Digital Upgrades and Cyber Security
An Industry Perspective

John Connelly
Engineering Manager – Capital Projects
Exelon Generation Company

December 17, 2015

Exelon Generation®

Industry Perspective

- Our shared goal is safe and reliable operation – digital technology is a key enabler for increasing margins of safety and reducing initiating events

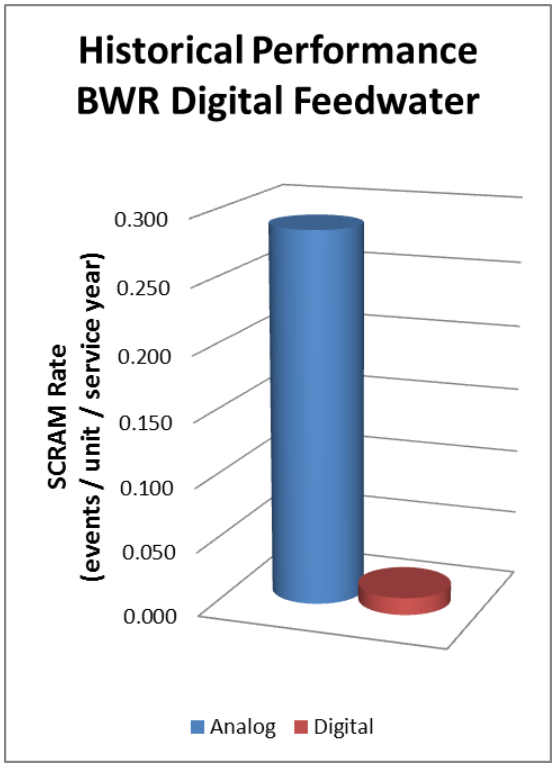
- Modernization is essential to address three industry imperatives:
  - Reduction of initiating events
  - Improving equipment reliability
  - Managing component obsolescence

- The industry needs a clear, unambiguous, graded and stable regulatory framework for both digital I&C and cyber security

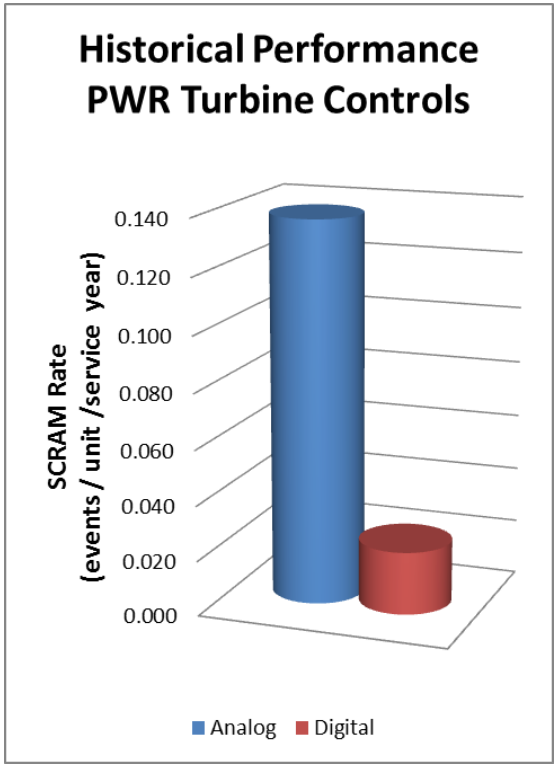
- Tangential issues risk unintended consequences:
  - Cyber Security (10 CFR 73.54 / RIS 2014-XX)
  - Redefining “digital” (RIS 2013-XX)
  - SECY-15-0106 / IEEE-603 2009

Exelon Operating Experience – Tangible Performance Improvements

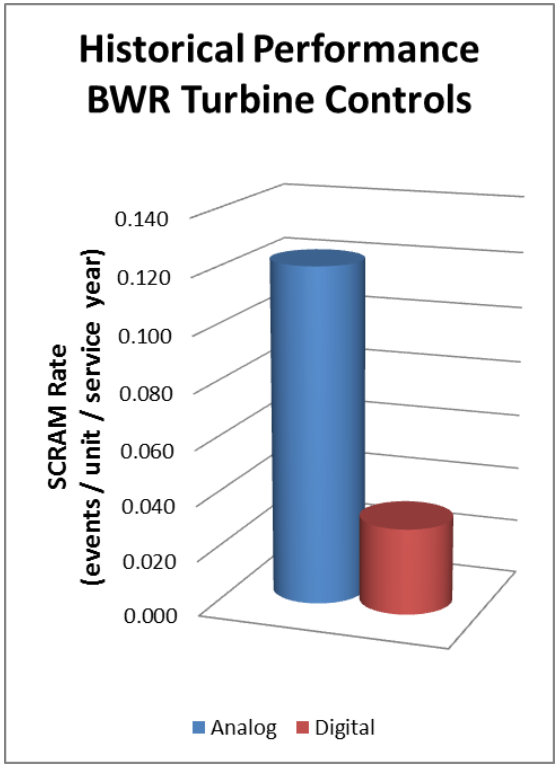
- Exelon began installing digital upgrades in the early 90's beginning with the feedwater systems at Dresden, LaSalle, Quad Cities and Limerick
- Turbine controls were upgraded beginning in 2004 at Byron, Braidwood, Dresden, LaSalle, Quad Cities and Limerick and continue across the balance of the fleet
- 488 "unit years" of operating experience conclusively demonstrates a significant reduction in initiating events
- Exelon continues to implement targeted non-safety related system upgrades across the fleet - not likely to modernize safety related systems



95% SCRAM rate reduction



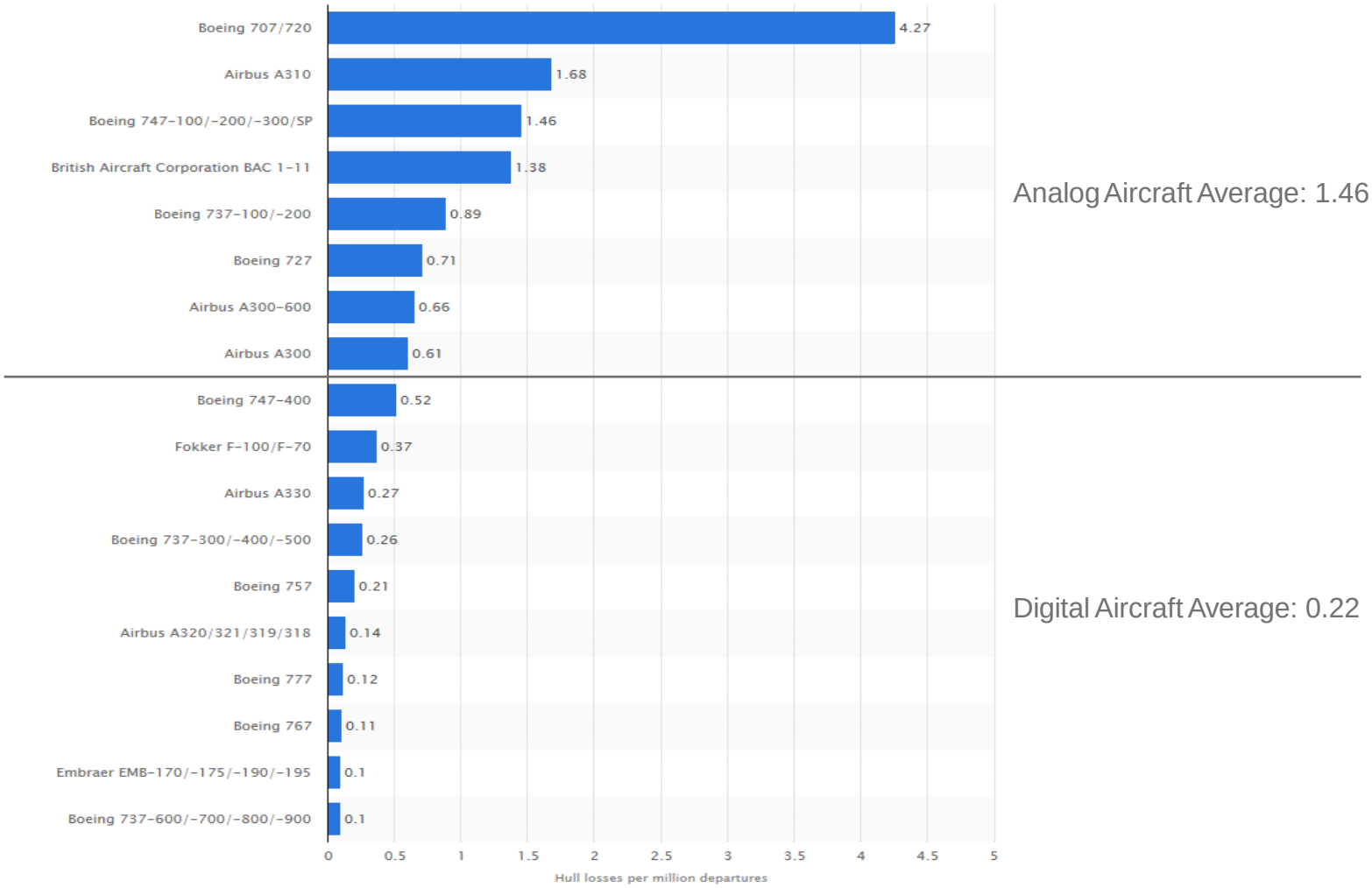
83% SCRAM rate reduction



74% SCRAM rate reduction

Exelon Generation

Looking Outside Nuclear – Commercial Aviation



Analog Aircraft Average: 1.46

Digital Aircraft Average: 0.22

While <u>not</u> the only contributor to improved safety performance, “digital” aircraft hull losses average 15% that of analog aircraft

Exelon Generation

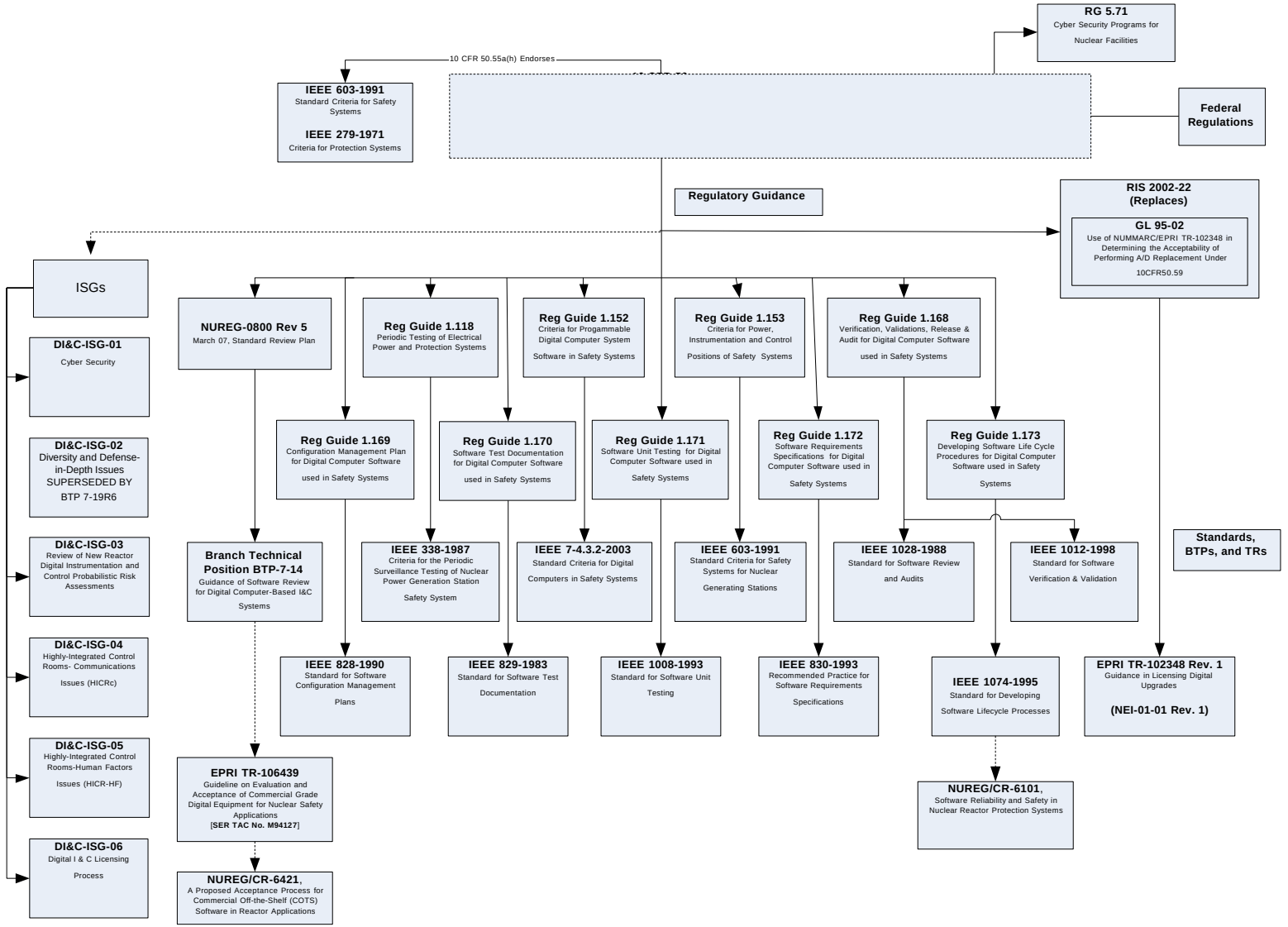
Managing Equipment Obsolescence

- Electronic components have finite service lives – nearly all electronic will become obsolete over time – managing this life-cycle is critically important
- Exelon is a member of the Proactive Obsolescence Management System (POMS) coalition
- POMS provides participating utilities insights to equipment obsolescence issues so they can be actively managed:
  - A typical plant contains approximately 17,000 I&C components
  - Up to 25% of those components can be at or near the point of obsolescence
  - This population includes AP-913 “Critical Components”
- While the industry proactively manages these issues and mitigation strategies are in place, the ability to use standardized and well vetted digital components greatly simplifies our mitigation strategies
- Digital technology is the preferred solution in the commercial marketplace because it is highly reliable and feature rich - the nuclear sector cannot and more importantly *should not* avoid using well vetted digital solutions

Cyber Security

- For Exelon, the scoping criteria of 10 CFR 73.54 yields a population of roughly 25,000 digital components that must be considered Critical Digital Assets (CDA's) – very significant resource implications and full compliance (MS-8) will continue to strain the organization
- Cyber security and digital I&C are inextricably linked yet are not coordinated within the agency
  - Cyber Security best practices can directly conflict with engineering best practices
  - Altering the definition of "digital" (RIS 2013-XX) forces a substantial population of components into the scope of 10 CFR 73.54 (ASICS, FPGA's and CPLD's) - components that have effectively no cyber security attack surface because they are not microprocessor based and do not typically execute sequential code
- NEI 13-10, Rev 3 provides implementation guidance for a graded and consequence based approach to cyber security
  - Improved our ability to focus limited resources on assets of greatest importance
  - Opportunities exist to further enhance and refine the process – principally security assets
  - Incremental improvements necessitate reworking resource intensive compliance assessments – timely resolution of implementation issues is critical to meeting MS-8 compliance dates
- The industry implemented Cyber Security in a consistent fashion per NEI 08-09 r6 - as the implementation effort has matured, ambiguities and discontinuities have emerged that need to be addressed

Existing Regulatory Framework



Exelon Generation

IEEE-603-2009 / SECY-15-0106

- Proposed changes could negatively impact regulatory stability by introducing conflicts with existing regulatory guidance – most notably DI&C-ISG-4
- Expands scope to include Safety Systems rather than Reactor Protection Systems
- Expanded applicability brings in systems that were not originally designed to either IEEE-279 or IEEE-603 criteria
- Reactor Protection System and Safety System diversity strategies use different means to compensate for failures - increasing scope and requirements for Safety Systems puts modernization initiatives at risk

What Do We Need?

- A clear, unambiguous, graded and stable regulatory framework for both digital I&C and cyber security
- Maintaining IEEE-603-1991 as the endorsed standard does not adversely impact the industries ability to modernize and more importantly allows the staff and industry to resolve high priority technical issues without introducing more variables
- The agency and industry should work to develop consensus solutions to key technical issues (mitigation of common cause failure risk, application of 50.59 process, applicability of codes and standards…) – the Digital Working Group is an ideal vehicle for this work
- The agency and industry should continue efforts to improve NEI 08-09 (Rev 7) to resolve known issues
- The agency and industry should continue efforts to improve NEI 13-10 (Rev 4) to provide clarity through worked examples and improved program focus
- Leverage methodologies from sectors that have already conquered these issues:
  - Naval Reactors (NAVSEA 08)
  - Aerospace
  - Petrochemical