

November 2, 2006

ORGANIZATION: NUCLEAR ENERGY INSTITUTE (NEI)

SUBJECT: SUMMARY OF OCTOBER 19, 2006, MEETING WITH NEI AND  
NUCLEAR POWER INDUSTRIES REGARDING INSTRUMENTATION  
AND CONTROL TECHNICAL ISSUES

On October 19, 2006, United States Nuclear Regulatory Commission (NRC) staff from the offices of Nuclear Reactor Regulation (NRR), Research (RES), and Nuclear Security and Incident Response (NSIR) held a public meeting at NRC Headquarters with nuclear power industry representatives and members of the public. NRC staff organized the meeting to address issues that stakeholders had expressed at earlier public meetings and comments on DG-1145 (guidance for Combined Operating License applications). The four issues were communication between safety channels and between safety and non-safety systems, improved defense-in-depth and diversity methodologies (D3), cyber security issues related to Regulatory Guide (RG) 1.152, "Criteria for Use of Computers In Safety Systems of Nuclear Power Plants," and human factors and advanced control room design. The meeting provided a platform for discussions of the three meeting objectives: common understanding of the four priority issues, discussion of industry and NRC plans to address the issues, and agreement on the path forward to resolve the issues. At the meeting the next steps towards resolution were planned for each of the four issues. There was consensus that open communication and dialogue between all parties will be an essential element of continuing successful progress.

The main challenge in the area of communications is development of NRC safety review guidance to provide reasonable assurance that inter-channel communications and safety to non-safety communications will not degrade safety functions through unintended behaviors or inadequately managed failure modes. NRC and industry agreed to further dialogue regarding NRC research projects on digital system communications which are due for completion in August, 2007. The next steps to address Instrumentation and Control (I&C) communications include the following:

- NRC will address the inconsistencies between RG 1.152 and the Standard Review Plan (SRP) in the SRP update.
- During the meeting industry representatives stated that they believe NRC has approved communication designs in the past. Industry agreed to provide information describing those precedents.
- NRC and industry agreed to hold a meeting in December, 2006 to discuss updates of IEEE 7.4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," and NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants."
- Industry plans to provide a 'straw man' meeting the safety – non-safety communication requirements for NRC feedback.

The essential aim of work in the D3 area is to develop a practical regulatory approach for addressing software common-cause failure (CCF), as well as a practical approach for near term use in D3 evaluations for digital upgrades and new plant designs. Associated action items include the following:

- Industry will provide peer review to the NRC of Draft NUREG/CR-XXXX, "Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments." Industry will provide their comments by December of 2006.
- NRC staff stated they will continue research to support risk-informing digital I&C applications including modeling of digital system reliability and implementation of these models in current generation Probabilistic Risk Assessments. NRC and industry agreed to further dialogue related to research and development efforts in the area of digital system reliability modeling.
- NRC will continue work on a new research effort to provide additional information on how to use current staff guidance [NUREG/CR-6303, "Method for Performing Defense-In-Depth and Diversity Analyses of the Reactor Protection System"].
- NRC and industry agreed to schedule a meeting in January of 2007 for further discussion of D3 issues.

For cyber security, NRC and industry sought to reconcile guidance in NEI-04-04, "Cyber Security Program for Power Reactors," and RG 1.152 security guidance. There are several upcoming plans and events addressing cyber security issues. NRC stated that a proposed rule that includes cyber security requirements will be published in the Federal Register on October 26, 2006. Action items from the meeting include:

- Nuclear Energy Institute plans to provide a document to the NRC which compares NEI-04-04 and RG 1.152 by December 15, 2006. NRC staff agreed to then evaluate that comparison.
- NRC staff will evaluate including in the SRP update alternate methods for meeting RG 1.152.

Regarding the area of Human Factors and Advanced Control Room Design, industry discussed a need for common understanding of Minimum Inventory (MI). This concerns the minimum required inventory of fixed position instrumentation and controls. NRC outlined its research activities and potential impacts on existing guidance. Actions in response to these issues include:

- Industry agreed to submit a technical paper on the "Minimum Inventory" (MI) of instrumentation and controls concept, and how they should be identified. Industry will provide NRC staff with a schedule for this submission. NRC will review that technical paper.
- NRC staff noted that an NRC Technical Report on human factors issues in new and advanced reactors is currently planned for publication for public comment in 2007.
- NRC staff described a research project on the I&C engineering aspects of advanced control room designs which is currently underway and is planned to yield a draft NUREG/CR that could be made available for public comment in the fall of 2007.
- EPRI agreed to provide technical reports on 'role of operator' and 'computer based procedures.' Industry will provide NRC staff with a schedule for this submission.

**/RA/**

S. K. Mitra, Project Manager  
Guidance Infrastructure and Financial Review Branch  
Division of New Reactor Licensing  
Office of New Reactors

Enclosures:

- As stated
1. Agenda
  2. List of Attendees
  3. Meeting Slides

Regarding the area of Human Factors and Advanced Control Room Design, industry discussed a need for common understanding of Minimum Inventory (MI). This concerns the minimum required inventory of fixed position instrumentation and controls. NRC outlined its research activities and potential impacts on existing guidance. Actions in response to these issues include:

- Industry agreed to submit a technical paper on the "Minimum Inventory" (MI) of instrumentation and controls concept, and how they should be identified. Industry will provide NRC staff with a schedule for this submission. NRC will review that technical paper.
- NRC staff noted that an NRC Technical Report on human factors issues in new and advanced reactors is currently planned for publication for public comment in 2007.
- NRC staff described a research project on the I&C engineering aspects of advanced control room designs which is currently underway and is planned to yield a draft NUREG/CR that could be made available for public comment in the fall of 2007.
- EPRI agreed to provide technical reports on 'role of operator' and 'computer based procedures.' Industry will provide NRC staff with a schedule for this submission.

**/RA/**

S. K. Mitra, Project Manager  
Guidance Infrastructure and Financial Review Branch  
Division of New Reactor Licensing  
Office of New Reactors

- Enclosures: 1. Agenda  
2. List of Attendees  
3. Meeting Slides

ADAMS ACCESSION NO. ML

OFFICE	NRR/APOB	NRO/NGIF	NRR/EICA
NAME	R. Harrington	S. Mitra	A. Howe
DATE	11/02/06	11/02/06	11/02/06

**OFFICIAL RECORD COPY**

Hard Copy  
Ronald Harrington  
Allen Howe  
S. K. Mitra

Email  
PUBLIC  
NRR\_DE  
Steven Arndt  
Michael Boggi  
James Bongarra  
Fred Burrows  
Norbert Carte  
Mathew Chiramal  
Nilesh Chokshi  
John Grobe  
Ronald Harrington  
Wesley Held  
Patrick Hiland  
Allen Howe  
William Kemper  
Alan Kuritzky  
Hulbert Li  
Michael Mayfield  
S.K. Mitra  
Scott Morris  
Julius Persensky  
Paul Rebstock  
Nancy Salgado  
Roman Shaffer  
Martin Stutzke  
Rob Tregoning  
Michael Waterman

External e-mail  
andracjd@westinghouse.com  
  
Robert\_J\_atkinson@dom.com  
  
wesley.bowers@exeloncorp.com  
  
brinkmcb@westinghouse.com  
  
Mark.burzynski@areva.com  
  
Warren\_a\_busch@fpl.com  
  
gcesare@enercon.com  
  
rfink@cdfservices.com  
  
fuld@sbcglobal.net  
  
Matt.gibson@pgnmail.com

kah@nei.org  
  
hayestp@westinghouse.com  
  
rajarrett@tva.gov  
  
kak@nei.org  
  
Christopher.Kerr@exeloncorp.com  
  
Gregory.krueger@exeloncorp.com  
  
Phil.liddle@areva.com  
  
jlmldigitech@erds.com  
  
James.p.mcquighan@constellation.com  
  
Richarde.miller@ge.com  
  
Joseph.murray@ips.invensys.com  
  
jnaser@epri.com  
  
Michael.nifontoff@navy.mil  
  
tedquinn@cox.net  
  
Frank\_quinn@comcast.net  
  
draleigh@scientech.com  
  
crice@mpr.com  
  
jhr@nei.org  
  
Thomas.e.roberts@navy.mil  
  
jwr@nei.org  
  
kenscarola@nuclearautomation.com  
  
njstring@southernco.com  
  
rtorok@epri.com  
  
Jenny\_weil@platts.com  
  
wilsontc@notes.westinghouse.com

Combination Mailing List

cc:

Mr. Charles Brinkman  
Westinghouse Electric Co.  
Washington Operations  
12300 Twinbrook Pkwy., Suite 330  
Rockville, MD 20852

Mr. David Lochbaum, Nuclear Safety  
Engineer  
Union of Concerned Scientists  
1707 H Street, NW, Suite 600  
Washington, DC 20006-3919

Mr. Paul Gunter  
Nuclear Information & Resource Service  
1424 16<sup>th</sup> Street, NW, Suite 404  
Washington, DC 20036

Mr. James Riccio  
Greenpeace  
702 H Street, NW, Suite 300  
Washington, DC 20001

Mr. Adrian Heymer  
Nuclear Energy Institute  
Suite 400  
1776 I Street, NW  
Washington, DC 20006-3708

Mr. George Alan Zinke  
Project Manager  
Nuclear Business Development  
Entergy Nuclear  
M-ECH-683  
1340 Echelon Parkway  
Jackson, MS 39213

Ms. Marilyn Kray  
Vice President, Special Projects  
Exelon Generation  
200 Exelon Way, KSA3-E  
Kennett Square, PA 19348

Mr. Laurence Parme  
Manager, GT-MHR Safety & Licensing  
General Atomics Company  
P.O. Box 85608  
San Diego, CA 92186-5608

Mr. Joseph D. Hegner  
Lead Engineer - Licensing  
Dominion Generation  
Early Site Permitting Project  
5000 Dominion Boulevard  
Glen Allen, VA 23060

Mr. Edward L. Quinn  
Longenecker and Associates  
Utility Operations Division  
23292 Pompeii Drive  
Dana Point, CA 92629

Mr. Paul Leventhal  
Nuclear Control Institute  
1000 Connecticut Avenue, NW  
Suite 410  
Washington, DC 20036

Mr. Jay M. Gutierrez  
Morgan, Lewis & Bockius, LLP  
1111 Pennsylvania Avenue, NW  
Washington, DC 20004

Mr. W. Edward Cummins  
AP600 and AP1000 Projects  
Westinghouse Electric Company  
P.O. Box 355  
Pittsburgh, PA 15230-0355

Mr. Gary Wright, Manager  
Office of Nuclear Facility Safety  
Illinois Department of Nuclear Safety  
1035 Outer Park Drive  
Springfield, IL 62704

Mr. Brendan Hoffman  
Research Associate on Nuclear Energy  
Public Citizens Critical Mass Energy and  
Environmental Program  
215 Pennsylvania Avenue, SE  
Washington, DC 20003

Mr. Lionel Batty  
Nuclear Business Team  
Graftech  
12300 Snow Road  
Parma, OH 44130

Mr. Ian M. Grant  
Canadian Nuclear Safety Commission  
280 Slater Street, Station B  
P.O. Box 1046  
Ottawa, Ontario  
K1P 5S9

Mr. Glenn H. Archinoff  
AECL Technologies  
481 North Frederick Avenue  
Suite 405  
Gaithersburg, MD 20877

Dr. Regis A. Matzie  
Senior Vice President and  
Chief Technology Officer  
Westinghouse Electric Company  
20 International Drive  
Windsor, CT 06095

Mr. Ed Wallace, General Manager  
Projects  
PBMR Pty LTD  
PO Box 9396  
Centurion 0046  
Republic of South Africa

Mr. Dobie McArthur  
Director, Washington Operations  
General Atomics  
1899 Pennsylvania Avenue, NW, Suite 300  
Washington, DC 20006

Mr. Russell Bell  
Nuclear Energy Institute  
Suite 400  
1776 I Street, NW  
Washington, DC 20006-3708

Ms. Vanessa E. Quinn, Chief  
Radiological Emergency Preparedness  
Branch  
Nuclear and Chemical Preparedness and  
Protection Division  
Department of Homeland Security  
1800 South Bell Street, Room 837  
Crystal City-Arlington, VA 22202-3546

Mr. Ron Simard  
6170 Masters Club Drive  
Suwanee, GA 30024

Ms. Sandra Sloan  
Areva NP, Inc.  
3315 Old Forest Road  
P.O. Box 10935  
Lynchburg, VA 24506-0935

Ms. Anne W. Cottingham  
Assistant General Counsel  
Nuclear Energy Institute  
1776 I Street, NW, Suite 400  
Washington, DC 20006

Mr. David Repka  
Winston & Strawn LLP  
1700 K Street, NW  
Washington, DC 20006-3817

Mr. Robert E. Sweeney  
IBEX ESI  
4641 Montgomery Avenue  
Suite 350  
Bethesda, MD 20814

Mr. Eugene S. Grecheck  
Vice President, Nuclear Support  
Services  
Dominion Energy, Inc.  
5000 Dominion Blvd.  
Glen Allen, VA 23060

Agenda for Public Meeting Between  
Nuclear Power Industries and the NRC  
Regarding Significant Technical  
Instrumentation and Control Issues

October 19, 2006

Time (approx)	Topic
9:30	Introductory Remarks
9:45	Issue Identification, Prioritization, and Resolution Path Discussion Concerning the Following Topics: <ul style="list-style-type: none"><li>* Communication between channels and between safety and non-safety systems</li><li>* Improved defense-in-depth and diversity methodologies (D3)</li></ul>
12:00	Lunch
1:00	Discussion Continued: <ul style="list-style-type: none"><li>* Cyber security issues related to Reg Guide 1.152</li><li>* Human factors and advanced control room issues</li></ul>
4:15	Closing and Adjournment



**Nuclear Power Industries and NRC Meeting Regarding  
Significant Technical Instrumentation and Control  
Issues Thursday, October 19, 2006  
9:30 a.m. to 4:30 p.m.  
NRC Headquarters Conference Room O-3B4**

<b>Name</b>	<b>Organization</b>
James Andrachek	Westinghouse
Steven Arndt	NRC
Robert Atkinson	Dominion
Michael Boggi	NRC
James Bongarra	NRC
Wesley Bowers	Exelon
Charles Brinkman	Westinghouse
Fred Burrows	NRC
Mark Burzynski	Areva NP
Warren Busch	FP&L
Norbert Carte	NRC
Guy Cesare	NUSTART
Mathew Chiramal	NRC
Robert Fink	CDF Services
Bob Fuld	Westinghouse
Matt Gibson	Progress
Ronald Harrington	NRC
K. Tony Harris	NEI
Tom Hayes	Westinghouse
Wesley Held	NRC
Allen Howe	NRC
Ron Jarrett	TVA
Kimberly Keithline	NEI
William Kemper	NRC
Christopher Kerr	Exelon
Gregory Krueger	Exelon
Alan Kuritzky	NRC
Hulbert Li	NRC
Phil Liddle	Areva NP
Jerry Mauch	South Texas
James McQuighan	Constellation
Richard Miller	GE

<b>Name</b>	<b>Organization</b>
S.K. Mitra	NRC
Scott Morris	NRC
Joe Murray	INVENSYS
Joseph Naser	EPRI
Michael Nifontoff	NNPP
Julius Persensky	NRC
Edward (Ted) Quinn	GE Nuclear
Frank Quinn	STP
Deann Raleigh	LIS Scientech
Paul Rebstock	NRC
Chris Rice	MPR
James Riley	NEI
Thomas Roberts	NNPP
Jack Roe	NEI
Nancy Salgado	NRC
Ken Scarola	NAE
Roman Shaffer	NRC
Norman Stringfellow	SNC
Ray Torok	EPRI
Rob Tregoning	NRC
Michael Waterman	NRC
Jenny Weil	McGraw Hill
Tim Wilson	Westinghouse

# Instrumentation and Control Issues Meeting



October 19<sup>th</sup>, 2006

Category One Public Meeting

## Agenda

9:30 AM	Opening and Introductions (15 Minutes)
9:45 AM	Communication between Channels and between safety and non-safety systems (1 Hour)
11:00 AM	Improved Defense in Depth and Diversity methodologies (D3) (1 Hour)
12:00 PM	Lunch (1 Hour)
1:00 PM	Cyber security issues related to Reg Guide 1.152 (1 Hour)
2:15 PM	Human Factors and advanced control room issues (1Hour)
3:30 PM	Meeting Recap (30 Minutes)
4:00 PM	Closing and Adjournment (10 Minutes)

# Objectives

- ➔ Understand Priority Issues
- ➔ Discuss Industry and NRC Plans to Address Issues
- ➔ Develop Plan for Path Forward

# Digital I&C and Human Factors

Industry/NRC Meeting  
October 19, 2006

Jim Riley - NEI



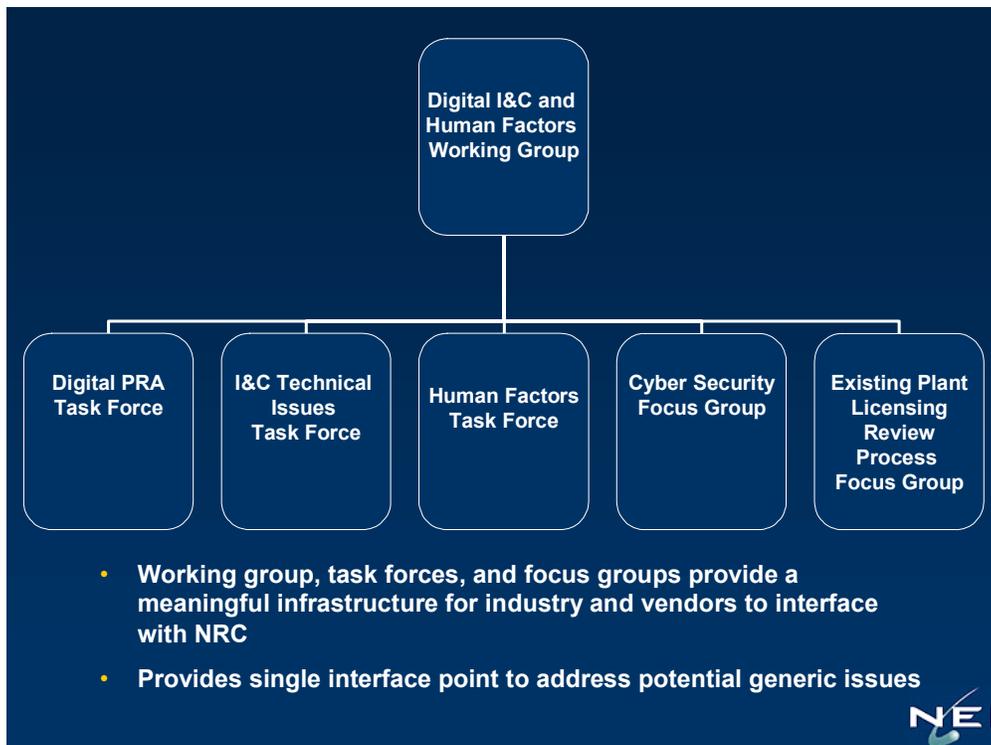
## Shared Vision

The reliability, efficiency, and safety improvements gained by using digital technology in U.S. nuclear power plants dictate that the behaviors and actions of both the regulator and industry embrace and encourage its timely use and safe implementation.



## Today's Goals

- Reach agreement on certain technical and process issues
- Begin developing plans to resolve identified issues
- Set the stage for future interactions as issues become apparent
- Topic Areas
  - Safety / non-safety and interchannel communications
  - Alternative for performing D3 evaluations
  - Cybersecurity
  - Human Factors



## **Digital PRA Task Force**

Coordinates industry efforts relative to the use of risk insights associated with digital technology for both existing and new plants. The group also reviews NRC research activities associated with digital applications.

## **I&C Technical Issues Task Force**

Coordinates industry efforts relative to I&C technical issues associated with the application of digital technology for both existing and new plants.

## **Human Factors Task Force**

Coordinates human factors and control room design issues associated with use of digital technology for both existing and new plants.

## **Focus Groups**

Coordinates with existing NEI task forces to address issues related to cybersecurity and licensing process.



# Communications Between Redundant Divisions and Between Safety and Non-Safety Systems

Presenter: Wes Bowers  
Exelon Corporation

## Current Situation

- All new plant designs and many operating plants use digital control systems that include communications between redundant safety divisions and between safety and non-safety systems.
- Industry standards provide sufficient guidance to enable licensees to design systems with reasonable assurance that inter-channel communications will not degrade safety functions through unintended behaviors or inadequately managed failure modes.
- NRC guidance is conflicting

## IEEE 603, Section 5.6 Requirements

- Independence between redundant portions of a safety system.
- Independence between safety systems and effects of design basis events.
- Independence between safety systems and other systems, both interconnected equipment and equipment in proximity.
- Effects of a single random failure.
- Detailed criteria.

## IEEE 7-4.3.2 Requirements

- Additional detailed criteria for independence are contained in section 5.6 of IEEE 7-4.3.2.
- Guidance for establishing communication independence is provided in Annex E of IEEE 7-4.3.2. Annex E is an informative annex; however, it provides guidance that if met, will result in a design that meets the standard requirements.

## Regulatory Guide 1.152

- Reg. Guide 1.152 endorses IEEE Std 7-4.2.3 but does not endorse Annex E.
- Reg. Guide discussion states that Annex E provides “insufficient guidance”
- Reg. Guide states additional guidance is in:
  - Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems“
  - Appendix 7.1.C, "Guidance for Evaluation of Conformance to IEEE Std 603.“
  - Section 7.9, "Data Communication Systems," in NUREG-0800.

## The Dilemma

- Review of Appendix 7.0-A and Appendix 7.1.C fails to identify any additional guidance.
- NUREG-0800 states that Annex G of IEEE 7-4.3.2 (Annex G in previous revision of IEEE 7-4.3.2 is Annex E in current revision) “describes an acceptable means for providing communications independence.” Review of NUREG-0800 fails to identify any guidance that is not in Annex G (E) of IEEE 7-4.3.2.
- Annex E and Annex G wording is identical.

## **What Needs to be Accomplished?**

- Explore NRC staff concerns of “inadequate guidance” with IEEE 7-4.3.2 Annex E to clearly identify and define the concerns.
  - Is there a technical concern?
- Explore NRC staff needs for documentation in submittals
  - Recent experience indicates staff wants more detail than is typically provided in a licensee submittal
- Identify guidance necessary to allow communication between redundant safety divisions and between safety and non-safety systems.

## **Possible Solutions**

- Revise Regulatory Guide 1.152 to endorse IEEE 7-4.3.2, Annex E, as is.
- Revise IEEE 7-4.3.2, Annex E to incorporate additional guidance. Endorse the revised Annex E in a revision to Regulatory Guide 1.152.
- Revise NUREG-0800 to incorporate additional guidance.
- There are other options; however, whatever way we move to resolution needs to be:
  - Timely
  - Allow stakeholder involvement



## Improved Defense-in-Depth and Diversity Methodologies

Jack Stringfellow, Southern Nuclear  
Ray Torok, EPRI

Public Meeting Between the Nuclear Power  
Industries and the NRC Regarding Significant  
Technical Instrumentation and Control Issues

19 October, 2006  
Washington, D.C.

1

## D3 Overview – The Problem Statement

- A practical regulatory approach for addressing software common-cause failure (CCF) has proven elusive
- Industry and NRC need a practical approach for near term use in D3 evaluations for digital upgrades and new plant designs that:
  - applies risk insights, including consideration of the risk significance of I&C equipment in the context of the integrated plant design;
  - reflects and credits digital system design features and practices used in various industries to ensure high dependability in critical applications; and
  - reflects realistic plant behaviors and dependencies among plant systems during postulated accidents

## Proposed Resolution Path

- Start with existing EPRI D3 Guideline
  - *Guideline for Performing Defense-In-Depth and Diversity Assessments for Digital Upgrades: Applying Risk Informed and Deterministic Methods*, EPRI – 1002835, December 2004
- Meet with NRC to clarify concerns/comments and continue meetings throughout development process
- Coordinate with NRC Research efforts
- Produce updated guidance that addresses the known concerns
- Submit the revised D3 Guideline to NRC for review and approval

## Objectives for Today

- Briefly review EPRI D3 Guideline (“Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods” EPRI 1002835)
- Review NRC comments and industry responses
- Obtain some clarification on comments
- Schedule a technical meeting to address comments in near future

## D3 Guideline - Purpose

EPRI D3 Guideline was developed to:

- Provide a practical, technically sound approach that enhances BTP-19 guidance
- Help make the regulatory environment more stable and predictable
- Provide improved safety focus by applying risk insights

## D3 Guideline - Summary

- Presents three methods for D3 evaluation
  - **Extended Deterministic** – based largely on BTP-19 approach
    - Susceptibility assessment uses “defensive measures” – deterministic evaluation of system design features and behaviors
    - Use risk insights from PRA
  - **Standard Risk-Informed** – risk focus with realistic assumptions
    - Update PRA and regenerate risk results
  - **Simplified Risk-Informed** – risk focus with conservative assumptions
    - Use input from existing PRA to estimate change in risk
- Risk-informed methods use Regulatory Guide 1.174 acceptance guidance (based on  $\Delta$ CDF,  $\Delta$ LERF )

## D3 Guideline - Overview

- The D3 Guideline helps the analyst determine:
  - When I&C systems are susceptible to digital CCF
  - Where D3 in the I&C is of value in the context of the plant design (as opposed to focusing on just the digital system)
  - How reliable a digital system needs to be
  - Whether there is reasonable assurance that appropriate levels of D3 and reliability have been achieved
- The D3 Guideline does not attempt to:
  - Identify the complete spectrum of failure modes that may apply to particular digital system designs
  - Precisely determine the probabilities of such failure modes
  - Develop detailed models of digital equipment for use in PRA

## Comments on D3 Guideline Introduction

1 of 9

- NRC comment: “The ... method proposes to reduce the number of common cause failures to be evaluated ... by taking credit for defensive measures against CCFs. The criteria for screening out CCFs need additional detail and technical justification ... and ... examples.”
- Response: Additional discussion needed to define details and examples
- The defensive measures investigation is based on a few basic principles:
  - Systematic identification of faults and failures that could be risk-significant
  - Identification of the measures taken by the system designer or operator to avoid or eliminate failures
  - Evaluation of the coverage and effectiveness of these measures
  - Details assessed on a case basis, using engineering judgment
  - Consider actual system design and behaviors, rather than unrealistic assumptions and process-based criteria

## Comments on D3 Guideline Item 1 -

2 of 9

- NRC comment: “The simplified risk method needs to be described in more detail. This method appears to require information and analysis that are not available in existing PRAs.”
  - Response: The method has been demonstrated using existing PRAs. Not clear what additional detail would help. More discussion needed.
- NRC comment: “External events are not discussed with respect to the PRA analysis.”
  - Response: External events are included as initiating events. See Section 4.4.4 and the definition of initiating event.

## Comments on D3 Guideline Item 1, cont'd -

3 of 9

- NRC comment: “The modeling methods needed to support the standard risk informed method are not currently available.....”
  - Response: Agree that methods are still evolving, but in many cases, valuable risk insights can be obtained without precise modeling.
  - NRC comment suggests that useful risk insights cannot be derived using current PRAs, conflicts with 1997 National Research Council report on Digital I&C in Nuclear Plants:
    - “a software failure probability can be used for the purposes of performing ... PRA in order to determine the relative influence of digital system failure on the overall system..”
    - “.. subjective interpretations of probability may be used and may, in fact, be all that is available. Subjective probabilities may be sought in formal and informal processes in which groups of experts weigh available evidence and make judgments.”
  - The D3 guideline approach is consistent with the assertions and recommendations of the National Research Council

## Comments on D3 Guideline Item 2 -

4 of 9

- NRC comment: “EPRI TR-102835 does not specify how to develop a reliability model of digital system and acknowledges the weakness of the state-of-the-art modeling of digital systems.”
  - Response: Not needed because:
    - Several modeling approaches may be adequate
    - Risk insights are insensitive to modeling details
- NRC comment: “EPRI concluded that, with appropriate (defensive) measures, there should be reasonable assurance that ... digital CCFs are ... much less likely than single failures assumed as part of a plant’s design basis. This conclusion is not justified by the information presented in the topical report.”
  - Response: The D3 Guideline approach does not rely on an assumption that digital failure and digital CCF are less likely than single failures used in design basis. Guideline needs to clarify this.
  - Defensive measures can eliminate the possibility of many types of digital failures and digital CCFs. The D3 Guideline makes the general statement that sufficient use of appropriate defensive measures provides reasonable assurance that the digital failure likelihood is acceptably low.

## Comments on D3 Guideline Item 3 -

5 of 9

- NRC comment: “ assumptions/statements made throughout the reports need supporting information data to substantiate the conclusion.”
  - Response: Request that NRC staff provide specific instances
- NRC comment: “... the report states that the addition of new equipment (assumed to be diverse backup) can have a negative impact on plant safety and that this additional risk should be evaluated, but there are no data present to substantiate the conclusion.”
  - Response: Will add supporting information for this conclusion. Intent was simply to express the position that adding complexity can have undesired and adverse effects and can decrease reliability.

## Comments on D3 Guideline Item 4 -

6 of 9

- NRC comment: “.... IEEE-379 states that certain CCFs will be treated as single failures.”
  - Response: IEEE-379 does not apply to software common cause failures because:
    - IEEE-379 applies to design basis events, but software CCF is beyond design-basis (see SRM to SECY 93-087)
    - Also, IEEE-379, Section 5.5,
      - Includes CCFs resulting from “...cascade failures and design basis events” in the single failure analysis
      - Excludes “Common-cause failures ...that can result from.....design deficiencies, manufacturing errors, maintenance errors, and operator errors.”

## Comments on D3 Guideline Item 5 -

7 of 9

- NRC comment: “EPRI TR-102348 requires additional information on how to perform D3 reviews, and more information, data and analysis to support the topical report conclusions associated with modeling methods and D3 defensive measures.”
  - Response: More discussion is needed to identify additional information needed
  - The D3 Guideline restricts the discussion to “what-to-do” guidance, because there are usually several valid approaches for how to perform specific tasks.
  - Detailed “how-to” guidance is a topic for a separate guideline

## Comments on D3 Guideline Item 6 -

8 of 9

- NRC comment: "... it is not clear that the approach described in EPRI TR-102835 for a limited D3 assessment with respect to the low likelihood of a single failure is justified."
  - Response: Further discussion is needed to understand this comment
- NRC comment: "... the guidance in RG 1.174 provides that the risk informed approach be consistent with the defense-in-depth philosophy."
  - Response: EPRI agrees. The approaches outlined in the guideline include both quantitative and qualitative analyses to assure existing D3 is appropriately maintained

## Comments on D3 Guideline Item 6 -

9 of 9

- NRC comment: "... the limited D3 review approaches proposed in the EPRI topical report do not appear to be consistent with RG 1.174."
  - Response: Section 4.3 of the D3 Guideline specifically explains how the approaches in the guideline meet the five principles of RG 1.174. Further discussion needed to understand this comment.
- NRC comment: "Note that approaches that are not consistent with existing guidance typically require additional review and analysis to determine whether or not they can be approved. Accordingly, the NRC staff cannot provide assurance that the proposed approach would be found acceptable."
  - Response: Additional discussion is needed on where NRC believes the D3 Guideline is not consistent with existing risk-informed regulatory guidance.

## Conclusions

- Use of risk insights will improve D3 evaluations
- We believe EPRI D3 Guideline provides an acceptable framework for D3 evaluations
- Additional discussion with NRC, including technical experts, is needed to address comments
- Recognize we will need to address revised positions from proposed SECY paper
- Industry is prepared to participate in workshops related to use of risk insights in digital applications
- When can we meet?

# Cyber Security

## Regulatory Guide 1.152 Rev 2 Challenges

NRC / Industry Meeting  
October 19, 2006  
Matt Gibson



## Problem Statement

- RG 1.152 R2 includes additional requirements for security in various lifecycle stages that go beyond what the current consensus standards provide.
- Due to review and approval scheduling issues this guide may not have been vetted against 10 CFR 73.55 and NEI 04-04 for potential conflict and overlap.
- RG 1.152 security guidance, based on life cycle methods, is at a level of detail that restricts the methods used to satisfy design requirements. This is especially true, when commercial grade dedication is involved.



## Specific Items

- Level of detail in RG 1.152 Section C.2 more appropriately belongs in reference documents
- Lifecycle items are addressed elsewhere
- COTS must be addressed



## C.2.2 Requirements Phase

- C.2.2.1: System Features – Move to IEEE 7-4.3.2. These requirements are generic and redundant and no additional clarification is needed in RG 1.152
- C.2.2.2: Development Activities – Move to IEEE 7-4.3.2 and clarify that unused features (code) are acceptable if tested and validated.



## C.2.3 Design Activities

- C.2.3.1: System Features – Move specific requirements to IEEE 7-4.3.2 including expectations and definitions for pre-developed software. Risk analysis should use NEI 04-04 methods.
- C.2.3.2: Development Activities – This process is covered by NEI 04-04 and reinforced by 10 CFR 73.55



## C.2.4 Implementation Phase

- C.2.4: Integrate summary requirement into IEEE 7-4.3.2
- Remainder of section should be per NEI 04-04.



## C.2.5 thru C.2.9

- These sections are fully redundant to NEI 04-04 and Codified in 10 CFR 73.55



## Recommendation

- Revise RG 1.152 to remove Security requirements and endorse NEI 04-04 (short term)
- Endorse NEI 04-04 in upcoming SRP update for Chapter 7. Cite 10 CFR 73.55 in Chapter 7 (short term)
- Revise IEEE 7-4.3.2 to be Cyber security aware (for selected items) and coordinate requirements contained in NEI 04-04 ( long term)



# Human Factors Discussion

Industry/NRC Meeting  
October 19, 2006

Tony Harris – NEI  
Joseph Naser – EPRI  
Bob Fink – CDF Services  
Warren Busch – FP&L



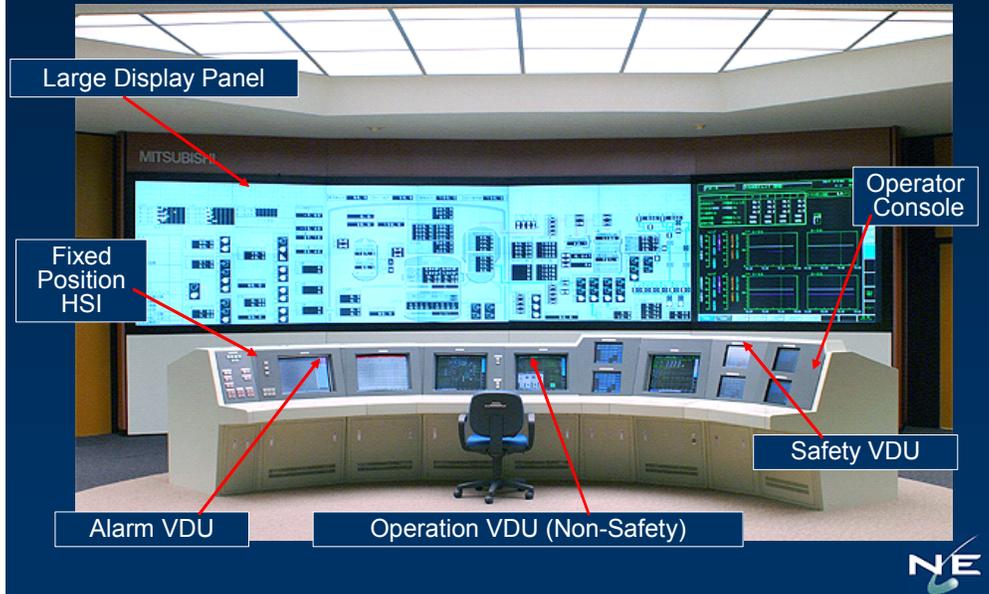
## General Environment

- New plants will fully computerize control rooms
  - Concept is not new
  - Already in use in many other industries and in nuclear plants in other countries
- Existing plants are modernizing their control rooms
- DG-1145 Development Ongoing
- Standard Review Plan Update Ongoing



# HSI System

## Computerized Main Control Room - APWR



## Challenges

- Understanding research efforts NRC is planning or has in progress and how this might impact existing guidance
- Concept of minimum inventory lacks clarity, expectations of timing don't match development process timeline
- Resolution of safety / non-safety interface issue could significantly impact control room design
- Potential changes to NUREG-0711



## Common Vision

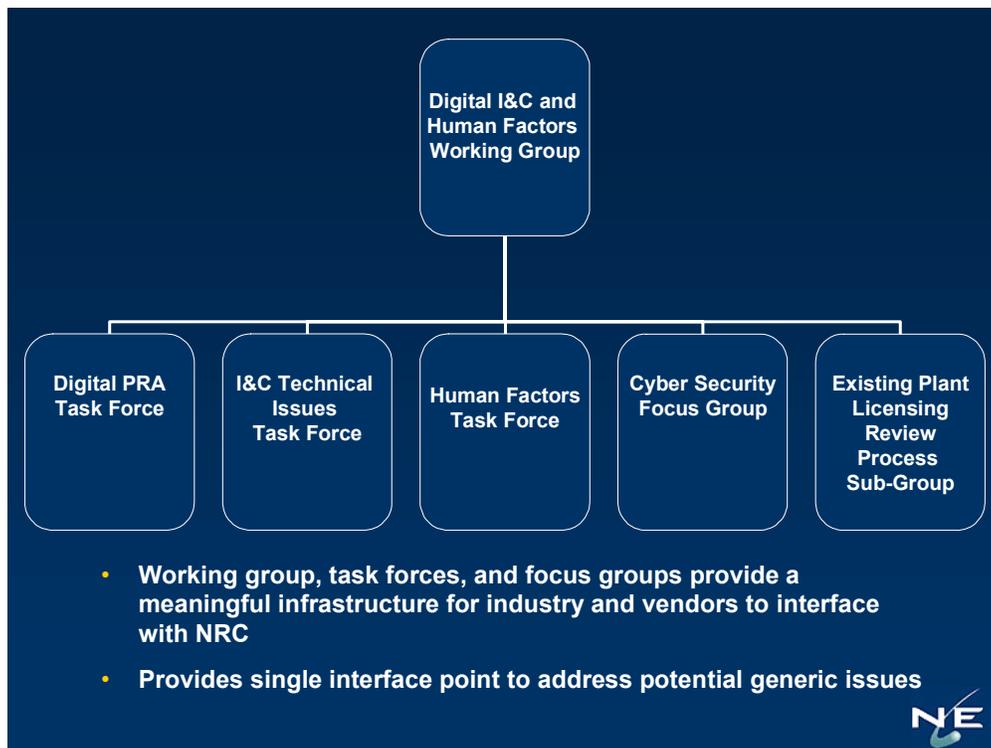
- Ensuring consistent, high quality submittals from licensees adopting advanced control systems
- Identify and resolve issues generically when applicable
- Timely and properly focused research efforts



## Today's Goals

- Set the stage for future interactions as issues become apparent
- Achieve a better understanding of research activities needed to support licensing of advanced control systems
- Identify a strategy for resolving minimum inventory clarity issue
- Understand potential common concerns NRC may have identified in reviews to date (e.g., RAIs)





## Human Factors Task Force

The Human Factors Task Force coordinates human factors and control room design issues associated with use of digital technology for both existing and new plants.

### MEMBERSHIP

- NEI
- Utilities
- New Plant Vendors
- EPRI

### PRIORITY ISSUES

- DG-1145 Re-write
- Identifying and resolving technical issues
- Interfacing with NRC on research initiatives



## NRC Research Plans

- We would like to hear about the NRC research activities needed for both new and existing plants
  - Human Factors Research
  - I&C Research on issues associated with "glass control rooms" and other related areas
- We would like to understand the basis for the research, schedule for completion, and potential impact on existing guidance
  - Concerned about potential impact on new plant schedules



## Minimum Inventory

- Issue identified in design certification reviews and DG-1145 comment period
- Intended in part to deal with lack of detail available at design certification stage
- Different interpretations of the intent have arisen
  - Ensure adequate backup capability in case of large-scale failure of computer-based HSIs
  - Ensure selected HSIs are in fixed positions (spatially dedicated, continuously visible or SDCV)



## Minimum Inventory (cont'd)

- Existing regulatory guidance documents lack clarity
- Must go to detailed design review results to see how it has been applied
  - Not always consistent among the reviews
- Interacts with other issues such as HSI failure modes/backups, level of qualification needed for different HSIs, and RG 1.97 PAM instrumentation guidance



## Minimum Inventory (cont'd)

- Industry approach has been developed (EPRI 1010042)
  - Provides method for addressing underlying technical issues for minimum inventory and other inter-related technical/design issues
  - Provides guidance for implementing this method, clarifies existing regulatory and industry guidance



## Minimum Inventory (cont'd)

- Summary of method:
  - Determine HSI failure modes and concept of operations for failed/degraded conditions
  - Categorize functions and tasks into groups
    - Ex: Credited manual actions, monitoring and backing up automatic actions, manual actions called out in EOPs, post-accident monitoring, etc.
  - For each group, determine requirements for HSI qualification, independence, and accessibility



## Minimum Inventory (cont'd)

- Requirements determined for HSI resources needed for each function/task group:
  - Prompting indications and alarms
  - Controls plus immediate feedback needed to confirm control actions
  - Indications and alarms for monitoring performance
- Results captured in a table or matrix



## Minimum Inventory (cont'd)

Table 6-2  
HSI Design Requirements Applicable to each Function/Task Category

Functions/Tasks and Associated HSIs	Qualification <sup>1</sup>	Independence, Diversity, Simplicity <sup>2</sup>	Accessibility <sup>3,4</sup>	Applicable Regulatory and Industry Requirements and Guidance
1. Perform Credited Manual Actions (6.5.4.3.1)				
Prompting indications	Fully qualified	Independent of DCS HSIs	SDCV	SAR safety analyses identify credited actions IEEE 603 Reg. Guide 1.97 (Category 1, Type A)
Prompting alarms	No qualification requirement. However, consider providing alarm capability on same qualified display used for prompting indications .	Independence from DCS HSIs should be considered, whether qualified or not	Consider SDCV display for these alarms	
Controls & immediate feedback indications	Fully qualified	Independent of DCS HSIs	SDCV, or one-step accessible if supported by appropriate HFE analyses	
Performance	Intermediate	Independent of	SDCV for	



## Minimum Inventory (cont'd)

- Result: integrated approach that treats minimum inventory within the context of the related regulatory and design issues
- Addresses levels of qualification of different HSIs
- Addresses levels of accessibility of HSIs (e.g., SDCV or “one-step accessible”)
- Acceptable means of meeting regulatory guidance



## Minimum Inventory Proposed Approach for Resolution

- Industry needs to update work done in EPRI to address lessons learned from design certifications and clarify relationship to RG 1.97 R4
- Industry develops and submits “white paper” to the NRC for review and endorsement
- Meeting / teleconference to discuss concerns / issues
- NRC endorsement of white paper through upcoming SRP update or other means



## NRC Reviews

- HF Task Force would like to hear NRC thoughts on potential common concerns NRC may have identified in reviews to date (e.g., RAIs)
- Look to understand how we can help resolve these issues
- Are there other issues out there that the staff wants to discuss or is contemplating research on?



## Summary

- Industry appreciates the time NRC has taken to meet with us today
- Means now established for NRC and industry interactions on human factors issues
  - Industry wants to understand scope and impact of NRC research plans
  - Industry proposal for dealing with minimum inventory can be a pilot for resolving generic issues going forward
  - Safety / non-safety communication issue could have significant impact for ongoing design efforts and new plant schedules
  - Industry appreciates NRC staff feedback on issues seen to date in reviews and other possible issues

