Nuclear Regulation
NEA/CNRA/R(2022)3
April 2025

www.oecd-nea.org

Consensus Position on Regulatory Inspections of Digital Instrumentation and Control Systems and Components Important to Safety Used at Nuclear Power Plants (CP-15)

BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CNRA/R(2022)3

Unclassified **English text only**

8 April 2025

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

Consensus Position on Regulatory Inspections of Digital Instrumentation and Control Systems and Components Important to Safety Used at Nuclear Power Plants (CP-15)

This document is available in PDF format only.

JT03563943

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 38 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation’s statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 34 countries: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czechia, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia (suspended), the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States. The European Commission and the International Atomic Energy Agency also take part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes;
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management and decommissioning, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Corrigenda to OECD publications may be found online at: *www.oecd.org/about/publishing/corrigenda.htm*.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES (CNRA)

The Committee on Nuclear Regulatory Activities (CNRA) addresses NEA programmes and activities concerning the regulation, licensing and inspection of nuclear installations with regard to both technical and human aspects of nuclear safety. The Committee constitutes a forum for the effective exchange of safety-relevant information and experience among regulatory organisations. To the extent appropriate, the Committee reviews developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them and assist in the development of a common understanding among member countries. In particular it reviews regulatory aspects of current safety management strategies and safety management practices and operating experiences at nuclear facilities including, as appropriate, consideration of the interface between safety and security with a view to disseminating lessons learnt. In accordance with *The Strategic Plan of the Nuclear Energy Agency: 2017-2022*, the committee promotes co-operation among member countries to use the feedback from experience to develop measures to ensure high standards of safety, to further enhance efficiency and effectiveness in the regulatory process and to maintain adequate infrastructure and competence in the nuclear safety field.

The committee promotes transparency of nuclear safety work and open public communication. In accordance with the NEA Strategic Plan, the committee oversees work to promote the development of effective and efficient regulation.

The committee focuses on safety issues and corresponding regulatory aspects for existing and new power reactors and other nuclear installations, and the regulatory implications of new designs and new technologies of power reactors and other types of nuclear installations consistent with the interests of the members. Furthermore, it examines any other matters referred to it by the NEA Steering Committee for Nuclear Energy. The work of the committee is collaborative with and supportive of, as appropriate, that of other international organisations for co-operation among regulators and consider, upon request, issues raised by these organisations. The Committee organises its own activities. It may sponsor specialist meetings, senior-level task groups and working groups to further its objectives.

In implementing its programme, the committee establishes co-operative mechanisms with the Committee on the Safety of Nuclear Installations (CSNI) in order to work with that committee on matters of common interest, avoiding unnecessary duplications. The committee also co-operates with the Committee on Radiological Protection and Public Health (CRPPH), the Radioactive Waste Management Committee (RWMC), and other NEA committees and activities on matters of common interest.

Foreword

Regulatory inspections of digital instrumentation and control (I&C) hardware and software for systems and components important to safety at nuclear power plants are needed to verify that such systems are suitable for their intended applications. This consensus position (CP) provides guidance for preparing and conducting regulatory inspections of digital I&C hardware and software for systems and components during design and manufacturing at the manufacturer's facility, as well as during installation, commissioning, operation and maintenance in nuclear power plants. Guidance is given for different quality management activities and for each digital I&C system and component life cycle phase.

The Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) believes that sharing experience and regulatory practices is a major element in the efforts made by the regulatory body and the industry to maintain and improve the safe operation of nuclear power plants. Considering the importance of digital I&C topics, the CNRA established a Working Group on Digital Instrumentation and Control (WGDIC[1]) to promote harmonisation and improvements in nuclear safety through the development of regulatory guidance to address digital I&C topics and technical issues of concern to its member countries, for both operating and new reactors. The WGDIC reports on a regular basis to the Committee. The WGDIC constitutes an international forum for nuclear regulatory organisations to co-operate in the development of consensus positions (CPs), representing the common understanding and harmonisation of regulatory practices. The CPs provide a consistent set of regulatory expectations for the industry and may be used by members in the development of guidance in their own national regulatory frameworks.

The audience for this CP is primarily regulatory bodies, although the information and ideas are expected to be of interest to licensees, other nuclear industry organisations, the general public, and of special interest to emerging nuclear countries which have yet to develop well-established regulatory regimes.

The goal of the WGDIC is not to independently develop new regulatory standards. CPs are not legally binding and do not constitute additional obligations for the regulators or the licensees but are guidelines, recommendations or assessments that the WGDIC participants agree are good to highlight during their safety reviews of new reactors and operating plant upgrades. CNRA members are encouraged to implement CPs through their national regulatory processes.

This report was approved by the CNRA during its 47th meeting held on 2-3 June 2022.

[1] The WGDIC was ended on 31 December 2022 as the CNRA restructured the organisation and governance of its work activities, including subsidiary bodies. This report is also available on the Working Group on New Technology (WGNT) SharePoint site.

Acknowledgements

The Nuclear Energy Agency (NEA) thanks the following WGDIC member countries, which participated in the development of this consensus position and endorsed its publication.

Canada	Canadian Nuclear Safety Commission (CNSC)
The People's Republic of China	National Nuclear Safety Administration (NNSA)
Czechia	State Office for Nuclear Safety (SÚJB)
Finland	Finnish Centre for Radiation and Nuclear Safety (STUK)
France	Nuclear Safety Authority (ASN), Institute for Radiological Protection and Nuclear Safety (IRSN)
Germany	Federal Office for the Safety of Nuclear Waste Management (BASE), TÜV Rheinland Industrie Service GmbH (TIS)
Hungary	Hungarian Atomic Energy Authority (HAEA)
India	Atomic Energy Regulatory Board (AERB)
Japan	Nuclear Regulation Authority (NRA)
Netherlands	Authority for Nuclear Safety and Radiation Protection (ANVS)
Poland	The Office of Technical Inspection (UDT)
Russian Federation	Rostechnadzor, VO Safety
Spain	Nuclear Safety Council (CSN)
Korea	Korea Institute of Nuclear Safety (KINS)
Sweden	Swedish Radiation Safety Authority (SSM)
United Kingdom	Office for Nuclear Regulation (ONR)
United States	United States Nuclear Regulatory Commission (USNRC)

This consensus position is compatible with the related safety standards of the International Atomic Energy Agency (IAEA) available at the time of publication.

[2] The People's Republic of China was an invitee of the WGDIC.

The IAEA and the following standard development organisations participated in their capacity as WGDIC observers in the development of this consensus position:

IEC	International Electrotechnical Commission
IEEE	Institute of Electronic and Electrical Engineers

Table of contents

List of abbreviations and acronyms

AERB	Atomic Energy Regulatory Board (India)
ANVS	Authority for Nuclear Safety and Radiation Protection (Netherlands)
ASN	Autorité de sûreté nucléaire (French Nuclear safety authority [ASNR since January 2025]) (France)
BASE	Federal Office for the Safety of Nuclear Waste Management (Switzerland)
CNRA	Committee on Nuclear Regulatory Activities (NEA)
CNSC	Canadian Nuclear Safety Commission (Canada)
CSN	Nuclear Safety Council (Spain)
CP	Consensus Position
DICWG	Digital Instrumentation and Control Working Group under MDEP
HAEA	Hungarian Atomic Energy Authority (Hungary)
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electronic and Electrical Engineers
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (French Institute for Radiological Protection and Nuclear Safety [ASNR since January 2025])
ISO	International Organization for Standardization
KINS	Korea Institute of Nuclear Safety (Korea)
MDEP	Multinational Design Evaluation Programme
NEA	Nuclear Energy Agency
NNSA	National Nuclear Safety Administration (United States)
NRA	Nuclear Regulation Authority (United States)
ONR	Office for Nuclear Regulation (United Kingdom)
RB	Regulatory Body
SSM	Swedish Radiation Safety Authority (Sweden)
STUK	Finnish Centre for Radiation and Nuclear Safety (Finland)
SÚJB	State Office for Nuclear Safety (Czechia)
TIS	TÜV Rheinland Industrie Service GmbH (Germany)
UDT	Office of Technical Inspection (Poland)
USNRC	United States Nuclear Regulatory Commission (United States)
WGDIC	Working Group on Digital Instrumentation and Controls (NEA)
WGIP	Working Group on Inspection Practices (NEA)

Executive summary

The Nuclear Energy Agency (NEA) Working Group on Digital Instrumentation and Controls (WGDIC) has agreed that a consensus position on the topic of regulatory inspections of digital instrumentation and control (I&C) hardware and software for systems and components important to safety at nuclear power plants is warranted given the increased use of digital I&C in new reactor designs and upgrades on operating plants, the safety implications of this increased use, and the need to develop a common understanding from the perspectives of regulatory authorities. This action follows the WGDIC examination of the regulatory requirements of the participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) publications. The WGDIC developed this consensus position based on its recent experience with the new reactor application reviews and operating plant issues.

This consensus position provides guidance for facilitating the process of preparing and conducting regulatory inspections[3] of digital I&C hardware and software for systems and components during design and manufacturing at the manufacturer's facility as well as during installation, commissioning, operation and maintenance in nuclear power plants. The guidance herein is not to be construed as a requirement or regulation; instead, it is intended to serve as a source of information to be used for developing clear and sufficient regulatory guidance for performing regulatory inspections of digital I&C hardware and software for systems and components important to safety.

[3] For the purpose of this consensus position, the term "inspection" also includes "audit."

Introduction

The licensee is responsible for the achievement and demonstration of safety when proposing or using digital instrumentation and control (I&C) hardware and software for systems and components important to safety at nuclear power plants.

The primary purpose of 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 authorisation. For example, an RB performs inspections to verify whether the plants are operating safely and securely within the established regulations and authorised conditions for a nuclear power plant. Such inspection activities aim to assess the inspectee's ability to safely operate a nuclear power plant in accordance with the country's regulations, licence requirements and adopted safety standards.

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 I&C system life cycle processes. RB inspection activities for software-based systems typically include quality management system reviews, technical reviews, walk-throughs and audits. The guidance discussed herein is for preparing and conducting regulatory inspections of digital I&C architectures, systems and components during various life cycle phases, such as design, manufacturing at the manufacturer's facility, installation, commissioning, operation and maintenance in nuclear power plants.

Additional information on digital I&C inspections can be found in the "Proceedings of the Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C)", developed by the WGDIC and the (NEA) Working Group on Inspection Practices (WGIP) held on 9-13 June 2019 in Toronto, Canada (NEA, 2023). This document describes a series of regulatory inspection practices that apply to digital I&C systems in operating reactors and new reactors and 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[4].

[4] A set of regulatory requirements applicable to a nuclear installation.

Definitions[5]

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 (ISO/IEC 17000:2020).

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 (ISO/IEC 17000:2020). 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: Organisational structure of the I&C systems of the plant which are important to safety (IEC 61513:2011).

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 (adapted from IEC 61513:2011).

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 (adapted from IEC 61513:2011).

Fail-safe design: Design of system functions so that they respond to specified faults in a predefined, safe way (see IEC 62340:2007).

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 (IAEA Safety Glossary 2018).

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 (IEEE Std 7-4.3.2:2016).

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 (adapted from IAEA Safety Glossary, 2018).

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 (IEC 63084 TR). 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 (IEEE Std 730:2014).

[5] The standards in parentheses included in the definitions may be found in the list of references at the end of this report.

Quality management system: All the planned and systematic activities implemented within the quality programme, and demonstrated as needed, to provide adequate confidence that an entity will fulfil requirements for quality (adapted from IEEE/EIA 12207.0:1996).

Unit testing: Testing an I&C component. Unit testing may be performed on hardware or software (adapted from IEEE Std 1012-2016).

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 (IEC 61513).

Validation: Confirmation by examination and by provision of other evidence that a system fulfils in its entirety the requirement specifications as intended (IAEA SSG-39).

Walk-through: 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 (adapted from ISO/IEC/IEEE 24765:2010(E)).

Scope

This consensus position (CP) provides guidance on the inspection of digital I&C hardware and software for systems and components important to safety. Specifically, the CP provides guidance to regulatory bodies (RBs) for performing a comprehensive inspection through the examination of governing documents for life cycle activities (e.g. design, manufacturing, verification and validation), and the sampling of the results of the implementation of these governing documents for the systems and components in question. The consensus positions that follow in this document give the full set of those aspects that could be inspected; the expectation is that the RB would select those appropriate for the systems and components in question in order to achieve an adequate sample.

It is recognised that each country may have differing approaches for performing inspections, which may include the use of a multidisciplinary team. Some parts of the inspection may be performed in the RB's facility, especially those that require extensive examination of large document sets (e.g. analysis documents).

Guidance is given for different quality management activities defined for each I&C system life cycle phase including:

- Requirements (e.g. plant requirements, functional requirements, systems requirements), which consist of developing a description of what functions the digital I&C software and hardware must accomplish.
- Design, which consists of translating requirements into a hardware/software architecture and detailed design.
- Implementation, which includes translating the completed software design into code, manufacturing and testing the hardware system components. Software and hardware unit testing is conducted in this phase.
- System integration, which consists of combining software components and hardware components into a single system.
- Hardware qualification, which consists of the generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements.
- Installation and commissioning, which consists of installing and testing the integrated digital I&C system in its operational environment and is the last phase where changes to a system or component can be done before commencement of plant operations at power.
- Operation and maintenance, which consists of ensuring the continued use, and the safe and secure operation of the software and hardware as designed. It also involves ensuring safe and secure operation when changes to the digital I&C system are made after its initial commissioning.

Inspection guidance is also included for the following activities that are performed throughout the I&C system life cycle.

- Quality management system to be applied for I&C system life cycle processes and verification and validation activities. It includes a variety of elements, such as equipment design control, procurement document control, manufacturing quality control, qualification assessment (e.g. testing, analysis, combined testing and analysis, and experience), storage, installation and commissioning, installation surveillance and maintenance, periodic testing, and documentation.

- Verification and validation activities, which are necessary for ensuring that the final product is suitable for use.
- Configuration management process that is ensured during the life cycle for I&C systems.
- I&C system life cycle activities dealing with computer security programs.

Consensus Positions on Regulatory Inspections of Digital Instrumentation and Control Systems and Components Important to Safety Used at Nuclear Power Plants

1.1. General commendable practices

1. The inspectee should facilitate effective inspection by the regulatory body (RB), or organisations acting on its behalf, and make available, and provide on request, all the information necessary for the RB to carry out its inspection programme.
2. The RB should verify that the inspectee uses a documented plan for necessary activities that are not specific to I&C development, such as:

   a. quality management and assurance;

   b. classification of items important to safety;

   c. purchasing;

   d. manufacturing; and

   e. production, maintenance and management of documentation (e.g. configuration management).

   It is recognised that each country may have differing approaches for verifying the inspectee's documented plan, which may include the use of a multidisciplinary inspection approach.
3. The RB should verify that compliance to relevant standards is adequately demonstrated by the inspectee.

1.2. Quality management system for I&C system life cycle processes

4. 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 includes 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.
5. 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.
6. 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 life cycle model. The result of such activities should be a well-defined and methodical software life cycle, which is essential to a high-quality software development program.
7. 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.

8. The RB should verify that the inspectee has documented evidence to demonstrate that processes can effectively verify that the I&C systems supplied conform to the procurement documents.

9. 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.

10. The RB should verify that the inspectee uses a documented plan for the activities associated with all life cycle phases.

11. 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.

12. The RB should verify whether the I&C development activities were performed in accordance with the applicable approved plans.

13. The RB should verify that the inspectee uses corrective actions processed in accordance with the quality management system.

14. The RB should verify that the inspectee selects the manufacturer/vendor for a component or system using a systematic method including predefined criteria and conditions, which include:

    a. a mature and updated quality management system;

    b. a mature organisation, management, and safety culture;

    c. available competences with relevant up-to-date knowledge and experiences; and

    d. a plan for long-term support.

    Typically, this selection process requires an audit by the inspectee, in addition to a paper-based review or assessment. Depending on the country's regulatory framework, the RB may participate as an observer during such an audit or may participate in the approval process. It is recognised that in some countries the RB does not engage in the manufacturer/vendor selection process.

1.3. Inspection elements within the I&C system life cycle processes and verification and validations

1.3.1. Requirements

15. The RB should verify that the inspectee has a process for identifying, specifying, and tracing the requirements throughout the I&C system life cycle and the associated outputs have been adequately documented.

16. The RB should verify that the requirements identified by the inspectee address design aspects such as:

    a. functionality;

    b. performance;

    c. reliability;

    d. environmental qualification;

    e. cyber security;

    f. testability;

    g. maintainability; and

h. ageing management, including spare parts availability.

17. 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 I&C system to component level. Requirements should include those for addressing common cause failures (additional information can be found in MDEP Generic Common Position DICWG-01: *Treatment of Common Cause Failure Caused by Software within Digital Safety Systems*).

18. 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:

    a. potential failure conditions;

    b. operating modes;

    c. self-supervision;

    d. failure detection and annunciation; and

    e. fail-safe behaviour.

19. 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 system requirements, and identify the hardware, software and operational requirements.

20. The RB should assess the requirement activities of the I&C system life cycle by verifying that:

    a. The hardware and software design requirements are documented and that they incorporate applicable regulatory requirements, standards and codes.

    b. The requirements documentation specifies the functional and performance characteristics, interfaces, installations considerations, design constraints, and security constraints.

    c. A formal process is documented and implemented to ensure changes to hardware and software requirements are evaluated, reviewed, approved and documented.

1.3.2. Design

21. The RB should evaluate the design activities of the I&C system life cycle. The RB should verify whether:

    a. The design is developed with an understanding of the origin of the safety requirements.

    b. The completed design demonstrates the following attributes:

        i. unambiguous;

        ii. correct and demonstrably complete with respect to the requirements;

        iii. consistent;

        iv. well structured;

        v. readable;

        vi. understandable to the target audience (e.g. designers, implementers, testers, maintainers and regulators);

        vii. verifiable;

viii. able to be validated;

ix. traceable;

x. maintainable; and,

xi. documented.

c. To the extent required, the design supports deterministic behaviour and time response requirements for the function important to safety.

d. The design takes into account best practices in terms of cyber security in order to avoid the creation of security vulnerabilities.

e. The design is modular to support activities related to other life cycle phases such as testing and integration.

22. The RB should verify that the inspectee performed an I&C system hazard analysis (additional information can be found in MDEP Generic Common Position DICWG-10: *Hazard Identification and Controls for Digital Instrumentation and Control Systems*).

23. The RB should verify that the inspectee performed a reliability analysis to show that the digital I&C system fulfils its system reliability requirements. It is recognised that each country may have differing RB requirements for determining the digital I&C system reliability.

24. The RB should verify that the inspectee ensures that the chosen analysis methods are suitable for use, and that relevant input data are available for those methods.

1.3.3. Implementation

25. The RB should assess the implementation activities of the I&C system life cycle. It should:

a. Verify that procedures are established and implemented for compliance with coding rules, methods and standards.

b. 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)

c. Verify that procedures are established and implemented for manufacturing hardware system components in accordance with specifications and detailed design drawings and testing them.

1.3.4. Integration

26. 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.

27. The RB should verify the integration activities of the I&C system life cycle:

a. Verify 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.

b. Verify that the hardware and software integration plan identifies what is being integrated, defines the integration environment, discusses the management of interfaces, defines the integration sequence, and discusses the testing to verify that the integration has been completed satisfactorily. The configuration of a system to be integrated should be wellknown in advance, and all possible deviations should be documented. (Note: For a single component, integration of software parts and hardware parts is typically a straightforward 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.

c. Verify 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.

d. Verify that hardware and software integration test activities and tasks; primary test methods and standards; test cases; test coverage; and acceptance criteria are documented.

1.3.5. Hardware qualification

28. 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.

29. 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.

30. 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 software-free device, which initially consisted only of electrical components, now includes software-based or programmable-based technology.

1.3.6. Installation and commissioning

31. 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 the correct connection of cables, correct versions of cards and other components inside the cabinets 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.

32. The RB should assess the system installation testing activities of the I&C system life cycle. It should:

    a. Verify that there are provisions documented in procedures for modifications to the hardware or software made during installation.

    b. Verify that adequate installation testing has been performed (additional information can be found in MDEP Generic Common Position DICWG-11: *Digital I&C System Pre-installation and Initial On-site Testing*). For example, the overall I&C interconnections with other systems should be verified during installation testing activities.

c. Verify 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.

33. Commissioning, which could incorporate site acceptance testing, is the last phase where changes to a system or component can be made 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).

34. It might be necessary for the inspectee to perform some tests in overlapping steps or phases to ensure safety of the plant and personnel. For such cases, the RB should verify that the inspectee has plans in place for determining which tests can be performed onsite with real process parameters and which can be performed in a simulator or similar, and how the overall test coverage is documented.

35. When upgrading an old system with a new digital system or component, the RB should verify that the inspectee can demonstrate that the new system preserves the existing plant safety properties (e.g. considering timing constraints, delays and response times).

36. 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.

37. The RB should verify that procedures are implemented to document and resolve conditions that deviate from expectations based on requirement specifications, design documents, user documents, or standards prior to placing the system into operation.

1.3.7. Operation and maintenance

38. 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.

39. The RB should assess the operation activities of the I&C system life cycle:

    a. Verify that documentation for the methods, plan, and deployment of the digital I&C system hardware and software include, at a minimum, the following:

        i. Documentation to support the operations, including user manuals, configuration control documents, instructions, procedures and other associated documentation.

        ii. A description of the functions that the system is to perform and general discussion of the means to carry out those functions.

        iii. The controls needed over operation activities to prevent unauthorised changes to hardware, software and system parameters.

        iv. Specification of the monitoring activities needed to detect unauthorised access to the system.

        v. Modifications of systems to make sure that the original design basis is respected or revisions to the design basis are appropriately addressed.

        vi. A description of the facilities used to operate the hardware and software.

vii. 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.

viii. A description of the backup procedures for data and code and the intervals at which backup should occur.

ix. 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.

x. 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.

xi. Contingency plans needed to ensure appropriate response to control of access issues.

b. Verify that the assumptions used for equipment qualification are maintained (e.g. electromagnetic interference, electrical loading, radiation, humidity, submergence, temperature).

c. Verify that procedures have been established for managing ageing and obsolescence of the digital I&C equipment.

d. Verify 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.

e. Verify 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.

f. Verify 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).

40. The RB should verify that the inspectee has a defined and implemented programmes 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.

1.3.8. Verification and validation

41. The RB should verify whether the inspectee performed a comprehensive assessment for a given digital I&C system or component to verify that the requirements properly satisfy the essential properties of the system.

42. The RB should assess the verification and validation activities of the I&C system life cycle by taking into account whether:

a. The extent and type of the verification and validation activities are suitable for the safety class of the system or component involved.

b. Procedures are established to identify the verification and validation activities for all hardware and software requirements.

c. Procedures are established and implemented for performing design reviews, alternate calculations, analysis, or testing to verify the adequacy of the software and hardware design.

d. Procedures are established and implemented for review of quality management system, technical reviews, inspections, walk-throughs and audits.

e. 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.

f. Procedures are established for the documentation and resolution of all non-conformances identified during the I&C system life cycle. 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.

g. Procedures are established for problem identification, extent of condition, and risk mitigation for issues that have the potential to significantly impact the system quality.

h. The verification and validation are 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.

43. The RB should verify that the inspectee provides sufficient evidence to demonstrate that the processes used to evaluate the software hazard analysis can be effectively used to identify the adequacy of the software hazard analysis produced.

44. Testing includes many successive phases starting from unit level testing to factory acceptance testing of the full integrated system, or component, for the final hardware/software configuration that will be installed on the plant. The last phase is commissioning, i.e. testing in the target environment.

    The RB should verify whether:

    a. The inspectee has provided sufficient evidence that the overall testing processes is conducted in accordance with approved test specifications, procedures and plans.

    b. Documentation of the actual test configuration is in place when test runs are performed on prototypical equipment configurations.

45. The RB should verify that the inspectee provides sufficient evidence of the processes followed to identify or verify critical characteristics for a component or system that would ensure that the requirements for a given test would be met. Critical characteristics depend on the system's functionality, and can include response time, measurement accuracy, tolerance to input errors, tolerance to internal failures or errors.

46. The RB should verify that the inspectee provides sufficient evidence of the processes followed to document and evaluate any test anomaly and associated change in test configuration to ensure

that the original test configuration requirements would still be met. The final test configuration, or configuration to be shipped onsite, should be carefully documented, and deviations from design should be recognised and updated in the upstream documents.

47. If several connected systems are required to be tested, they should be tested by the inspectee in an integrated way. If they are tested separately (e.g. due to logistical reasons), the RB should verify that the inspectee provides justification that systems behave the same way as when they are integrated. For example, timing issues of signals between systems (e.g. co-ordination signals, check-backs) should be carefully analysed by the inspectee if the systems have been implemented using different technologies and tested separately.

48. Standards have some requirements on measuring test coverage of software, but no strict requirements for the target value of coverage. The value naturally depends on the type of test coverage. Several overlapping coverage metrics might be needed to demonstrate that software and the whole system are sufficiently tested. Additional information can be found in MDEP Generic Common Position DICWG-11: *Digital I&C System Pre-installation and Initial On-site Testing*.

49. The RB should evaluate the testing activities of the I&C system life cycle. It should:

    a. Verify that there are provisions documented in procedures to ensure that all testable hardware and software requirements are covered by acceptance testing.

    b. Verify that documentation supporting hardware and software testing includes the following:

        i. Qualifications, duties, responsibilities and skills required of persons and organisations assigned to testing activities.

        ii. Special conditions and controls, equipment, tools, and instrumentation needed for the accomplishment of testing.

        iii. Test instructions and procedures that incorporate the requirements and acceptance limits in applicable design documents.

        iv. Test prerequisites and the criteria for meeting these requirements and acceptance limits.

        v. Test items and the approach taken by the testing program.

        vi. Test logs, test data and test results.

        vii. Pass/fail criteria.

        viii. Test records that indicate the identity of the tester, the type of observation made, the results and acceptability, and the action taken in connection with any deficiencies.

        ix. Test plans, test activities and task, test cases, and test coverage test methods and standards.

    c. Verify that the results of testing are documented, reviewed, analysed and approved by a qualified individual to ensure test requirements have been fulfilled.

    d. Assess whether the process established to incorporate changes to the hardware and software due to test results, is adequate to ensure that all test anomalies are documented, tracked and resolved.

    e. Verify that the actions taken to address testing anomalies discovered during testing, which may impact system hardware and software requirements, include revisions to system hardware and software requirement documentation and subsequent design documentation as necessary.

f. 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. Note: See also MDEP Generic Common Position DICWG-03: *Verification and Validation Throughout the Life Cycle of Digital Safety Systems.*

50. 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 leverage the evaluation guidance documented in WGDIC Consensus Position CP-14, *Qualification of I&C Platforms for Use in Systems Important to Safety,* during this verification. (Note: Also see MDEP Generic Common Positions DICWG-07: Selection and Use of Industrial Digital Devices of Limited Functionality and DICWG-10: *Hazard Identification and Controls for Digital Instrumentation and Control Systems*.)

51. 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 (Note: See WGDIC CP-14).

52. 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.

1.3.9. Configuration management

53. The RB should verify that procedures are implemented for configuration control of plant design basis inputs for the I&C system requirements.

54. The RB should verify that procedures are implemented by the inspectee to ensure life cycle outputs are reviewed, approved, baselined, updated as necessary, and placed under configuration control.

55. The RB should assess the configuration management activities of the system life cycle by verifying that procedures for configuration control are applied by the inspectee to the initial development of I&C systems, changes made during development and modifications after they have been placed in service, which include:

a. Identification and control of all hardware and software designs and code.

b. Identification and control of all hardware and software design functional data (e.g. data templates and data bases).

c. Identification and control of all hardware and software design interfaces.

d. Control of all hardware and software design changes including:

i. Description and rationale for the change;

ii. An evaluation of the change request;

iii. Identification of the hardware and software baseline affected by the change, and status of the change throughout the system life cycle.

e. Control of hardware and software documentation (e.g. user, operating and maintenance documentation).

f. Control and retrieval of qualification information associated with hardware and software designs and code.

g. Audits of hardware and software configuration.

h. Status accounting or the process of recording and reporting configuration item descriptions (e.g. hardware, firmware) and all departures from the baseline during design and production.

56. The RB should verify that procedures are implemented by the inspectee to establish a hardware and software baseline at the completion of each life cycle phase.

57. The RB should verify that procedures are implemented by the inspectee to establish access control to the configuration management platform.

58. 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 life cycle activities.

59. 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.

60. The RB should verify that the inspectee has a process for determining which product information needs to be updated through the product life cycle and which would be considered obsolete after project completion.

61. 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.

62. 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.

1.3.10. I&C system life cycle activities with computer security programmes

63. The RB should leverage the evaluation guidance documented in WGDIC CP-08, *Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants*, when assessing the implementation of computer security programmes within the I&C system life cycle activities performed by an inspectee.

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 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.

In support of the continual evolution of digital I&C technology and its associated challenges, the WGDIC will continue to assess any gaps not being addressed by contemporary regulations and guidance related to the regulatory inspections of digital I&C hardware and software. Future revisions to this CP will allow the bridging of those gaps while ensuring its relevance and technical adequacy.

References and further reading

Bel V., Canadian Nuclear Safety Commission, et al. (2018), Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations, www.julkari.fi/bitstream/handle/10024/136773/safety_critical_software.pdf.

IEC (2017), Nuclear power plants - Instrumentation and control important to safety - Platform qualification for systems important to safety, IEC 63084 TR, https://webstore.iec.ch/en/publication/34127.

IEC (2011), Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems, Ed.2, IEC 61513, https://webstore.iec.ch/en/publication/5532.

IEC (2007), Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)", IEC 62340:2007, https://webstore.iec.ch/en/publication/6874.

IAEA (2018), Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

IAEA (2016), Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, www.pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf.

IAEA (2010), Application of Configuration Management in Nuclear Power Plants, IAEA Safety Reports Series No. 65, www-pub.iaea.org/MTCD/Publications/PDF/Pub1461_web.pdf.

IEEE (2016), IEEE Standard for System, Software, and Hardware Verification and Validation, IEEE Std 1012-2016.

IEEE (2016), IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2.

IEEE (2014), IEEE Standard for Software Quality Assurance Processes, IEEE Std 730:2014.

IEEE (2008), IEEE Standard for Software Reviews and Audits, IEEE Std 1028.

IEEE/EIA (1998), Standard for Information Technology - Software Life Cycle Processes, IEEE/EIA Standard - Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207).

ISO/IEC (2020), Conformity assessment – Vocabulary and general principles, ISO/IEC 17000:2020.

ISO/IEC/IEEE (2017), Systems and software engineering – Vocabulary, 24765:2017(E).

NEA (2023), Proceedings of the Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C), OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_84412.

NEA (2022), Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants [CP-08], OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_75241.

NEA (2018), Consensus Position on the Qualification of I&C Platforms for Use in Systems Important to Safety [CP-14], OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_19884.

NEA (2016), Hazard Identification and Controls for Digital Instrumentation and Control Systems, Generic Common Position DICWG-10, www.oecd-nea.org/mdep/common-positions/MDEP_GCP-DICWG-10_HazardIDandControl.pdf.

NEA (2014), Selection and Use of Industrial Digital devices of Limited Functionality, Generic Common Position DICWG-07, www.oecd-nea.org/mdep/common-positions/DICWG_GCP-DICWG-07.pdf.

NEA (2013), Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems, Generic Common Position DICWG-01, www.oecd-nea.org/mdep/common-positions/dicwg-01.pdf.

NEA (2013), Verification and Validation Throughout the Life Cycle of Digital Safety Systems, Generic Common Position DICWG-03, www.oecd-nea.org/mdep/common-positions/gcp-dicwg-03_VV_Ver_H.pdf.

NEA (2013), Digital I&C System Pre-installation and Initial On-site Testing, Generic Common Position DICWG-11, www.oecd-nea.org/mdep/common-positions/gcp-dicwg-11-ver-e.pdf.

US NRC (2018), Quality Assurance Inspection of Software Used in Nuclear Applications, US Nuclear Regulatory Commission Inspection Procedure 35710, www.nrc.gov/docs/ML1727/ML17278A510.pdf.