U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Description of Preliminary Staff Evaluation for Use of IEC 60880 and IEC 61513 for Software Development

Steven Arndt, Deanna Zhang, Richard Stattel and Paul Rebstock

August 29, 2019

Agenda

- Background
- Issues To Be Addressed
- Preliminary Evaluations of Software Regulatory Guides
    - ➢ Review methodology
    - ➢ RG 1.168
    - ➢ RG 1.169
    - ➢ RG 1.171

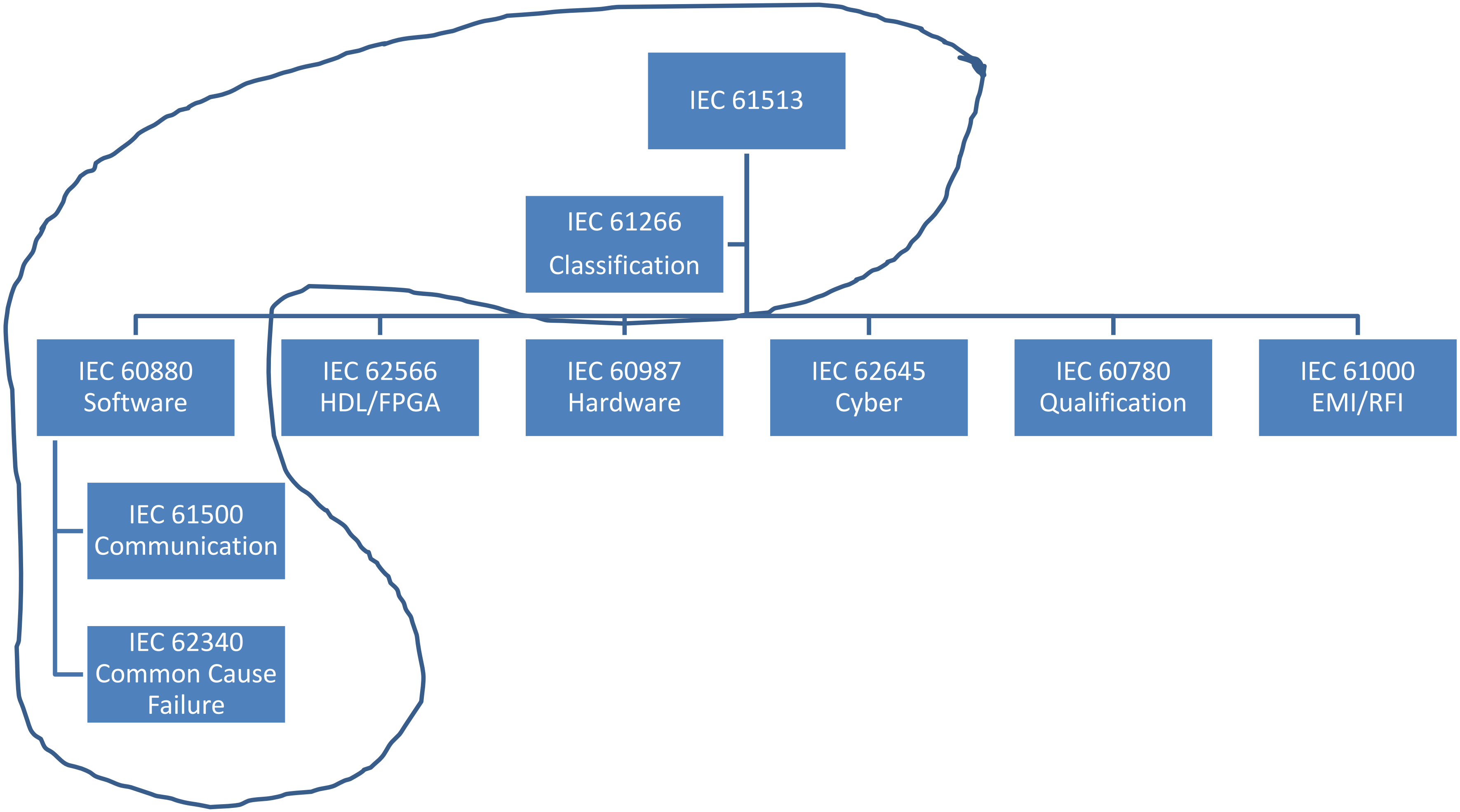
Background

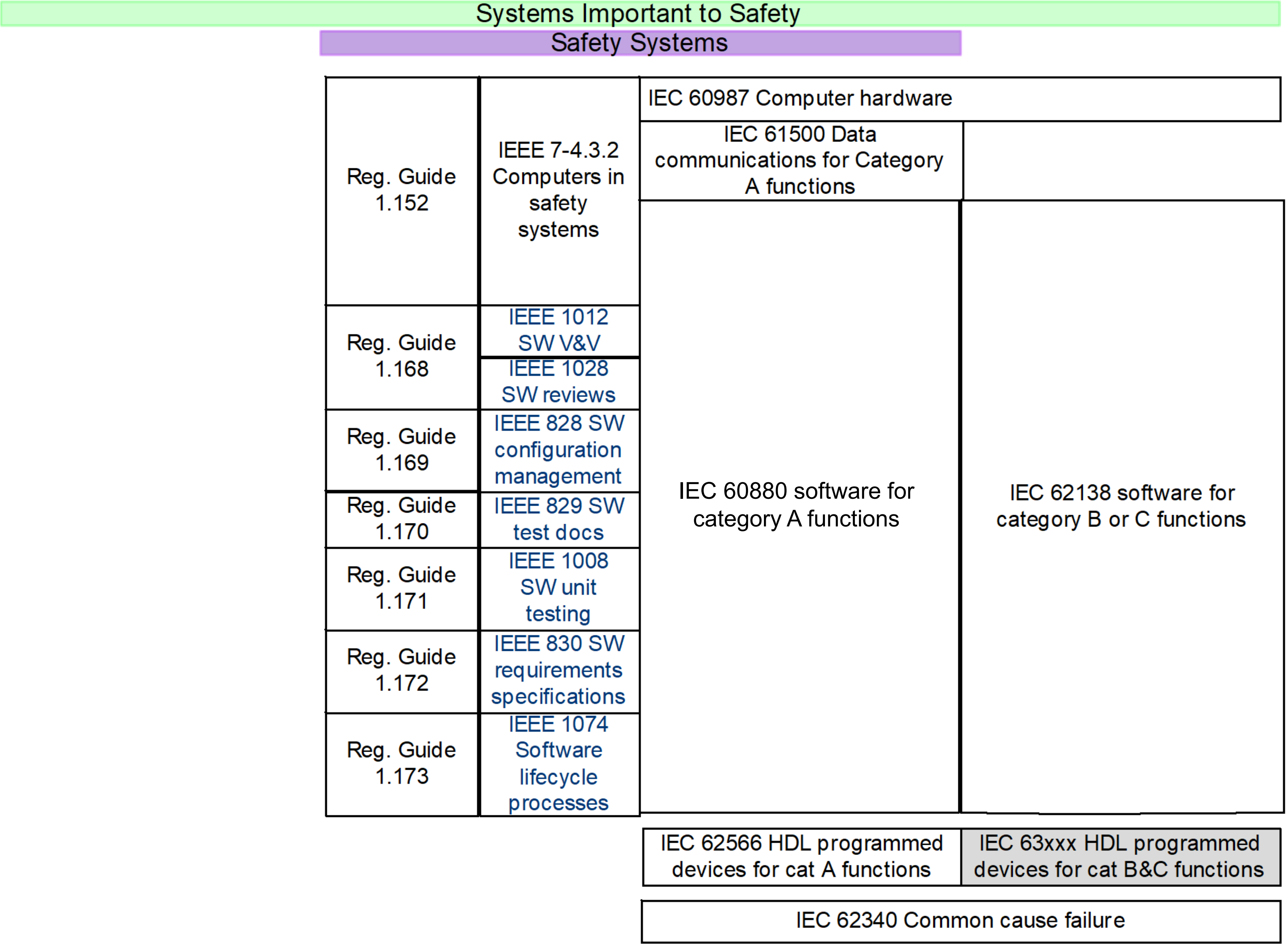
- Original plan was to develop guidance that endorses specific IEC standards (e.g., IEC 61513) as an alternative to the IEEE standards incorporated by reference (IBR) in 10 CFR 50.55a(h)
  - ➢ Endorse IEC standards as an alternative to IBR IEEE Standards in accordance with 10 CFR 50.55a(z)
  - ➢ Evaluate such endorsement's impact current regulatory guidance, including the current regulatory guides, with respect to other IEC and/or IEEE standards
- Initial evaluation determined:
  - ➢ Endorsing IEC standards as alternatives to IBR standards may not be useful for operating reactors
  - ➢ Several digital I&C platforms that have been developed using IEC standards were previously approved by the NRC for use in safety applications of nuclear power plants
  - ➢ Potential to endorse, via most likely a regulatory guide, a subset of IEC standards with focus on software development as one potential way to satisfy regulatory requirements related to quality

Issues to be Addressed

- Software development standards are the focus for endorsement
  - ➢ This effort evaluates whether IEC 60880 could be endorsed as one way to meet regulations related to quality
  - ➢ Identify which other IEC standards need to be endorsed if there are gaps within IEC 60880 for a certain topic
  - ➢ Significant differences in the classification of systems in IEC and IEEE nuclear standards will need to be addressed
    - o Use IEC 61266 to categorize functions performed and corresponding safety class; or
    - o Limit application to "safety-related" systems that is equivalent to Class 1 systems performing Category A functions

IEC 61513 and IEC Software Standards





Systems Important to Safety

Safety Systems

Reg. Guide 1.152	IEEE 7-4.3.2 Computers in safety systems	
Reg. Guide 1.168	IEEE 1012 SW V&V IEEE 1028 SW reviews	
Reg. Guide 1.169	IEEE 828 SW configuration management	
Reg. Guide 1.170	IEEE 829 SW test docs	
Reg. Guide 1.171	IEEE 1008 SW unit testing	
Reg. Guide 1.172	IEEE 830 SW requirements specifications	
Reg. Guide 1.173	IEEE 1074 Software lifecycle processes	

IEC 60987 Computer hardware

IEC 61500 Data communications for Category A functions

IEC 60880 software for category A functions

IEC 62138 software for category B or C functions

IEC 62566 HDL programmed devices for cat A functions

IEC 63xxx HDL programmed devices for cat B&C functions

IEC 62340 Common cause failure

Preliminary Evaluations of Software Regulatory Guides

- How have we done the evaluation?
  - ➢ Review of the underlying regulations
  - ➢ Review of the what is needed to demonstrate that the regulations are being meet and the system is safe
  - ➢ Evaluation of the method by which the regulatory guides and endorsed IEEE standards provide that assurance
  - ➢ Review the IEC 60880 criteria
  - ➢ Determine whether IEC 60880 provides equivalent demonstration of safety and/or if additional criteria are needed

Preliminary Review of Software Verification and Validation

Software Verification and Validation

- RG 1.168 endorses IEEE Std 1012-2004 for meeting the NRC’s requirements for verification and validation of safety-related system software.
- IEEE Std 1012-2004 is a computer society standard.
  - It establishes a minimum set of V&V activities for software based on a Software Integrity Level (SIL) classification.
  - RG 1.168 states that software used in nuclear power plant safety systems should be assigned integrity level 4 or the equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4.

Software Verification and Validation

- IEC 60880 includes software verification (Section 8) and software integration (Section 10) criteria for nuclear software applications used to perform safety functions with the highest category of safety (i.e., Category A).
- NRC staff evaluated IEC 60880 to determine if the criteria provided in this standard meet the underlying V&V regulatory requirements cited in RG 1.168.

Examples of Evaluation

- Examples of criteria within IEC 60880 that support compliance with underlying regulatory requirements for software verification:
  - ➢ IEC 60880, Section 8 provides criteria for establishing independence between a verification team and the development team
    - o These criteria provide an acceptable way of meeting the quality requirements in IEEE 603 Section 5.3, “Quality”
    - o These criteria are consistent with the criterion of IEEE Std 7-4.3.2-2003, Section 5.3.4, “V&V Independence Requirements” and are consistent with IEEE 1012 Section 5 and Section C.3 of RG 1.168
  - ➢ Section 8 also includes requirements for performing verification of outputs from each of the development life cycle phases
    - o These activities confirm the adequacy of the software requirements specification in fulfilling the system requirements
    - o These requirements are compatible with IEEE Std 1012-2004, Section 5, “Software V&V Process,” and thus provide an acceptable means of establishing quality in safety I&C systems as required by IEEE 603-1991, Section 5.3

Examples of Evaluation Contd.

- Example of criteria within IEC 60880 that meets the underlying regulatory requirements for software validation:
  - ➢ Section 10 provides criteria for validating design of an integrated system
  - ➢ These criteria provide an acceptable way of meeting the objectives of the validation activities prescribed in IEEE Std 1012-2004, Table 2

Examples of Evaluation Contd.

- Examples where criteria in IEC 60880 are not sufficient to provide one acceptable way of meeting underlying regulatory requirements for verification and validation:
  - Rather than prescribe a minimum set of V&V activities to be performed for each phase of development, IEC 60880 is results oriented
    - Criteria within this standard are the resulting characteristics of the safety system
    - Users of this standard is allowed to decide which V&V activities would be needed to achieve the required results
  - The IEC standard does not include tables of V&V activities or any equivalent list of activities to be performed for safety software
    - Mapping of activities performed to activities prescribed by this standard cannot be performed
    - Documentation focuses on system design performance results rather than completion of specified V&V activities

Software Verification and Validation (IEC 61513)

- IEC 61513 includes criteria for deriving the I&C requirements from the plant safety design base and design of the entire I&C architecture and assignment of the I&C functions

  Several V&V activities are specified within this criterion. Examples include:

  - Performance of Requirements Traceability
  - Assignment of Software Integrity Levels
  - Verifying requirements specifications to ensure correct assignment of functions to systems

- NRC staff is evaluating IEC 61513 to determine if the criteria provided in this standard can be used as a means of meeting the underlying V&V regulatory requirements cited in RG 1.168

Verification Definition Differences

- Verification (IEEE Std 1012-2004)
  - ➢ Process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase
  - ➢ Process of providing objective evidence that the software and its associated products:
    - o Conform to requirements (e.g., for correctness, completeness, consistency, accuracy) for all life cycle activities during each life cycle process (acquisition, supply, development, operation, and maintenance);
    - o Satisfy standards, practices, and conventions during life cycle processes; and successfully complete each life cycle activity; and
    - o Satisfy all the criteria for initiating succeeding life cycle activities (e.g., building the software correctly)
- Verification (IEC 60880)
  - ➢ Confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

Validation Definition Differences

- Validation (IEEE Std 1012-2004)
  - ➢ Process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements
  - ➢ Process of providing evidence that the software and its associated products:
    - o Satisfy system requirements allocated to software at the end of each life cycle activity;
    - o Solve the right problem (e.g., correctly model physical laws, implement business rules, use the proper system assumptions); and
    - o Satisfy intended use and user needs

➢ Validation (IEC 60880)

- ➢ Confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (e.g., functionality, response time, fault tolerance, robustness)

Preliminary Review of Software Configuration Management

Software Configuration Management

- RG 1.169 endorses IEEE Std 828-2005 for meeting the NRC's requirements for configuration management for safety-related system software
- IEEE Std 828-2005 is a computer society standard.
  - ➢ No minimum set of activities established for configuration management for nuclear safety software applications.
  - ➢ RG 1.169 identifies the minimum set of activities for nuclear safety software applications
- IEC 60880 provides criteria for software configuration management for nuclear software applications used to perform safety functions with the highest category of safety (i.e. Category A)
- Staff evaluated IEC 60880 to determine if the criteria provided in this standard meet the underlying configuration management regulatory requirements cited in RG 1.169

Examples of Evaluation

- Examples where criteria within IEC 60880 that meet the underlying regulatory requirements for configuration management include Sections 5.6.4, 5.6.5, 5.6.7, and 5.6.9
  - ➢ These sections provide criteria for identifying software such as the following:
    - o Each produced version of each software entity shall be uniquely identified
    - o It shall be possible to identify the relevant versions of all software documentation associated with each software entity
    - o It shall be possible to identify the versions of all software entities which together constitute a complete version of the final product
  - ➢ These criteria provide an acceptable way of meeting:
    - o 10 CFR Part 50, Appendix A, GDC 1
    - o IEEE Std 603-1991, Clause 5.3 requirements for quality

Examples of Evaluation Contd.

- Examples where criteria within IEC 60880 that meet the underlying regulatory requirements for configuration management include Sections 6.4.2, 7.1.1.9, 7.1.4.3, and 7.4.1
  - ➢ These sections provide criteria to ensure configuration management of software documentation such as the following:
    - o The software requirements specification shall be presented according to a standard whose formality should not preclude readability
    - o Comprehensive and clearly written documentation shall be provided
    - o The configuration data shall be documented
  - ➢ These criteria provide an acceptable way of meeting:
    - o 10 CFR Part 50, Appendix A, GDC 1
    - o IEEE Std 603-1991, Clause 5.3 requirements for quality

Examples of Evaluation Contd.

- Examples where criteria in IEC 60880 were insufficient to provide one acceptable way of meeting underlying regulatory requirements for configuration management:
  - ➢ Section 5.6, including its subsections references the system level configuration management requirements in IEC 61513, including provision of a configuration management plan or the quality assurance plan
  - ➢ Control of software vendors supplying safety systems software not addressed in IEC 60880
  - ➢ Software configuration audits not addressed in IEC 60880

Preliminary Review of Software Unit Testing

Provisions for Software Unit Testing

- Software Unit Testing is addressed in RG 1.171
  RG 1.171 endorses, with clarifications and additions, IEEE 1008-1987 “IEEE Standard for Software Unit Testing”
  - ➢ RG 1.171 endorses the 2008 edition of IEEE Std 829 “IEEE Standard for Software Test Documentation”, in lieu of the version cited in IEEE 1008-1987

Regulatory Requirements for Software Unit Testing

- The regulatory requirements cited in RG 1.171 include:
  - Requirements related to quality and documentation
  - Requirements for periodic testing
  - Requirements related to the development and testing of design changes
  - Requirements for documentation of test plans and results
  - No explicit requirements for unit testing

Provisions for Software Unit Testing in IEC 60880

- Annex E (nonmandatory) presents general recommendations for system testing
- Annex B (mandatory) presents considerations for unit and integration tests (B4.g), and for testing related to modifications (B1.d)
- Various sections within IEC 60880 contain provisions for:
  - Testing modifications;
  - Selection of test cases; and
  - Documentation of test plans and results
- Requirements are generally not very specific and consensus must be attained as to whether they are adequate to meet the regulatory requirements cited in RG 1.171

Next Steps

Stakeholder Engagement

- NRC would like to work with an industry working group
  - Help identify a subset of the suite of IEC standards that would be of most use to industry
  - Provide early feedback on NRC strategy for endorsement
  - Provide feedback on overlaps, gaps, and possible challenges to endorsement
- Table top/example review
  - Identify a specific system or platform to evaluate the new process to ensure the guidance is practical and well understood
  - Make a selection as soon as possible
  - Review will be done over the course of a few months, so will need to be appropriately scoped

Proposed Project Plan

(Key Milestones)

- Public meeting to engage stakeholders on the proposal, identify participants for the working group, and identify a subset of the suite of IEC standards that would be of most use to industry (Done)
- Formalize project plan and select IEC standards to include (Done)
- Work with OGC to determine appropriate guidance document (Done)
- Coordinate with IEEE and IEC (Done)
- Conduct review of IEC nuclear (45a) standards to determine overlaps, gaps and possible challenges with endorsement of IEC 61513 suite of standards (in-progress)
- Select system or platform for example review (Fall 2019)
- Develop possible solutions to previously identified concerns associated with endorsement of IEC standards (Fall 2019)
- Complete example review (Early 2020)
- Brief ACRS (Early 2020)
- Publish draft guidance for public comment (Spring 2020)

Discussion

Acronyms

- ACRS: Advisory Committee on Reactor Safeguards
- CFR: Code of Federal Regulations
- GDC: General Design Criterion
- I&C: Instrumentation and Controls
- IBR: Incorporated by Reference
- IEC: International Electrotechnical Commission
- IEEE: Institute of Electrical and Electronics Engineering
- NRC: Nuclear Regulatory Commission
- RG: Regulatory Guide
- SIL: Software Integrity Level
- V&V: Verification and Validation