Digital I&C Platforms Approved

• GE NUMAC System
  – September 1995

• Areva Teleperm XS (microprocessor-based)
  – May 2000

• Doosan HF-6000 (microprocessor-based)
  – May 2011

• Schneider-Electric Triconex (microprocessor-based)
  – April 2012 (originally evaluated December 2001)
Digital I&C Platforms Approved

• Westinghouse Common Q (microprocessor-based)
  – February 2013 (originally evaluated in 2000-2001)
• Westinghouse ALS platform (FPGA-based)
  – September 2013
• Rolls Royce SPINLINE 3 platform
  – November 2014
• Lockheed Martin NuPAC
  – March 2017
• NuScale HIPS platform (FPGA-based)
  – June 2017
Digital I&C Platforms Under Review

- Toshiba power range monitoring (PRM) system (FPGA-based)
- Mitsubishi MELCO (FPGA for peripheral modules)
- Radly RadICS (FPGA-based)
- HFC-6000 Amendment (FPGA-based)
Examples of Digital Upgrades

• Duke Oconee Reactor Protection System & Engineered Safety Features Actuation System Upgrade
• Wolf Creek Simple Safety Actuation Function
• Diablo Canyon Plant Protection System and Engineered Safety Features Actuation
• Others (e.g., Watts Bar Common Q Post Accident Monitoring System)
Technical Challenges

• Evaluation of potential software design errors, which could impact system operability and reliability, make analysis of digital systems challenging and impact their regulatory treatment

• Introduction of (relatively) new technology, which makes difficult to keep guidance up to date

• Protection against digital system vulnerabilities and possible adverse interactions (either malicious or non-malicious) [this is under the scope of NSIR review]
DI&C Action Plan

- SRM-SECY-16-0070 approved the implementation of the IAP
- The IAP will ensure safety and security while improving the predictability and consistency of the agency’s regulatory process for licensing and oversight of digital I&C systems

10 CFR 50.59
Software CCF
Commercial Grade Dedication
Licensing Process
IAP – Software Common Cause Failure

- RIS supplement provides near-term clarification for digital upgrades
- Evaluating NEI’s proposed guidance in NEI 16-16
- Evaluate existing policy on software common cause failure
How Software Common Cause Failure is Currently Addressed

• Regulation is technology neutral

• SRM-SECY-93-087 defines criteria for addressing software common cause failure
  – BTP 7-19: guidance for implementation
  – NUREG/CR-6303: guidance for performing diversity and defense-in-depth analysis
  – NUREG/CR-6707: guidance for diversity

• Consider adequate degree and nature of diversity applied to nuclear power plant safety systems
Can certain technology base be used to address CCF?
Diversity in FPGA-based Platforms

Evaluation was limited to specific manufacturer claims regarding the built-in diversity

• Westinghouse ALS
  – Can use built-in diversity (i.e., platform design attributes)

• Rolls Royce SPINLINE 3
  – Not used

• Lockheed Martin NuPAC
  – Not addressed at this level

• Approved Doosan HFC-6000 Safety System
  – Can use two safety system design: separate transmission of measurements and separate implementation of actuation output
Diversity in FPGA-based Applications

• Wolf Creek Main Steam and Feedwater Isolation System
  – 1st FPGA-based application
  – ALS platform, using diverse cores

• Diablo Canyon RPS
  – ALS platform, using built-in diversity

• NuScale – small modular reactor
  – NuScale HIPS
  – Equipment (architecture) and design diversity
Acronyms

• ALS – Advanced logic system
• ASIC – Application specific integrated circuits
• CPLD – Complex programmable logic device
• CPU – Central processing unit
• FPGA – Field programmable gate arrays
• HIPS – Highly integrated protection system
• IAP – Integrated action plan
• I&C – Instrumentation and control
• NSIR – Office of Nuclear Security and Incident Response
• NuPAC – Nuclear protection and control
• RIS – Regulatory issue summary