Nuclear Energy Agency's Consensus Position on Regulatory Inspections of Digital Instrumentation and Control Systems and Components Important to Safety used at Nuclear Power Plants – Inspection Framework

Mr. Ismael L. Garcia, P.E.[1*]

[1] U.S. Nuclear Regulatory Commission, Rockville, MD

ABSTRACT

The regulatory inspections on I&C systems important to safety reflect the applied technology. They include specific activities and generate specific outputs according to the instrumentation and control (I&C) system lifecycle processes. Regulatory Body (RB)'s inspection activities for software-based systems typically include quality management system reviews, technical reviews, walk-throughs, and audits. This paper documents a framework for preparing and conducting regulatory inspections of digital I&C architectures, systems, and components during various lifecycle phases, such as design, manufacturing at the manufacturer's facility, installation, commissioning, operation, and maintenance in nuclear power plants.

Keywords: control, digital, inspections, instrumentation, regulatory body

1. INTRODUCTION

The responsibility for the achievement and demonstration of safety when proposing or using digital I&C hardware and software for systems and components important to safety at nuclear power plants lies with the licensee. The primary purpose of regulatory inspections performed by a regulatory body (RB) is to independently provide a high level of assurance that activities, performed by the inspectee, comply with applicable laws, regulations, and conditions of authorization. For example, an RB performs inspections to verify whether the plants are operating safely and securely within the established regulations and authorized conditions for a nuclear power plant. Such inspection activities aim at assessing the inspectee's ability to safely operate a nuclear power plant in accordance with the country's regulations, license requirements, and adopted safety standards.

This paper documents an evaluation framework intended to apply to all digital I&C systems important to safety, both hardware and software, and was derived from work performed by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC). In this context, hardware includes industrial digital devices of limited functionality, for example, while software includes firmware and logic in any form, including supporting data; this includes, but is not limited to application, operational and pre-existing software and software tools, intellectual property cores, field programmable gate arrays, complex programmable logic devices, network equipment, and items intended for non-safety purposes with the potential to interfere with safety systems.

* Ismael.Garcia@nrc.gov

2. DISCUSSION

2.1. Definition of Terms

The following definitions are specific to this paper:

• **Audit:** Process for obtaining relevant information about an object of conformity assessment and evaluating it objectively to determine the extent to which specified requirements are fulfilled [1].

• **Inspection:** Examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements [1].
Note: Inspection activities typically include quality management system reviews, technical reviews, walk-throughs, and audits.

• **Inspectee:** An entity that undergoes an inspection including a manufacturer, vendor, applicant, or licensee.

• **I&C architecture:** Organizational structure of the I&C systems of the plant which are important to safety [2].

• **I&C system:** System, based on electrical and/or electronic and/or programmable electronic technology, performing instrumentation and control (I&C) functions as well as service and monitoring functions related to the operation of the system itself [2].

• **I&C component:** One of the parts that make up an I&C system. An I&C component may be hardware or software/programmable logic and may be subdivided into other components [2].

• **Fail-safe design:** Design of system functions so that they respond to specified faults in a predefined, safe way [3].

• **Safety class:** For nuclear power plants, the classes into which systems and components and other items of equipment are assigned on the basis of their functions and their safety significance [4].

• **Software:** The programs used to direct operations of a programmable digital device. Examples include computer programs and logic for programmable hardware devices, and data pertaining to its operation [5].

• **System important to safety:** A system that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public [4].

• **Qualification:** Process of determining whether a system or component is suitable for operational use. The qualification is performed in the context of a specific class of the I&C system and a specific set of qualification requirements [6].
Note: Qualification of I&C systems is always a plant- and application-specific activity while platform qualification relies to a large degree on qualification activities performed outside the framework of a specific plant design (these are called “generic qualification” or “pre-qualification”).

• **Quality:** The degree to which a product or process meets established requirements; however, quality depends upon the degree to which those established requirements accurately represent stakeholder needs, wants, and expectations [7].

• **Quality Management System:** All the planned and systematic activities implemented within the quality program, and demonstrated as needed, to provide adequate confidence that an entity will fulfil requirements for quality [8].

• **Unit Testing:** Testing an I&C component. Unit testing may be performed on hardware or software [9].

• **Verification:** Confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity [10].

• **Validation:** Confirmation by examination and by provision of other evidence that a system fulfils in its entirety the requirement specifications as intended [11].

• **Walk-throughs:** A static analysis technique in which a designer or programmer leads members of the development team and other interested parties (e.g., RB) through a segment of documentation or code, and the participants ask questions and make comments about possible errors, violation of development standards, and other problems [12].

2.2. Inspection Framework

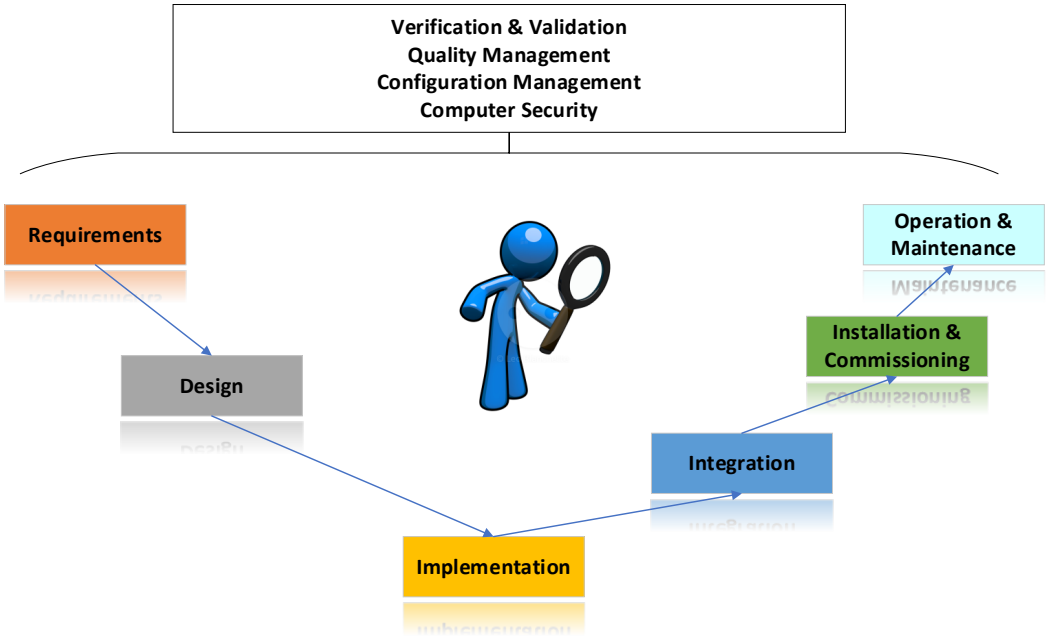

Figure 1. Regulatory inspections of digital instrumentation and control systems and components important to safety used at nuclear power plants – Inspection framework.

Fig. 1 above shows the inspection framework intended to apply to all digital I&C systems important to safety at nuclear power plants, both hardware and software. As shown in Fig. 1, the framework addresses the different quality management activities defined for each I&C system lifecycle phase.

2.2.1. General guidance

The inspectee should facilitate effective inspection by the RB, or organizations acting on its behalf, and make available, and provide on request, all the information necessary for the RB to carry out its inspection

programme. Furthermore, the RB should verify that the inspectee uses a documented plan for necessary activities that are not specific to I&C development, such as quality management and assurance, classification of items important to safety, purchasing, manufacturing, production, maintenance and management of documentation (e.g., configuration management). Nonetheless, each RB may have differing approaches for verifying the inspectee's documented plan, which may include the use of a multidisciplinary inspection approach. The RB should verify that compliance to relevant standards is adequately demonstrated by the inspectee.

2.2.2. Quality management system for I&C system lifecycle processes

The RB should verify that the inspectee has a suitably accredited quality management system to ensure that design basis documents and related or derived information or records are sufficient and adequate and are maintained over time to reflect design changes or, as applicable, changing conditions at the plant. This quality management system may include documents and information that may be derived from the design basis documentation and that may have an impact on safety, such as procedures or manuals relating to operation, maintenance, or modification of such systems. The RB should verify that the inspectee performs quality management system reviews to identify consistency with and deviations from plans, or adequacies and inadequacies of management procedures. The RB should also verify that the inspectee has the necessary technical knowledge to conduct a successful quality management system review. The RB should verify whether the quality management system includes the competences, qualification requirements, and allocated resources (e.g., personnel, equipment, infrastructure, and the working environment) of the inspectee necessary for developing, operating and maintaining I&C systems that meet important to safety requirements.

The RB should verify that the inspectee provides sufficient evidence to demonstrate that the implemented processes include fundamental quality assurance activities such as mapping of required activities to the lifecycle model. The result of such activities should be a well-defined and methodical software lifecycle, which is essential to a high-quality software development program. The RB should verify that the inspectee provides sufficient evidence to demonstrate that processes can effectively pass down requirements (e.g., technical, quality, security) to lower tier suppliers in purchase orders which indicate the important to safety nature of the system and provide adequate oversight in the procurement of such equipment from lower tier suppliers. The RB should verify that the inspectee has documented evidence to demonstrate that processes can effectively verify that the I&C systems supplied conforms to the procurement documents. The RB should verify that the inspectee uses a documented plan for the activities associated with all lifecycle phases. The RB should verify that the documented plan identifies the need for timely engagement with the RB and that it accounts for regulatory activities and hold-points. The RB should verify whether the I&C development activities were performed in accordance with the applicable approved plans. The RB should verify that the inspectee uses corrective actions process in accordance with the quality management system.

2.2.3. Requirements

The RB should verify that the inspectee has a process for identifying, specifying, and tracing the requirements throughout the I&C system lifecycle and the associated outputs have been adequately documented. The RB should verify that the requirements identified by the inspectee address design aspects such as: functionality, performance, reliability, environmental qualification, cybersecurity, testability, maintainability, and, aging management including spare parts availability.

The RB should verify that the requirements identified by the inspectee include those derived from plant level to the overall I&C architecture, from the I&C architecture to I&C systems, and from the I&C system to I&C components. Requirements should include those for addressing common cause failures. The RB

should verify that the inspectee identified all requirements for the systems and components to ensure that requirements properly satisfy the essential properties of the system. Relevant requirements should address system aspects such as potential failure conditions, operating modes, self-supervision, failure detection and annunciation, and fail-safe behavior.

The RB should verify that the inspectee provides sufficient evidence to demonstrate that there are processes in place to support the development of the architecture of the system in order to derive the system functions from the system requirements, and identify the hardware, software, and operational requirements. The RB should assess the requirements activities of the I&C system lifecycle by performing the following: (1) Verifying that the hardware and software design requirements are documented and that they incorporate applicable regulatory requirements, standards and codes; (2) Verifying that the requirements documentation specifies the functional and performance characteristics, interfaces, installations considerations, design constraints, and security constraints; and (3) Verifying that a formal process is documented and implemented to ensure changes to hardware and software requirements are evaluated, reviewed, approved, and documented.

2.2.4. Design

The RB should evaluate the design activities of the I&C system lifecycle. Specifically, the RB should verify whether: (1) The design is developed with an understanding of the origin of the safety requirements; (2) The completed design demonstrates the following attributes: (a) Unambiguous; (b) Correct and demonstrably complete with respect to the requirements; (c) Consistent; (d) Well structured; (e) Readable; (f) Understandable to the target audience (e.g., designers, implementers, testers, maintainers, and regulators); (g) Verifiable; (h) Able to be validated; (i) Traceable; (j) Maintainable; and, (k) Documented; (3) To the extent required, the design supports deterministic behavior and time response requirements for the function important to safety; (4) The design takes into account best practices in terms of cyber security, in order to avoid the creation of security vulnerabilities; and (5) The design is modular, to support activities related to other lifecycle phases such as testing and integration.

2.2.5. Implementation

The RB should assess the implementation activities of the I&C system lifecycle by performing the following: (1) Verify that procedures are established and implemented for compliance with coding rules, methods, and standards; (2) For software, verify that implementation activities, such as the creation of an executable code, development of operation documentation, software unit testing, and management of software releases are completed in accordance with a documented implementation plan (e.g., system test plan, verification and validation plan, configuration management plan, etc.); and, (3) Verify that procedures are established and implemented for manufacturing hardware system components in accordance with specifications and detailed design drawings and testing them.

2.2.6. Integration

The RB should verify that the inspectee provides sufficient evidence of the integrated software- and hardware-development processes to develop an integrated product for which the used methodology is well documented, understood, and questioned. The RB should verify the integration activities of the I&C system lifecycle include the following: (1) Verifying that the plans for integrating hardware and software components into a system are adequately documented. The plan should include information such as schedule, resource and staffing estimates, and criteria for the commencement of hardware and software integration. The plan

should also identify what is being integrated, define the integration environment, discuss the management of interfaces, define the integration sequence, and discuss the testing to verify that the integration has been completed satisfactorily. The configuration of a system to be integrated should be well-known in advance, and all possible deviations should be documented. (Note: For a single component, integration of software parts and hardware parts is typically a straight-forward task, which is performed using dedicated tools). I&C system integration should be representative of the final configuration of the I&C system at the site; (2) Verifying that there are provisions in the procedures to ensure the complete integration of all hardware and software units and comprised software modules or any other division of functional parts; and, (3) Verifying that hardware and software integration test activities and tasks; primary test methods and standards; test cases; test coverage; and acceptance criteria are documented.

2.2.7. Hardware qualification

For digital I&C hardware, the RB should verify that the inspectee provides sufficient evidence to demonstrate that the qualification testing encompasses the specified service conditions (e.g., electrical loading, radiation, humidity, submergence, temperature, electromagnetic interference), including end-of-life conditions, while ensuring that such conditions would not degrade the function important to safety of the device(s) being tested. The RB should verify that the inspectee provides sufficient evidence to demonstrate that measures have been established for the selection and suitability review of components to be used in functions important to safety. Where components have been previously qualified, their use should be demonstrated to be adequately covered by the previous qualification. The evidence of the previous qualification activities (e.g., qualification reports, type-testing certificate) should be made available to the RB.

The RB should verify that the inspectee provides sufficient evidence to demonstrate that the processes and plans implemented can be effectively used to determine whether or not any manufacturing differences or changes to a given part would affect any design or qualification assumptions. For example, a device which initially consisted only of electrical components was software-free now includes software-based or programmable-based technology.

2.2.8. Installation and commissioning

Installation should be carefully performed by the inspectee in accordance with the manufacturer's installation instructions. The approved configuration with correct versions of the software and hardware as well as configuration parameters should be restored if the systems or components have been shipped empty. The RB should verify that the installation inspection performed by an inspectee includes checking of correct connection of cables, correct versions of cards and other components inside cabinet and correct versions of software components. The installation inspection should be performed while the work is being executed and not just afterwards, to ensure that appropriate working methods are being followed.

The RB should assess the system installation testing activities of the I&C system lifecycle by performing the following: (1) Verifying that there are provisions documented in procedures for modifications to the hardware or software made during installation; (2) Verifying that adequate installation testing has been performed. For example, the overall I&C interconnections with other systems should be verified during installation testing activities; (3) Verifying that acceptance test activities and tasks; primary test methods and standards; test cases; test coverage; and acceptance criteria are adequately documented. The evidence of the installation verification activities should be made available to the RB.

Commissioning, which could incorporate site acceptance testing, is the last phase where changes to a system or component can be done before commencement of plant operations at power. During the commissioning tests, the functionality of the system or component should be tested as thoroughly as possible. The I&C system or component should be tested by the inspectee to ensure that it works with the plant's process systems, and that signal exchange with other I&C systems and human machine interfaces are working properly. The RB should verify that the inspectee ensures that commissioning test coverage is sufficient, both in terms of functionality and physicality (i.e., from sensor to actuator). The RB should verify that procedures are established and implemented for the performance of commissioning testing to demonstrate the installed system will perform its intended function important to safety as described in the system design basis. The RB should verify that procedures are implemented to document and resolve conditions that deviate from expectations based on requirements specifications, design documents, user documents, or standards prior to placing the system into operation.

2.2.9. Operation and maintenance

The RB should verify that procedures are implemented by the inspectee to assess any detected faults, determine whether they may affect safety, and document their resolution. The assessment should address the necessary improvements and corrective actions. The RB should assess the operation activities of the I&C system lifecycle by performing the following:

(1) Verifying that documentation for the methods, plan, and deployment of the digital I&C system hardware and software include, at a minimum, the following: (a) Documentation to support the operations, including user manuals, configuration control documents, instructions, procedures, and other associated documentation; (b) A description of the functions that the system is to perform and general discussion of the means to carry out those functions; (c) The controls needed over operation activities to prevent unauthorized changes to hardware, software, and system parameters; (d) Specification of the monitoring activities needed to detect unauthorized access to the system; (e) Modifications of systems to make sure that the original design basis is respected or revisions to the design basis are appropriately addressed; (f) A description of the facilities used to operate the hardware and software; (g) A description of the procedures for executing the software in all operating modes and procedures for ensuring the software state is consistent with the plant operating mode at all times; (h) A description of the backup procedures for data and code and the intervals at which back up should occur; (i) A comprehensive list of the error messages, a description of the error indication, the probable reason for the error indication, and steps to be taken to resolve the error; (j) Controls for continuously maintaining and monitoring I&C important to safety system performance to ensure it is consistent with pre-established system performance measures e.g., fan changes, filter changes; and, (k) Contingency plans needed to ensure appropriate response to control of access issues;
(2) Verifying that the assumptions used for equipment qualification are maintained (e.g., electromagnetic interference, electrical loading, radiation, humidity, submergence, temperature);
(3) Verifying that procedures have been established for managing ageing and obsolescence of the digital I&C equipment;
(4) Verifying that procedures have been established for monitoring the system's performance, recording problems for analysis, taking corrective and preventative actions, and confirming restored capability after servicing. Verify that procedures include instructions for documenting, evaluating, correcting, and reporting software or hardware errors. The evaluation should include how an error impacts previous use of the software or hardware and the development process;
(5) Verifying that there are provisions included in procedures to prohibit informal changes made to the software or hardware during maintenance that improve the performance or other attributes or adapt the design outputs to a modified environment. These changes are considered design changes and should be done in accordance with the software and hardware modification procedures; and,

(6) Verifying that maintenance is not used to perform design changes but instead, it is limited to the process of repairing nonconforming items or implementing pre-planned actions necessary to maintain performance (e.g., control setpoints or tuning parameters).

The RB should verify that the inspectee has a defined and implemented program for systems important to safety periodic examination, inspection, maintenance and/or tests, that includes applicable functional tests, instruments checks, verification of proper calibration and response time tests, and maintenance of all associated records. The tests should verify periodically the basic functional capabilities of the system, including functions important to safety, major functions not important to safety, and special testing used to detect failures unable to be revealed by self-supervision or by alarm or anomaly indications. The RB should verify that the periodic testing does not adversely affect the intended system functions.

2.2.10. Verification and validation

The RB should verify whether the inspectee performed a comprehensive assessment for a given digital I&C system or component to verify that requirements properly satisfy the essential properties of the system. The RB should assess the verification and validation activities of the I&C system lifecycle by taking into account if:

(1) The extent and type of the verification and validation activities are suitable for the safety class of the system or component involved;
(2) Procedures are established to identify the verification and validation activities for all hardware and software requirements;
(3) Procedures are established and implemented for performing design reviews, alternate calculations, analysis, or testing to verify the adequacy of the software and hardware design;
(4) Procedures are established and implemented for review of quality management system, technical reviews, inspections, walkthroughs, and audits;
(5) Measures are established for conducting reviews which ensure conformance of the software and hardware to design requirements and satisfactory completion of the software development activities/phases;
(6) Procedures are established for the documentation and resolution of all non-conformances identified during the I&C system lifecycle. These procedures should account for cases where test results do not conform to the requirements. For such cases, the RB should verify that an evaluation is performed by the inspectee. For example, if response time or accuracy requirements are not met for a system or component, it should be assessed by the inspectee to determine if it invalidates plant level requirements or accident analysis. This analysis should be documented and made available to the RB;
(7) Procedures are established for problem identification, extent of condition, and risk mitigation for issues that have the potential to significantly impact the system quality; and,
(8) The verification and validation were carried out by personnel with adequate technical competence and knowledge, and independent of the designers and developers. The extent and type of independence of the verification and validation should be suitable for the safety class of the system or component involved. Depending on the country's regulatory framework, this may include independence of design tools and verification and validation tools.
The RB should verify that digital I&C system testing is conducted on a completely integrated system, in which all hardware and software functionality has successfully passed integration testing and have been combined into one final system. The RB should verify that the inspectee provides sufficient evidence that any pre-developed items are appropriately qualified and suitable to perform intended functions important to safety and the qualification programmes address all topics affecting the suitability of each system or component for its intended functions. The RB should verify that the functions important to safety that have to be performed by the pre-developed items are adequately covered by their qualification. The RB should verify that the interfaces invoking pre-developed items are clearly identified and thoroughly

validated by the inspectee. The RB should verify that functions important to safety do not interface with pre-developed items by means not clearly identified and thoroughly validated.

2.2.11. Configuration management

The RB should verify that procedures are implemented by the inspectee to establish a hardware and software baseline at the completion of each lifecycle phase. The RB should verify that procedures are implemented by the inspectee to establish access control to the configuration management platform. The RB should verify that procedures are implemented by the inspectee to ensure that changes made to the hardware or software are evaluated, reviewed, approved, and documented. The evaluation should include an analysis (e.g., regression analysis) to determine the impact of the changes on all I&C system lifecycle activities. The RB should verify that a configuration management process is established by the inspectee in an early phase of project. The configuration management process should be set up for software and hardware version control and the issuing of correct versions. The configuration management process may include provisions for informing all relevant personnel, including the RB per the country's regulatory requirements, of pending changes and approved modifications. The RB should verify that the inspectee has a process for determining which product information needs to be updated through the product lifecycle and which would be considered obsolete after project completion. The RB should verify that provisions are included by the inspectee in the procedures to ensure hardware and software tools used to support system development and verification and validation processes are under configuration management. For operational plants, the RB should verify that procedures are implemented to ensure that I&C system design requirements, the facility configuration documentation, and installed I&C system configuration are aligned.

2.2.12. I&C system lifecycle activities with computer security programmes

The RB should leverage the evaluation guidance documented in WGDIC CP-08, "Impact of Cyber Security Features on Digital I&C Systems Important to Safety," [13] when assessing the implementation of computer security programmes within the I&C system lifecycle activities performed by an inspectee.

3. CONCLUSIONS

While there are different approaches for performing the regulatory inspections of digital I&C hardware and software for systems and components important to safety at nuclear power plants, the WGDIC concludes that the agreed-upon guidance documented herein describes a series of regulatory inspection practices that apply to digital I&C systems in operating reactors and new reactors, which can help verify that they are designed, manufactured, installed, commissioned, operated and maintained in accordance with the regulatory requirements, manufacturer's design, operating recommendations and facility's licensing basis. Furthermore, the evaluation framework discussed by this paper is not to be construed as a requirement, regulation, or acceptable guidance by either domestic or international regulators. Instead, it is intended to serve as a potential foundation or technical basis to be used for developing clear and sufficient regulatory guidance for RB inspections of digital I&C systems important to safety at nuclear power plants.

ACKNOWLEDGMENTS

This paper was derived from the work performed by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) Working Group on Digital Instrumentation and Control (WGDIC), which I have the honor and privilege to have served as the Chairman. For additional information concerning the NEA/CNRA WGDIC visit: https://www.oecd-nea.org/nsd/cnra/.

(Note: The goal of the NEA/CNRA WGDIC was not to independently develop new regulatory standards. As such, the technical work develop by the NEA/CNRA WGDIC is not legally binding and do not constitute additional obligations for the regulators or the licensees. Instead, the technical work resulting from the NEA/CNRA WGDIC constitutes guidelines, recommendations, or assessments that the NEA/CNRA participants agree are good to highlight during their safety reviews of operating and new reactors. The development of technical guidance for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants follows the WGDIC examination of the regulatory requirements of the participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) documents.)

REFERENCES

1. "ISO/IEC 17000:2020, Conformity assessment — Vocabulary and general principles," https://www.iso.org/standard/73029.html (2020).
2. "IEC 61513:2011, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," https://webstore.iec.ch/publication/5532 (2011).
3. "IEC 62340:2007, Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)," https://webstore.iec.ch/publication/6874 (2007).
4. "IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection," https://www.iaea.org/publications/11098/iaea-safety-glossary-2018-edition (2018).
5. "IEEE Std. 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," https://standards.ieee.org/standard/7-4_3_2-2016.html (2016).
6. "IEC 63084 TR: Nuclear power plants – Instrumentation and control important to safety – Platform qualification for systems important to safety," https://webstore.iec.ch/publication/34127 (2017).
7. "IEEE 730-2014, IEEE Standard for Software Quality Assurance Processes," https://standards.ieee.org/ieee/730/5284/ (2014).
8. "IEEE 12207.0-1996, IEEE/EIA Standard - Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207) Standard for Information Technology -- Software Life Cycle Processes," https://standards.ieee.org/ieee/12207.0/2375/ (1998).
9. "IEEE 1012-2016, IEEE Standard for System, Software, and Hardware Verification and Validation," https://ieeexplore.ieee.org/document/8055462 (2017).
10. "IEC 61513: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," https://global.ihs.com/doc_detail.cfm?document_name=IEC%2061513&item_s_key=00378381 (2011).
11. "IAEA SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants," https://www.iaea.org/publications/10838/design-of-instrumentation-and-control-systems-for-nuclear-power-plants (2016).
12. "ISO/IEC/IEEE 24765:2010, Systems and software engineering — Vocabulary," https://www.iso.org/standard/50518.html (2010).
13. "Generic Common Position DICWG-08: Impact of Cyber Security Features on Digital I&C Safety Systems," https://www.oecd-nea.org/mdep/common-positions/dicwg_8_rev_f.pdf (2012).