
# Gap Assessment of IEC and IEEE Standards for Safety Assurance of Digital Systems

Russell Sydnor, Sushil Birla & Michael Waterman

Software Certification Consortium - 9th Meeting – May 5 & 6, 2012

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

# Presentation Outline

- Background
- Current IRSN Collaboration

  *Institute DE Radioprotection ET Surete Nucleaire*
- Gaps in software assurance criteria
- Criteria Assessments
  - IEC Standards
  - IEEE Standards

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

# Background

- NRC Digital I&C Research Plan
  - Analytical Assessment of DI&C Systems
    - Expert Elicitation and Expert Clinic
  - Safety Assessment of Automated Tools
  - Standards Development
  - Collaborative and cooperative research
- IRSN Collaboration
  - 2009 - Initiated the NRC – IRSN collaboration in DI&C
  - 2010-2011 – the role of failure mode and effects analysis in regulatory assurance of complex logic in digital safety systems
  - 2011- 2012 – proposal for collaboration on standards for assurance of software in systems of the highest safety classification

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

# Current Collaboration

Proposal - Develop criteria for evaluation of software for systems of the highest safety classification

- Agreed upon topics for which more specific criteria are needed
- Research will be iterative and evolutionary
  - Information exchange
  - Sharing comments on draft standards
  - Technical peer review
- Influence regulatory positions, Standards and further research efforts

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

# Software Assurance Gaps

- NRC conducted an Expert Elicitation and Expert Clinic
  - Documented outcomes in RIL-1001 Software-Related Uncertainties in the Assurance of Digital Safety Systems—Expert Clinic Findings, Part 1
- Identified topics on which more specific criteria are needed
  - Validation of Requirements
  - Verification: Adequacy of coverage
  - Architecture: Complexity
  - Impact of change: Hidden/obscure dependencies
  - Tool Automated Processes
  - Organizational Capability and Competence

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

# Assessment Scope

- French NPP designs
  - IAEA Nuclear Safety Guide
  - **IEC Standards** implement IAEA safety principles
- US NPP designs
  - 10 CFR 50 & 52
  - Regulatory Guides
  - **IEEE Standards**
- Do the standards have useful criteria?

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

# IEC Assessments

IEC 61226 (classification of system importance)

IEC 61513 (general safety requirements for systems)

IEC 62340 (requirements for coping with CCF)

IEC 60880 (software aspects for computer-based systems of the highest classification)

IEC 62566 (under development – will address development of HDL-programmed integrated circuits)

## Conclusions –

Standards are “relevant and sufficient” in some areas – specifying process and plans- establish sound principles –but more technical detail and criteria needed in most areas.

“lack of objective criteria to measure coverage of validation”

“standards provide a reasonable assurance but not formal criteria”

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

# IEEE Assessments

IEEE 603-2009 (Nuclear Safety Systems)

IEEE 7-4.3.2-2010 (digital safety systems)

IEEE 1012-2004 (V&V)

IEEE 1028-2008 (reviews and audits)

IEEE 1074-2006 (lifecycle process)

IEEE 828-2005 (configuration management plans)

IEEE 829-2008 (test documentation)

IEEE 830-1998 (software requirements)

## Conclusions –

System level standards have adequate evaluation criteria for system design, software standards have adequate guidance for software development lifecycle process.

Adequate software assurance evaluation criteria are lacking in both system and software lifecycle standards

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

# Next Steps

- Share findings with IRSN
- Determine which topic areas to address under the collaboration
- Identify research initiatives of interest
  - to provide input
  - to participate
  - to fund?

Questions?