Proposed Annotated Outline for Architecture Section DI&C-ISG-06 Revision 2

September 6, 2017

[[Note: The purple text below and in comment bubbles indicates the Outline discussed during the August 17th public meeting.]]

Table of Contents

A. Introduction

B. Purpose

B.1 Background (explains original document)

B.2 Revision (explains changes to document)

C. Digital I&C Review Process

C.1 Original Process Overview

C.1.1 Pre-Application (Phase 0)

C.1.2 Initial Application (Phase 1)

C.1.3 Continued Review and Audit (Phase 2)

C.1.4 Implementation and Inspection (Phase 3)

C.2 Alternate Tier 1 Process

C.2.1 Pre-Application

C.2.2 Application, Review, and Audit

C.2.3 Implementation and Inspection

D. Review Areas for License Amendment Process

D.1 System Description

The reviewer should confirm that the LAR provides a functional block diagram, showing major input and output interfaces with the plant and with operators.

The reviewer should confirm that the LAR identifies and describes the existing system in the plant, including design, operational, maintenance, calibration, surveillance, and engineering functions implemented.

Proposed Annotated Outline for Architecture Section DI&C-ISG-06 Revision 2
September 6, 2017

D.2 System Architecture

The reviewer should evaluate the differences between the existing system and the proposed system.

D.2.1 Existing Architecture

The reviewer should confirm that the LAR describes the physical and functional architecture of the existing system through text and diagrams (e.g., functional/architecture block diagrams and functional logic diagrams). This description should include:

- System design functions,
- Connections between safety systems,
- Connections between safety and non-safety systems and identification of signal and data isolation devices, and
- Temporary connections (e.g., for maintenance workstations).

The reviewer should confirm that the LAR identifies and describes the existing input and output interfaces with the plant; interfaces with control room displays, indicators, and controls, including the system's role for post-accident monitoring requirements and any references by emergency plan implementing procedures.

The LAR should describe and illustrate the existing system architecture, including identification of which portion(s) of the system are being replaced.

Commented [PG1]: From Outline: Describe and illustrate the existing system architecture, including identification of which portion(s) of the system are being replaced.

D.2.2 Replacement System Scope Functions

The reviewer should confirm that the LAR identifies each UFSAR-described design function performed by the portion(s) of the system being replaced. Any new LAR-proposed design functions should also be described. These design functions are safety functions implemented in the application-specific software or logic.

These are different than auxiliary features which are dependent on the new digital equipment. These features should have been previously reviewed as part of the digital equipment's topical report Safety Evaluation if Tier 1 or Alternate Tier 1. The LAR should address any application specific implementations of service/test functions, and any changes to the standard service/test functions since topical report approval. The auxiliary features, unlike the safety functions, are not directly related to the performance of safety functions, but relate to specific activities on the system, including the functions necessary for the configuration, validation, qualification, installation, commissioning, operation, periodic testing, maintenance, incorporation of design modifications and

Commented [PG2]: From Outline: Define the functions performed by the portion(s) of the system being replaced. This is accomplished by attaching the System Requirements Specification for the upgraded portion(s) to the LAR. Address the following clauses (defining the functional design basis) from IEEE Std. 603-1991

- Clause 4.1, Design Basis Events
- Clause 4.2, Safety Functions and Protective Actions
- Clause 4.3, Permissive Conditions
- Clause 4.4, Variables Monitored
- Clause 4.5, Criteria for Manual Protective Actions
- Clause 4.6, Minimum Number and Location of Sensors
- Clause 4.7, Range of Conditions
- Clause 4.8, Conditions Causing Functional Degradation
- Clause 4.9, Methods Used to Determine Reliability
- Clause 4.10, Critical Points in Time or Plant Conditions
- Clause 4.11, Equipment Protective Provisions

Clause 4.12, Special Design Basis

security. Note that auxiliary features/test functions may be described in a different LAR Section.

Each design function's description should include a description of equipment from sensor to actuated device(s) including logical operation, manual vs automatic and any functional dependencies (e.g., digital signal split between a safety function and sent to a display in the control room).

Each design function's characteristics should include, for example, identification of the I&C systems' safety functions; all monitored variables used to control each protective action; the minimum number and location of sensors and equipment required for protective purposes; plant conditions; and the range of transient and steady-state conditions throughout which the safety systems must perform, including conditions having the potential for functional degradation of safety system performance.

IEEE Std 603-1991 Clause 4 sections should be addressed for each design function. Note that while most IEEE Std 603-1991 Clause 4 sections may be addressed for each design function, some may be addressed for the system. For example, IEEE Std 603-1991 Clause 4.9 may identify reliability methods used for all design functions.

D.2.2.1 Design Functions

Through a review of system design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other submitted design details, the reviewer will confirm that the application contains information sufficient to demonstrate that the design bases information requirements contained conclude that the I&C system design satisfies the applicable requirements of Clause 4 of IEEE Std 603-1991.

The functional description should address the Section 4 clauses (defining the functional design basis) from IEEE Std. 603-1991. Note that the clauses do not need to be listed section by section but rather the information required by these clauses needs to be addressed for each design function.

D.2.2.2 System Requirements Specification

The System Requirements Specification (SyRS) should be an attachment to the LAR. The reviewer should confirm that the SyRS contains a description of the system level design, hardware and software design requirements, and the arrangement of equipment to assess the allocation of design functions described in D.2.2.1. The I&C architecture, plant design bases described above, and functional assignments are inputs to the SyRS.

The SyRS should be consistent with all material presented in the LAR. The reviewer is not expected to perform a design verification of the SyRS. Rather, the reviewer should confirm 1) that the SyRS contains the following information and 2) that following information is consistent with the design information contained in the LAR:

The SyRS should contain the:

- Functional and performance requirements should be consistent with the Replacement Scope Functions and Performance section above.
- For each safety function, the following should be established:
    a. Functionality, including input/output ranges and setpoints (respectively allowed ranges). For trip functions, the specification defines the margins between setpoints and allowable values (e.g., those including all uncertainties due to calibration errors or instrument drifts);
    b. Performance, including accuracy and response times. Where appropriate, performance requirements are defined for different initial plant conditions and design basis events.
    c. Appropriate signal filtering, signal validation and interlocks should be specified to minimize the potential of spurious actions.
    d. Requirements specification of each safety function should state its categorization and whether there are independence constraints from other functions in a safety group.
    e. Reliability targets
- Boundaries and interfaces with other systems including isolation requirements. Other boundary and interface information to be specified include:
    - Intended location and the physical constraints relevant to the installation of the system in the plant;
    - Physical and functional interfaces of the system with the supporting systems and equipment;
    - Physical and functional interfaces of the system with other systems and equipment with which it exchanges information;
- Interfaces with the operator or maintenance technician,

- Environmental conditions applicable to the system. The normal and extreme ranges of environmental conditions that the system is required to withstand should be specified in accordance with the constraints imposed from the plant design framework. Environmental conditions to be specified include:
  - Temperature, humidity, pressure, radiation and electromagnetic interference during normal operation and accident conditions;
  - Conditions imposed by potential hazards external to the system including seismic conditions or flooding
  - Power supply and heat removal conditions.
- Environmental qualification of hardware required based on design bases functions. For computer-based systems, this qualification includes the hardware (including compliance with the applicable environmental conditions), the operating system software and representative application software, both integrated in the hardware, per IEEE Std 7-4.3.2 Clause 5.4.
- For each auxiliary feature, the SyRS should establish the requirements for the auxiliary features available in the system's NRC-approved platform. The precision of the requirements for these functions is determined on a case by case basis pending equipment complexity. These functions could include self-diagnostics/testing, maintenance, etc.

D.2.3 Replacement System Architecture

The LAR should describe the system architecture, contrasting the existing system architecture with the revised system architecture. This section is intended to provide a basis for discussion of the Fundamental Design Principles in D.2.4. The replacement architecture section implements the Design Functions provided in Section D.2.2, augmented with the auxiliary features (features to support the design functions) described in this section. This section describes why certain design choices are to be implemented, along with explaining what the design provides and how the design is to be implemented. From an understanding of the system architecture as well as documenting implementation of consensus standards, regulatory requirements, and regulatory guidance, the reviewer determines that adequate evidence is provided to draw a conclusion that public health and safety will be protected.

The reviewer should confirm that the LAR provides documentation of the auxiliary features and design functions, as defined in this section.

Commented [PG3]: From Outline: Describe and illustrate the new system architecture.
Address the following clauses (defining the service function design basis) from IEEE 603-1991 and/or IEEE 7-4.3.2-2003:
- Clause 5.2, Completion of Protective Action
- Clause 5.5, System Integrity
- Clause 5.7, Capability for Test and Calibration
- Clause 5.8, Information Displays
- Clause 5.9, Control of Access
- Clause 5.10, Repair
- Clause 6.5, Capability for Testing and Calibration
- Clause 6.6, Operating Bypass
- Clause 6.7, Maintenance Bypass
- Clause 6.8, Setpoints (partial – multiple setpoints for single variable, depending on plant condition)
- Clause 7.3, Completion of Protective Action
- Clause 7.4, Operating Bypass
- Clause 7.5, Maintenance Bypass

The LAR should describe the architecture of the replacement system through text and diagrams, with emphasis on changes from the existing system. The LAR should provide drawings to explain the modification, block diagrams showing channels and divisions, and drawings showing changes to control boards. Providing drawings showing the existing and the replacement system are supplemented with text to describe not only what is being changed, but also how the change meets regulation and plant design criteria.

The reviewer should confirm that the LAR defines the extent to which the replacement system architecture is constrained by the existing plant architecture (including electrical divisions and mechanical trains), sensor and actuator physical arrangement, capabilities of the sensors and actuators, existing plant wiring, and functions performed by the existing system.

The LAR should define the mapping of logic channels and logic divisions to electrical divisions, as well as any required mapping of engineered safety features mechanical trains.

The LAR should state how compliance with separation requirements is maintained by architecture features per IEEE Std 603-1991, Clause 5.6.3.2 Equipment in Proximity.

If a diverse actuation system (DAS) is required, Section 2.5 will confirm that the integration of the system and DAS meets regulatory requirements (e.g., NUREG-6303, BTP 7-19, etc.), including DI&C ISG 04, Section 2. Confirm that, if a DAS is required, the architecture section describes the interconnections and interactions between 1) the primary protection system, 2) any portions of the existing system that remain, 3) the DAS, the priority logic, and 4) any affected licensee personnel.

The LAR should document the location of the system in the existing plant ventilation and fire zones. The LAR should document that no new fire hazards are introduced by the replacement system, and where possible, existing fire hazards are resolved.

The LAR should discuss any interfaces with post-accident monitoring sensors, and confirm that the replacement design does not adversely affect the required capabilities, including independence, diversity, and data display. For RG 1.97 A, B, and C variables and instrumentation credited for SRM-SECY-93-087 Point 4, the LAR should provide a comparison of the existing signal flow against the replacement system, demonstrating that no adverse effects were introduced.

For Tier 1, Tier 2, and Tier 3, the digital equipment vendor is identified in the submission. For Alternate Tier 1, the digital equipment vendor is identified by reference to the approved topical report and revision as the approving SE Report.

The reviewer should confirm that all Application Specific Action Items (ASAI) from the SE Report are identified and addressed. Any ASAI that do not apply to this application should be dispositioned and that disposition justified.

The reviewer should confirm that changes to the system design functions are identified, documented, and justified to meet the existing design basis.

The reviewer should confirm that added, deleted, or modified connections (including temporary connections for maintenance) between safety and safety and safety and non-safety systems are described and justified.

Changes to the following should be described:

- System design functions,
- Connections between safety systems,
- Connections between safety and non-safety systems and identification of signal and data isolation devices, and
- Temporary connections (e.g., for maintenance workstations).

D.2.3.1 Functional Allocation

Commented [PG4]: From Outline: Describe and explain the decomposition and allocation of functions to the various elements of the proposed architecture (e.g., hardware, software, plant personnel using human system interfaces).

The LAR should describe and explain allocation of design functions to the various elements of the proposed architecture (e.g., hardware, software, and licensee personnel using human system interfaces). These design functions are safety functions implemented in the application-specific software or logic.

The requirements for auxiliary features are based on the need for those features to support the design functions, in all modes of plant and system operation. These features (such as internal diagnostics) should have been previously reviewed as part of the digital equipment's topical report Safety Evaluation if Tier 1 or Alternate Tier 1. The LAR should address any application specific implementations of auxiliary features, and any changes to the auxiliary features since topical report approval.

The distribution of functions into physical hardware should be discussed, and drawings provided as required to illustrate the distribution.

The reviewer should confirm that the range of system response time includes all interlock and monitoring functions, which are identified during the design of the system architecture. The response time range should be valid for all modes of

replacement system operation as well as all plant modes, if either affects the system response time range.

Based on the distribution of functions, the requirements for interfaces justify the rationale for each interface or logical group of interfaces.

The reviewer should confirm that the LAR identifies and describes the mapping of logic drawings (i.e., functions) to logic elements in the system. The LAR should define any changes as well as reuse of existing plant interfaces.

The reviewer should confirm that the LAR documents the mapping of design functions and auxiliary features to software, hardware, and human implementations, or some combination of the software, hardware and human implementation.

Use of system redundancy to implement single failure tolerance should be documented. Use of internal redundancy within a division to enhance reliability should be documented.

Use of self-test and self-diagnostic features should be discussed, especially if those features are used to support reduction of frequency, or elimination, of surveillance tests or calibrations.

The reviewer should confirm that the LAR documents and defends any added complexity in the replacement system architecture. This defense should be based on enhancing safety by enhancing system reliability, reduction or elimination of surveillance testing with the resultant reduction in human error, elimination of operator manual actions with the resultant reduction in human error, or other accepted principles.

D.2.3.2 Interfaces External to the Replacement System

The LAR should define the interfaces between the portions of the system being replaced and the portions of the system and the plant that are not changed.

The reviewer should confirm that the LAR defines the connections between this system and other safety systems with a rationale and set of requirements for each connection.

Commented [PG5]: From Outline: Define all interfaces between the portion(s) of the system being replaced and:
- . the portions of the plant remaining unchanged
- . plant personnel (e.g., operators, maintainers, engineers).

Address the following clauses from IEEE 603-1991 and/or IEEE 7-4.3.2-2003:
- . Clause 5.13, Multi-Unit Stations
- . Clause 8, Power Source Requirements

This includes the communications to external systems. Features that affect SDOE are documented, but discussed in the SDOE section.

The reviewer should confirm that the LAR defines the connections between this system and any non-safety systems with a rationale and set of requirements for each connection.

The reviewer should confirm that the LAR identifies and describes the following:

- Existing, modified, and added input and output interfaces with the plant.
- Existing, modified, and added interfaces with control room displays, indicators, controls, and alarm systems, including the system's role and interfaces with post-accident monitoring and any reference by emergency plan implementing procedures.
- Existing, modified, and added human-system interfaces for the licensee's maintenance and engineering workstations used for test and maintenance.
- Support and auxiliary systems including power, heating, ventilation, and air conditioning (HVAC) and the system interface to the emergency diesel generator (EDG). The impact of single failure in the HVAC and the diverse means of annunciation of HVAC failure, along with a coping procedure, should be provided in the LAR.
- Confirm compliance to DI&C-ISG-04 Section 1. If applicable, confirm compliance to DI&C ISG 04 Section 2. Features that affect the Secure Operating Environment are mentioned, but review guidance is in the SDOE section;
- Compliance with IEEE 603-1991 Clause 8 for all power sources, including ac sources, dc sources, UPS sources, transfer between electric power sources, pneumatic sources, and hydraulic sources.

The LAR should document all sensors and actuators that the replaced system uses, including the functionality and purpose for each.

The reviewer should confirm that the LAR defines any connection allowing communication from a non-safety system to a safety system with a documented purpose, and that the safety system is designed with protection from any adverse action by the non-safety system. Confirm that the safety function and the SDOE of the safety system is not compromised by the connection.

The reviewer should confirm that the LAR documents the required electrical isolation for any signal crossing electrical or classification boundaries.

The reviewer should confirm that the LAR defines the hardwired interfaces, including any manual actuation means provided for operator use.

The reviewer should confirm that the defined use of the hardwired interfaces is consistent with the previous system, with any changes documented and the rationale for the change discussed.

The reviewer should confirm that the manual operator actuation means is not subject to a common cause failure that would disable the automatic function.

The LAR should demonstrate compliance to the following clauses from IEEE 603-1991 and/or IEEE 7-4.3.2-2003:

- Clause 5.12, Auxiliary Features – including diverse actuation system (DAS) if required.
- Clause 5.13, Multi-Unit Stations – including multi-divisional safety and non-safety related displays in DI&C ISG 04.
- Clause 5.15, Architectural Features added/changed to enhance reliability.

The LAR should demonstrate data communications compliance to DI&C-ISG-04 Sections 1 and 3.

D.2.3.3 Interfaces Internal to the Replacement System

The LAR should define interfaces between the different elements of the proposed architecture that are within the scope of the upgraded portion(s) of the system.

Interfaces should include all communication interfaces with permanently installed and temporary workstations. Features that affect SDOE are mentioned, but review guidance is found in the SDOE Section D.8.

Use of redundancy in interfaces internal to a division should be justified based on increasing reliability.

The reviewer should confirm compliance to DI&C-ISG-04 Sections 1 and 3.

The reviewer should confirm that the LAR lists all application-specific internal hardwired signal interfaces within the portion of the system being replaced.

D.2.3.4 Regulatory Considerations

The system design and architecture information should be reviewed for compliance to the following IEEE Std 603-1991 and IEEE 7-4.3.2 criteria:

- Clause 5.2 and 7.3 of IEEE Std. 603 1991, Completion of Protective Action
- Clause 5.5 of IEEE Std. 603 1991, System Integrity and Clause 5.5.1 of IEEE Std. 7-4.3.2-2003

Commented [PG6]: From Outline: Define interfaces between the different elements of the proposed architecture that are within the scope of the upgraded portion(s) of the system.
This includes workstations. Features that affect SDOE are mentioned, but discussed in the SDOE section.

- Clauses 5.7 and 6.5 of IEEE Std. 603 1991 and Clause 5.5.2 of IEEE Std. 7 4.3.2 2003, Capability for Test and Calibration
- Clause 5.8 of IEEE Std. 603 1991, Information Displays
- Clause 5.9, Control of Access in IEEE Std. 603-1991 and consider Clause 5.9 of IEEE Std. 7 4.3.2-2010
- Clause 5.10 of IEEE Std. 603 1991, Repair
- Clause 6.5 of IEEE Std. 603 1991 and Clause 5.5.2 of IEEE Std. 7 4.3.2 2003, Capability for Testing and Calibration – Confirm that new auxiliary features support any elimination or reduction of surveillance testing and calibration, including testing voters and output devices. Confirm that any auxiliary features required to support the platform self-test and self-diagnostics capabilities credited in the LAR provide the required functionality to implement any annunciation of detected issues or concerns.
- Clauses 6.6 and 7.4 of IEEE Std 603-1991, Operating Bypass – Confirm that the bypassed status is displayed in the control room
- Clauses 6.7 and 7.5 of IEEE Std 603-1991, Maintenance Bypass – Confirm the architecture and design only allows a single channel or division to be in Maintenance Bypass at any time, and that the bypassed status is displayed in the control room.
- Clause 6.8, Setpoints – For any setpoints that automatically or manually adjust based on plant conditions, confirm that the design provides notification to the control room operator of the current settings in each channel or division. Note that setpoint methodology is not part of this LAR section (see Section D.7).

D.2.4 Fundamental Design Principles in the New Architecture

Describe how the fundamental design principles are reflected in the new system architecture.

D.2.4.1 Redundancy

Confirm that the upgraded system design meets the requirements of the following clauses from IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003:

- Clause 5.1, Single Failure Criterion
- Clause 5.15, Reliability
- Clause 6.7, Maintenance Bypass
- Clause 7.5, Maintenance Bypass

Commented [PG7]: From Outline: Address the following clauses from IEEE 603-1991 and/or IEEE 7-4.3.2-2003:
- Clause 5.1, Single Failure Criterion
- Clause 5.15, Reliability

Confirm that the upgraded system design meets the requirements of the following GDCs:

- GDC 21, Protection System Reliability and Testability
- GDC 24, Separation of Protection and Control Systems

Confirm that the upgraded system design and architecture conforms to the guidance in RG 1.53 R2, which endorses IEEE Std. 379-2000.

D.2.4.2 Independence

Commented [PG8]: From Outline: Address the following clauses from IEEE 603-1991 and/or IEEE 7-4.3.2-2003:
- Clause 5.6, Independence
- Clause 5.11, Identification
- Clause 6.3, Interaction with Other Systems

This review addresses the physical, electrical, and functional independence attributes of the upgraded system. Data communications independence is addressed in the external and internal interface sections of this ISG by reviewing the system design and architecture information for compliance to DI&C-ISG-04.

Confirm that the upgraded system design meets the independence requirements of the following clauses from IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003:

- Clause 5.6, Independence
- Clause 5.11, Identification
- Clause 6.3, Interaction with Other Systems

Confirm that the upgraded system design meets the independence requirements of the following GDCs:

- GDC 13, Instrumentation and Control
- GDC 21, Protection System Reliability and Testability
- GDC 22, Protection System Independence
- GDC 24, Separation of Protection and Control Systems

Confirm that the physical and electrical independence attributes of the upgraded system design conform to the guidance in RG 1.75 R3, which endorses IEEE Std. 384-1992.

[Need to add a sentence or paragraph on functional independence – perhaps something similar to the DSRS (page 7.1-14).]

D.2.4.3 Deterministic Behavior

Commented [PG9]: From Outline: Address the following clauses from IEEE 603-1991:
- Clause 6.1, Automatic Control
- Clause 6.2, Manual Control
- Clause 7.1, Automatic Control
- Clause 7.2, Manual Control

This review evaluates the predictability and repeatability of the upgraded system design to assure that is behaves such that:

- input signals and system characteristics result in output signals through known relationships among system states and responses to those states

- the system produces the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow timely completion of credited actions

This review evaluates the predictability and repeatability of digital data communication outputs to:

- verify that system timing derived from the analyses of DBEs has been satisfied in the upgraded system design
- confirm that the upgraded system design and communication protocols provide features to assure that the system produces the correct response to inputs within the time credited to produce a response
- confirm that hazards that could challenge predicted behavior have been adequately identified and accounted for in the design

If an NRC-approved platform is used, and the system design and architecture information specifies the use of the platform's standard data communications, and the deterministic behavior of these communications have already been reviewed and approved by the NRC as part of the generic topical report, then the review is limited to the acceptable use of the communications in the system design and architecture. Compliance to any restrictions on the platform communications should be reviewed in the platform topical report SE. The review should confirm that the response time requirements can be met using these standard platform communications.

Confirm that the upgraded system design meets the deterministic behavior requirements of the following clauses from IEEE Std. 603-1991 and IEEE Std. 7-4.3.2:

- Clause 5.2, Completion of Protective Action
- Clause 5.5, System Integrity
- Clause 6.1, Automatic Control
- Clause 6.2, Manual Control
- Clause 7.1, Automatic Control
- Clause 7.2, Manual Control

Confirm that the upgraded system design meets the deterministic behavior requirements of the following GDCs:

- GDC 13, Instrumentation and Control
- GDC 21, Protection System Reliability and Testability
- GDC 29, Protection Against Anticipated Operational Occurrences

D.2.4.4 Defense-in-Depth & Diversity

This review is focused on whether the safety functions can be achieved in the event of a postulated CCF in the upgraded digital system.

Confirm that the upgraded system design does not invalidate the previously accepted design of the equipment used to address ATWS events (i.e., to meet the requirements of 10 CFR 50.62).

Confirm that the upgraded system design meets the defense-in-depth requirements of the following GDCs:

- GDC 13, Instrumentation and Control
- GDC 22, Protection System Independence
- GDC 24, Separation of Protection and Control Systems

Confirm that the upgraded system design meets the requirements of 10 CFR 50.34 (f)(2)(xiv), Containment Isolation Systems.

Confirm that the D3 evaluation addresses vulnerabilities to CCF in accordance with Staff Requirement Memorandum (SRM) to SECY-93-87, item 18.II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems.

Confirm that the D3 evaluation conforms to the guidance in BTP 7-19, including use of a NUREG/CR-6303 analysis methodology.

D.2.4.5 Simplicity of Design

This principle is more subjective than the others; therefore, rather than attempting to evaluate the adequacy of the upgraded system design's simplicity on some absolute basis, address it by evaluating the rationale for those design decisions that result in the upgraded system being more complex than it might otherwise need be.

Consider the resultant simplicity (or lack thereof) of design decisions, in particular, that impact redundancy, independence, deterministic behavior, and defense-in-depth and diversity. For design decisions that involve more complex approaches than might otherwise have been chosen, confirm that the benefit(s) obtained, particularly with respect to the fundamental design principles, justify the reduction in simplicity.

Design decisions involving such trade-offs may be driven by the need to satisfy a regulatory requirement (e.g., surveillance testing, improved maintainability and/or operability for faulted conditions).

Commented [PG10]: From Outline: BTP 7-19, RIS 2015-?? – Consider some of old ISG-6 D.6
(New 603-2017/2018 Clause 5.16)

Commented [PG11]: From Outline: This principle is more subjective than the others; therefore, rather than attempting to justify the adequacy of proposed design's "simplicity", address it by explaining the rationale for those design decisions that result in the system being more complex than it might otherwise need be. This will often be the result of needing to satisfy a regulatory requirement (e.g., surveillance testing and improved maintainability/operability for faulted conditions).
Address the following clauses from IEEE 603-1991:
- Clause 6.4, Derivation of System Inputs

Confirm that the upgraded system design meets the requirements of IEEE Std. 603-1991, Clause 6.4, Derivation of System Inputs.

D.2.5 New Design Basis

Address the differences, if any, between the design basis for the old system and the design basis for the new system (e.g., need for a diverse actuation system).

D.3 (Summary of) Modification Hardware Planning and Processes (e.g., EQ, EMC)

D.4 (Summary of) Application Software Planning and Processes (e.g., V&V, CM)

D.5 Platform Topical Report SE Report

D.5.1 Applicability of Topical Report

D.5.2 Disposition of Topical Report Post-SE Report Platform Changes

D.5.3 Resolution of Topical Report SE Report Open Items

D.6 (Unified Compliance Matrix for) IEEE Stds. 603 and 7-4.3.2

D.7 (Changes to) Technical Specifications (e.g., safety limits, setpoints)

D.8 Secure Development and Operational Environment

Enclosure A – Sample Summary of Level 0 Public Meeting to Discuss Plans to Request NRC Approval in Support of a Digital I&C Upgrade License Amendment Request

Enclosure B.1 – Information to be Provided in Support of a Digital I&C Upgrade License Amendment Request (Alternate Tier 1 Process)

Enclosure B.2 – Information to be Provided in Support of a Digital I&C Upgrade License Amendment Request (Current Tiers 1, 2, and 3)

Enclosure C – Sample Safety Evaluation for Digital I&C License Amendment