MITSUBISHI BRIEFING TO THE NRC COMMISSIONERS ON INSTRUMENTATION AND CONTROLS

February 1, 2011

C. Keith Paulson, Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.

MITSUBISHI'S HISTORY OF I & C REGULATORY INTERACTIONS

US-APWR

- Early 2006 — Mitsubishi's first meeting with the NRC to discuss DCD regulatory review
- November 2006 — First Mitsubishi I & C presentation to the NRC Staff
- March 2007 — I & C Topical Reports submitted
  - System Design & Design Process
  - Platform Design
  - Defense-in-Depth & Diversity & HIS/HFE
- December 2007 — Software Program Manual
- December 2007 — US-APWR Design Control Document
- February 2009 — First DCD RAIs received

NRC REVIEW SUMMARY AND STATUS

1. The NRC review of the Mitsubishi Digital I & C started out slowly. Early schedule impacts were caused by:

   A. Mitsubishi's position in the NRC priority ranking
   B. Change/Availability of reviewers

<u>Stat Status</u>

Substantial improvement in resources and priority have occurred within the last six months. Several Public Meetings and conference calls have been held with critical current areas that have been identified as requiring focused attention.

NRC REVIEW SUMMARY AND STATUS CONTINUED

2. Current issues impacting the pace of Mitsubishi's I & C review:

   A. The regulatory "template" to be required for the Software Program Manuals (SPMs) has been evolving for several years. In general, Mitsubishi's initial documents were completed during this time period.

      NRC reviews of the Mitsubishi SPMs content identified additional information was necessary.

<u>Status</u>

Several supplier reviews have identified an accepted form and content for SPMs. Mitsubishi has resubmitted the SPMs following the content accepted by the NRC.

NRC REVIEW SUMMARY AND STATUS CONTINUED

B. The NRC staff identified that the review time required to assure the Mitsubishi data communication interactions complies with ISG-04, Highly Integrated Control Rooms Communication Issues, would be significant.

Status

Mitsubishi has proposed three modifications that will assure operation of the safety functions even if non-safety signals are assumed present. These modifications should reduce the Technical Staff review time.

LESSONS LEARNED

- Digital I & C designs for control and protection systems has been under review in the U.S. for more than 20 years. ISG documents were developed with industry support to provide a regulatory process that would "fast-track" the review time. Key areas addressed were:

  1. Interdivision Data Communication – (ISG-04)
  2. Defense in Depth and Diversity, PRA – (ISG 2 & 3)
  3. Licensing Process – (ISG 6)

- The ISG efforts to "fast track" the regulatory review of digital I & C provided a good start, but has not yet met all its objectives.

LESSONS LEARNED CONTINUED

- Suppliers have simplified their designs to achieve reductions in the I & C regulatory acceptance review period thereby not considering the benefits of the original design.

- Availability of NRC technical staff limits the pace of current and future the reviews.

MITSUBISHI'S I & C DESIGN CAN ENHANCE THE NRC GENERIC REVIEW

US-APWR

- Mitsubishi has already implemented Digital I & C Safety and Protection Systems in Japanese Plants and has complete design information.
- Japanese Regulatory Requirements follow very closely those required by U.S. Regulations.
- Availability of complete design information can compliment and expedite the evolving regulatory review process.

RE-FAST TRACKING DIGITAL I & C REVIEWS

US-APWR

- Rekindle the ISG efforts for New Plants and Operating Plants.
- Where possible, use risk informed decision-making to determine measurable cost/benefits decisions.
- Use I & C designs that have completed advanced stages of engineering to support additional ISG efforts.
- Prudently expand NRC technical staff to reduce review times, and support ISG updates including related risk informed decisions.
- Based on industry commitments, focus independently, but collaboratively on new and operating plants.
- Reconsider operating plant upgrade requirements to focus on front- loaded risk.

U.S. EPR^{TM} Digital I&C

Thomas E. Sliva
Vice President, New Plants Projects
AREVA NP Inc.

1 February 2011

AREVA

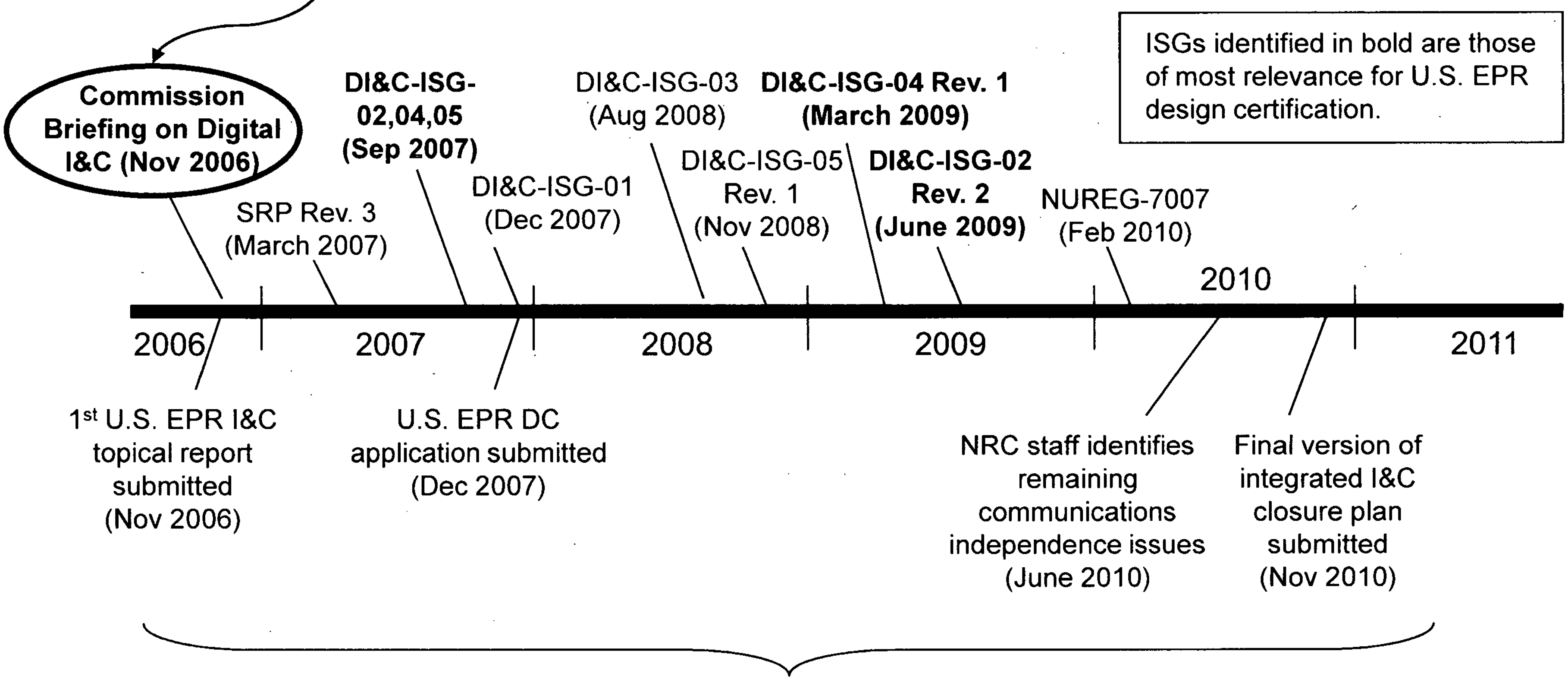
U.S. EPR Digital I&C Progress

- **Nov 2006: First U.S. EPR I&C topical report submitted**
- **Dec 2007: Submittal of U.S. EPR design certification application**
  - 256 Chapter 7 RAIs have been formally received and 195 responses have been submitted
- **Frequent interactions with NRC staff beginning in April 2006**
  - **28 meetings**
  - **11 audits**
  - **Monthly management phone calls initiated in April 2009**
  - **Weekly phone calls initiated in January 2010**
- **June 2010: NRC staff identifies remaining areas of concern regarding communications independence**
- **July 2010 to November 2010: AREVA proposes design modifications to reduce "complexity" and to address other NRC concerns regarding communications independence**
- **November 2010: Final version of integrated I&C closure plan submitted**

While progress has been made in 4+ years of discussion and review of the U.S. EPR I&C design, a few technical issues remain to be fully resolved.

Timeline

Emphasis on stability, predictability, and timeliness



Frequent interactions between NRC staff and AREVA have allowed the review to progress in a changing environment.

What's Left?

- **Execute closure plan to resolve communications independence issues, including identification of details of design changes, implementation in supporting documents, and preparation and submittal of revised licensing documentation**
  - Resolution of criteria for connection of a Service Unit (a non-safety device) to the TXS safety systems (Protection System and Safety Automation System)
  - Resolution of amount of design information and level of detail required to support design certification Safety Evaluation Report, especially regarding communications
- **Resolution of NRC staff questions regarding Diversity and Defense-in-Depth (D3)**
- **Review by Advisory Committee on Reactor Safeguards (ACRS)**

Key Challenges to Reaching Closure

- **Stabilization of guidance and its interpretation**
  - Examples:
    - DI&C-ISG-02 on Diversity and Defense-in-Depth (D3)
    - DI&C-ISG-04 on Communications Issues in Highly Integrated Control Rooms
    - NUREG/CR-7007 "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"
- **Getting beyond "too complex" to defining specific requirements and expectations**
- **Recognizing and balancing tradeoffs between "simplicity" and the benefits of enhanced safety and reliability offered by digital I&C**
- **Gauging the influence of other regulatory bodies on I&C design**

Progress has been made, but continued attention and diligence is needed to achieve closure for new plant digital I&C reviews, to ensure predictability and timeliness in future reviews, and to leverage digital I&C more effectively to achieve the potential it offers to improve plant safety and reliability.

AREVA

Implementation Phase of the Digital I&C Upgrade to Oconee Nuclear Station

February 1, 2011

Tom Ray, Engineering Manager
Duke Energy Corporation
Oconee Nuclear Station

Project Status

- Reactor Protection and Engineered Safeguards System to be installed on Unit 1 - April 2011, Unit 3 - April 2012, Unit 2 - October 2013
- Design Change package approved
- Site Acceptance Testing completed
- Installation and Post Mod Test Procedures approved

Site Acceptance Testing Activities

- Site Acceptance Test Plan covers the testing scope
- Site Acceptance Test Procedures govern the test performance
- Design requirements and operational modes of the system were tested
- NRC inspection of Site Acceptance Testing was performed

Operation and Maintenance Activities

- Maintenance and Operations classroom training completed
- Maintenance and Operations procedure development in progress
- Operations Training Simulator modified to represent the digital system
- Simulator training for Operations personnel is in progress

Operation and Maintenance Activities

- ***Maintenance Training System procured as part of the upgrade project***
- ***Maintenance Training System is duplicate of Channel A with other channels simulated***
- ***Maintenance Training System used to perform technician qualification***

NRC Inspection Followup Actions

- Software Plans
- Configuration Management
- Keyswitch Admin Controls
- Operation and Maintenance Procedures
- Cyber Security
- Post Modification Testing

Post Installation Monitoring

- Enhanced post installation monitoring implemented in 2006 for significant modifications
- Process requires identification of critical design features for monitoring system performance
- System Engineer performs monitoring to ensure adequate design margin

Digital Directives

- Oconee implemented directives for digital lifecycle and software design controls
- Directives incorporate guidance from industry and NRC standards
- Developed in 1997 to support Integrated Control System upgrade
- Directives enhanced as additional upgrades have been performed

Status of Preparations to Pilot ISG-6: Licensing Process

2/1/2011

Scott Patterson
Program Manager for I&C Obsolescence
Pacific Gas & Electric Company
Diablo Canyon Power Plant

BACKGROUND

- ***Public meetings with Staff March and November 2006***
  - ***Platform diversity questions***
  - ***Risk of Common Cause Failure (CCF)***
- ***Licensing process did not allow Staff to provide formal feedback without LAR submittal by licensee***
- ***High project risk without Staff acceptance of concept prior to LAR submittal***

Background, Cont.

- ISG-6 Enabled Phase 0 Meetings
  - Venue to help reduce risk
  - Discuss Staff opinions and recommendations
  - Formal meeting minutes
  - Excellent staff support to date
- Diversity and Defense-in-Depth Evaluation submitted 4/9/2010; revised August, 2010

The Present

- ***Diversity and Defense-in-Depth Topical Report approval pending***
- ***Application development proceeding***
  - ***Design Documentation issued***
  - ***Vendor Contracts awarded***
- ***ISG-6 Revision 1 approved on 1/19/2011***
- ***Next Phase 0 Meeting 2/3/2011***

The Path Forward

- Complete LAR and ISG-6 Phase 1 documentation
  - Submit Summer 2011
- Vendor Topical Report approval
- Complete and submit ISG-6 Phase 2 documentation 2012
- SER Approval 2013
- Installation 2014

Challenges for PG&E

- Schedule
  - D3 Topical Report approval
  - Vendor Topical Report approval
  - ISG-6 process for pilot plant
- ISG-06
  - Minimum required detail
  - Licensing stability
- Budget
  - Competing projects
- Resources
  - Continuity and availability

Conclusion

- PG&E will communicate pilot plant experience to the Staff and industry
- Support improvements to the ISG-6 guidance
- Goal is a more predicable and stable licensing experience for future licensees

Acronyms

- *I&C – Instrumentation and Controls*
- *ISG-06 – Digital I&C Interim Staff Guidance: Licensing Process*
- *LAR – License Amendment Request*
- *PG&E – Pacific Gas & Electric Co.*
- *SER – Safety Evaluation Report*

Position statement on Digital I&C Software Reliability

NRC Meeting, February 1, 2011

Dr. Gerard J. Holzmann
Laboratory for Reliable Software
Jet Propulsion Laboratory / California Institute of Technology
Pasadena, CA 91109

Background

Software controls are being included in virtually every type of system build today, including those that are safety-critical. This includes engine-controls in cars, flight-controls in commercial airplanes, and the standard operation of an increasing number of medical devices. In many of these cases the size and complexity of the software controls is growing rapidly.

The growing size of software is in part motivated by an increasing desire for expanded functionality, as well as increased flexibility in operation and maintenance. But the expanded functionality can come at a price. There are currently *no* techniques that can provide strict *guarantees* on the reliability of complex software systems. By careful design, development, testing and verification one can significantly reduce the probability of software failure, but at present there are no known techniques that can provably eliminate the possibility of failure.

Systems View

Software controls, no matter how important, generally define only some of the components in a system. Like any other component (e.g., a bolt or a valve), a software component is not infallible: it can and will occasionally fail. But, the simple fact that the individual components that we use to build larger systems are not perfect does not imply that systems as a whole cannot be reliable. In many engineering disciplines we have learned to construct reliable systems from unreliable parts: it is why our bridges and skyscrapers do not routinely fall over and it is why NASA is able to remotely operate spacecraft even decades after they are launched. How one builds redundancy into software, though, is fundamentally different from how it is traditionally done in hardware. Clearly, duplicating a faulty piece of software does not make it any more reliable. Successful methods are based on the use of self-checking code, strict compartmentalization (software *modularity*), and design diversity (*defense in depth*).

Failure in Complex Systems

We have studied the types of software failures that occur in spacecraft over a roughly forty-year history of the use of software controls on spacecraft used in deep space missions. Based on this, a number of key observations can be made.

- Software triggered failures often follow a common pattern and have relatively few root-causes. This is good news, because it means that our software design and development practices can be adjusted to avoid the known vulnerabilities. This motivates the adoption of targeted coding standards focused on risk-reduction (remarkably many coding standards today do not have this as their primary focus). This can be combined with the use of strong state-of-the-art static source code analysis techniques[1] to verify compliance with the standard. It is commonly observed that without automated means for compliance checking, coding rules have virtually *no*

[1] For a brief overview see http://spinroot.com/static/.

impact on software development. This then leads to a simple litmus test for the quality of a software design and development process: *which coding standards are used and how is compliance with that standard verified*?

- The failure data for spacecraft largely matches observations made by Charles Perrow[2] when writing about failure in complex systems: major failures, often defeating multiple layers of protection, can result from the unintended coupling of sub-systems or system components that were designed and assumed to be independent. The unintended coupling allows small failures to propagate and connect in unforeseen ways. These observations reinforce the importance of self-checking, decoupling, and modularity, but it also raises the bar for a *defense-in-depth* strategy that includes software components. Many of the problems that lead to major failures in larger system can also be caught early in the design cycle through the use of model-based engineering techniques that are integrated with verification methods (e.g., logic model checking[3] techniques). A second litmus test is then: *which verification capabilities exist in the software development process to effectively support early fault detection?*

- Concurrency related defects in software are among the hardest to prevent and predict, and they are among the hardest to identify with conventional software test methods. A standard example of a concurrent software system is the real-time multi-tasking system commonly used in embedded systems. But concurrency problems can also strike seemingly sequentially executing code, as for instance, used in medical devices. Software-based systems interact with their environment through peripheral devices (sensors and actuators), and generally have watchdog timers that can generate asynchronous *interrupts*. The interrupt-handlers define concurrent threads of execution, and their interaction with the main code of an application can have unintended consequences, sometimes leading to significant failure. Also from this perspective, the conclusion is inevitable that the highest standards in software quality control and the use of the strongest design verification techniques are essential for the development of safety-critical systems. Where appropriate, strong *evidence* of the successful application of these techniques should be made available to regulators.

What This Means

In safety-critical software development *any* statement about software reliability, be it as a separate component or as a functional part in a larger system, must be supported by strong supporting *evidence*. Complete and convincing insight should further be provided about the set of assumptions that underpin safety cases. This type of *evidence-based* safety argument should include evidence of a well-controlled software development *process*, evidence of *standards* used, and of *mechanisms* used to secure full *compliance* with these standards. Safety-critical software development requires the use of best-in-class static *source code analysis* tools and model-based design and design-verification techniques. Critical parts of the software that involve concurrency should be *formally verified* with the best available technologies.

Pasadena, 24 January 2011

---

[2] C. Perrow, *Normal accidents: living with high-risk technologies*, Basic Books, NY, 1984.

[3] See, for instance, http://spinroot.com/.

Digital I&C Software Reliability

February 1, 2011

Gerard J. Holzmann
Laboratory for Reliable Software
Jet Propulsion Laboratory /
California Institute of Technology

Background

- Software controls are ubiquitous and have reached safety-critical systems
- Code size & complexity is rapidly growing (often exponentially fast)
- Software test and verification methods have not kept pace
  - meaning: virtually all software will have latent defects

Systems

- **Software is a system component**
  - no one system component should be assumed to be perfect
- **Building reliable systems from unreliable components requires special precautions**
  - for software this includes self-checking code, strict partitioning, design diversity (defense-in-depth), and independent, non-software backup

Failures : common causes

- Software failures often follow a common pattern
  - many of these common causes can be prevented with the use of risk-based coding standards and strong compliance checkers

Failures : unintended coupling

- ***Software failures in complex systems are often caused by unintended coupling between (assumed to be) independent system components***
  - ***many of these causes can be prevented with the use of model-based design verification techniques***

Failures : race conditions

- ***Software failures are often caused by concurrency (race conditions)***
  - ***many of these failures can be prevented with the use of model-based design verification techniques***

Evidence for safety

- ***Safety claims must include strong evidence with all relevant assumptions made explicit***
  - ***this includes evidence of standards used, compliance verification and design verification techniques used, use of source code analysis, and formal design and code verification methods***

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital Instrumentation and Control

February 1, 2011

Agenda

- ***Steering Committee activities***
- ***Operating reactor licensing***
- ***New reactor licensing***
- ***Research support***
- ***International activities***

Steering Committee Activities

- Steering Committee established in 2007
- Project Plan developed with input from all stakeholders
- Communication enhanced with stakeholders
- Seven ISGs issued

Steering Committee Activities

- ISGs used to support new and operating plant licensing reviews
- ISGs have improved predictability, consistency and effectiveness
- Incorporating ISGs into regulatory infrastructure
- Sunsetting Steering Committee and Task Working Groups

Operating Reactor Licensing Accomplishments

- ***Infrastructure***
  - *Improved review process*
  - *Updating current platform topical reports and reviewing new topicals*
- ***New technology***
  - *Wolf Creek*
  - *Oconee*

Status of Operating Reactor Reviews

- ***Ongoing reviews***
  - ***Grand Gulf***
  - ***Crystal River***
  - ***Columbia***
- ***Watts Bar Nuclear Plant Unit 2***
  - ***Review includes 3 safety-related digital platforms and 3 balance of plant digital platforms***

Digital I&C System Platforms and Applications

- **New Platforms**
  - *HFC-6000*
  - *Advanced Logic Systems*
  - *Spinline 3*

Digital I&C System Platforms and Applications

- Update to topical reports
  - Common Q
  - Tricon
- Software validation tool
  - SIVAT V&V

ISG-6 Pilot for Diablo Canyon

- *ISG-6 and Oconee lessons learned*
- *Digital to digital replacement of RPS and ESFAS*
- *Amendment request expected Spring 2011*
- *Will use pilot to further improve review process*

Operating Reactor Challenges

- Operational issues
  - 50.59
  - Maintenance Rule
  - Inspection of start-up testing and other site reviews
  - Technical Specifications

New Reactor Licensing Accomplishments

- ***Completed review of GEH's ESBWR Design Certification application***
- ***Completed review of WEC AP1000 Design Certification Amendment***

Status of New Reactor Reviews

- Design certification and COL application reviews
- ISG documents being used
- Stakeholder interactions on I&C DAC

I&C DAC/ITAAC Inspections

- ***Submitted draft I&C inspection procedure to ACRS***
- ***Test of inspection procedures with South Texas applicant***
  - ***Scheduled for March 2011***

New Reactor Challenges

- Quality and completeness of I&C submittals
- Nexus between complexity and safety
- Design approaches and schedule expectations

Research Support

- Digital I&C research guided by the Digital System Research Plan
- Research divided into four areas:
  - Safety Aspects
  - Security Aspects
  - Advanced Nuclear Power Concepts
  - KM and Research Collaboration

DI&C Research at National Labs

- I&C Research requires both digital expertise and knowledge of nuclear technology
- ORNL, SNL, PNNL, BNL, INL provide extensive expertise
- Diverse Lab work includes D3, FPGAs, Cyber, FMEA, EMP
- University research and international interactions complement National Labs

Research Products

- ***NUREG/CR – 7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems***
- ***NUREG/CR – 7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems***

Research Products

- NUREG/CR – 6991, Design Practices for Communications in Highly Integrated Control Rooms
- Digital Platform Cyber Assessments & Regulatory Guide 5.71, Cyber Security Programs

Software Failure Mode Identification and Analysis

- ***Goal: Assess analytical methods to support licensing of software including FMEA techniques***
- ***FMEA may be useful for system hazard review***
- ***KAERI has one successful limited scope case of using FMEA for software assurance***

Software Failure Mode Identification and Analysis

- Traditional FMEA contribution to software assurance is limited
  - Too many potential fault modes in software
  - Software faults driven by systemic causes
- Research products - NUREG/IA and Research Information Letters

Digital System Operational Experience

- **Goal: Factor digital OpE into regulatory practices**
- **Digital OpE limited in US NPP safety systems**
  - **Quantification not currently meaningful**
  - **Collaboration via the EPRI MOU provides access to event details**

Digital System Operational Experience

- Obtaining international and non-nuclear OpE
  - COMPSIS, EDF & Korean via EPRI MOU
  - Non-Nuclear Digital OpE
- Compiling inventory, classification and data for analysis

Digital System PRA Research

- Goal: Identify methods and data needed to quantify the reliability of digital I&C systems for PRAs and support risk-informed licensing process
- Five completed NUREG/CRs on reliability models for digital systems
  - Identified a set of desirable characteristics
  - Applied modeling methods to an example system

Digital System PRA Research

- Additional research is needed to
  - Improve current methods
  - Augment existing data
  - Principal focus at present is the quantification of software reliability
- Long term significant research effort

International Activities

- Active international cooperation
  - Multi-lateral programs
  - Bi-lateral exchanges
  - Support development of international standards (IAEA, IEC)

International Activities

- ***Multi-lateral programs***
  - ***Multinational Design Evaluation Program (MDEP)***
    - ***NRC Leads digital working group***
    - ***AP1000 working group***
    - ***EPR working group***
  - ***European I&C (7 Country Project)***

International Activities

- Bi-lateral exchanges:
  - Finland
  - France
  - Canada
  - China
  - Korea
  - Japan
  - Others

International Activities

- **Support development of international standards**
  - IAEA Safety Guide
  - IEC Standards
    - Inputs from multi-lateral exchanges
    - New and updated standard
    - Interactions with IEEE
  - Other standards

International Activities

- NRC international cooperation in the digital I&C area has
  - Improved operating experience and lessons learned sharing
  - Improved knowledge of and coordination of regulatory positions (MDEP and other activities)
  - Increased research collaboration

Acronyms

ACRS	Advisory Committee on Reactor Safeguards
BNL	Brookhaven National Laboratory
COL	Combined License
COMPSIS	Computer Systems Important-to-Safety
DAC	Design Acceptance Criteria
D3	Diversity and Defense-in-Depth
EDF	Electricité de France
EMP	Electromagnetic Pulse

Acronyms

EPR	Evolutionary Power Reactor
EPRI	Electric Power Research Institute
ESFAS	Engineered Safety Features Actuation System
ESBWR	Economic Simplified Boiling Water Reactor
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Arrays
GEH	General Electric Company, Hitachi Nuclear Energy

Acronyms

HFC	Doosan HF Controls
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
ISG	Interim Staff Guidance

Acronyms

ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
KAERI	Korea Atomic Energy Research Institute
KM	Knowledge Management
MDEP	Multinational Design Evaluation Program
MOU	Memorandum of Understanding
NPP	Nuclear Power Plant
OpE	Operational Experience

Acronyms

ORNL	Oak Ridge National Laboratory
PNNL	Pacific Northwest National Laboratory
PRA	Probabilistic Risk Assessment
RPS	Reactor Protection System
SIVAT	SImulation VAlidation Test Tool
SNL	Sandia National Laboratory
V&V	Verification and Validation
WEC	Westinghouse Electric Company