included Qualitative D3 Analysis

BTP 7-19 Point 2 Analysis: I&C Analysis of Common Cause Failures

Shelby Small
I&C Engineering Lead – U.S. EPR DC Project
9/2/09

AREVA

Scope of I&C Presentation

- This presentation addresses the portion of the I&C analysis performed specifically to support the BTP 7-19 Point 2 plant response analysis
- This presentation is not intended to address the complete scope of BTP 7-19 (Defense-in-Depth and Diversity) and SRP 7.8 (Diverse I&C Systems)
- BTP 7-19 Point 2:
  - "...analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods."
- I&C engineering role in Point 2 analysis:
  - Identify postulated software common cause failures (SCCF) that could credibly be assumed to occur concurrent with a Chapter 15 Anticipated Operational Occurrence (AOO) or Postulated Accident (PA)
  - Establish I&C functionality that is unaffected by postulated SCCF, and can be assumed to function normally in the BTP 7-19, Point 2 best-estimate plant response analysis

I&C Analysis Overview

- Identify software common cause failures (SCCF) that could credibly be postulated to occur simultaneously with an AOO or PA
  - 3 premises form the basis for a systematic identification of credible SCCFs
- Define boundaries for effects of each postulated SCCF
  - Based on the nature of the identified vulnerability
- Identify I&C functionality that is assumed to function normally following SCCF
  - Based on the boundaries for effects of SCCF

Goal: Identify, analyze and disposition credible vulnerabilities to SCCF

Identification of Credible SCCF: Premise #1

Premise #1:

- For a CCF to occur, two conditions must be present:
  1.) An identical, latent defect must exist in multiple redundancies of a system
  2.) A triggering condition must occur, in multiple redundancies, that exposes the latent defect

- What Premise #1 means:
  - If two I&C systems do not contain identical defects, they are not subject to the same CCF
  - If two I&C systems are not subjected to the same triggering condition, they are not subject to the same CCF

- Basis for Premise #1: IEC 62340 and Draft NUREG/CR-XXXX (Diversity Strategies)

Identification of Credible SCCF: Premise #2

Premise #2:

- Only latent ***software*** defects and triggering conditions that could reveal ***software*** defects are considered for the BTP 7-19, Point 2 analysis

- What Premise #2 means:
  - Hardware design defects are not considered
  - Triggering conditions that could only reveal hardware defects are not considered

- Basis for Premise #2: BTP 7-19
  - "The above four point position is based on the NRC concern that software design errors are a credible source of common-cause failures. Software cannot typically be proven to be error-free and is therefore considered susceptible to common-cause failures because identical copies of the software are present in redundant channels of safety-related systems."

Identification of Credible SCCF: Premise #3

Premise #3:

- **A triggering condition un-related to occurrence of AOO or PA will not reveal a latent defect simultaneously with occurrence of AOO or PA**

- **What Premise #3 means:**
  - **Only Triggering conditions that could credibly exist concurrent with an AOO or PA, and latent defects that could be revealed by these triggers are considered in the BTP 7-19, Point 2 analysis**

- **Basis for Premise #3:**
  - **SCCF (latent defect in multiple redundancies revealed by a corresponding trigger) in a TXS system is a *rare event*; 140,000,000+ TXS processor hours with no such failure occurring…**
  - **A postulated TXS SCCF (extremely rare) concurrent with an AOO or PA is an *extremely rare event* (the SCCF must occur in a very small, specific window of time)**
  - **A postulated TXS SCCF, concurrent with an AOO or PA, where the SCCF trigger is unrelated to occurrence of the AOO or PA is an *incredible event* that is not considered**

Identification of Credible SCCF: Premise #3 (continued)

- **Triggering conditions can be placed into one of two broad categories:**
  - **Non-plant event trigger (e.g., EMI/RFI)**
  - **Plant event trigger (AOO or PA)**
- **Latent software defects can be placed into one of two broad categories:**
  - **Revealed by non-plant event trigger**
  - **Revealed by plant event trigger**

	Latent error: Revealed by non-plant event trigger	**Latent error:** Revealed by plant event trigger
Trigger: "non-plant" event	Rare Event 1: Outside scope of Point 2 analysis	Not compatible
Trigger: plant event	Not compatible	Rare Event 2: In scope for point 2 analysis

- **Rare Event 1: Occurs during normal operation; results in system lockup or spurious actuation (self-revealing)**
- **Rare Event 2: Occurs during AOO or PA; results in loss of function credited to mitigate AOO or PA**

AREVA

Identification of Credible SCCF: Defects and Triggering Conditions

- It is not possible to identify all specific defects that could be introduced into a design
- It is not possible to identify all specific triggering conditions that could occur during system operation

However…

- It is possible to comprehensively identify bounding *sources* of defects and bounding *categories* of triggering conditions
  - Sources of latent defects are identified based on the digital I&C system life-cycle
  - Categories of triggering conditions are identified based on Section 2 of Draft NUREG/CR on diversity strategies, and on digital system properties

Then…

- A matrix is constructed to identify all possible combinations of sources of defects and categories of triggering conditions

Example Defect/Trigger Combination Matrix

Note: This is an example to illustrate the concept. The finalized matrix will be included in the D3 technical report submittal (Nov. 2009).

Source of Latent Defect

Category of Triggering Condition	Incorrect specification of I&C system functional requirements	Incorrect specification of I&C system performance requirements	Inadequate seismic requirements	Inadequate environmental requirements (temp. humidity, etc.)	Inadequate EMI/RFI requirements	Incorrect implementation of functional requirements	Incorrect implementation of performance requirements	Incorrect implementation of environmental requirements	Incorrect integration of software and hardware	Overly complex system architecture	Complicated interactions between systems	Incorrect setpoint, parameter or software version loaded on processor
Maintenance (e.g., bypass of multiple redundancies simultaneously)												
Input signal Trajectories (plant conditions or manual inputs)												
Specific sequences of internal states												
Equipment aging												
Data communication timing mechanism												
System internal timing mechanism												
Seismic events												
Extreme temperature, humidity												
EMI/RFI												

AREVA

Identification of Credible SCCF: Premise #2 Applied

Note: This is an example to illustrate the concept. The finalized matrix will be included in the D3 technical report submittal (Nov. 2009).

Source of Latent Defect

Category of Triggering Condition

	Incorrect specification of I&C system functional requirements	Incorrect specification of I&C system performance requirements	Inadequate seismic requirements	Inadequate environmental requirements (temp. humidity, etc.)	Inadequate EMI/RFI requirements	Incorrect implementation of functional requirements	Incorrect implementation of performance requirements	Incorrect implementation of environmental requirements	Incorrect integration of software and hardware	Overly complex system architecture	Complicated interactions between systems	Incorrect setpoint, parameter or software version loaded on processor
Maintenance (e.g., bypass of multiple redundancies simultaneously)												
Input signal Trajectories (plant conditions or manual inputs)												
Specific sequences of internal states												
Equipment aging												
Data communication timing mechanism												
System internal timing mechanism												
Seismic events												
Extreme temperature, humidity												
EMI/RFI												

Triggering condition eliminated; inability to reveal a software defect (Premise #2)

Source of defect eliminated; inability to cause a software defect (Premise #2)

AREVA

Identification of Credible SCCF: Premise #3 Applied

Note: This is an example to illustrate the concept. The finalized matrix will be included in the D3 technical report submittal (Nov. 2009).

Source of Latent Defect

Category of Triggering Condition	Incorrect specification of I&C system functional requirements	Incorrect specification of I&C system performance requirements	Inadequate seismic requirements	Inadequate environmental requirements (temp. humidity, etc.)	Inadequate EMI/RFI requirements	Incorrect implementation of functional requirements	Incorrect implementation of performance requirements	Incorrect implementation of environmental requirements	Incorrect integration of software and hardware	Overly complex system architecture	Complicated interactions between systems	Incorrect setpoint, parameter or software version loaded on processor
Maintenance (e.g., bypass of multiple redundancies simultaneously)												
Input signal Trajectories (plant conditions or manual inputs)												
Specific sequences of internal states												
Equipment aging												
Data communication timing mechanism												
System internal timing mechanism												
Seismic events												
Extreme temperature, humidity												
EMI/RFI												

Triggering condition eliminated; not concurrent with AOO or PA (Premise #3)

AREVA

Identification of Credible SCCF: Simplified Matrix

- **The matrix is simplified after application of Premises #2 and #3**

Note: This is an example to illustrate the concept. The finalized matrix will be included in the D3 technical report submittal (Nov. 2009).

Source of Latent Defect

Category of Triggering Condition	Incorrect specification of I&C system functional requirements	Incorrect specification of I&C system performance requirements	Inadequate EMI/RFI requirements	Incorrect implementation of functional requirements	Incorrect implementation of performance requirements	Incorrect integration of software and hardware	Overly complex system architecture	Complicated interactions between systems	Incorrect setpoint, parameter or software version loaded on processor
Input signal Trajectories (plant conditions or manual inputs)									
Specific sequences of internal states									
Data communication timing mechanism									
System internal timing mechanism									

AREVA

Identification of Credible SCCF: Defect/Trigger Compatibility

- **If the source of the defect is such that it could not logically be revealed by a given triggering condition, the combination is eliminated**
- **The remaining combinations are vulnerabilities to be considered in scope of BTP 7-19 Point 2**

Note: This is an example to illustrate the concept. The finalized matrix will be included in the D3 technical report submittal (Nov. 2009).

Source of Latent Defect

Category of Triggering Condition	Incorrect specification of I&C system functional requirements	Incorrect specification of I&C system performance requirements	Inadequate EMI/RFI requirements	Incorrect implementation of functional requirements	Incorrect implementation of performance requirements	Incorrect integration of software and hardware	Overly complex system architecture	Complicated interactions between systems	Incorrect setpoint, parameter or software version loaded on processor
Input signal Trajectories (plant conditions or manual inputs)	1			2					3
Specific sequences of internal states		4			5				
Data communication timing mechanism		6			7	8	9	10	
System internal timing mechanism		11			12	13			

= Combination of defect + trigger ruled out from BTP 7-19 Point 2 analysis consideration due to incompatibility.

= Identified vulnerability

AREVA

Establishing Boundaries of Effects

- The assumption is made that each identified vulnerability exists in the protection system and results in no PS response to AOO or PA
  - However, many of the identified vulnerabilities would only affect a single PS function; the remainder of the PS would function correctly
  - With few exceptions, the assumption that no PS functions respond to the AOO or PA is conservative
- Premise #1 is used to define boundaries for the effects of each identified vulnerability
  - Example: An identical vulnerability with the source of defect "overly complex system architecture" does not exist in two systems with fundamentally different architectures.
- I&C functionality that is outside the boundaries of effects is assumed to function normally for the BTP 7-19 Point 2 analysis

Identification of I&C functionality assumed to function normally following SCCF

- I&C functionality that is outside the boundaries of effects is assumed to function normally for the BTP 7-19 Point 2 analysis

- Preliminary result:

Identified PS vulnerabilities to SCCF concurrent with AOO or PA do not affect functions outside of the PS if those functions do not rely on a PS output

U.S. EPR™ Diversity and Defense-in–Depth (D3) Analysis Methodology

Ben Stitt
Advisory Engineer
U.S. New Plants Process Department

NRC September 2, 2009

AREVA

D3 Perspective

- A software common cause failure (SCCF) of the digital Protection System (PS) is postulated
  - The SCCF is due to a latent software error in all redundant divisions of the PS that is triggered by an Anticipated Operational Occurrence (AOO) or a Postulated Accident (PA)
  - Failure of the PS is due to a common cause software failure; it is <u>not</u> a single failure
  - The Postulated SCCF is a low probability event and is evaluated as a *Beyond Design Basis Event (BDBE)*
  - The D3 Analysis is performed using best estimate (BE) Methods

D3 Analysis Methodology

▶ D3 Analysis Using Best Estimate Approach

- ◇ Use NRC approved SRELAP5 code for plant system response
  - FSAR models adapted for BE analyses

- ◇ Normal operating plant systems not actuated by PS remain available

  -Examples:

  - Main Feedwater Control is available and in automatic
  - Main Steam System is operating normally, including Turbine Bypass System
  - Other plant support systems continue to operate normally (HVAC, Component Cooling Water, etc…)

D3 Analysis Methodology (cont.)

▶ D3 Analysis Using Best Estimate Approach (cont.)

◇ **Plant Initial Conditions**

- Plant is operating at nominal conditions; rated reactor power, temperature and pressure
- All control rods withdrawn
  - Control rod withdrawal and rod ejection events evaluated from PDIL (Power Dependent Insertion Limit) to enable event
- BE neutronics parameters and power distributions
  - Includes BE core decay heat
  - Equilibrium cycle basis

D3 Analysis Methodology (cont.)

▶ D3 Analysis Using Best Estimate Approach (cont.)

◇ **Plant End State**

- Post-trip mitigation actions completed
- Plant in stable controlled condition (e.g., Hot Standby for non-LOCA events)

◇ **Basic Analysis Assumptions**

- No concurrent Loss of Offsite Power (LOOP)
- No "additional" Single Failures postulated
- No concurrent Preventive Maintenance
- No stuck Control Rods
- Nominal control and trip setpoints
- No manual operator actions credited before 30 minutes (without justification)

D3 Analysis Methodology (cont.)

▶ BTP 7-19 Acceptance Criteria

- ◇ AOOs: Radiological releases less than 10% of 10CFR100 limits
- ◇ PAs: Radiological releases less than 100% of 10CFR100 limits
- ◇ Integrity of the primary coolant pressure boundary maintained
- ◇ Integrity of the containment maintained

D3 Analysis Methodology (cont.)

▶ AREVA U.S. EPR™ D3 Analysis Targets

- ◇ AOOs: Preliminary conservative target
  - Show that DNB (Departure from Nucleate Boiling) will not occur; therefore, FSAR radiological dose analysis remains bounding
- ◇ PAs: Preliminary conservative target
  - Show that fuel failures in FSAR remain bounding; therefore, FSAR radiological dose analysis remains bounding
- ◇ Maintain peak RCS pressures below 120% of design pressure (consistent with ATWS)
- ◇ Maintain containment pressure below structural integrity limit for ultimate pressure capacity (consistent with SRP 3.8.1)

Chapter 15 Event Evaluation

- **Evaluation Approach**
  - All FSAR Chapter 15 events evaluated
  - Events dispositioned into categories
    - Event is bounded by another event of the same type (i.e., same SRP section) based on qualitative arguments
    - Event is analyzed to demonstrate that acceptance criteria are satisfied
- **Event Example Selection**
  - Examples selected that cover a representative spectrum of events involving different process parameters and mitigation requirements

Chapter 15 Events, Examples

- **15.1.3 Increase in Steam Flow – Calculation Performed**
  - PS protection primarily from low DNB reactor trip (RT)
  - DAS protection primarily from high neutron flux RT
    - Will cause increased peak core power compared to FSAR analysis
  - Calculated to confirm DNB ratio limits not exceeded
    - BE analysis assumptions greatly increase DNB ratio margin
  - Post-RT response is controlled by normal process system operation

- **15.2.2 Turbine trip – Qualitative Argument**
  - PS protection primarily from RT on high RCS pressure
  - DAS protection primarily from RT on high RCS pressure
    - DAS setpoint selected to allow PS actuation first, while providing adequate protection
  - RCS pressure limit not challenged
  - Post-RT response is controlled by normal process system operation

Chapter 15 Events, Examples (cont.)

▶ 15.3.2 Complete loss of RCS flow – Calculation Performed

- ◇ PS protection from RT on low ~~RCS flow~~ RCP speed
- ◇ DAS protection from RT on low RCS flow
- ◇ Calculated to confirm adequate DNB ratio margin
  - DAS setpoint selected to allow PS actuation first, while providing adequate protection
  - BE analysis assumptions greatly increase DNB ratio margin
- ◇ Post-RT response is controlled by normal process system operation

Chapter 15 Events, Examples (cont.)

- **Section 15.6.5 Loss of Coolant Accidents (SBLOCA) – Combination of Qualitative Argument and Calculation**
  - PS protection
    - RT on low RCS pressure
    - SIS actuation on low RCS pressure
  - DAS protection
    - RT on low RCS pressure
      - DAS setpoint selected to allow PS actuation first, while providing adequate protection
    - SIS actuation on low RCS pressure
      - DAS setpoint selected to allow PS actuation first, while providing adequate protection
  - BE model assumptions
    - BE decay heat and break flow model
    - All four MHSI trains available
    - Partial cooldown by Turbine Bypass System (Automatic MSRT actuation not available with postulated PS failure)
      - Reduces RCS pressure to below MHSI cutoff pressure
  - FSAR analysis bounding for peak cladding temperature (PCT)

Chapter 15 Events, Examples (cont.)

- **Section 15.6.5 Loss of Coolant Accidents (SBLOCA) – Combination of Qualitative Argument and Calculation (cont.)**
  - ◇ No automatic RCP trip included in DAS
  - ◇ Calculated to confirm manual RCP trip is acceptable
    - Cover full break spectrum of SBLOCAs
    - Cover manual trip times up to 30 min
  - ◇ Post-RT response is controlled
    - Heat removal by steam generators (MFW, turbine bypass)
    - RCS makeup by MHSI/LHSI
    - Containment isolation by DAS
    - Manual main control room HVAC re-alignment

Overall D3 Conclusions

- AREVA D3 Analysis Methodology is systematic and comprehensive
- Analysis is consistent with BTP 7-19 and DI&C-ISG-02
- Results of Analysis Methodology will provide a basis for design of an effective diverse actuation system (DAS)
- Docketed analysis (November 2009) will provide a basis to close D3 issue

Next Steps

- Complete the D3 analysis and submit November 2009
- Meet in early January 2010 to address any NRC review questions