

**COMMISSION BRIEFING SLIDES/EXHIBITS**

**BRIEFING ON DIGITAL INSTRUMENTATION AND CONTROL**

**JULY 18, 2007**

# Digital I&C – Industry Perspectives

July 18, 2007

Amir Shahkarami  
Sr. VP Engineering & Technical Services  
Exelon Corporation



NUCLEAR  
ENERGY  
INSTITUTE

# Topics

- **Objective**
- **Communication**
- **Project Plan**
- **Conclusions**

# Objective

- **Safety-focused application of digital technology**
  - Design certification
  - Current operating plants
  - New plants
  - New facilities
- **Stable, predictable and timely licensing process with realistic guidance**
- **Enhance plant safety, availability and reliability**

# Communication

- **NEI Digital I&C and Human Factors Working Group**
  - Reports to industry Chief Nuclear Officers
  - Participate on the Digital I&C Steering Committee
  - Coordinate with NEI New Plant Working Group
  - Major vendor participation
  - Integrated, focused attention to ensure safety-focused, stable and predictable licensing process

# Project Plan

- **Disciplined Framework**
  - Issue scope and definition
  - Deliverables
  - Milestones
  - Accountability
  - Integrated approaches to resolution
- **Fundamental tool for management oversight and coordination**

# Conclusions

- **Progress has been made**
- **Project plan provides a framework going forward**
  - **Integrate lessons learned and other improvements**
- **Maintain focused management attention during the longer term**



ELECTRIC POWER  
RESEARCH INSTITUTE

# **Digital Instrumentation & Control – EPRI Role**

July 18, 2007

Chuck Welty

Technical Executive

Electric Power Research Institute



# Acronyms

EPRI	–	Electric Power Research Institute
I&C	–	instrumentation and control
R&D	–	research and development
MCR	–	main control room
PRA	–	probabilistic risk assessment
HFE	–	human factors engineering
ANT	–	advanced nuclear technology
SER	–	safety evaluation report
PLC	–	programmable logic controller
ASIC	–	application specific integrated circuit
FPGA	–	field programmable gate array
CCF	–	common-cause failure

# EPRI Digital I&C R&D

- Substantial past/ongoing activities on digital I&C, MCR, risk and human factors
- Guided by extensive utility advisory structure
  - Expertise – I&C, PRA, HFE and ANT
- Several products with SERs
- Basis for industry technical positions
- Areas of information exchange and interaction with NRC

EPRI has substantial expertise and proven capabilities

# EPRI R&D on Digital I&C

- Licensing digital upgrades 1992-2004
- Verification & validation 1992-1998
- Electromagnetic interference 1992-
- Commercial devices – PLCs, ASICs, FPGAs, wireless, etc. 1993-
- Control room/human factors 2001-
- Defense-in-depth and diversity 2002-
- Applying risk methods 2002-

# Current EPRI Support

- Defense-in-depth and diversity
  - Use design and diversity for CCF protection
- Risk-informed methods
  - Existing methods provide insights to focus design and review efforts
- Human factors
  - Bases for minimum inventory of interfaces, computerized procedures, graded HFE design approach
- Ongoing evaluation of operating experience

# Future EPRI Activities

- Interaction with NRC Research has not been as extensive as it could be – we want to help improve this
- Interim Staff Guidance documents are only a start – our advisors expect us to continue to work with NRC to resolve the issues completely



# Digital Modernization Hurdles and Solutions

7-18-07

Ken Brown

Vice President Invensys



# About Invensys

- Invensys PLC – 30,000 employees, in 60 countries
  - Invensys Process Systems (IPS)
    - Comprised of Foxboro, Triconex, Wonderware, Simsci-Esscor, Avantis, Validation Technologies
- IPS is presently providing input to the industry working groups and the NRC



# Digital Instrumentation and Control Issues in the Nuclear Industry

- Diversity, Defense in Depth – D3
- Risk Informed Digital I&C
- Operator Training
- Cyber Security
- Lessons Learned from other Industries





# Diversity, Defense in Depth

- IPS – install a highly available, highly reliable Triple Modular Redundant (TMR) controller for Reactor Protection and ESFAS with a diverse digital controller I/A series
- Use technology to solve this issue – not challenge the license base or operation position



## Diversity, Defense in Depth

- Invensys and our customers need a workable and understandable position on issues of concern – causing confusion and delays
- Common Cause Failure – extensive diagnostics and a highly developed platform substantially reduce this risk



# Risk Informed Digital I&C

- Consultative teaming relationship
- TMR technology – deployed on safety, mission critical, and life critical systems
- This technology currently supports High Probabilistic Reliability Analysis numbers
- Need to evaluate and take credit for methodologies used in other countries and industries



# Operator Training

- TMR, Fault Tolerant, High Diagnostic systems allow for minimal training for Operations
- Can be used on Important To Safety and Safety Related applications minimizing training



# Cyber Security

- Invensys is committed to industry leading cyber security initiatives
- Utilize Wurldtech Securities Achilles Level 1 assessment test as Cyber Security benchmark



# Lessons Learned from other Industries

- Triconex is by far the most trusted safety system in the continuous process industries
- Make obsolescence “Obsolete
- Provide Digital Commercial Off The Shelf Technology (COTS) Solutions under a 10CFR Appendix B program
- IPS safety platform meets safety criteria for Hydro Carbon Industry and Rail Signaling Industry



# Conclusion

- We are pleased with the progress being made by the recent working groups
- Facilitate technology transfer from other Mission Critical / High Reliability industries
- Staff should continue to develop consultative relationships with key technology providers



## Conclusion

- IPS encourages the staff to engage I&C design early in COL phase for new builds
- IPS is committed to the industry, to help resolve I&C issues, on existing and new plant designs to accelerate the renaissance of nuclear power





---

# **AP1000**

# **Digital Instrumentation and**

# **Control**

**July 18, 2007**

**Cynthia McGinnis**

**Westinghouse Electric Company**

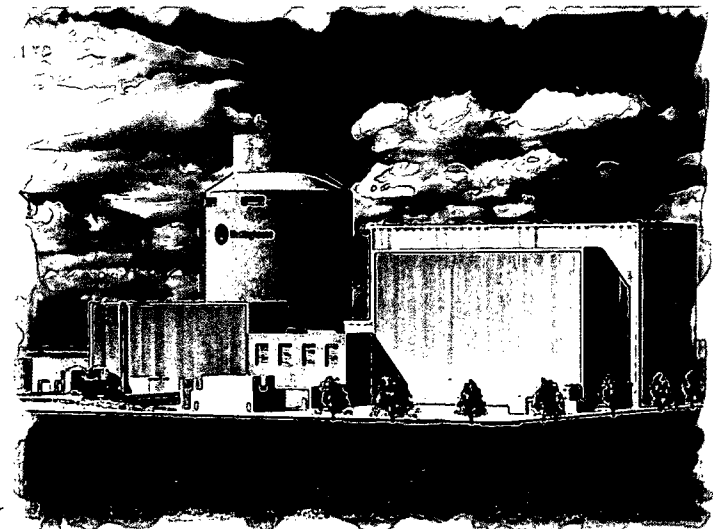


# AP1000 Design Certification Finality

---



- **Functional Design**
- **Applicable codes and standards**
- **Basic architecture**
- **Diversity/Defense-in-Depth**
- **Minimum Inventory**
- **Diverse Actuation Functions**
- **Design Acceptance Criteria**



# **AP1000 I&C Design and Licensing Efforts**

---



- **Plant Simplicity Drives I&C Safety System Simplicity**
  - **One-time component actuation**
- **Common Q Platform**
- **“Simple” digital I&C implementation**
- **Technical Reports**
- **Existing requirements and Guidance remain applicable**

# Fundamentals the Same as Operating Plants

---



- **Functional Basis – Simplistic and Transparent**
- **Architecture Basis**
  - **Divisional Independence**
  - **Safety/Non-Safety Separation**
  - **Isolation**
- **Communications and Architecture driven from operating plant design and experience**
- **Analog to Digital Implementation does not impact Fundamental Philosophy**

# **AP1000 I&C Evolutions**

---

- **Diverse Actuation Functions**
  - **Functionality resolved in Design Certification**
  - **Separate sensors/actuators from those used by the Safety System**
  - **New Plant (clean sheet) flexibilities**
- **Priority for safety system actuation**
- **Cyber Security Issues**
  - **AP1000 Technical Report**
  - **Consistent with NEI-04-04**

# **AP1000 Licensing Efforts**

---

- **Design Certification resolved many I&C issues for the AP1000 Design**
- **Technical Reports/DCD Revision 16 to resolve I&C DAC**
- **NRC interactions to establish sufficient information for reasonable assurance**
- **Simplistic digital I&C application results in acceptable use of existing regulatory requirements and guidance**

# **AP1000 Licensing Efforts**

---

- **Development of Cyber Security Plan**
  - **TR is developed and submitted**
  - **Continued work with Industry and Staff to resolve the issues/concerns**
  - **Consistent with NEI-04-04**
- **Westinghouse-proposed schedule for resolution by Spring 2008**

# Conclusions/Comments

---

- **Design Certification resolved many I&C issues for AP1000**
- **Existing NRC regulatory requirements and guidance sufficient to evaluate AP1000 I&C safety system**
- **Licensing basis for I&C in the design certification rule**
- **Propose to resolve I&C DAC in DCD amendment currently under NRC staff review**
- **Result in elimination of the DAC from the AP1000 Design Certification Rule upon successful NRC reasonable assurance conclusion**
- **Operating plant upgrade issues different**





# **DIGITAL I&C**

# **&**

# **Grid Operations**

July 18<sup>th</sup> 2007

Tom Bowe

PJM Interconnection

[bowet@pjm.com](mailto:bowet@pjm.com)





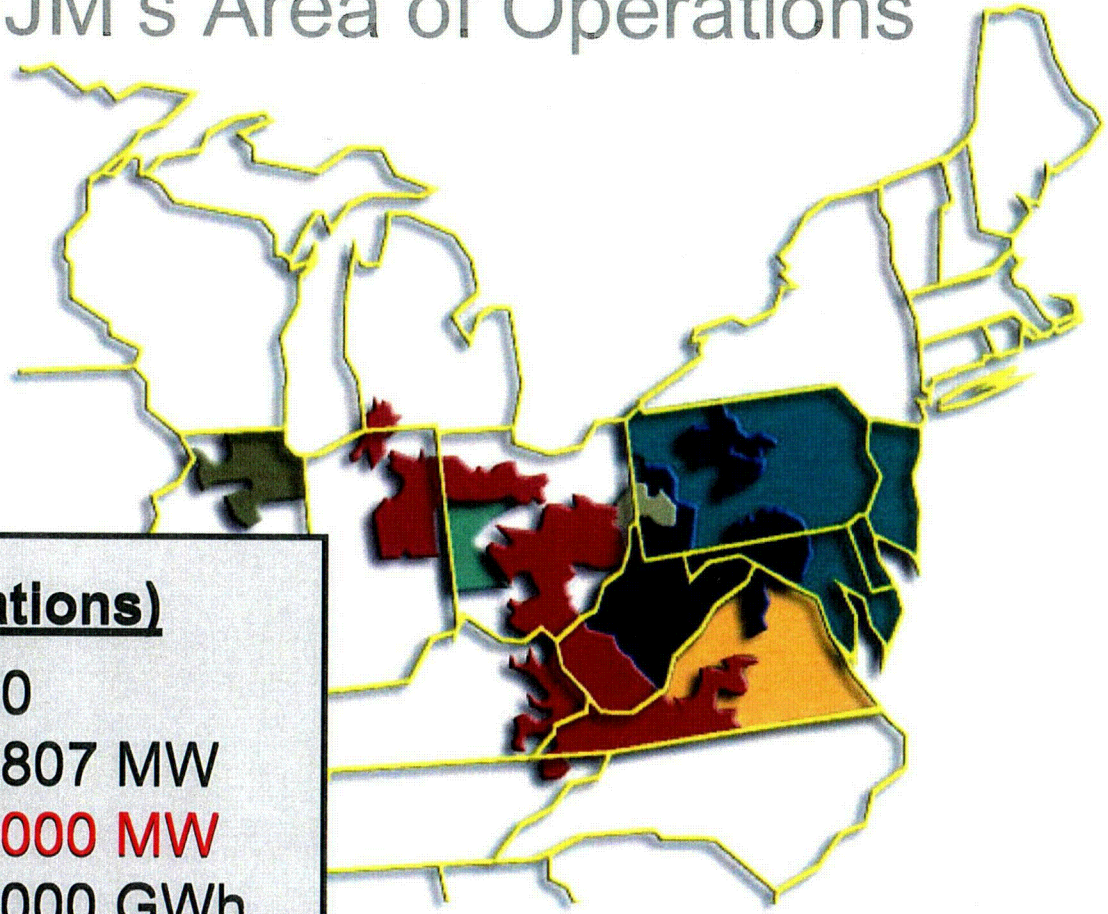
# PJM's MISSION

- Maintain the safety, adequacy, reliability and security of the bulk power system
- Create and operate a robust, competitive, and non-discriminatory electric power market
- Ensure that no Member or group of Members has undue influence

**RTO = Regional Transmission Operator**



# PJM's Area of Operations



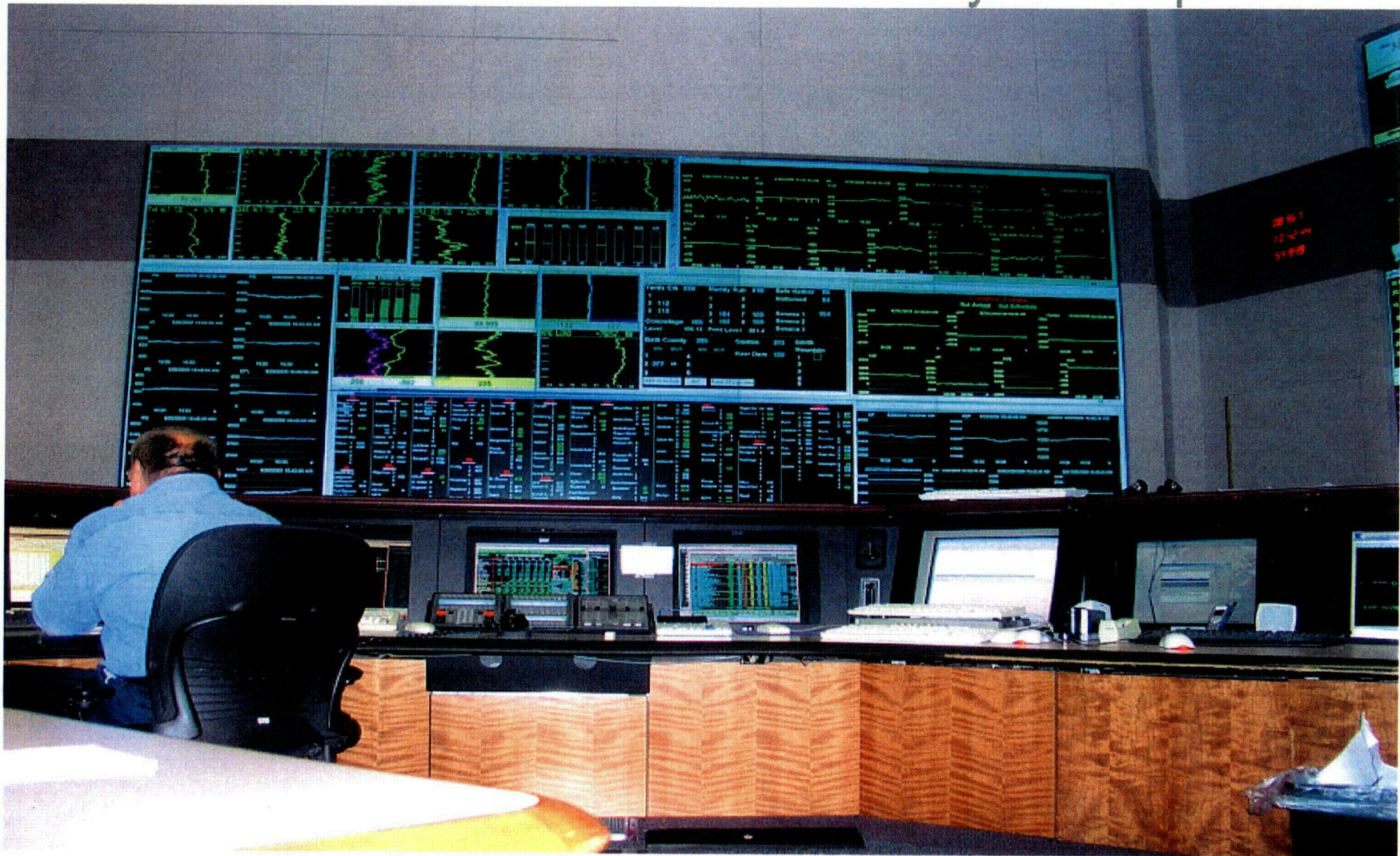
## PJM RTO (Post-integrations)

Generating Units	1,400
Generation Capacity	170,807 MW
Peak Load	<b>144,000 MW</b>
Annual Energy	648,000 GWh
Transmission Miles	55,000
Area (Square Miles)	186,000
Customers	21 Million
Population Served	<b>50+ Million</b>
States (+ D.C.)	13 states + D.C.

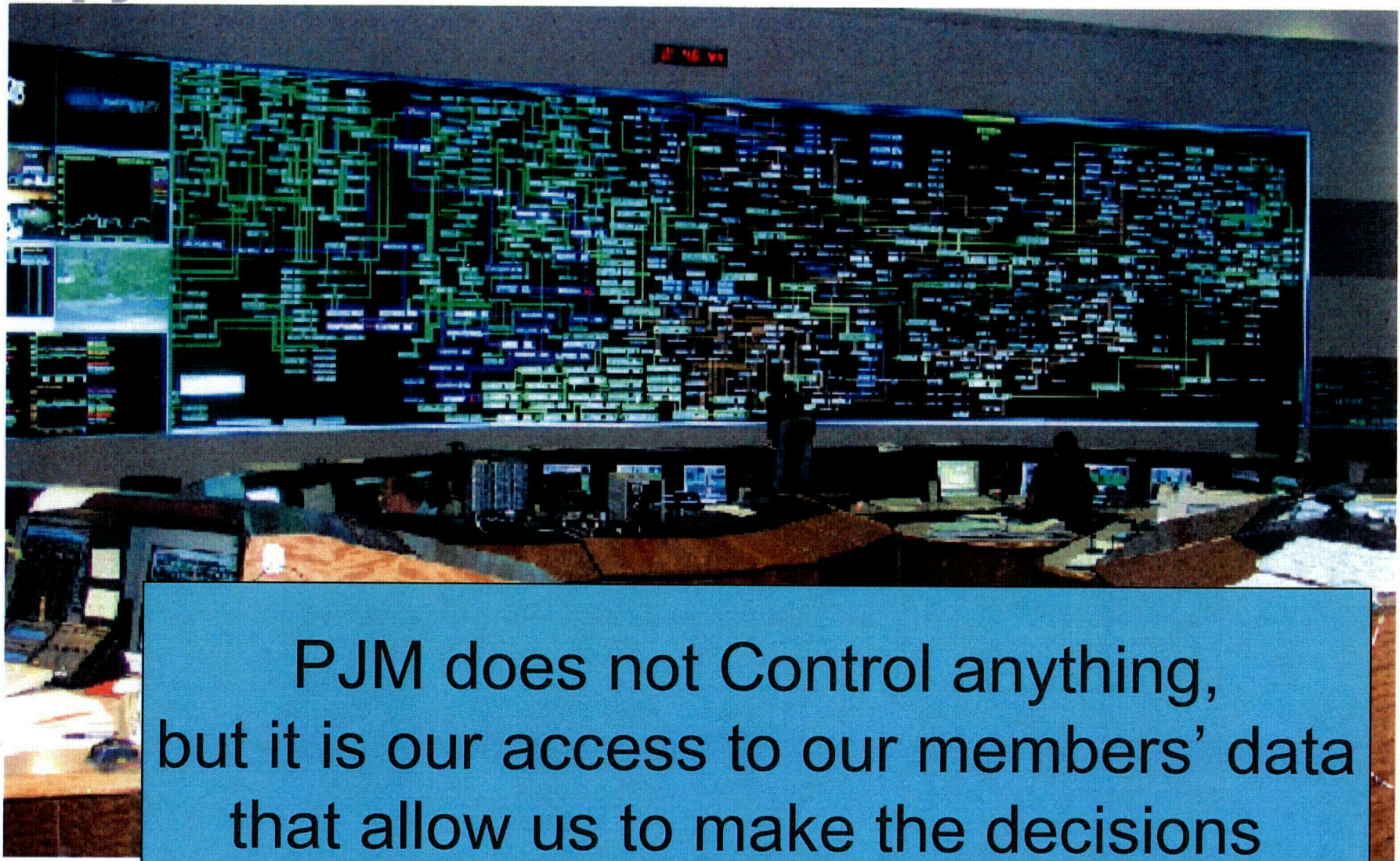




# Generation System Operator







PJM does not Control anything,  
but it is our access to our members' data  
that allow us to make the decisions  
that protect the grid





## Back-Up Capability

- We Must Maintain Situational Awareness & a Wide Area View
  - Y2K
  - September 11<sup>th</sup> 2001
  - August 14<sup>th</sup> 2003
- PJM exists on its data streams
  - Multiple and Diverse Communication Paths
- Digital I&C Provides for Greater Visibility and Flexibility
- Creative Training

- Starts with Defining – “What is Critical?”
- If everything is critical than nothing is . . .
- Must also define the “Electronic Perimeter”
  - Defense in Depth
  - Network Segmentation
- Conduct Independent Vulnerability Assessments
- NERC Critical Infrastructure Protection Standards (CIP 002-009) and/or ISO 17799



## PJM's Advanced Control Center Concepts

- Visualization with a focus on human factors and role vs. function based displays
- The evolution of intelligent event processing and intelligent agents
- Improvements in control through advanced algorithms, improved visualization, advanced look ahead, modeling of heuristics.
- Synchronized control centers for rapid recovery





# **COMPUTING SUBSYSTEMS**

## **(Safety and Reliability Challenges)**

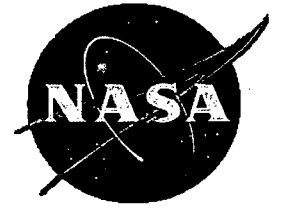
**July 18, 2007**

**Homayoon Dezfuli, Ph.D.**  
**Manager, System Safety**  
**Office of Safety and Mission Assurance**  
**NASA Headquarters**



# Role of Computing Subsystems

- **Perform safety-critical and mission-critical functions**
  - Power management
  - Telemetry
  - Data and information handling
  - Communication
  - Hardware automation and control
- **Have contributed to several spacecraft accidents**
  - Software data specification errors
  - Software design specification errors



# What is NASA Doing?

- **Improving system engineering (SE) processes to better handle hardware/software, software/human and software/software interfaces and design trade studies**
- **Improving software assurance processes**
- **Exploring the applicability of risk assessment techniques to risk-inform the SE and software assurance processes**



# Challenges for Risk-informing Software Safety

- **Need: Ability to predict (or bound) with a given level of confidence the likelihood of mission failure due to latent software defects to support**
  - Risk management decisions (e.g., designing SW testing regimes for risk significant configurations)
  - Risk acceptability decisions (e.g., showing that a probabilistic safety criterion is being met)
- **Based on results to-date, it appears that a combination of techniques is needed to satisfy this need**



# Exploratory Ideas

- **Risk management decisions**
  - Application of scenario-based accident modeling techniques to identify system-critical configurations, flight mode changes, and flight transients
  - Risk-informed testing regimes
- **Risk acceptability decisions**
  - Assignment of initial reliability levels (ranges) based on attributes such as design complexity, and SW quality V&V process considerations (risk classification of software elements)
  - Adjustment of reliability levels based on V&V and risk-informed test process findings (updating of initial reliability levels)
- **Continue focused research**
  - Beneficial to work with NRC



**Briefing on Digital Instrumentation  
and Controls  
Update on New Reactors  
Update on Digital Research Platform**

---

**July 18, 2007  
Luis Reyes  
Executive Director for Operations**

# Acronyms

---

ABWR	Advanced Boiling Water Reactor	NFPA	National Fire Protection Association
ACRS	Advisory Committee on Reactor Safeguards	NMSS	Office of Nuclear Material Safety and Safeguards
APWR	Advanced Pressurized Water Reactor	NRC	Nuclear Regulatory Commission
BWR	Boiling Water Reactor	NRO	Office of New Reactors
COL	Combined License	NRR	Office of Nuclear Reactor Regulation
D3	Diversity and Defense-in-Depth	NSIR	Office of Nuclear Security and Incident Response
DC	Design Certification	NUREG	technical report ( <u>Nuclear Regulatory Commission</u> )
DOE	Department of Energy	OGC	Office of General Counsel
EIS	Environmental Impact Statement	PRA	Probabilistic Risk Assessment
EPR	Evolutionary Power Reactor	PWR	Pressurized Water Reactor
EPR	Evolutionary Power Reactor	RAI	Request for Additional Information
EPU	Extended Power Uprate	RES	Office of Nuclear Regulatory Research
ESP	Early Site Permit	RG	Regulatory Guide
ESBWR	Economic Simplified Boiling Water Reactor	RIS	Regulatory Issue Summary
FPGA	Field-Programmable Gate Array	SRM	Staff Requirements Memorandum
FPL	Florida Power & Light Company	SRP	Standard Review Plan
FY	Fiscal Year	SWP	Strategic Workforce Planning
GDC	General Design Criteria	TVA	Tennessee Valley Authority
I&C	Instrumentation and Control	TXU	Texas Utilities Energy Corporation
INPO	Institute for Nuclear Power Operations	SER	Safety Evaluation Report
IT	Information Technology	SGI	Safeguards Information
LLTF	Lessons Learned Task Force	TWG	Task Working Group

# Agenda

---

**Introduction**

**L. Reyes**

**Readiness for New Reactors**

**W. Borchardt**

**Digital I&C Research Platform**

**R. Croteau**

**Digital I&C Steering Committee**

**J. Grobe**

**Diversity and Defense-in-Depth**

**M. Mayfield**

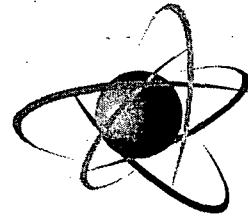
**Highly-Integrated Control Room**

**M. Cunningham**

**Digital Risk Assessment**

**M. Cunningham**





**U.S. NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

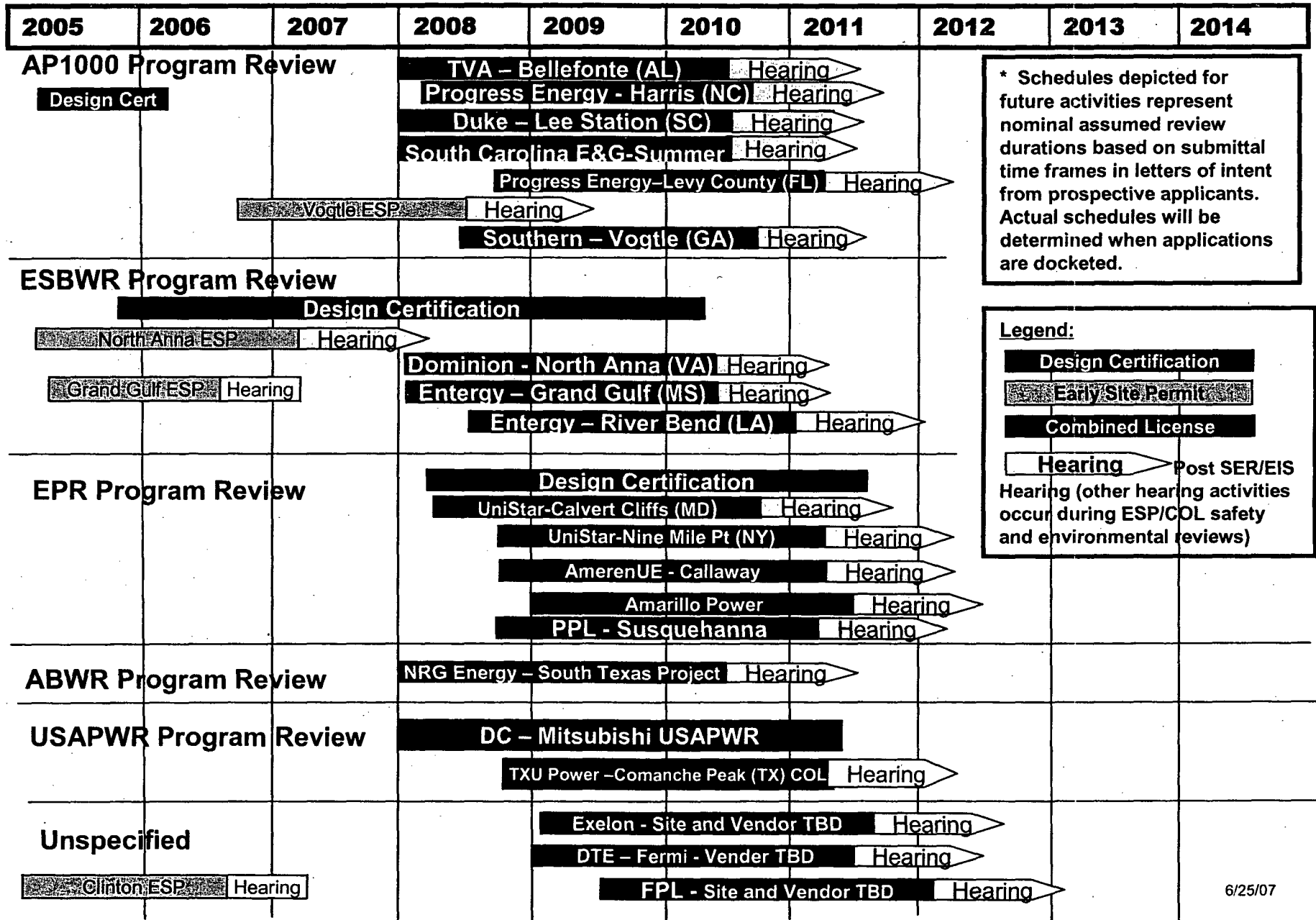
# **Readiness for New Reactors**

---

**William Borchardt  
Office of New Reactors**

# New Reactor Licensing Applications

An estimated schedule by Fiscal Year



# **New Reactor Infrastructure**

---

- **Approved Rulemakings: Part 52 and Limited Work Authorizations**
- **Finalized Regulatory Guide 1.206 “Combined License Applications for Nuclear Power Plants”**

# **New Reactor Infrastructure**

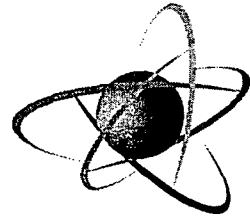
---

- **Completed final wave of staff transfers from NRR**
- **Populating Licensing Program Plan**
- **Developed Combined License application acceptance review guidance**

# **Pre-application Activities**

---

- **Pre-Combined License interactions and site visits, and application readiness assessment visits**
- **Public outreach**
- **Design Centered Working Group meetings**
- **International interactions**
- **Orders imposing safeguards information protection requirements**



**U.S.NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

# **Research Platform**

---

**Rick Croteau**

**Office of Nuclear Regulatory Research**

# Test Facility

---

- **Develop a defined set of concepts**
  - **Input from interested stakeholders**
  - **Investigating other similar facilities**
- **Conduct a public workshop**
  - **September 6 & 7 - technical issues**
  - **September 11 - non-technical issues**
- **Prepare Commission paper**
  - **Results of workshop**
  - **Recommendations on path forward**



# **Digital Instrumentation and Controls Steering Committee**

---

**Jack Grobe**  
**Office of Nuclear Reactor Regulation**



# **Background**

---

- **November 8, 2006, Commission briefing**
- **December 6, 2006, Staff Requirements Memorandum**
- **January 12, 2007, memorandum established the Digital I&C Steering Committee**

# **Key Challenges**

---

- **Assuring predictability through refined Regulatory Guidance**
- **Anticipating future needs**
  - **Evolving technology**
  - **Industry priorities**
- **Improving stakeholder interactions**
- **Expanding domestic and international interactions**

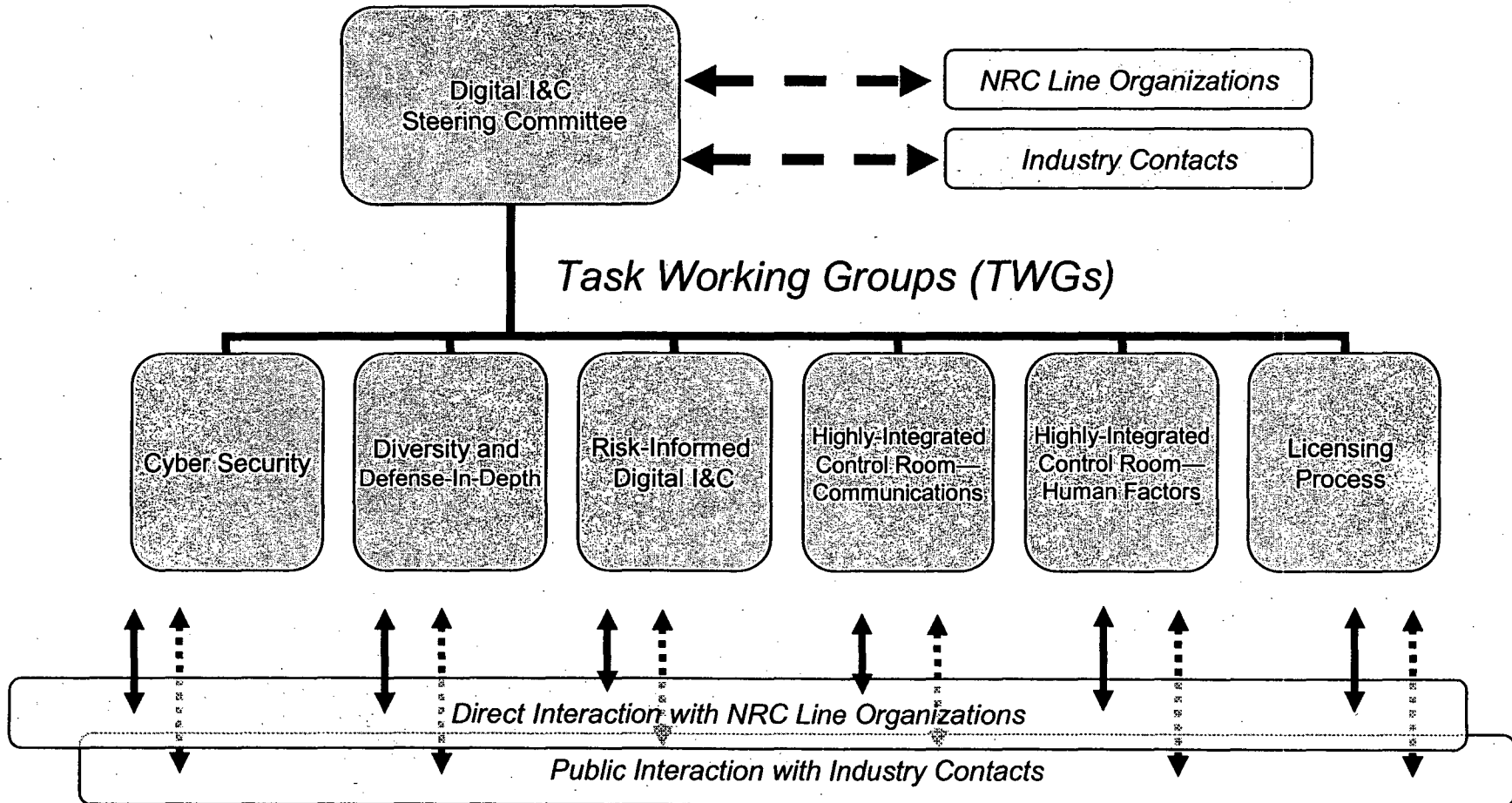
# **Digital I&C**

## **Future Workload**

---

- **Operating reactor modifications**
- **Design Certification**
- **Combined License**
- **Fuel-cycle facilities**

# Steering Committee



# **Structure of Project Plan**

---

- **Defined problem statements under each Task Working Group**
- **Developing Interim Staff Guidance (near-term)**
- **Interactive effort with industry**
- **Revise Regulatory Guides and industry standards (long-term)**

# **Stakeholder Interactions**

---

- **Conducted 30 public meetings with the industry since November 2006**
  - **5 Public Steering Committee meetings**
  - **25 Public Task Working Group meetings**
- **ACRS interactions**
- **Expanded domestic and international interactions**



# **Diversity and Defense-in-Depth**

---

**Michael Mayfield  
Office of New Reactors**

# **Diversity and Defense-in-Depth**

---

- **Common-cause failures are credible**
- **Current guidance has been successfully used**
- **Staff is working to improve existing guidance**



# **Diversity and Defense-in-Depth**

---

- **Seven key issues being addressed:**
  - **Adequate diversity**
  - **Operator action**
  - **Component vs. system level actuation**
  - **Effects of common-cause failures**
  - **Common cause failure applicability**
  - **Echelons of defense**
  - **Single failure**

# **Diversity and Defense-in-Depth**

---

- **Development of Interim Staff Guidance is well underway**
  - **Acceptable diversity and defense-in-depth criteria**
  - **Criteria on remaining issues under internal review**

# **Diversity and Defense-in-Depth**

---

- **Path forward**
  - **Issuance of Interim Staff Guidance**
  - **Continued interaction with industry**
  - **Update Regulatory Guides and Standard Review Plan**



# **Highly Integrated Control Room—Communications and Risk Assessment**

---

**Mark Cunningham**  
**Office of Nuclear Reactor Regulation**

# **Highly-Integrated Control Room—Communications**

---

- **Communications issues**
  - **Between safety divisions**
  - **Between safety and nonsafety equipment**
- **Staff is working to improve guidance**

# **Highly-Integrated Control Room—Communications**

---

- **Four key technical areas**
  - **Inter-divisional communications**
  - **Command prioritization**
  - **Multi-divisional control/display stations**
  - **Network configuration**

# **Highly-Integrated Control Room—Communications**

---

- **Improved guidance on schedule**
  - **Inter-divisional communications**
  - **Command prioritization**

# **Highly-Integrated Control Room—Communications**

---

- **Continuing interactions**
  - **Multi-divisional workstations**
    - **Non-safety workstations for safety indication and control**
  - **Network configuration**



# **Highly-Integrated Control Room—Communications**

---

- **Path forward**
  - **Issuance of Interim Staff Guidance**
  - **Continued public interaction with industry**
  - **Update Regulatory Guides and Standard Review Plan**

# **Digital Risk Assessment**

---

- **Expanding Use**
  - **Risk insights in design certifications**
  - **Risk-informing regulatory practices**
- **Staff is working to develop guidance**

# **Digital Risk Assessment**

---

- **Risk insights**
  - **Information sources**
    - **Industry white papers**
    - **NRC research**
    - **Operating experience**
- **Path forward**
  - **Continued public interactions with industry**
  - **Develop Interim Staff Guidance**

# **Digital Risk Assessment**

---

- **Risk-informing regulatory practices**
  - **State of technology**
- **Path Forward**
  - **Continued public interactions with industry**
  - **Develop guidance**

# Summary

---

- **Steering committee is functioning effectively**
- **Project plan is in place**
- **Interim Staff Guidance is being developed**
- **Stakeholder interactions**
- **Strong industry support**
- **Staff is on-schedule to complete near-term deliverables**