Nuclear Regulation
NEA/CNRA/R(2018)3
August 2019
www.oecd-nea.org

Consensus Position on the Qualification of Instrumentation and Control Platforms for Use in Systems Important to Safety at Nuclear Power Plants (CP-14)

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CNRA/R(2018)3

Unclassified

English text only

9 August 2019

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

Consensus Position on the Qualification of Instrumentation and Control Platforms for Use in Systems Important to Safety at Nuclear Power Plants [CP-14]

This document is available as PDF only.

JT03450249

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 36 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, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, 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 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, 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 sound 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 analyses in areas such as energy and the sustainable development of low-carbon economies.

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.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES (CNRA)

The Committee on Nuclear Regulatory Activities (CNRA) is responsible for 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 power plants including, as appropriate, consideration of the interface between safety and security with a view to disseminating lessons learnt. In accordance with the *NEA Strategic Plan for 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 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 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, the Radioactive Waste Management Committee, and other NEA committees and activities on matters of common interest.

Foreword

The qualification of instrumentation and control (I&C) platforms for use in systems important to safety at nuclear power plants is needed to demonstrate that these I&C platforms are suitable for their intended applications. Therefore, this consensus position (CP) provides evaluation guidance for the qualification of platforms developed for general industrial use as well as those developed specifically for nuclear applications important to safety. The evaluation guidance discussed herein addresses the following: 1) the scope of qualification; 2) methods of qualification; 3) documentation; 4) the use of the qualification; and 5) the maintenance of qualification.

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 instrumentation and control (DI&C) topics, the CNRA established a Working Group on Digital Instrumentation and Control (WGDIC) to promote harmonisation and improvements in nuclear safety through the development of regulatory guidance to address DI&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 CPs representing the common understanding and harmonisation of regulatory practices. The CPs provide a consistent set of regulatory expectations for 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 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. All members of the WGDIC are encouraged to implement CPs through their national regulatory processes.

Table of contents

Acknowledgements

The Nuclear Energy Agency (NEA) would like to thank the following WGDIC member countries which participated in the development of this consensus position and endorse its publication.

Canada:	Canadian Nuclear Safety Commission (CNSC)
China:	National Nuclear Safety Administration (NNSA)
Czech Republic:	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)
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)
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.

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

International Electrotechnical Commission (IEC)

Institute of Electrical and Electronics Engineers (IEEE)

List of abbreviations and acronyms

CP	Consensus position
CPLD	Complex programmable logic device
CPU	Central processing unit
CSA	Canadian Standards Association
EMC	Electromagnetic compatibility
EPLD	Erasable programmable logic device
EPRI	Electric Power Research Institute (United States)
EQ	Equipment qualification
FPGA	Field programmable gate array
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission (Switzerland)
IEEE	Institute of Electrical and Electronics Engineers (United States)
ISO	International Standards Organization (Switzerland)
I&C	Instrumentation and control
I/O	Input/Output
PCB	Printed circuit board
SSG	Specific safety guide
TR	Technical report
WGDIC	Working Group on Digital Instrumentation and Control (NEA)

Consensus Position on the Qualification of I&C Platforms for Use in Systems Important to Safety at Nuclear Power Plants

Executive Summary

The Nuclear Energy Agency (NEA) Working Group on Digital Instrumentation and Control (WGDIC) has agreed that a consensus position on the topic of the qualification of instrumentation and control (I&C) platforms for use in systems important to safety is warranted given the increase of use of digital I&C in new reactor designs and upgrades on operating plants, the safety implications 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 participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) documents. The WGDIC proposes a consensus position based on its recent experience with the new reactor application reviews and operating plant issues. This consensus position provides evaluation guidance regarding the following: 1) the scope of qualification; 2) methods of qualification; 3) documentation; 4) the use of the qualification; and 5) the maintenance of qualification. 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 assessing a given digital I&C platform qualification for use in systems important to safety.

Introduction

I&C platforms are used for systems important to safety in nuclear power plants. Some of these platforms were developed specifically for nuclear power applications but many were developed for a wide range of industrial applications. The qualification of I&C platforms for use in systems important to safety at nuclear power plants is needed in order to demonstrate that these I&C platforms are suitable for their intended applications.

This consensus position provides evaluation guidance for the qualification of platforms developed for general industrial use as well as those developed specifically for nuclear applications important to safety. In some cases, an I&C platform may be qualified with a specific application in mind, in others a generic qualification may be undertaken. This consensus position provides evaluation guidance for the qualification of platforms for both generic and specific applications.

Definitions

Accreditation: The formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards. (ISO - https://www.iso.org/certification.html).

Application software library: Collection of software modules implementing typical application functions. Note: When using pre-existing equipment (here platform), such a library is considered to be part of the system software and qualified as such. (IEC 63084 TR, 2017).

Certificate: A document issued by an accredited body stating the applicable conditions to be met for certification and certifying compliance with relevant standards if the conditions are met. (Adapted from IAEA Safety Glossary 2016).

Certification: The provision by an accredited body of written assurance (a certificate) that the product, service or system in question meets specific requirements. (Adapted from ISO - https://www.iso.org/certification.html).

Critical characteristics: Those important design, material, and performance characteristics of a commercial off-the-shelf item that, once verified, will provide reasonable assurance that the item will perform its intended safety function. (Adapted from EPRI TR-106439).

Deterministic behaviour: Characteristic of a system or component, such that any given input sequence that is within the specifications of the item always produces the same outputs. (IAEA SSG-39, 2016).

Deterministic timing: Characteristic of a system or component, such that the time delay between the stimulus and response has a guaranteed maximum and minimum value. (IAEA SSG-39, 2016).

Functional requirements: Requirements that specify the required functions or behaviours of an item. (IAEA SSG-39, 2016).

Graded approach: A process or method in which the stringency of the control measures and conditions to be applied is commensurate, to the extent practicable, with the likelihood and possible consequences of, and the level of risk associated with, a loss of control. (Adapted from IAEA Safety Glossary, 2016).

Non-functional requirements: also known as quality requirements – Requirements that specify inherent properties or characteristics of an item other than the required functions and behaviours. Example characteristics include analysability, assurability, auditability, availability, compatibility, documentation, integrity, maintainability, performance, reliability, safety, security, usability and verifiability (Adapted from IAEA SSG-39, 2016).

Platform: Set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant-specific configurations and of the related application software may be supported by software tools. An I&C platform usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software (IEC 63084 TR).

User: A generic term for licensee (operator), requesting party, duty holder, applicant, dedicating entity or similar.

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").

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).

Sub-supplier: Supplier of components and/or services to the main supplier of the I&C platform.

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, 2016).

Scope

This consensus position applies to the qualification of the hardware and software of I&C platforms intended for systems important to safety at nuclear power plants.[1] It should be noted that qualification in this context is the process of determining whether an I&C platform is suitable for operational use.

This consensus position provides evaluation guidance for the qualification of platforms developed for general industrial use as well as those developed specifically for nuclear applications important to safety.

This consensus position provides evaluation guidance regarding the following:

- Scope of qualification;
- Methods of qualification;
- Documentation;
- Use of the qualification;
- Maintenance of qualification.

Specifically, this consensus position discusses the kind of information and considerations associated with the platform qualification for each of the areas listed above that would need to be assessed as part of the evaluation.

The acceptability of the overall qualification will be a decision for the regulatory body of the country in which the platform is to be used.

This consensus position does not assume that a particular digital I&C technology is used for the I&C platform (e.g. microprocessor, field programmable gate arrays, electronics).

1. It is recognised that different countries use different classification schemes for systems important to safety. It should be noted that not all countries require the qualification of systems of lower classifications.

Consensus Position on the Qualification of I&C Platforms for Use in Systems Important to Safety at Nuclear Power Plants

Scope of the qualification

1) The scope of the platform qualification should be defined, and should comprise components including but not limited to:

   a. The hardware supporting, or with the potential to affect, the safety function, for example:

      - Central processing unit (CPU);
      - Memory chips;
      - I/O Modules;
      - Communications interface modules;
      - Other hardware as necessary to fulfill the safety function.

   b. The software[2] supporting, or with the potential to affect, the safety function including for example:

      - Operating system;
      - Library functions, e.g. software blocks intended for a specific task;
      - Communications software, e.g. drivers;
      - I/O modules software;
      - Other software as necessary to fulfill the safety function

   c. Embedded components such as power supplies, industrial digital devices of limited functionality, complex programmable logic devices, application specific integrated circuits or field programmable gate arrays (FPGA) devices.

   d. Software and hardware tools (e.g. calibration tools) used in the design, development, verification, validation, manufacturing, maintenance or modification of the platform. It should be noted that the MDEP Common Position DICWG 02 – *Software Tools* identifies the expectations for the justification of software tools.

   e. Documentation e.g. specifications, design documents, operation and maintenance manuals.

2) Although the specific application may not be known at the time of qualification, the range (or envelope) of applications for the I&C platform and their critical characteristics should be defined, e.g. deterministic behaviour for systems of the highest safety classification. This thereby facilitates the generic qualification of the platform and provides the opportunity to use the qualification for multiple applications. It does not, however, remove the requirement to qualify the application itself.

2. Some I&C platforms do not contain any software; in this case, the portion of this consensus position related to software may not apply to those platforms.

3) The definition of the range of applications should include, but not be limited to, the following:

   a. The highest safety classification that the platform may fulfill;

   b. The types of safety function(s) that the platform may fulfill e.g. reactor trip, post-trip cooling, main steam supply control;

   c. The non-functional requirements applicable to the platform, e.g. dependability, equipment qualification (EQ), physical constraints, performance.

4) The platform should be classified according to its importance to safety, which will be driven by the applications.

5) Any constraints that the platform qualification imposes on its potential application (e.g. maximum CPU load to maintain determinism[3]) should be explicitly identified and justified in the qualification documentation.

6) The platform qualification should address, to the extent practicable, any digital I&C security requirements that may exist in the regulatory framework of the country in which the platform is proposed for use (see MDEP DICWG-08 for consensus positions on security).

Methods of qualification

General guidance

7) A graded approach should be taken to the qualification of the I&C platform, the rigour applied should be commensurate with the safety classification of the intended application.

8) The qualification should include an evaluation of the outputs of the platform development process and a validation that the product is capable of meeting the functional and non-functional requirements.

9) The configuration management of the development and modification of the platform should be considered in the qualification.

10) The platform should be subject to equipment qualification (e.g. electromagnetic compatibility [EMC], environmental and seismic) in accordance with the standards and expectations applicable in the country in which it will be used.

11) Access should be provided by the supplier to those artifacts from the design, implementation, manufacture, verification and validation of the platform necessary to facilitate the qualification.

12) Access to such artifacts should be provided to the organisation undertaking the qualification and also, as necessary, to the regulatory body for the country within which the platform is to be used.

13) If the information necessary to undertake the qualification of the platform is not available, then the decision may be that the platform is not suitable for use in systems important to safety. It is recognised that some countries may have different expectations of what information needs to be made available in order to accept the qualification.

3. Regulators have witnessed examples where the performance of an I&C platform could not be guaranteed because of a CPU load limit being exceeded.

14) The methods of qualification of I&C platforms for use in systems important to safety will vary depending upon the provenance of the platform. The platform may have been developed specifically for use in nuclear safety applications or may have been developed for general industrial use. The following consensus positions respectively apply to these two scenarios.

Platforms Developed for Nuclear Safety Applications

15) The platform should be developed using the recognised nuclear standards, practices and regulatory framework applicable in the country in which it is to be used.

16) Any deviations from the recognised nuclear standards, practices and regulatory framework should be identified and justified. The methods by which any deviations may be justified may include those identified in consensus position 19 below.

17) For some countries this is considered to be the only acceptable approach for systems of the highest safety classification.

Platforms Developed for General Industrial Use

18) The platform supplier should expect to provide the following information prior to commencement of the detailed qualification exercise:

a. The demonstration of an accredited quality management system;

b. A commitment to provide the necessary resources to support the qualification;

c. A commitment to provide access to all artifacts necessary to complete the qualification, including those from sub-suppliers and certification bodies;

d. Confirmation of the continued support of the platform.

19) The qualification of the platform may incorporate a combination of some or all the following methods:

a. Development process review

b. Confirmation of the implementation of the supplier's quality management processes

c. Independent Confidence Building Measures

d. Operating experience

e. Certification

The method or combination of methods used for the qualification should be justified. The acceptability of the overall qualification will be a matter for the regulatory body for the country in which the platform is to be used e.g. in some countries methods a. and b. are considered mandatory. Consensus positions 20 to 26 describe each of these methods.

20) The platform design, development, manufacture, verification and validation, and maintenance should be reviewed against the nuclear standards, practices and regulatory framework applicable for the country in which it is to be used. (Note: This is known as a commercial grade survey in some countries.)

a. Any discrepancies should be addressed through the undertaking of compensating activities, by the supplier, the user and/or another competent organisation. Compensating activities should be targeted at the discrepancies

found and may include, but are not limited to, the reverse engineering and verification of design documentation or additional analysis and testing.

21) Confirmation of the implementation of the supplier's quality management processes should be undertaken. This should include activities such as witnessing at the supplier's premises the hardware fabrication and assembly, software development and testing, and supplier inspection activities. The approach taken to the supplier's procurement and use of components and products (e.g. FPGAs, EPLDs, CPLDs, PCBs, operating system, software tools.) from a sub-supplier should also be demonstrated to be adequate for the platform in question.

22) The development processes and products of sub-suppliers should be verified as being appropriate for use in the platform by meeting the critical characteristics inherited from the platform using the methods described herein. It is recognised that each country may have differing degrees of requirements for verifying the development processes and products of sub-suppliers.

23) It is acknowledged that sub-suppliers will themselves utilise components from other suppliers. Such components should be justified using the methods described in consensus position 19. The platform qualification documentation should explicitly state and justify the depth to which analysis of the supply chain has been undertaken. This justification should consider the criticality of the components in fulfilling the safety functions performed by the platform.

24) Independent confidence building measures (including tests, inspections and analyses) may be used to supplement the review of the platform development process by demonstrating that the platform product itself fulfills the range of applications and critical characteristics defined for its qualification.

    a. The independent confidence building measures should be implemented and/or observed by an organisation other than the platform supplier to avoid undue commercial influences for this aspect of the qualification (Note: the supplier should also conduct their own tests, inspections and analyses as part of the platform development process).

25) Operating experience may be used to support the qualification of the platform. The amount of field data and the conditions under which the data is to be collected should be demonstrated to be sufficient as defined by the nuclear standards, practices and regulatory framework applicable to the country. The data should be shown to be applicable to the manufacturer, model and version of the platform and its components. The platform operating experience should be shown to be relevant to the range of intended nuclear applications. The extent to which operating experience may be relied upon will vary from country to country; however, this method alone is insufficient to support the qualification of a platform for use in a system important to safety.

26) Platform suppliers may utilise a certification organisation to assess the supplier's development process and product against a particular standard or standards. The certification organisation issues a certificate claiming compliance with that standard or standards. The acceptability of product certificates as a direct means of qualification varies between countries. It is not usually the case that a certificate alone would be considered acceptable as a qualification for the platform.

    a. The evidence generated as a result of a certification exercise should be made available in order to allow confirmation by the platform user and regulatory

body of the acceptability of the certification process itself, as well as the platform product. Such evidence would usually be similar to that generated using the methods described in consensus position 19 onwards. Information concerning the accreditation of the certifying body should be readily available and access should be provided to the certifying body personnel in order to confirm their competency for the activities they have undertaken.

b. Where certification of a platform forms part of its qualification the certificate and evidence supporting it should identify the make, model and version of all components within the scope of that certification. The range of applications and critical characteristics for which the platform has been certified should be explicitly stated.

27) It is recognised that, regardless of the methods employed, sufficient evidence to complete an adequate qualification of an I&C platform may not always be available. In some cases, full access to qualification evidence that does exist will not always be possible due to supplier's intellectual property concerns. In such circumstances the acceptability of the approach taken by the user to accommodate this situation will be a decision for the regulatory body for the country in which the platform is used.

28) Platforms developed for general industrial use will usually contain functions not required for the fulfillment of nuclear safety functions. Depending upon the safety class of the platform it may be necessary to remove such functions or to demonstrate that they do not interfere with the fulfillment of the safety functions. It should be noted that the modification of the platform to remove such functions may lead to unintended consequences and reduce or remove the credit that may be taken for operating experience.

29) Platforms developed for general industrial use will usually include a number of pre-developed software library modules that may be configured by the user to implement their functional requirements as part of the development of their application software. It is often the case that facilities are provided to allow users to define their own application software library functions. In such cases these library functions should be qualified by the user using the methods described in common positions 15 and 16 above. The impact of the addition of these application software library functions to the platform should be considered and demonstrated not to affect the qualification of the platform.

Documentation

30) A report should be produced following completion of the qualification exercise by the qualifying party.

31) As a minimum, the qualification report should clearly identify the following:

a. The make, model and version of all components of the platform (hardware and software, including embedded components) that are considered to be within the scope of the qualification;

b. The range of applications and critical characteristics that the platform has been qualified against;

c. The tools that have been assessed as part of the qualification exercise;

d. The artifacts (e.g. documentation, code, hardware) that were assessed as part of the qualification exercise;

e. Any constraints that the platform qualification imposes on its application (e.g. maximum CPU load or number of I/O to maintain determinism);

f. A justification of the method or combination of methods used for the qualification;

g. A justification of the depth to which analysis of the supply chain has been undertaken.

32) The qualification report itself should be subject to configuration management.

Use of the qualification

33) The safety justification of an I&C system for use in an important to safety application should integrate the qualification of the platform with the justification for the application.

34) The I&C platform may be qualified for use for a specific application or for use in a range of applications (sometimes referred to as generic qualification). In either case the user should demonstrate that they understand the scope of qualification and that the platform is used within the range of applications (envelope) and critical characteristics for which it was qualified.[4]

35) In some cases, a platform may have been previously qualified using standards and practices not recognised within the nuclear sector or in the country in which it is to be used. If credit is to be taken for the previous qualification the user should demonstrate equivalence of the standards and practices used with those applicable in the nuclear sector in the country of use. Any differences should be justified and may warrant further analysis and/or testing.

36) Application-specific testing or analyses may be required to supplement the vendor's tests and build confidence in the platform and its functionality, and/or to examine its response to specific conditions or abnormal events which are not performed in the vendor’s qualification.

37) There may be additional items that were not included as part of the platform qualification. These items should be identified in the qualification documentation and addressed in the applications using the platform. Examples would include architectural and interface requirements.

Maintenance of the qualification

38) The user is responsible for ensuring that the qualification of the platform used in their I&C application represents the current configuration on their plant.

39) The user should ensure that changes in other systems or equipment do not invalidate the qualification of the platform e.g. the introduction of new equipment that invalidates the environmental qualification of the platform (temperature, EMC, etc.).

4. It should be noted that this consensus position does not provide guidance on the qualification of the application and does not remove the requirement for the application to be qualified using the nuclear standards, practices and regulatory framework applicable for the country in which the system is to be used.

40) The user should ensure that changes in the configuration or use of the platform in their application do not invalidate the qualification e.g. increasing the load on the CPUs which then exceeds the limit that maintains determinism.

41) The user and the supplier should have configuration control and change management systems in place to facilitate maintenance of the qualification.

42) The platform supplier should provide a means by which the users may be informed of faults or changes to their products.

43) The user should establish and maintain a process by which any faults or changes reported by the platform supplier are monitored in a timely manner such that the faults or changes may be understood and their impact analysed.

44) In the process of deciding whether to use a platform developed for general industrial use the user should consider the life expectancy of the platform (anticipating obsolescence) and the sustainability of the manufacturer. The user should make arrangements to ensure access to development and qualification records should manufacturer support no longer be available.

45) The user should establish and maintain a process to periodically monitor changes to standards and regulations that may challenge an existing qualification.

Conclusions

While there may be different approaches to the qualification of digital instrumentation and control platforms for use in systems important to safety at nuclear power plants, the WGDIC concludes that the guidance herein represents an effective and technically viable approach. This conclusion is based on the collective scientific and technical knowledge and experience of the WGDIC members that was brought together to develop this consensus position (CP). As such, this CP represents the common understanding from the WGDIC members and harmonisation of regulatory practices related to the qualification of digital instrumentation and control platforms for use in systems important to safety at nuclear power plants.

In support of the continual evolution of digital instrumentation and control technology and its associated challenges, the WGDIC will continue to assess any gaps not being addressed by contemporary regulations and guidance related to the qualification of I&C platforms for use in systems important to safety at nuclear power plants. Future revisions to this CP will allow the bridging of those gaps while ensuring its relevance and technical adequacy.

Any enquiries associated with this CP should be directed to NEA via the WGDIC website.

References

1. IEC 63084 TR (2017) - Nuclear power plants - Instrumentation and control important to safety - Platform qualification for systems important to safety
2. IEC 61508 (2010) - Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1 to 7
3. IEC 61511 (2016) - Functional safety - Safety instrumented systems for the process industry sector – Parts 1 to 3
4. IEC 61226 (2009) - Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
5. IEC 61513 (2011) - Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
6. EPRI (1999), TR-106439 – Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications
7. EPRI (2014) NP 5652 - Guideline for the Acceptance of Commercial Grade Items in Nuclear Safety Related Applications
8. IAEA (2016), SSG-39 - Design of Instrumentation and Control Systems for Nuclear Power Plants
9. CSA (2015), N290.14-15 - Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants
10. MDEP (2012) Generic Common Position DICWG-02 - Common Position On Software Tools For The Development Of Software For Safety Systems
11. MDEP (2012) Generic Common Position DICWG-08 – Common Position on the Impact of Cyber Security Features on Digital I&C Safety Systems
12. TF SCS (2018) Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations
13. IEEE 7-4.3.2 (2016) - Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations
14. IAEA (2016), Safety Glossary - Terminology Used in Nuclear Safety and Radiation Protection