Presenters

• Steve Swanson	SNC
• Ray Torok	EPRI
• Glenn Lang	Westinghouse
• Dave Blanchard	Applied Reliability
• Thuy Nguyen	Electricite de France

Meeting Purpose

- Update staff on industry project and plan
- Present technical approach
- Provide forum for questions and discussion
- Follow approach of previous efforts
  - Licensing digital upgrades, EPRI TR-102348, NEI 01-01
  - Evaluation of commercial grade digital equipment, EPRI TR-106439
- Help ensure that new guideline document addresses NRC concerns

Risk-Informed Defense-in-Depth for Digital Upgrades

NRC/Industry Meeting
U.S. Nuclear Regulatory Commission
White Flint, MD
December 4, 2003

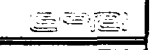
Agenda

• 08:30	**➔ Welcome and Introduction, purpose of meeting**
• 08:40	Project Genesis/basis
• 08:55	Guideline approach/outline
• 09:10	Proposed D3 methods - Deterministic, Probabilistic, Simplified Risk-Informed
• 10:00	BREAK (15 minutes)
• 10:15	Assessment of digital system reliability
• 11:00	Future plans and schedule
• 11:15	Status of NRC approach for assessing D3 evaluations
• 12:00	Adjourn

Utility Perspective

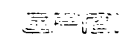
- Priorities
  - Safety
  - Reliability
  - Economics
  - Preference
- Need guidance to ensure focus on these priorities
- Ensure efforts maintain safety

There is no "simple" digital I&C upgrade project



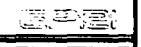
Agenda

• 08:30	Welcome and Introduction, purpose of meeting
• 08:40	→ **Project genesis/basis**
• 08:55	Guideline approach/outline
• 09:10	Proposed D3 methods - Deterministic, Probabilistic, Simplified Risk-Informed
• 10:00	BREAK (15 minutes)
• 10:15	Assessment of digital system reliability
• 11:00	Future plans and schedule
• 11:15	Status of NRC approach for assessing D3 evaluations
• 12:00	Adjourn



Genesis/Basis of EPRI Project

- Potential software common-cause failure still an unsettled issue for digital upgrades
- Per Branch Technical Position (BTP-19), need to ensure "adequate coping capability" or diversity & defense-in-depth (D3)
- Current D3 methods/expectations may be overly restrictive
  - Deterministic (BTP-19) approach can increase costs without providing significant benefits
  - Requires analysis that may not improve plant safety
  - Can require backups that add complexity and cost without significant improvement in plant safety
  - Can discourage plant upgrades that would enhance plant safety



Project Basis, cont'd

- Risk-informed approach appears promising
  - Keeps focus on safety
  - Plant design/safety model determines where diversity is important
  - Allows consideration of digital system advantages, e.g.,
    - Self testing
    - Data validation
    - Fault-tolerance
  - All plants now have tools, methods and PRA models
  - PRAs will have to be updated to include digital upgrades
  - Consistent with updated technical and regulatory trends

Project is Consistent with USNRC PRA Policy

- "The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."
- "PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state of the art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices."

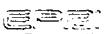
Federal Register, Vol. 60, p. 42622,
Aug 16, 1995

Project Basis, cont'd

- Technical issues to resolve
  - Software reliability difficult to address
  - Qualitative vs quantitative risk assessment
- Regulatory issue – no guidance on use of risk for D3 for digital upgrades
- Project purpose – develop a practical risk-informed approach and seek NRC approval

Project Approach

- Industry working group for oversight and guidance started in early 2002
  - I&C, PRA, licensing and NSSS experts
  - Develop communications between I&C design and PRA (for industry and NRC)
  - EPRI target steering committee on risk issues
- Collaboration with:
  - Equipment suppliers
  - Owners' groups
  - Individual plants to demonstrate methods
- NEI and NRC interfaces
- Develop guideline and seek NRC review and approval

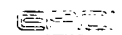


Working Group on Risk-Informed D3 for Digital Upgrades

Jay Amin	TXU	Jerry Mauck	Framatome
Jim Andrachek	Westinghouse	Jim Mcquighan	Calvert Cliffs
Paul Bisges	AmerenUE	Thuy Nguyen	EPRI, EdF
Dave Blanchard	Applied Reliability	Denny Popp	Westinghouse
Jay Bryan	Duke	Joe Ruether	NMC Prairie Island
Ray Disandro	Exelon	Clayton Scott	Triconex
Larry Erin	Westinghouse	Bill Sotos	STP
Bob Fink	MPR	Andrea Sterdis	Westinghouse
Bruce Geddes	Framatome	Jeff Stone	Calvert Cliffs
John Hefler	Altran	Jack Stringfellow	SNC
Tim Hurst	Hurst Technology	Steve Swanson	SNC
Ron Jarrett	TVA	Dinesh Taneja	Bechtel
Glenn Lang	Westinghouse	Dan Tirsun	TXU
Peter Lobner	DS-S	Ray Torok	EPRI
Rich Luckett	NEI	Philip Wengloski	Calvert Cliffs

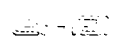
Scoping Studies Using Plant PRAs Bring Digital I&C D3 Issue into Perspective

- For redundant mechanical trains in the same system, I&C diversity is of little benefit from a safety perspective
  - Mechanical components that must rotate or change position dominate system reliability
- For 'high frequency initiators' I&C diversity may be useful
  - Between initiating and mitigating systems
  - Between mitigating systems
- Results depend on:
  - I&C single train failure probabilities
  - Likelihood of "systematic digital common cause failure" (digital CCF)
    - In redundant trains
    - In different systems

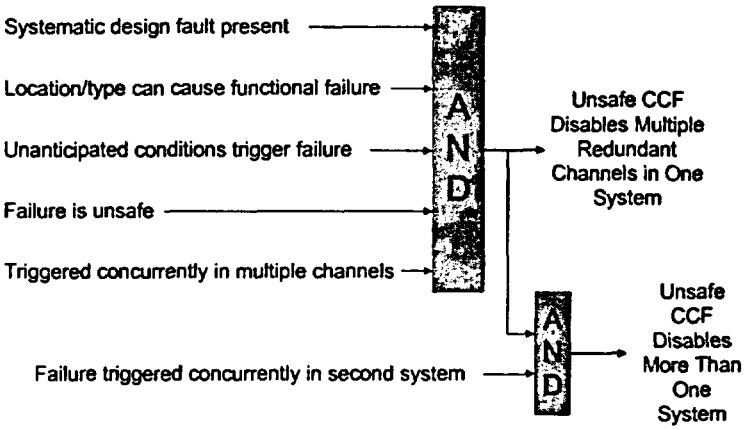


Software – A Different Animal

- Doesn't wear out
  - Problems are designed in
  - Proven for tested conditions
  - Untested or unanticipated conditions can be problematic
- Many design techniques, features, characteristics affect potential for digital CCF
  - Simplicity, testability
  - Data validation, self-checking and diagnostics
  - Shared processors, memory,signals, communications
  - Generic susceptibility, e.g., Y2K
  - Same operating system on identical processors, performing different functions
- High integrity digital systems typically use processes and design features that enhance dependability



Error Forcing Context Needed for Digital CCF to Disable Multiple Systems



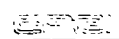
Conclusion: There are good reasons why the likelihood of digital CCF will be quite low for well-designed installations

Practical Approach to Digital System Reliability

- Ultimately, PRA needs 'realistic' assessment – not 1or 0
  - Purpose of PRA is to understand relative contributions to risk of various systems, components, events
  - A conservative PRA is potentially a misleading PRA
  - Simplified D3 approach may use bounding values
- Qualitative approaches for likelihood of failure
  - Compare digital and analog failure data
  - Examine failure histories of similar systems
  - Credit design features, characteristics, development process, standards
  - Credit diversity for like platforms in diverse applications
- Use PRA to help validate qualitative treatment
  - Assess practical I&C failure rate targets considering all risk contributors
  - Investigate sensitivity to failure probability assumptions
  - Overall plant risk is determined primarily by the plant design; component failure probabilities are secondary

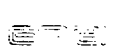
Agenda

• 08:30	Welcome and Introduction, purpose of meeting
• 08:40	Project Genesis/basis
• 08:55	**➔ Guideline approach/outline**
• 09:10	Proposed D3 methods - Deterministic, Probabilistic, Simplified Risk-Informed
• 10:00	BREAK (15 minutes)
• 10:15	Assessment of digital system reliability
• 11:00	Future plans and schedule
• 11:15	Status of NRC approach for assessing D3 evaluations
• 12:00	Adjourn



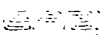
EPRI Guideline Approach – 3 Alternative Methods for D3 Evaluation

- Deterministic – BTP-19 approach
  - Analyze SAR events with 'beyond design basis,' 'best-estimate' approach
  - Use relaxed acceptance criteria per BTP-19
- Probabilistic – focus on plant risk
  - Update PRA to include digital equipment
  - Regenerate PRA results
  - Use Regulatory Guide 1.174 acceptance guidance (Δ-risk)
- Simplified risk-informed – risk focus with conservative assumptions
  - Use input from existing PRA
  - Assume loss of mitigating systems due to digital CCF
  - Evaluate Δ-risk with RG 1.174 acceptance criteria



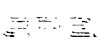
Guideline for Performing D3 Assessments for Digital I&C Upgrades – Outline (abridged)

- Introduction – background, purpose, glossary, etc.
- D3 evaluation and its role in I&C modernization
  - What is a D3 evaluation?
  - Relationship to 10 CFR 50.59
  - Factors influencing risk for digital upgrades
- Performing D3 evaluations
  - When D3 evaluation is needed
  - Digital CCF vulnerabilities
  - Overview of D3 evaluation methods
- Documentation and licensing submittals
- Additional guidance
  - Details of D3 evaluation methods
  - Estimating probability of digital CCF
- References



Guideline Contents (cont'd)

- Appendices
  - I&C fundamentals for PRA personnel
  - PRA fundamentals for I&C personnel
  - Use of PRA in determining I&C architecture
  - Updating the PRA to reflect digital I&C

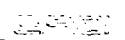


Agenda

- 08:30 Welcome and Introduction, purpose of meeting
- 08:40 Project genesis/basis
- 08:55 Guideline approach/outline
- 09:10 **→Proposed D3 methods - Deterministic,** Probabilistic, Simplified Risk-Informed
- 10:00 BREAK (15 minutes)
- 10:15 Assessment of digital system reliability
- 11:00 Future plans and schedule
- 11:15 Status of NRC approach for assessing D3 evaluations
- 12:00 Adjourn

Deterministic Approach to D3 Evaluation - Regulatory and Industry Guidance

- SECY-93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water- Reactor (ALWR) Designs, Section Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems", USNRC, April 1993
- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems", October 1994
- NUREG-0800, Standard Review Plan, Appendix 7A, "Review Process for Digital Instrumentation and Control Systems, HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, USNRC
- NEI-01-01, EPRI Report TR-102348, Revision 1, "Guidance on Licensing Digital Upgrades, a Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule", NEI and EPRI, March 2002



Deterministic Approach Overview

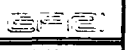
- Develop a simplified I&C logic diagram
- Identify potential digital CCF sources in actuation paths
- Review initiating event analysis results in plant SAR
  - Determine primary and backup mitigating functions for each initiating event
- Identify events where primary and backup mitigating functions degraded by digital CCF
- Perform best-estimate analyses for identified events
- Determine if plant response meets relaxed acceptance criteria
- If not, modify I&C design or use alternate approach
- Document the results of evaluation

Simplified Functional Block Diagram

- Only important features of system included
  - Execution paths
  - Closed loop feedback paths
- Ancillary paths not included
  - System alarms
  - System status indications
- Subfunction blocks
  - Analog input module
  - Signal compensation module
  - Communication input module

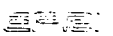
Potential Digital CCF Sources

- Key Principles
  - Only one set of common software blocks are assumed to fail at a time
  - Common software blocks are assumed to fail in the same mode
  - Failure modes considered include fail high, fail-as-is, and fail low
  - For simple components or modules that are widely used and have extensive operating history (e.g., analog-to-digital converters), no digital CCF would be assumed (NEI 01-01 Section 5.2.3)



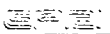
Plant Initiating Events

- Key principles
  - Evaluate those events analyzed in plant SAR
    - Anticipated operational occurrences (AOOs) - ANS Condition II events
    - Design basis events (DBEs) - ANS Condition III and IV events
  - Identify primary and backup mitigating functions for each initiating event



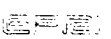
Tools Used For Conducting D3 Evaluation

- Engineering judgment/hand calculations
- Reference to existing analyses
- Engineering simulator
- Thermal hydraulic codes



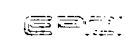
Initiating Event Analyses

- Evaluate initiating events where primary and backup mitigating functions degraded by digital CCF
  - Use best-estimate initial conditions, e.g.,
    - Nominal power, temperature and pressures
    - Best-estimate fuel neutronic parameters
    - ANS best estimate decay heat model
    - Pipe break flow model
  - Use best-estimate assumptions, e.g.,
    - NSSS controls systems operate normally
      - Pressurizer pressure and level control
      - RCS temperature control
      - Steam generator level control
      - Steam dump control
      - Steamline pressure control
    - No stuck control rods following reactor trip
    - No single failure assumed



Relaxed Acceptance Criteria

- Acceptance criteria specified in NUREG/CR-6303
  - For each AOO
    - No violation of RCS pressure boundary integrity
    - Radiation release within 10% of 10 CFR Part 100 guideline limits
  - For each DBE
    - No violation of RCS pressure boundary integrity
    - No violation of containment pressure boundary integrity
    - Radiation release within 10 CFR Part 100 guideline limits



Acceptable Plant Response Alternatives

- No mitigating function required - plant achieves new steady state condition
- Taking credit for plant function, system, or component (FSE) not susceptible to postulated digital CCF
- Credit defendable operator actions
- Implementing changes in I&C design
- Using alternative D3 approach
- Adding diverse automatic actuation functions

Evaluation Documentation Should Include:

- Simplified functional diagram illustrating software blocks assumed
- Plant SAR primary and backup mitigating functions assumed for each initiating event
- Identification of protection functions degraded by postulated digital CCF
- Identification of initiating events in which primary and backup mitigating functions degraded
- Results of re-analyzed initiating events using best-estimate initial conditions and assumptions
- Description of mitigation approaches credited for each re-analyzed initiating event

Agenda

• 08:30	Welcome and Introduction, purpose of meeting
• 08:40	Project Genesis/basis
• 08:55	Guideline approach/outline
• 09:10	→ **Proposed D3 methods** - Deterministic, **Probabilistic**, Simplified Risk-Informed
• 10:00	BREAK (15 minutes)
• 10:15	Assessment of digital system reliability
• 11:00	Future plans and schedule
• 11:15	Status of NRC approach for assessing D3 evaluations
• 12:00	Adjourn

Risk-Informed Perspective on D3 Evaluations for Digital Upgrades

A risk-informed approach:

- Provides the capability to review the effects of the digital upgrade beyond the design basis events considered in the SAR
  - Based on an integrated view of the entire plant design
- Considers all aspects of plant design, including existing diversity in the mechanical and electrical systems
  - Introduction of potential common cause failures where they defeat existing diversity in these mechanical and electrical systems should be avoided
  - Attempting to improve safety by introducing diversity into systems where it does not already exist is of little value

Risk-Informed D3 Evaluations

- Two Approaches
  - Probabilistic Method
  - Simplified Risk-Informed Method

Regulatory and Industry Guidance on Risk-Informed Methods

- USNRC Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998
- Standard Review Plan NUREG 0800 Chapter 19, "Use of Probabilistic Risk Assessment in Plant Specific Risk-Informed Decision Making: General Guidance," July 2001
- EPRI TR-105396, "PSA Applications Guide," August 1995
- NEI-01-01, EPRI Report TR-102348, Revision 1, "Guidance on Licensing Digital Upgrades, a Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule", NEI and EPRI, March 2002

Probabilistic Method

- Estimate
  - CDF, LERF post upgrade using plant-specific PRA
- Directly incorporate
  - potential intra/inter common cause events into event tree and fault tree models
- Use realistic-to-bounding assumptions
  - Reliability of digital equipment
  - Effects of common-cause failure of digital equipment
- Use Regulatory Guide 1.174 acceptance guidance

Probabilistic Method

- Directly incorporate common cause effects
  - Identify initiating events (IEs) and mitigating systems that could be affected by upgrade
  - Include events in logic models that reflect IE or loss of mitigating system due to digital CCF
    - Within systems
    - Between systems
- Assign failure probabilities
  - Sensors
  - Logic
  - Actuation devices

Probabilistic Method

- Realistic or bounding failure probability assignment
  - Sensors, actuation devices from plant-specific PRA or generic sources
  - Logic ($P_{logic} = P_{digital\ train} * P_{unsafe\ failure} * \beta$)
    - A division of digital equipment is assumed to be at least as reliable as the analog equipment it replaces (possible bounding assumption)
    - Consideration given to design of upgrade (more realistic assumptions), e.g.,
      - Qualified platform
      - FMEA for specific failure modes
      - Self-diagnostic capability
      - Fault tolerance
      - Functional similarity/differences in processes
      - Potential for simultaneous failure

P = failure probability

β = common cause factor

Probabilistic Method

- Acceptance guidance (Regulatory Guide 1.174)
  - Plant will continue to meet regulations
  - **Change is consistent with defense-in-depth philosophy**
    - Similar to Significance Determination Process (SDP) of Reactor Oversight Program (ROP)
  - Safety margins will be maintained
  - **Any increase in risk will be small**
    - Figures 3 & 4 of Reg Guide 1.174
  - Change will be monitored after implementation
- Perform sensitivity studies to assess impact of key assumptions

Agenda

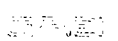
• 08:30	Welcome and Introduction, purpose of meeting
• 08:40	Project Genesis/basis
• 08:55	Guideline approach/outline
• 09:10	➔ **Proposed D3 methods** - Deterministic, Probabilistic, **Simplified Risk-Informed**
• 10:00	BREAK (15 minutes)
• 10:15	Assessment of digital system reliability
• 11:00	Future plans and schedule
• 11:15	Status of NRC approach for assessing D3 evaluations
• 12:00	Adjourn

Simplified Risk-Informed Method

- Directly estimate
  - ΔCDF, ΔLERF
- Conservative assumptions
  - Reliability of digital equipment
  - Effects of failure of digital equipment
- Use Regulatory Guide 1.174 as acceptance guidance
- Credit/Add diversity or relax assumptions where it has significant impact on risk and can be justified

Simplified Risk-Informed Method

- Initial conservative assumptions
  - For initiating events where at least one mitigating system is affected by the upgrade, all mitigating systems are assumed to fail as a result of SDCCF
  - Train of digital equipment has equivalent reliability to train of analog equipment
  - IE frequency due to digital I&C assumed to be the same as that for analog I&C
  - Probability arguments for SDCCF are ignored – essentially assuming SDCCF is certain ($\beta = 1$)



Simplified Risk-Informed Method

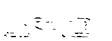
- Useful information from PRA
  - Initiating events (IEs) and frequencies
  - Mitigating systems for each accident sequence
  - Time available for operator action (if needed)
  - Failure probability of diverse actuation systems (if needed)
  - Conditional failure probabilities of selected mitigating systems (where IE could disable one or more systems)
  - Conditional LERF (if needed for ΔLERF)

Simplified Risk-Informed Method

- For each initiating event (IE), calculate the contribution to CDF as:

$$\Delta CDF_{IE} = IE_{freq} * P_{digital\ train} * \beta$$

- Total the individual contributions
- Check total against acceptance guidance
- If total exceeds acceptable level, identify dominant IEs for further consideration



Simplified Risk-Informed Examples

Risk insights: Where does digital CCF and defense against its occurrence have the biggest potential impact?

- $\Delta CDF_{IE} = IE_{freq} * P_{digital\ train} * \beta$

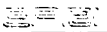
  Turbine trip

  $\Delta CDF_{turb\ trip}$ = 1.0/yr * 1E-4/demand * 1.0
  = 1E-4/yr

  LOCA

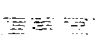
  $\Delta CDF_{large\ Loca}$ = 1E-5/yr * 1E-4/demand *1.0
  = 1E-9/yr

The higher frequency events in which multiple, redundant systems are available to mitigate the event are often the most important to consider. For the lower frequency events, such as LOCA, it is difficult to make I&C CCF a significant risk contributor.



Simplified Risk-Informed Method, cont'd

- If a given IE has a high ΔCDF, then 3 options:
  - Credit existing or new diverse actuation systems
    - Diverse I&C must not be subject to same common cause assumed to fail mitigating systems
  - Credit operator action
    - Sufficient time and information must be demonstrated
    - I&C must not be subject to same common cause assumed to fail mitigating system
  - Justify lower values for digital I&C probability of failure and/or β



Simplified Risk-Informed Example With Backups Credited

Risk Insights: There is ample opportunity to provide adequate defense-in-depth that is worthwhile with existing plant equipment and operating procedures.

- $\Delta CDF_{IE} = IE_{freq} * P_{digital\ train} * P_{DAS} * P_{OP} * \beta$

  DAS = diverse actuation system, OP = operator action

- For turbine trip use:

  $P_{DAS(AMSAC)}$ = 1E-2

  $P_{OP(initiate\ AFW/feed\&bleed)}$ = 1E-2

  $\beta_{FW(given\ turbine\ trip)}$ = 1E-2 (assumes FW and turbine controls on like platforms, with diverse functionality)

- Then:

  $\Delta CDF_{turb\ trip}$ = 1.0/yr * 1E-4/demand * 1E-2 * 1E-2 * 1E-2
  = 1E-10/yr

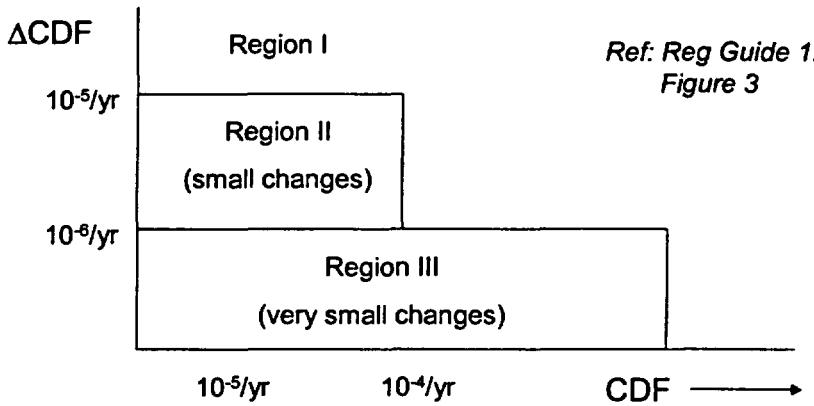
The risk-informed approach is helpful in understanding the importance of each backup

Simplified Risk-Informed Method

- Acceptance guidance (Reg Guide 1.174)
  - Plant will continue to meet regulations
  - Change is consistent with defense-in-depth philosophy
    - Similar to Significance Determination Process (SDP) of Reactor Oversight Program (ROP)
  - Safety margins will be maintained
  - Any increase in risk will be small
    - Figures 3 & 4 of Reg Guide 1.174
  - Change will be monitored after implementation

Simplified Risk-Informed Method

- Any increase in risk will be small

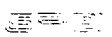


Simplified Risk-Informed Approach

- Other issues addressed in guideline
  - ΔLERF
    - Conditional LERF from PRA provided
      - Containment isolation, Combustible gas control & in-vessel recovery systems are not affected by the upgrade
  - External Events
    - Seismic Margins Assessment (SMA)
    - Fire Vulnerability Evaluation (FIVE)
  - PRA Quality

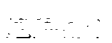
Questions and Comments

→**On the three D3 evaluation methods**



Agenda

- 08:30 Welcome and Introduction, purpose of meeting
- 08:40 Project Genesis/basis
- 08:55 Guideline approach/outline
- 09:10 Proposed D3 methods - Deterministic, Probabilistic, Simplified Risk-Informed
- 10:00 BREAK (15 minutes)
- 10:15 → **Assessment of digital system reliability**
- 11:00 Future plans and schedule
- 11:15 Status of NRC approach for assessing D3 evaluations
- 12:00 Adjourn



Assessment of Digital System Reliability

→**Objective and Approach**
- Digital Failures (individual channels)
- Unsafe Digital Failures
- Digital Common Cause Failures (multiple channels)

Objective

Assessment of potential for

Unsafe Digital Failures

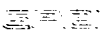
of single I&C channels

Digital Common Cause Failures

of multiple I&C channels

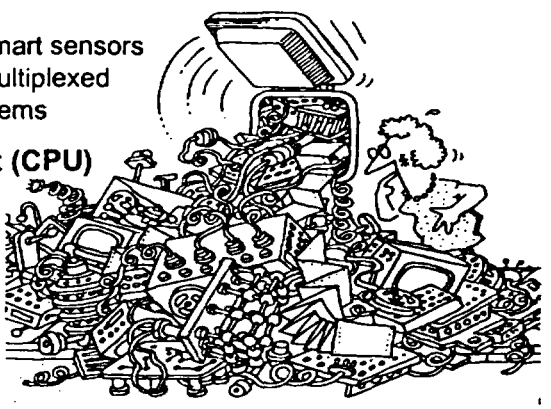
Digital Faults - Digital Failures

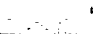
- **Digital Failures**
  - failure: termination of the ability of a functional unit to perform a required function
  - digital failures: occur deterministically and systematically when conditions are identical
- **Digital Faults**
  - fault: abnormal condition that may cause a failure
  - digital faults: specification faults or development faults
    - do not cover
      - weaknesses leading to increased "human errors"
      - incorrect parameters during operation



Digital Faults: Beware of Complexity!

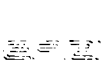
- **Control Software**
  - Operating System Software (OSS)
  - Application Function Library (AFL)
  - Specific Application Software (SAS)
- **"Smart" devices**
  - e.g., smart IO boards, smart sensors and actuator controls, multiplexed communication sub-systems
- **Central Processing Unit (CPU)**
  - also: ASICs, FPGAs, ...
- **Remember the KISS principle**





Main Parameters for PRA Modeling

- **Digital Failures**
  - P_{DF}: probability of digital failure (per unit of time or per demand)
    - R_{DFM}: proportion of failures to mitigate when necessary
    - R_{DFS}: proportion of spurious actuations
    - other (safe) failures
- **Digital Common Cause Failures (CCF)**
  - contribution of digital failures to β factors
    - β_{DI}: identical I&C channels
    - β_{DD}: I&C systems implementing diverse functions on same platform



Difficulty

- **Triggering conditions rare and difficult to identify**
  - identification during development → fault removal
  - residual digital faults: what nobody thought of
- **No widely accepted quantification approach**
  - consideration of design, operational conditions and of safety contexts may facilitate estimations
- **Best vs. Conservative estimates**
  - PRA with overly conservative values give incorrect insight
  - conservative estimates not required for beyond design basis analyses
  - significant uncertainties remain

→ **Realistic estimates with conservative treatment of uncertainties**

Assessment of Digital System Reliability

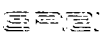
- Objective and Approach
- **→Digital Failures (individual channels)**
- Unsafe Digital Failures
- Digital Common Cause Failures (multiple channels)

Main Approaches for Estimating P_{DF}

- **Use of operational experience**
- **Conformance to safety standards**
  - quantified reliability levels result from consensus
- **Qualification / Safety Evaluation**
  - use of "pre-qualified" platforms
  - QA requirements of 10-CFR-50 Appendix B
- **Technical analysis**

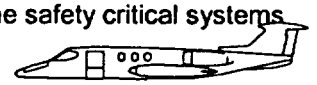
Operational Experience

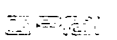
- **Used for**
  - direct estimation of probability of digital failure
    - of pre-developed items, or of comparable products
    - of comparable digital systems
  - confirmation / "calibration" of estimates by other approaches
- **Conditions**
  - credibility of information
  - statistically significant volume
  - applicability to case considered



Operational Experience Examples

- **Proven commercial platforms**
  - used by chemical, oil industries
  - very significant volume of experience, credible information
- **Flight control systems**
  - SW comparable to CS of safety systems
  - ≈ 10^8 h (10^4 y) of cumulated experience, no digital failure
  - same for other airborne safety critical systems
    - e.g., engine control





Conformance to Safety Standards Example: IEC 61508

- **Basic functional safety standard**
- **All industrial sectors**
  - possibly through « derived » standards
- **Many products certified**

SIL	Low demand mode (Probability of failure on demand)	High demand mode or Continuous mode (Probability of a failure per year)
4	$\geq 10^{-5}$ to $< 10^{-4}$	
3	$\geq 10^{-4}$ to $< 10^{-3}$	
2	$\geq 10^{-3}$ to $< 10^{-2}$	
1	$\geq 10^{-2}$ to $< 10^{-1}$	

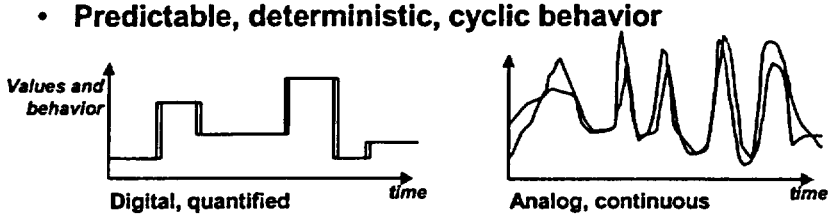
Qualification / Safety Evaluation

- **Usually for safety I&C systems**
- **Comparable to DAL A of DO-178B / ED-12B (used by civil aviation world-wide)**
  - accepted P_{DF}: 10^{-5} per year
  - no digital failure in $\approx 10^4$ years of cumulated experience
- **Comparable or better than SIL 4 of IEC 61508**
  - accepted P_{DF}: $\geq 10^{-5}$ to $< 10^{-4}$ per year or per demand

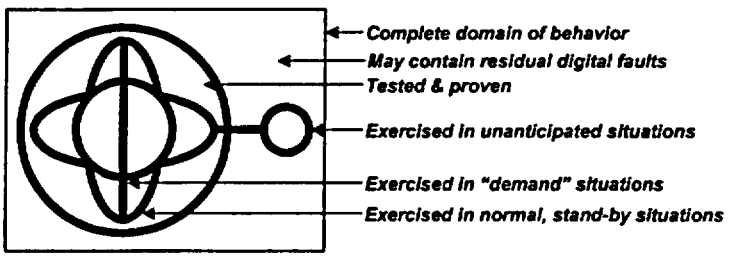
→ **Reasonable value for us to use is $P_{DF} = 10^{-4}$ a qualified system**

Well-Designed Digital I&C Systems

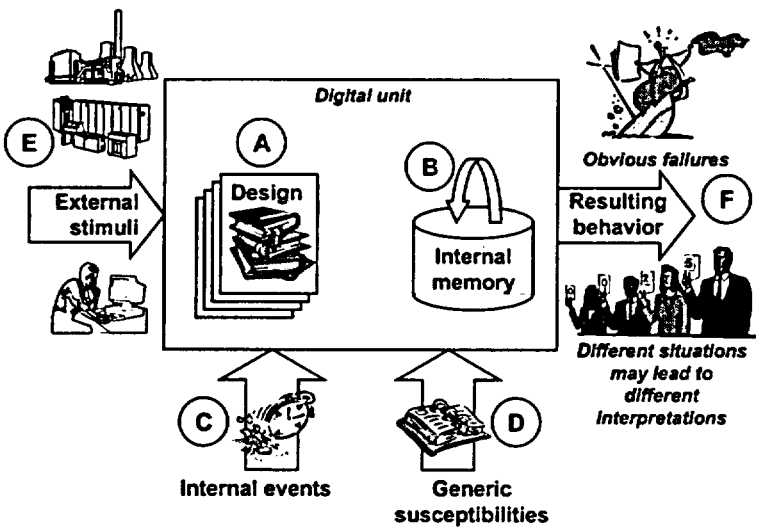
- **Predictable, deterministic, cyclic behavior**



- **Identification & control of factors influencing behavior**



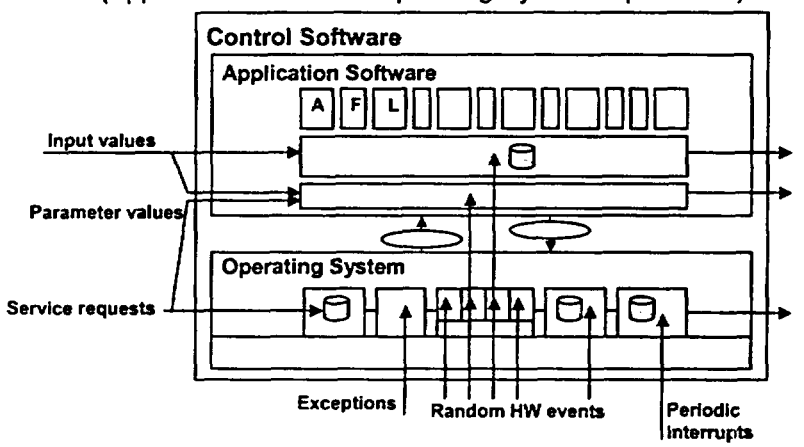
Factors of Influence



Modular Design Limits Exposure to Potential Failure Modes

Independent modules

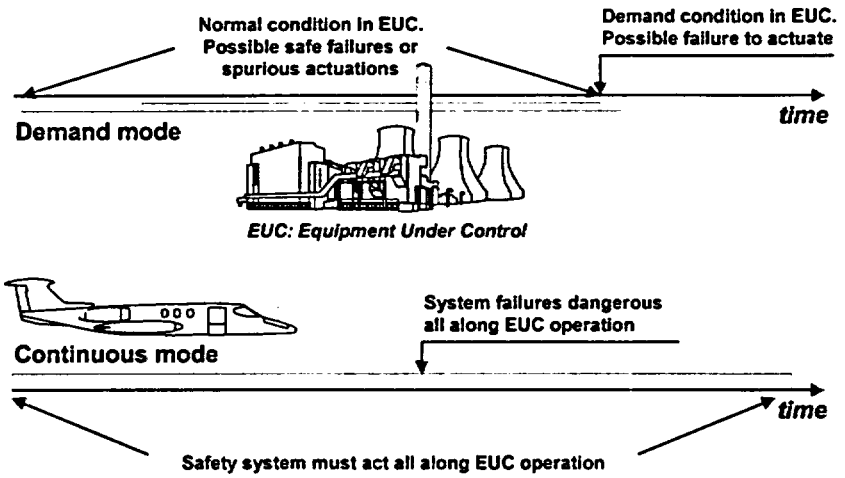
(Application Software / Operating System in particular)



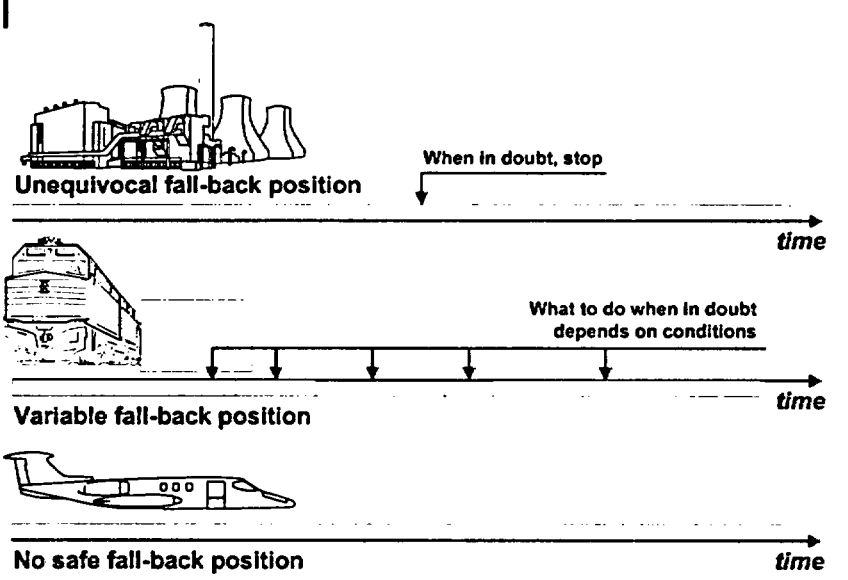
Assessment of Digital System Reliability

- Objective and Approach
- Digital Failures (individual channels)
- **→Unsafe Digital Failures**
- Digital Common Cause Failures (multiple channels)

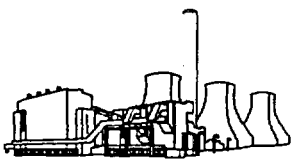
Demand vs. Continuous mode



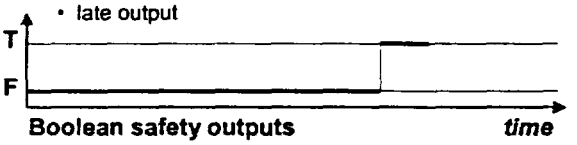
Safe Fall-back Position

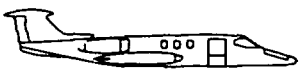


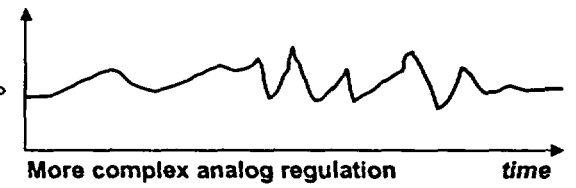
Characterization of Failure Modes



Possible failure modes:
- T instead of F: spurious actuation
- F instead of T: failure to actuate
- late output







Fault Tolerance and Experience

- **Self-surveillance - Defensive design**
  - surveillance of software by software
  - surveillance of hardware by software
  - surveillance of software by hardware
- **FMEA**
  - identification
    - of unsafe digital failure modes
    - of components that can cause unsafe digital failures
  - assessment of defensive means
- **Experience**
  - no unsafe digital failure experienced
  - analysis / verification of SW already in operation, using more advanced techniques than during development: no unsafe digital fault
  - experience from other industrial sectors

→Reasonable value for us to use for R_{DFM}: 10^{-1}

Assessment of Digital System Reliability

- Objective and Approach
- Digital Failures (individual channels)
- Unsafe Digital Failures
- **→Digital Common Cause Failures (multiple channels)**

Identical Channels on Qualified Platform

Specification Faults	Development Faults		
– dominant cause of systematic failures – likely to affect concurrently all identical channels – needs for safety actuation usually well-characterized	OSS	not affected by plant condition, only by events affecting single channels	P_{DF} low β low
	AFL	small, independent modules, proven algorithms, usually have no memory	P_{DF} very low
	SAS	automated code generation by trusted tools, unlikely to contain development faults	P_{DF} low
	CPU	massive operational experience, restricted usage of capabilities, stable conditions of use	P_{DF} very low
P_{DF} dominant R_{DFM} low	Smart dev.	functionally simple, very large operational experience, restricted usage of capabilities	P_{DF} low

→ Conclusion: β_{DI} not 1, but not << 1

- usually dominated by application

Diverse Functions on Same Qualified Platform

Specification Faults	Development Faults		
– still a dominant cause of failure and CCF – at a much lower level	OSS	in hardware / system configuration likely to be different	P_{DF} low β low
	AFL	likely to be used differently	P_{DF} very low β < 1
	SAS	different applications, very unlikely to have faults activated concurrently	P_{DF} low β low
	CPU	likely to be used differently	P_{DF} very low β < 1
P_{DF} dominant R_{DFM} low β low	Smart dev.	likely to be used differently	P_{DF} very low β < 1

→ **Conclusion : β_{DD} significantly less than 1**

– might be dominated by non-digital aspects

Agenda

- 08:30 Welcome and Introduction, purpose of meeting
- 08:40 Project Genesis/basis
- 08:55 Guideline approach/outline
- 09:10 Proposed D3 methods - Deterministic, Probabilistic, Simplified Risk-Informed
- 10:00 BREAK (15 minutes)
- 10:15 Assessment of digital system reliability
- 11:00 → **Future plans and schedule**
- 11:15 Status of NRC approach for assessing D3 evaluations
- 12:00 Adjourn

Ongoing Project Activities

- PRA analysis
  - Examples of confirming adequate D3 in specific I&C design
  - Identify minimum D3 required to help shape I&C design
- Software reliability
  - Gather and analyze digital reliability data
  - Develop 'check-list' approach to relate design features to estimated likelihood of failure
  - Develop guidance on verifying design features
  - Develop method for estimating likelihood of unsafe digital CCF for like platforms in similar and diverse applications (β factors for PRA model)

Project Deliverables and Schedule

Project will produce generic guidance documents for I&C, PRA, and licensing engineers

- High level, 'tier 1' guideline
  - "What-to-do" guidance
  - Suitable for NRC review
  - Draft in December 2003, final in mid-2004
- Second tier, "how-to-do" guidance
  - Estimating digital system, software reliability for D3 evaluation
  - Estimating likelihood of unsafe common mode failure (β factor for PRA)
  - Final report in 2005

Agenda

• 08:30	Welcome and Introduction, purpose of meeting
• 08:40	Project Genesis/basis
• 08:55	Guideline approach/outline
• 09:10	Proposed D3 methods - Deterministic, Probabilistic, Simplified Risk-Informed
• 10:00	BREAK (15 minutes)
• 10:15	Assessment of digital system reliability
• 11:00	Future plans and schedule
• 11:15	**→ Status of NRC approach for assessing D3 evaluations**
• 12:00	Adjourn