ELECTRIC POWER RESEARCH INSTITUTE

Generation of Risk Insights from PRA to Address Digital I&C Issues

NRC / Industry Meeting

Digital I&C

July 11, 2007

PRA Task Work Group
Problem Statement 2

Using current methods for PRAs, NRC has not determined how or if risk-insights can be used to assist in the resolution of specific key digital system issues licensing action requests.

Industry is developing a white paper that addresses:

- Modeling digital I&C with current techniques
- Consistency with current regulatory policy
- Example applications for which existing PRAs could be used in designing and operating digital I&C systems
- Simplified/screening techniques for generating risk-insights

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights Using Current PRA Methods

- Modeling digital I&C with current techniques
  - Rely heavily on white paper for problem statement 1
    - Assure the functional effects of digital CCF is modeled between
      - Control systems and mitigating systems
      - Redundant mitigating systems
    - Estimate digital I&C failure probability from
      - Operating experience
      - Systematic review of defensive measures
      - Consensus standards
    - Perform sensitivity studies to show results are not sensitive to digital I&C modeling

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights Using Current PRA Methods

- Provide a discussion on how generation of risk-insights from existing PRAs is consistent with current regulatory policy, e.g.
  - Regulatory Guide 1.174 and 1.177
  - Regulatory Guide 1.200 and 1.206
  - PRA Policy Statement
  - National Academy of Sciences Report on digital I&C
  - Various sections of the SRP
  - SRM for SECY 93-087

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights Using Current PRA Methods

- Provide a listing of example applications for which existing PRAs could be used in designing and operating digital I&C systems.
  - Optimizing the digital I&C system architecture in context with the overall plant design
  - Performance of D3 evaluations
  - Staff review of digital I&C submittals

Today's presentation will focus on example applications of PRA to digital I&C issues.

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights Using Current PRA Methods

- Provide a white paper on simplified techniques for deriving risk-insights from PRA.
  - Screening approach to identify what accident sequences and functions are most affected by digital CCF
  - Identification of key plant design features that keep the risk from digital failures low
  - Identification of what digital system diversity attributes and defensive measures are most important in the maintenance of acceptable risk.

© 2007 Electric Power Research Institute, Inc. All rights reserved.

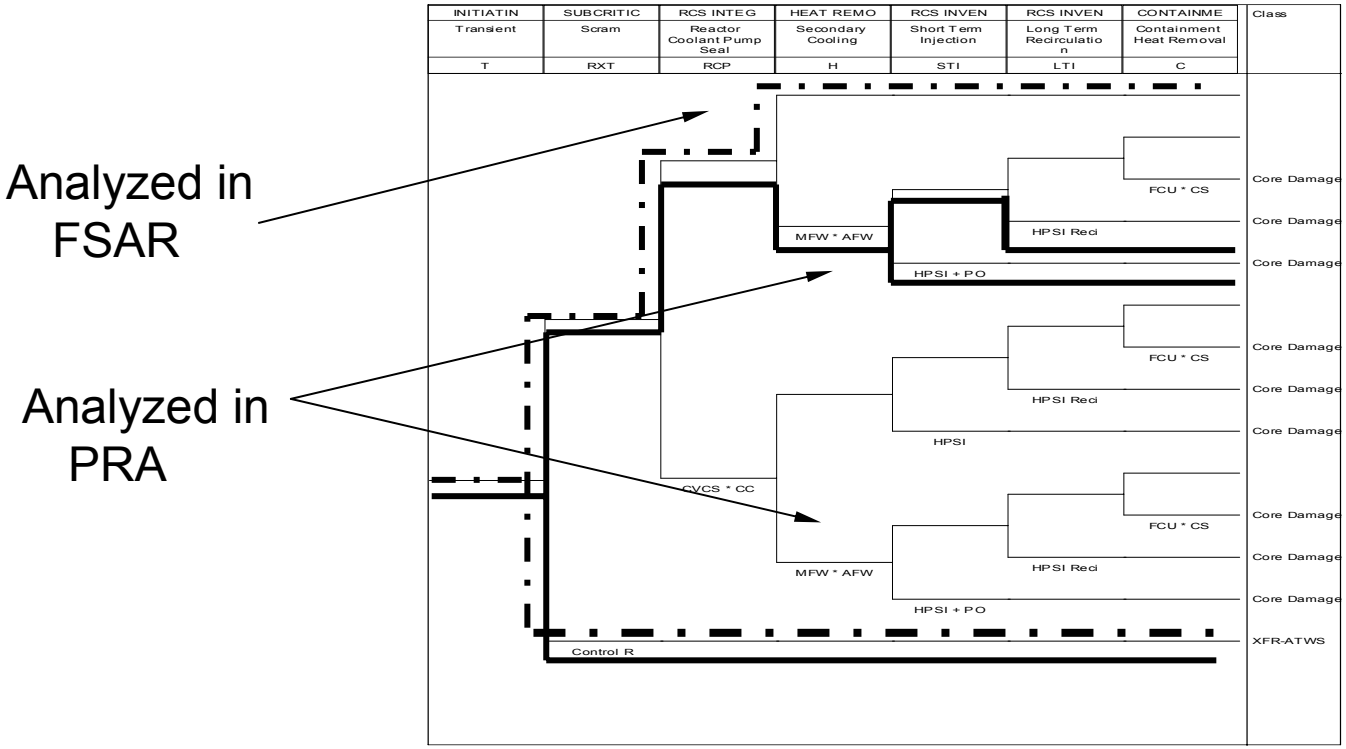
Generation of Risk Insights from PRA to Address Digital I&C Issues

Optimizing the digital I&C system architecture in context with the overall plant design

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Optimizing the digital I&C system architecture Why bring in the PRA?

- Risk significant 'beyond design basis' accident sequences are not evaluated under BTP-19



- Inordinate focus on low frequency low risk significant accidents under BTP-19 simply because they are difficult to address

© 2007 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Optimizing the digital I&C system architecture
Why bring in the PRA?

Example Results: CDF

BTP-19 criteria would be met by providing a single system that was diverse from the cause of the initiating event

PRA results would not necessarily support the conclusion that this is enough

Loss of FW

F_{IE} = 8.0E-2/yr

P_{df} = 1E-4/d

CDF = 5.1E-7/yr

Mitigating System Design	β_{cc}		
	1.0	0.1	0.01
1 system diverse from IE	1.6E-05	1.0E-05	9.6E-06
2 systems diverse from IE (but not each other)	8.7E-06	1.5E-06	8.2E-07
DAS for one system	8.2E-07	7.5E-07	7.4E-07
Op Action for both systems	7.4E-07	6.7E-07	6.6E-07
2 systems diverse from IE (and each other)	6.9E-07	6.9E-07	6.9E-07

The vendors generally provide a design that exceeds BTP-19 criteria

Medium LOCA

F_{IE} = 4.0E-5/yr

P_{df} = 1E-4/d

CDF = 1.42E-7/yr

Mitigating System Design	β_{cc}		
	1.0	0.1	0.01
2 systems diverse from IE	1.46E-07	1.43E-07	1.43E-07
DAS for one system	1.42E-07	1.42E-07	1.42E-07
2 systems diverse from IE (and each other)	1.43E-07	1.43E-07	1.43E-07

Current regulatory criteria would likely result in a design that had little impact on safety

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Optimizing the digital I&C system architecture Where do the industry/NRC currently stand?

- New Plants (DC/COL)
  - Already having an influence on the design of the digital I&C system
    - RG 1.206, C.I.19.2 'Uses of PRA and Severe Accident Evaluations'
    - Vendors have access to the PRAs
- Current Plants (Digital Upgrades)
  - Until recently, use of the PRA has been discouraged by the regulator
  - PRAs are developed and maintained by the utilities, vendors do not have ready access

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights from PRA to Address Digital I&C Issues

Use of PRA in D3 Evaluations

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights from PRA

- Risks and Benefits of DAS
  - Events requiring operator action within 30 minutes
    - Begin analysis with Large LOCA
    - Expand analysis to evaluate other applicable initiating events
- What Should Be the Scope of D3 Evaluations?

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights

- Description of the Example Plant

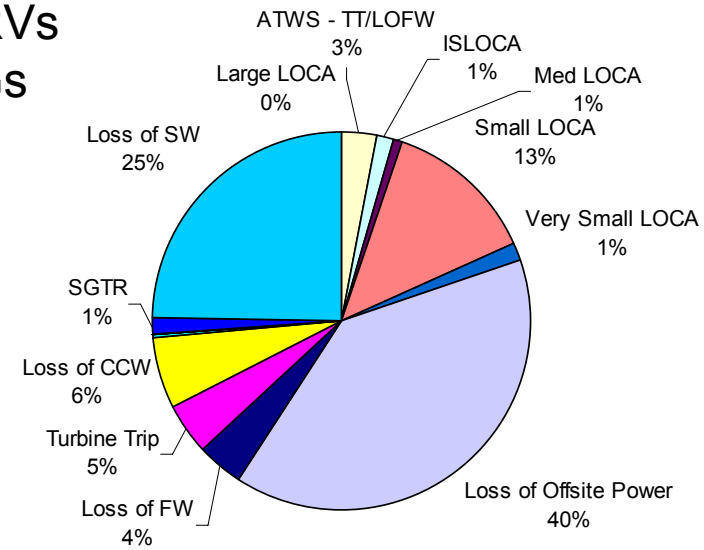
Mitigating Systems

- 4 SGs/loops
- 2 turbine MFW pumps/
  1 startup FW pump
- 3 Condensate pumps
- 2 motor AFW/
  1 turbine AFW pump
- 2 SI pumps/
  2 Charging pumps
- 2 RHR pumps
- 2 PORVs
- 2 EDGs

- PRA

18 initiating events,

~200 accident sequences



© 2007 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Generation of Risk Insights from PRA to Address Digital I&C Issues

Diverse Actuation System (DAS) for Large LOCA

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

a) Specific objectives that the proposed action is intended to achieve.

Address risks associated with

- Large LOCA
- coincident digital CCF of Safety Injection Actuation

b) General description of the activity that the licensee would be required to perform to implement the proposed action.

Provide '…an independent and diverse automated backup, achieving the same or equivalent function,...'

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

c) potential change in risk to the public from accidental offsite releases

$$\Delta \text{ Risk} = F_{LLOCA} \times P_{digital} \times P_{cont} \times Dose_{offsite}$$

F_{LLOCA} - Frequency of conditions leading to Large LOCA
$P_{digital}$ - ESFAS failure probability (digital CCF)
P_{cont} - Conditional containment failure probability
$Dose_{offsite}$ - Offsite dose given Large LOCA with no ECCS and failure of containment

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

c) Potential change in risk (continued)

Available sources of information:

F_{LLOCA} - NUREG/CR-5750 (Rate of Initiating Events at U.S. Nuclear Power Plants)

$P_{digital}$ - Perform sensitivity analysis over a wide range

P_{cont} - Level II PRA

$Dose_{offsite}$ - Plant specific PRA, SAMA, NUREG-1150

For acceptance criteria, use NUREG/BR-0058 (Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission)

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

c) Potential change in risk (continued)

F_{LLOCA} - NUREG/CR-5750
PWRs 5E-6/yr

$P_{digital}$ - Perform sensitivity analysis over a wide range

Assume initial value of 10^{-4}/demand

$\Delta CDF = 5E\text{-}6/yr * 10^{-4} < 1E\text{-}9/yr$

For acceptance criteria, use NUREG/BR-0058, Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

- Are there any risks associate with

  '…an independent and diverse automated backup, achieving the same or equivalent function,…'?

- ESFAS (SI function)
  - Actuate low head safety injection
  - Actuate high head safety injection (including charging)
  - Initiate MSIV closure
  - Initiate feedwater isolation
  - Backup reactor trip signal
  - Isolate turbine building cooling auxiliaries
  - Isolate containment cooling auxiliaries
  - Other???

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

- How frequent are trips due to spurious ESFAS?

  From NUREG/CR-5750:

  General transient frequency for PWRs is 1.2/yr

  Spurious ESFAS that lead to reactor trip – 36events/1725 gen trans or about 0.025/yr

- If a DAS (with a similar reliability to ESFAS) were to be installed capable of 'the same or equivalent functions'

$$\Delta CDF_{Spur\ DAS} = IE_{Spur\ DAS} * CCDP_{LOFW}$$
$$= 0.025/yr * 6E\text{-}6$$

$$\mathbf{\Delta CDF_{Spur\ DAS} = 1.5E\text{-}7/yr}$$

where

$\Delta CDF_{Spur\ DAS}$ – Increase in CDF due to additional reactor trips

$IE_{Spur\ DAS}$ – Initiating event frequency for spurious DAS

$CCDP_{LOFW}$ – Conditional core damage probability for Loss of FW

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Large LOCA)

- Sensitivity Studies

$$\text{Risk/Benefit}_{DAS} = \frac{(IE_{Spur\ DAS})}{(IE_{LLOCA})} \frac{(CCDP_{Spur\ DAS})}{(P_{digital})}$$

$IE_{Spur\ DAS}$ is a factor of 5000 greater than IE_{LLOCA}

$CCDP_{Spur\ DAS}$ is a factor of 25 less than $P_{digital}$

Do we believe that $P_{digital}$ is as high as 0.1 or that $IE_{Spur\ DAS}$ can be driven down in frequency by more than a factor of 1000?

- Perhaps there are other benefits to a DAS for safety injection beyond that for Large LOCA.

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights from PRA to Address Digital I&C Issues

Diverse Actuation System (DAS) for Operator Actions Taken in Response to Digital CCF within 30 minutes

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Op Act w/in 30m)

a) Specific objectives that the proposed action is intended to achieve.

Address risks associated with

- Any transient or accident requiring operator action within 30 min
- In response to a coincident digital CCF

b) General description of the activity that the licensee would be required to perform to implement the proposed action.

"In those instances where the protective action is required in less than 30 minutes, an independent and diverse automated backup, achieving the same or equivalent function, should be required."

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Op Act w/in 30m)

c) potential change in risk to the public from accidental offsite releases

Event Name	IE Frequency	Op Act <30m
Large LOCA	5.0E-06	Y(1)
Med LOCA	4.0E-05	Y(1)
Small LOCA	5.0E-04	
Very Small LOCA	4.4E-02	
SGTR	8.0E-03	
ISLOCA	1.7E-07	
Loss of Offsite Power	3.9E-02	
Loss of FW	8.1E-02	
Turbine Trip	1.9	
Loss of SW	4.7E-05	
Loss of CCW	6.4E-05	
Loss of DC Div I	1.8E-03	
Loss of DC Div 2	1.8E-03	
MSLB Outside Cont	1.8E-04	Y(2)
MSLB Inside Cont	8.7E-05	Y(2)
ATWS - LOSP	8.9E-08	Y(3)
ATWS - TT/LOFW	6.2E-06	Y(3)

All identified operator actions in this evaluation are those that would affect the outcome of the PRA. (There may be other operator actions in the safety analysis that are not considered important to the PRA)

(1) Operator action to initiate SI not credited in this PRA

(2) Success of operator action to isolate affected SG is implicit in the PRA (failure to take this action results in a lower CDF)

(3) Accident sequence already includes a DAS (diverse RTS)

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Op Act w/in 30m)

c) Potential change in risk (continued)

One additional event has been identified that would require a DAS (Medium LOCA). Other initiators would also require a DAS (e.g., MSLB), but the PRA indicates that there are no beneficial effects from a CDF perspective.

$F_{Med\ LOCA}$ - NUREG/CR-5750
PWRs 4E-5/yr

$P_{digital}$ - Perform sensitivity analysis over a wide range

Assume initial value of 10^{-4}/demand

$\Delta CDF = 4E\text{-}5/yr * 10^{-4} = 4E\text{-}9/yr$

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (DAS for Op Act w/in 30m)

- Sensitivity Studies

$$\text{Risk/Benefit}_{DAS} = \frac{(IE_{Spur\ DAS})}{(IE_{LLOCA} + IE_{MLOCA})} \frac{(CCDP_{Spur\ DAS})}{(P_{digital})}$$

$IE_{Spur\ DAS}$ is more than a factor of 500 greater than $IE_{LLOCA+MLOCA}$

$CCDP_{Spur\ DAS}$ remains a factor of 25 less than $P_{digital}$

Do we believe that digital systems are one to two orders of magnitude less reliable than comparable analog equipment or that $IE_{Spur\ DAS}$ can be driven down in frequency by a factor of 100?

The reduction in risk from the addition of accident sequences in which the operator has less than 30m to act does not appear to compensate for the potential negative effects of DAS spurious operation.

© 2007 Electric Power Research Institute, Inc. All rights reserved.

Generation of Risk Insights from PRA to Address Digital I&C Issues

Reconsidering the Scope of D3 Evaluations

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (D3 Scope)

- The scope of BTP-19 is not consistent with other regulations which are directed at addressing CCF
  - Basis for the scope of 10CFR50.62 (ATWS Rule) – Anticipated Transients
    - NUREG-0460 Vol 1
      - An overall safety objective for individual events of 10^{-6}/yr for ATWS
      - An estimated frequency of transients that would lead to significant consequences were SRAM not to occur of 5 to 8 per reactor year
      - An estimated failure to SCRAM probability of 10^{-5} to 10^{-4} per demand
    - Utility Group on ATWS, 'Quantitative Evaluation of Industry Proposed Modifications Relative to Existing Plant ATWS Requirements'
      - 'The proposed modifications are straightforward and well understood by the industry and the NRC Staff.'
      - 'Most importantly, the proposed modifications clearly decrease the risk of ATWS without simultaneously increasing other, competing risks.'

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (D3 Scope)

- What are the risk implications of applying a scope to D3 evaluations consistent with that for the ATWS Rule?
  - A quantitative evaluation of the example PWR has been performed for two cases:
    - Diverse actuation (either automatic or manual) has been provided for automatic mitigating systems for all anticipated transients and accidents
    - Diverse actuation is provided for transients only. No diverse actuation has been provided for accidents (e.g., LOCAs and steam line breaks)
  - Results

    Diverse actuation for both transients and accidents (current scope of BTP-19) – CDF = 1.42E-5/yr

    Diverse actuation for transients only (similar to the ATWS Rule) – CDF 1% to 2% <u>lower</u>.

© 2007 Electric Power Research Institute, Inc. All rights reserved.

D3 Evaluations
Generation of Risk Insights (D3 Scope)

- Conclusions
  - There appears to be a small but negative effect associated with providing diverse actuation systems (DAS) for some accident initiators.

    This is a result of the competing risks of addressing failure of mitigating system actuation for rare events vs. the creation of new, more frequent transients resulting from spurious operation of the DAS.
  - Unless it is simple to design a DAS that will not result in reactor trip should it spuriously actuate

    Consideration should be given to limiting the scope of D3 evaluations to anticipated transients, consistent with the scope of other regulations directed at addressing the effects of CCF, such as the ATWS Rule.

  Otherwise, there is no clear evidence that the resulting DAS will have a positive effect on safety (and may, in fact, be negative).

© 2007 Electric Power Research Institute, Inc. All rights reserved.