Nuclear Regulation
NEA/CNRA/R(2020)3
August 2023
www.oecd-nea.org

Proceedings of the Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C)

9–13 June 2019
Toronto, Canada

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CNRA/R(2020)3

Unclassified English text only

2 August 2023

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

Proceedings of the Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C)

9-13 June 2019, Toronto, Canada

This document is available in PDF format only.

JT03523944

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, the Czech Republic, 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, the Czech Republic, 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 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) 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

The main purpose of the Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C) was to provide a forum to exchange information on regulatory inspection activities in the field of digital instrumentation and control (DI&C) systems.

Participants had the opportunity to meet with their counterparts from other countries, from other organisations as well as from industry, to discuss current and future issues on the selected topics. They developed conclusions regarding these issues and identified methods that could help improve their own inspection programmes in this area.

The Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) believes that an essential factor in ensuring the safety of nuclear installations is the continued exchange and analysis of technical information and data. To facilitate this exchange, the Committee has established working groups and groups of experts in specialised topics. The Working Group on Inspection Practices (WGIP) was formed in 1990 and its 2018-2020 mandate directs the WGIP to "identify practical methods to help regulatory bodies advance the effectiveness and efficiency of their inspection practices and programmes." The WGIP facilitates the exchange of information and experience related to regulatory safety inspections between CNRA member countries.

The Working Group on Digital Instrumentation and Control (WGDIC) was established under the CNRA in late 2017 and held its first meeting in early 2018. It was formerly established as the Digital Instrumentation and Control Working Group (DICWG) under the Multinational Design Evaluation Programme (MDEP) and then transferred to the CNRA. The main objective of the WGDIC is to promote harmonisation and improvement in nuclear safety through the development of regulatory guidance to address DI&C topics and technical issues of concern to its member countries for operating and new reactors. This regulatory guidance is not intended to replace the guidance already available from international standards organisations; instead, the collective scientific and technical knowledge and experience of WGDIC members is brought together to develop consensus positions representing the common understanding and harmonisation of regulatory practices.

These proceedings cover the special "International Nuclear Regulatory Inspection Workshop" jointly held by the WGIP and WGDIC in Toronto, Canada, from 9-13 June 2019 on DI&C. They were approved by the CNRA at its meeting on 2-3 December 2019 [NEA/SEN/NRA(2019)2].

Participants at previous workshops noted that the value of meeting with people from other inspection organisations was one of the most important achievements. The focus of this workshop was on experience gained from regulatory inspection activities in three areas:

- inspection/treatment of software modifications;
- scope of testing;
- commercial upgrade to allow the use of not initially qualified DI&C.

Members of the workshop organising Committee acknowledged the excellent planning and arrangements made by the staff of the host organisation, the Canadian Nuclear Safety Commission (CNSC). Special recognition was given to the Canadian WGIP vice-chair, Mr Alexandre Leblanc and to the US WGDIC chair, Mr Ismael Garcia, for their essential co- ordination and efforts in the preparation of the workshop.

Special acknowledgement was also given to the WGIP and WGDIC members that facilitated the topic discussion groups: Mr Ismael Garcia (US NRC), Mr Mika Johansson (STUK), Mr Gilbert Chun (CNSC), Mr Louis Dumont (US NRC), Mr Yves Guannel (ASN) and Mr Mikko Heinonen (STUK).

The contribution of the NEA (Mr Luc Chanial, Acting Head of the Nuclear Safety Technology and Regulation Division, and WGIP Technical Secretariat, Mr Thomas Buckenmeyer, WGDIC Technical Secretariat, Mr Terumasa Niioka, Technical Secretariat, and Ms Akane Schmitz-Fraysse, Assistant) was also highlighted.

Table of contents

List of abbreviations and acronyms

ASN	Autorité de sûreté nucléaire (France)
BMU	Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (Germany)
CA	Corrective actions
CAP	Corrective action programme
CCF	Common cause failure
CNRA	Committee on Nuclear Regulatory Activities (NEA)
CNSC	Canadian Nuclear Safety Commission
CSNI	Committee on the Safety of Nuclear Installations (NEA)
CORDEL	Co-operation in reactor design evaluation and licensing
COTS	Commercial-off-the-shelf
CP	Commendable practices
DI&C	Digital instrumentation and control
DICWG	Digital Instrumentation and Control Working Group (NEA)
EDD	Embedded digital devices
EMI	Electromagnetic interference
FAT	Factory acceptance testing
FMEA	Failure mode and effects analysis
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS)
HTO	Human-Technology-Organisation
I&C	Instrumentation and control
IAEA	International Atomic Energy Agency
LOCA	Loss-of-coolant accident
MDEP	Multinational Design Evaluation Programme
NCSFI	Non-conforming, counterfeit, fraudulent and suspect items
NEA	Nuclear Energy Agency
OPEX	Operating experience
PSR	Periodic safety review
QA	Quality assurance
RB	Regulatory body

RWMC	Radioactive Waste Management Committee (NEA)
SAT	Site acceptance testing
SIL	Safety integrity level
SME	Subject matter expert
SMR	Small modular reactor
SPDS	Safety parameter display system
SSC	Systems, structures and components
STUK	Radiation and Nuclear Safety Authority (Finland)
TSO	Technical support organisation
US NRC	United States Nuclear Regulatory Commission
V&V	Validation and verification
WGDIC	Working Group on Digital Instrumentation and Control (NEA)
WGIP	Working Group on Inspection Practices (NEA)
WNA	World Nuclear Association

Executive summary

The main objectives of the Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C), which was jointly held by the Nuclear Energy Agency's (NEA) Working Group on Inspection Practices (WGIP) and the Working Group on Digital Instrumentation and Control (WGDIC), were to enable inspectors and experts in digital instrumentation and control systems from different organisations to exchange information and experience regarding regulatory inspection practices on DI&C, discuss inspection issues, and develop conclusions and commendable practices (CPs). These CPs are applicable to DI&C systems in operating reactors as well as new reactors and can help verify they are designed, installed, tested, operated and maintained in accordance with the regulatory requirements, manufacturer's design, operating recommendations and facility's licensing bases.

This special workshop focused on the three following topics:

- inspection/treatment of software modifications;
- scope of testing;
- commercial upgrade to allow the use of not initially qualified DI&C.

These topics were selected following discussions between the two working groups and after consideration of the results of a survey sent to member countries.

As part of the registration, participants were asked to respond to a questionnaire about practices in their countries on the three topics. The complete compilation of questionnaire responses is contained in the annex of this document.

Fifty participants from 14 countries took part in the workshop: Canada, the Czech Republic, Finland, France, Germany, Japan, Korea, the Netherlands, Poland, Slovenia, Spain, Sweden, the United Kingdom and the United States. Approximatively ten experts from the nuclear industry (operators and licensees) as well as from other sectors (e.g. Canadian Space Agency) contributed to the discussions.

Six discussion groups were established for the break-out sessions. Each group consisted of inspectors and DI&C experts from different countries and organisations to ensure diversity of views for each of the topics. Discussion groups met for three separate sessions on one topic. The exchange between participants was open and active, and the groups formulated conclusions and identified CPs.

Evaluation of the workshop was based on questionnaire responses received from the participants at the closing of the workshop. The evaluation showed that, as in past workshops, one of the highest values perceived was in meeting and exchanging information among participants from different organisations. Responses also showed that the format selected was highly effective, and participants mentioned the benefit of holding a joint workshop between two key Committee on Nuclear Regulatory Activities (CNRA) working groups.

The results of the evaluation also reflected that participants, in exchanging information, were provided a unique opportunity to "calibrate" their own inspection methods against

those from other countries. While exchanging inspection practices and learning new ideas were part of the main objectives, the opportunity to recognise and understand commonalities and differences was equally important.

Overall, participants held extensive and meaningful discussions, both in discussion group sessions and throughout the workshop. They exchanged ideas and practices regarding regulatory inspection activities on DI&C that will provide improved expertise when applied in the future.

The workshop conclusions for each topic included observations and CPs that were developed by the discussion groups. CPs are neither international standards nor guidelines. Each country should consider its historical, social and cultural background when determining its inspection practices on DI&C; the CPs can be a useful reference when a country improves those inspection practices on DI&C. Various and complementary points of view were expressed and the following key messages were identified:

- In the field of inspection/treatment of software modifications, the workshop highlighted that:
  - Software modification is not limited to source code modification. Participants exchanged their experiences concerning the high-level requirements on the software modification, e.g. quality assurance, DI&C system requirements. Participants agreed that all the relevant disciplines should participate in the modification of software.
  - The categorisation of software is an important factor for inspection by the regulatory body (RB) inspectors. There were minor differences in the inspection practices among RBs. Participants exchanged their experiences on the software inspection plan including verification approach, qualification and documentation.
  - The configuration management practices, procedures and outcomes are important factors for inspection by the RBs. Participants exchanged their experiences on configuration management, including the differences in the inspection practices among the RBs.
- In the field of scope of testing, the workshop highlighted:
  - The benefit of the RB witnessing a test for either software or hardware, rather than simply reviewing the test results, as well as the need for inspection guidance as some of the RBs do not have guidance available for performing DI&C inspections.
  - The minimum expertise or qualifications required for the RB personnel performing the inspections. Some of the RBs may only have one subject matter expert (SME) on DI&C inspections and may be at risk of losing that expertise pending departure of that SME from the organisation.
  - The benefit of having a technical support organisation or similar participate in the equipment testing inspections. Some of the RBs rely on a combination of a chief inspector from the RB and contractor support.
- In the area of commercial upgrades to allow the use of not initially qualified DI&C (i.e. commercial-grade dedication), the workshop highlighted that:
  - Licensees are willing to use commercial-off-the-shelf (COTS) products because of availability, many of which have embedded software or

firmware. This may cause challenges when analysing failure behaviour or cyber security aspects of the product.

- RBs should make sure that licensees have necessary competence and processes to analyse the suitability of these products.
- RBs should have policies on how to review these products and how to treat existing product certificates that do not comply with nuclear standards.

1. Organisation and overview of the workshop

1.1. Planning

Following the approval in December 2017 by the Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) to organise a Special International Nuclear Regulatory Inspection Workshop on Digital Instrumentation & Control (DI&C), the Working Group on Inspection Practices (WGIP) and Working Group on Digital Instrumentation and Control (WGDIC) worked together to establish the framework and content of this joint event.

The workshop was hosted in Toronto on 9-13 June 2019 by the Canadian Nuclear Safety Commission (CNSC).

Six potential topics were initially identified and three were selected according to the results of the survey included in the questionnaire sent to WGIP and WGDIC members. These three topics were presented at the December 2018 CNRA meeting. The Workshop Organising Committee further defined the issues to be discussed under each of them.

The responses to the questionnaire were used to prepare the opening topic presentations and the background material to conduct group discussions.

As part of registration, each participant selected their preferred topic for discussion.

In the plenary opening session, the three topic leads provided their preliminary analyses of the questionnaire responses. Subsequently, the participants were divided into six groups of seven to nine participants to discuss the topics in detail.

In the plenary closing session, the leads presented the results of the discussions and CPs that were derived so that workshop participants could benefit from the other topics.

The workshop announcement was transmitted mid-February 2019.

1.2. Overview of workshop

Leads and co-leads pre-meeting

Prior to the workshop, the organising Committee met to discuss and confirm the final organisational details.

Mr Alexandre Leblanc (CNSC), WGIP vice-chair, reminded the topic leads and co-leads of the general objectives of the workshop. He reviewed the document “Guidance on developing and approving commendable practices”, as approved by the CNRA on 1 July 2018, emphasising not to leave out a good practice even if it did not meet the guidance criteria; such practices could be considered as observations. Moreover, he suggested not to exclude proposals from industry representatives.

He noted the importance of the facilitator’s role in opening and leading discussions, guiding the group and continually monitoring to ensure full participation of the group members. He also reminded the organising Committee of various methods to manage an effective discussion and to promote active participation.

Instructions were given that the sub-groups for each topic must interact during the workshop. This would provide an opportunity to compare results.

Mr Leblanc also said that there were no objectives regarding the number of CPs. Participants were encouraged to focus on quality rather than quantity.

Meet-and-greet session

On the Sunday evening before the workshop, a reception was held to allow participants to meet in an informal setting.

This informal session was intended to create a good atmosphere between all participants and to make everyone feel comfortable in the next steps of the workshop.

Opening session

Mr Leblanc welcomed the participants to the workshop. He then introduced and gave the floor to Mr Luc Chanial (NEA), acting Head of the Nuclear Safety and Technology Division at the NEA.

Mr Chanial gave a brief overview of the NEA, including its main objectives and activities. Concerning the membership of the NEA, he highlighted the developing relationships with India and the People's Republic of China (hereafter "China"). He then described the CNRA, providing information on its role in the field of nuclear safety and giving details on the bodies within the Committee.

He explained the main reasons that led to a joint workshop between the WGIP and WGDIC, and emphasised the participation of industry in addition to 14 countries.

He thanked all the people involved in the organisation of the workshop. In conclusion, he encouraged participants to take part actively in the discussions during the three days.

Mr Gerry Frappier, Director General of the Directorate of Power Reactor Regulation, Canadian Nuclear Safety Commission (CNSC), welcomed the participants to Canada. He gave an overview of the CNSC's activities and structure, as well as a historical perspective that shaped the safety philosophy behind the CNSC. He spoke about the context of nuclear safety in Canada, the importance of international co-operation to enhance nuclear safety worldwide, the current nuclear reactors in Canada and the development of SMRs.

Regarding the field of DI&C, he identified some of the current opportunities and key challenges for the future, such as cyber security.

Mr Leblanc then took the floor. He described the WGIP mandate and some of the activities, such as reports and workshops. He highlighted that this workshop was unique in the sense that it was jointly organised with the WGDIC and that industry was invited.

He gave the floor to Mr Ismael Garcia (US NRC), chair of the WGDIC, who provided a brief overview of the WGDIC's past and recent activities. He noted that the WGDIC is focused on developing consensus positions representing the common understanding and harmonisation of regulatory practices.

Mr Leblanc then detailed the goals of the workshop, with a focus on the development of commendable practices. He introduced the leads and co-leads of the discussions, and explained what was expected from the participants for a successful workshop.

Topic leads presentations

Topic leads were invited to provide a presentation on their topic. The presentations focused on the importance of each topic and gave some thoughts and ideas to initiate group discussions:

- Mr Gilbert Chun (CNSC) presented topic one: “Inspection/treatment of software modifications”.
- Mr Ismael Garcia (US NRC) presented topic two: “Scope of testing”.
- Mr Mika Johanson (STUK) presented topic three: “Commercial upgrade to allow the use of not initially qualified DI&C (i.e. commercial-grade dedication)”.

Group discussion sessions

Participants were divided into six discussion groups, based on their preference given at registration.

Three half-day sessions were held. A facilitator and recorder worked with each group to stimulate and encourage discussions. For each of the three topics, two discussion groups were formed. The facilitators co-ordinated their discussion groups to give the participants sufficient time to express their views as well as to discuss the views with one other.

Host country presentations

This session was dedicated to various presentations from industry.

Ms Sara-Kristin Doherty, project manager at Ontario Power Generation, gave a presentation on the turbine and excitation controls upgrade project at the Darlington Nuclear Generating Station.

She started by giving an overview of the project status. She then detailed the different I&C systems upgraded for this project, mentioning that the analogue control system of the turbine control, including the turbine supervisory system, various protection components and relays, the main steam control valve electronic hydraulic converters and the servo-motors, had been entirely replaced, as well as the protection, the field breaker and the power components of the generator excitation.

She also explained how the CNSC performed inspections during the upgrade process and concluded by providing information on the main challenges generated by the upgrade and the way they were addressed.

Mr Mike Fairweather, certified training superintendent of the Point Lepreau Nuclear Generating Station, delivered a presentation on the practical application of digital inputs and controls for post transient review. He gave an overview of the Point Lepreau Nuclear Generating Station and proceeded to present the details of an I&C event that occurred as the nuclear power plant was coming out of refurbishment. On 30 October 2012, the turbine speed increased and then went through soft shutdown. The investigation conducted by the licensee concluded that the main reason for this event was the unit of measurement used to calibrate the main steam transmitters was incorrect (kPa instead of psi).

He concluded his presentation by talking about the challenges and benefits of digital circuits.

Mr Tom Rubenstein executive director of the Vogtle project of Westinghouse, provided an audio report on the situation of the AP1000 in China. He also discussed passive core cooling operations, including the role of DI&C during a LOCA, by using an illustrative animation.

He emphasised the need for DI&C, including future designs and the addition of a self-diagnosis function.

Mr Garry Johnson, from CORDEL, gave a video presentation on the safety parameter display system implementation (SPDS) as he could not attend in person. He reminded

participants that this system was required by the US NRC after the Three Mile Island accident to help control room operators make quick assessments of a nuclear power plant's safety status.

Mr Johnson provided a global overview of the development of the SPDS. He then detailed how the NRC and the licensee interacted to assess this system.

In conclusion, he listed some causes that could explain why the SPDS development was a challenge and provided some lessons learnt.

Closing presentation of topics

The topic leads made a closing presentation on each of the workshop topics. They presented a set of commendable practices developed by the discussion groups. Each presentation was followed by general questions and comments from the audience.

The workshop participants outlined and discussed CPs related to the various topics and viewed them as references for member countries. They are neither international standards nor guidelines. Each country should determine its inspection practices on DI&C while taking into account its own historical, social and cultural background. The CPs can serve as a useful reference when a country improves its inspection practices on DI&C.

Closing remarks

Mr Leblanc provided remarks on the success of the discussions.

He noted that, as in other WGIP workshops, there had been open and frank exchanges during the group discussions. He also noted that many participants had taken advantage of the scheduled informal sessions to further bilateral exchanges.

In conclusion, Mr Chanial noted the value of joint workshops, gathering complementary experience and developing competencies around key topics. He considered the discussions fruitful and valuable. He encouraged each participant to review the CPs identified at the workshop and to consider how they could be implemented in their inspection practices. He also highlighted the benefit of having the industry involved in the discussions.

Discussions on the workshop topics have shown that:

- These workshops continue to provide a unique environment for participants to exchange information on current issues, to gain insights, and to validate their own processes.
- The topics were well developed and the participants were well prepared and made important contributions.
- The development of CPs and of new challenges to be faced was successful and participants and their national organisations should benefit from the insights gained.

In closing, Mr Leblanc thanked Mr Luc Chanial, Mr Thomas Buckenmeyer and Mr Terry Niioka (NEA Technical Secretariats) for their reliable and valuable support. He highlighted the key role of Ms Cynthia Bechara (CNSC Administrative Assistant) in organising the workshop.

Mr Leblanc concluded by thanking all the workshop participants, facilitators and recorders, noting that without their contributions, hard work, and dedication the event would not have been a success.

Technical visit

As a bonus, the participants were offered a technical visit of the Darlington Nuclear Generating Station on 13 June 2019.

The visit focused on the following point of interests:

- the full-scale nuclear reactor mock-up;
- the innovative accelerator X-Lab;
- the Darlington maintenance and computing development facility.

Staff members of the nuclear power plant provided an introduction and acted as guides, providing a comprehensive and interesting tour of the nuclear power plant.

2. Topic A: Inspection/treatment of software modifications

2.1. Topic introduction

The topic of inspection/treatment of software modifications addressed two areas: "Modifications and Maintenance of Software" and "Configuration Management."

The modification and maintenance of software generally take place in response to a need for improved performance and/or a modified environment. To ensure that the modification and maintenance of software is correct, the regulatory body may perform an inspection of the licensee processes and the outcomes of the processes.

Configuration management is an essential part of quality management. Through configuration management inspection, regulatory bodies verify that modified software/hardware versions meet applicable regulations and/or standards.

The purpose of this task was to identify commendable inspection practices and to share information on methods, procedures and criteria used by a regulatory body.

2.2. Discussion group members

Group 1	Group 2
CHUN Gilbert, Canada‡ (Topic lead)	DUMONT Louis, United States (Topic lead)
NGUYEN Duc, Canada	CAZALET Cécile, France
JAKES Miroslav, Czech Republic*	KIM Hyungtae, Korea‡
KASAGAWA Yusuke, Japan*	GLOWACKI Andrzej, Poland*
HUH Chang Wook, Korea*	FAIRWEATHER Michael, Canada
MCDONALD Kulvinder, United Kingdom*	YAGUE Jorge, Spain
GALLETTI Greg, United States	DESGAGNE Eric, Canada
DEMMONS Scott, Canada	

*WGIP members ‡WGDIC members

2.3. Pre-workshop questionnaire

Ahead of the workshop, participants were invited to supply their national inspection approaches according to the questionnaire contained in the addendum (NEA/CNRA/R(2018)6/ADD1).

2.4. Opening presentation

To provide the two groups with a common basis to discuss the topic, Mr Chun made a presentation summarising the different responses that he had received to the pre-workshop questionnaire.

Eighteen countries and industry participants (via the World Nuclear Association's [WNA's] Cooperation in Reactor Design Evaluation and Licensing [CORDEL]) provided responses to the pre-workshop questionnaire and a review of the answers provided the following observations:

- Regulatory bodies (RBs) in most countries use the modification and maintenance procedure of software to inspect the licensee processes and outcomes of processes. In a few countries, the RBs focus on the testing of software after modification.
- Regulatory bodies in most countries use a configuration management plan or a software configuration management plan. In addition to the configuration management plan, the RBs in a few countries review the suitability report and source code.
- Regulatory bodies in most countries use the same criteria in the configuration management plan as for software and hardware modification. When there is a significant hardware modification, additional evaluations such as electromagnetic interference/radio frequency interference and seismic qualification are required.

2.5. Group discussion summary

The group discussions were carried out in two sub-groups, which noted the following points:

- They use the same criteria for commendable practices, i.e. safety significance, adoption by several RBs, level of innovation, relevance as a tool to harmonise/improve inspection practices and facilitate the work of RBs.
- They use the same sub-group roundtable questions to minimise significant deviation from the topic.
- In two areas, software inspection plan and configuration management, the two groups discussed different levels of detail. For example, one group focused on a risk-informed inspection plan, while the other group focused on the attributes of the inspection plan.

Throughout the discussions, the exchange of experience and practices among participants was very informative. The sub-groups met on a few occasions to discuss the results of each group. Generally, the sub-groups shared similar opinions and the participants agreed with the results of each group.

In addition to identifying some commendable practices, ideas of how to implement them were also discussed and can be found in the closing presentation as well as the section below.

2.6. Conclusions and closing presentation

The following CPs emerged from discussions during the workshop. It is important to note that these CPs are based on workshop discussions and do not reflect a consensus NEA

opinion. Nevertheless, they can be used as a benchmark for basic comparisons of the issues shared by inspectors of participating countries.

Although the discussions in the two sub-groups were different (reflecting the individual experiences of the participants and different emphasis on aspects of the workshop topics), both groups agreed on the CPs, as well as the justification for each, during a joint group meeting before the closing presentation by Mr Chun (see complete presentation in Annex G).

CPs for how to inspect software modifications are listed below; some sub-bullets provide guidance on how to implement the proposed CP.

CP 1: The RB should conduct software modification inspections utilising a multidisciplinary approach involving subject matter experts in quality assurance (QA) and digital instrumentation and control (DI&C).

The discussion group determined this was a CP based on two points. First was the improvement in the overall inspection process effectiveness resulting from simultaneously leveraging the expertise of subject matter experts in QA and DI&C during the inspection. Second was the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices," version one:

- Inadequate inspection of software modification by a single discipline can lead to safety significant consequences (criterion one).
- A multidisciplinary approach to conducting inspections has been adopted by several RBs (criterion two).
- Inspection by multi-disciplines minimises the potential oversight in software modification, including interface areas. It is a comprehensive and innovative inspection approach when compared to the traditional focused inspection approach which is rooted in a single subject area (criterion three).
- Many RBs have an inspection practice that follows a multidisciplinary approach. Considering that some RBs do not follow such an approach, sharing and adopting another country's inspection practice through the international I&C workshop would help promote harmonisation (criterion four).
- It will facilitate the work of the RB as the proposed multidisciplinary approach makes it possible to fulfil any potential knowledge gaps resulting from the execution of the inspection (criterion five).

CP 2: The RB should consider adopting a risk-informed sampling approach for software modification inspections, utilising safety and risk analysis, which should focus on the most safety-significant aspects of the modification.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- Risk-informed sampling ensures a focus on the most safety-significant aspects of the software modification (criterion one).
- A risk-informed sampling approach has been adopted by several RBs (criterion two).
- While there are different sampling approaches for software modification inspections, the discussion group reached a common understanding and consensus

on not excluding the risk-informed sampling approach from these approaches (criterion five).

CP 3: The RB should determine the safety classification of the software being modified and develop a risk-informed inspection plan that focuses on the modification process and outcomes (e.g. design change process, testing, regression analysis, requirements).

In particular, the inspection plan should verify that:

- Changes have been tested following software modifications in accordance with processes and procedures:
    a) The person that performs the test and the reviewer are both qualified.
    b) The person that performs the test is independent from the reviewer.
    c) Maintenance and testing equipment are validated in accordance with committed standards.
    d) The scope of testing is clearly identified and in line with the impact of the modification.

- Software changes are traceable and documented based on the design modification process. Configuration management of contractors, subcontractors, and licensees should be considered because of the importance of safety requirements, process adherence, access control established for configuration protection (e.g. users log in or log out), and quality assurance.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- A technically adequate inspection plan can be developed by factoring in safety classification, which is fundamental to safety significance and consequences (criterion one).
- Safety classification of target software has been adopted by several RBs (criterion two).
- The discussion group recognised and reached a common understanding on the importance and necessity of safety classification for the software being modified. Specifically, if there is no safety classification on the target software, then the highest safety classification should be assumed for the inspection, which would be contrary to a risk-informed approach (criterion five).

CP 4: It is important for the RB to inspect a licensee's software and hardware configuration management practices, procedures and outcomes to verify adequate version control for systems and components important to safety.

For example, the inspector should verify that configuration management is established, implemented and documented for software changes in accordance with the licensee process by reviewing the following:

- logs of configuration changes made, the purpose of the changes and observations made during the changes;
- defined test acceptance criteria;
- post-maintenance testing validation that changes are implemented correctly;
- verification and validation measures;

- established level of approving authority;
- sharing of lessons learnt and OPEX (Operating Experience);
- documented procedure(s) to ensure that only approved software is installed.

The discussion group determined this was a CP based on the rationale below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- Inadequate safety system configuration management practices can lead to safety significant consequences due to a lack of version control. An inadequate or wrong version of hardware/software could be installed in systems and components important to safety and potentially result in unexpected outcomes (criterion one).
- Verification of version control of both software and hardware has been adopted by several RBs (criterion two).
- The discussion group recognised and reached a common understanding on the importance of version control for hardware and software. Specifically, an inadequate or wrong hardware/software version could be installed in systems and components important to safety after the modification process has been completed (e.g. old software, programmable read-only memory could be installed in the computer instead of the newer, modified version) which could result in an unexpected outcome (criterion five).

3. Topic B: Scope of testing

3.1. Topic introduction

This topic was originally intended to address two areas from the pre-workshop questionnaire: equipment qualification and communication systems.

The process of testing digital instrumentation and control (DI&C) systems/components during equipment qualification makes it possible to verify that they meet the specified requirements. A regulatory body (RB) should have confidence that the scope of a licensee (or vendor) testing programme is effective; as such, inspectors could benefit from gaining insight regarding hardware and software testing.

DI&C architectures may employ data communications between safety systems, between redundant portions of a safety system, and between systems of different safety classes. One of the more significant regulatory implications is maintaining not only physical and electrical independence but also data communication independence, thereby ensuring that faults from data communications do not propagate and adversely affect safety functions.

The purpose of the task was to identify commendable inspection practices and share information about methods, procedures and criteria used to inspect licensee and/or vendor test programmes and communication systems.

3.2. Discussion group members

Group 3	Group 4
GARCIA Ismael, United States‡ (Topic leader)	GUANNEL Yves, France* (Topic Leader)
DULNY Karol, Poland	NEKUŽA Miloš, Czech Republic‡
KHAN Mahtab, United Kingdom	DURKOSH Donald, United States
STRATMANN Simone, Germany*	ZENG Charles, Canada
GORDON Tyra, Canada	SAVLI Sebastjan, Slovenia*
KATAOKA Kazuyoshi, Japan	SCHREURS Erik, Netherlands‡
MULLIN Daniel Richard, Canada	

*WGIP members ‡WGDIC members

3.3. Pre-workshop questionnaire

Ahead of the workshop, participants were invited to supply their national inspection approaches used according to the questionnaire contained in the addendum (NEA/CNRA/R(2018)6/ADD1).

3.4. Opening presentation

To provide the two discussion groups with a common basis for discussing the topic, Mr Ismael Garcia made a presentation summarising the different responses that he had received to the pre-workshop questionnaire.

Eighteen countries and industry organisations (via the World Nuclear Association's [WNA's] Cooperation in Reactor Design Evaluation and Licensing [CORDEL] working group) provided responses to the pre-workshop questionnaire and a review of the answers provided the following insights:

- For all countries, licensees (or vendors) qualify DI&C systems via analysis and/or testing techniques in compliance with approved standards. For some countries, the RB inspects and witnesses some testing while for others the RB simply assesses the test results.
- For some countries, the RB has criteria to review, accept, and inspect DI&C systems communications while for others that is not the case.

These observations were key starting points for the group discussions.

3.5. Group discussion summary

Due to time constraints during the workshop, only the topic of equipment qualification was discussed by the two groups. The discussions during the workshop included, but were not limited to, equipment qualification (e.g. electromagnetic, environmental, and seismic) of DI&C including how to inspect the licensee's (or vendor's) processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified. The group discussions were carried out in two sub-groups and identified the following areas for in-depth discussion:

- The benefit of the RB witnessing a test (for either software or hardware) rather than simply reviewing the test results:
  - Should there be guidance concerning the specific tests (e.g. seismic) the RB should inspect/witness? If so, what should this guidance contain? Some of the workshop attendees indicated that their corresponding RB did not have guidance available for performing DI&C inspections.
  - The minimum expertise or qualifications required for the RB personnel performing the inspections. Some of the workshop attendees indicated that their corresponding RB only had one subject matter expert (SME) on DI&C inspections and were therefore at risk of losing that expertise pending departure of that SME.

- The technical support organisation (TSO) involvement during equipment testing inspections was discussed. Some of the workshop attendees indicated that their corresponding RB relies on a combination of a chief inspector from the RB and contractor support.

Throughout the discussions, the exchange of experience and practices among participants was informative. The sub-groups met on a few occasions to discuss the results of each group. Generally, the sub-groups shared similar opinions and the participants agreed with the results of each group.

In addition to identifying some commendable practices, ideas of how to implement them were also discussed and can be found in the closing presentation as well as the section below.

3.6. Conclusions and closing presentation

The commendable practices (CPs) listed below emerged from discussions during the workshop. It is important to note that these CPs are based on workshop discussions and do not reflect a consensus NEA opinion. Nevertheless, they can be used as a benchmark for basic comparisons of issues shared by inspectors from participating countries.

Although the discussions in the two sub-groups were different (reflecting the individual experiences of the participants and the different emphasis placed on aspects of the workshop topic within the groups), both groups agreed on the CPs, as well as the justification for each, during a joint group meeting held before the closing presentation given by Mr Ismael Garcia (see complete presentation in Annex H).

CPs for how to inspect testing of DI&C systems/components are listed below; the sub-bullets provide guidance on how to implement the proposed CP.

CP 1: The RB should maintain a regulatory surveillance and oversight programme to verify that post-commission DI&C software and hardware upgrades are performed in accordance with the associated requirements and standards. The regulatory surveillance and oversight programme should verify that the licensee has an acceptable process in place for items such as:

- assessing the impact to the relevant SSCs resulting from DI&C system/component configuration changes or upgrades (either hardware or software);
- implementing a software and hardware maintenance plan for the DI&C equipment life cycle including spare parts management and update strategies; and,
- reviewing the quality management programme for new suppliers.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- It allows verification that post-commission DI&C software and hardware upgrades do not negatively impact safety or performance (criterion one).
- Verifying that the licensee has such a programme in place for post-commission DI&C software and hardware upgrades is a practice common to several RBs (criterion two).
- Considering that some RBs do not follow such a practice, improving the inspection practices as discussed herein would help promote harmonisation (criterion four).

CP 2: The RB should provide guidance for on-site inspections of DI&C systems/components that have nuclear safety significance to facilitate more effective and efficient inspections. The guidance should address aspects arising from the DI&C systems/components such as software/hardware configuration management and any lessons learnt from other RBs and other industries that employ safety-critical DI&C systems/components.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on

Developing and Approving Commendable Practices", version one:

- It allows/helps the RB to verify compliance of DI&C systems/components that have been implemented at nuclear power plants with the associated requirements and standards (criterion one).
- Providing guidance for on-site inspections of DI&C systems/components is a practice common to several RBs (criterion two).
- Considering that some RBs do not follow such a practice, improving the inspection practices as discussed herein would help promote harmonisation (criterion four); and,
- It will facilitate the work of RBs because it would result in more effective and efficient inspections (criterion five).

CP 3: The RB should develop an upfront scope of the assessment for licensee/vendor proposals or applications that is commensurate with the safety significance of the DI&C systems/components being assessed. The scope of the assessment should be communicated upfront to the licensee/vendor and should define the hardware- and software-related testing activities to be either inspected or observed by the RB.

The discussion groups identified several examples of hardware- and software-related testing activities to be either inspected or observed by the RB. These may include, but are not limited to:

- review software testing plan/strategy that should include known software vulnerabilities and resolution plans;
- review software development process including a vendor corrective action programme;
- review the Integrated Validation and Verification (V&V) summary report and any remaining unresolved items;
- review the software configuration management plan;
- review design information such as Failure Mode and Effects Analysis (FMEA) and the architecture diagrams;
- review the equipment qualification testing report;
- review specific tests such as:
  - central processor loading and duty-cycle;
  - loss of power/start-up;
  - cable connection (e.g. ageing effects);
  - removal of redundant components from service;
  - diagnostic testing/ fault testing;
  - cyber security feature testing.
- review the equipment receipt and storage plan (e.g. verify identification of hardware and software).

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- It allows the RB to fulfil its mandate of providing independent, efficient, and effective oversight while focusing resources on the safety significant aspects arising from the DI&C systems/components design being assessed (criterion one).
- Developing and providing an upfront scope of the assessment for licensee/vendor proposals or applications is a practice common to several RBs (criterion two).
- Considering that some RBs do not follow such a practice, improving the inspection practices as discussed herein would help promote harmonisation (criterion four).
- It will facilitate the work of RBs because it allows focusing resources on the safety significant aspects arising from the DI&C systems/components design being assessed (criterion five).

CP 4: The RB should maintain the regulatory capability (staff and expertise) to provide adequate surveillance and oversight to verify that the requirements and standards associated with the DI&C system/components are being met.

The discussion groups identified several examples of how a RB could develop the required expertise in the field of DI&C inspections. These may include, but are not limited to:

- participating in DI&C inspections being performed by other RBs;
- participating in industry and/or RB conferences;
- on-the-job learning with a technical support organisation (TSO) and/or subject matter expert (SME) with expertise that may include, but not limited to:
  - hands-on experience with DI&C testing;
  - recent DI&C inspection experience;
  - design experience for DI&C compliance with codes and standards.
- on a project-specific basis, using available vendor overview presentations;
- if the DI&C system/component has already been implemented in another country or used in another industry, the RB should access all feedback information such as uses, applications, critical characteristics and lessons learnt. To that extent, the RB should consider developing a memorandum of understanding or similar with other RBs and/or industries;
- maintaining the required regulatory capability could be done via SMEs within the RB or via external consultants (e.g. TSOs, other RB, other industry) with defined expertise;
- maintaining the required regulatory capability is particularly important since the application of this technology is rapidly evolving compared to other SSCs.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- It allows the RB to fulfil its mandate of providing independent and effective oversight and verifying safe construction and operation of nuclear power plants (criterion one).

- Maintaining such a regulatory capability is a practice common to several RBs (criterion two).
- Considering that some RBs do not follow such a practice, improving the inspection practices as discussed herein would help promote harmonisation (criterion four).

4. Topic C: Commercial upgrade to allow the use of not initially qualified DI&C

4.1. Topic introduction

Topics for this group were refocused when the pre-workshop questionnaire was analysed. It was agreed that topics "Use of Commercial Grade DI&C systems/components" and "Embedded Digital Devices" (EDDs) have so much in common that it was most efficient to discuss these topics together.

Licensees are willing to use commercial-off-the-shelf (COTS) products because they are often readily available and moderately priced. Nowadays many of these products include embedded software or firmware. Sometimes, when the product supplier assembles the product from pre-developed components, they may not be aware that some components have software inside.

Software-based products require new types of competence and skills when analysing failure behaviour of the component or cyber security aspects. In addition, in plant level design, the specific aspects of embedded digital devices must be considered, especially in plant modifications when new and old technology are mixed.

New competences and processes are required in the licensee's organisation as well as in the regulatory body.

The purpose of the task was to identify commendable inspection practices and share information related to abovementioned challenges.

4.2. Discussion group members

Group 5	Group 6
JOHANSSON Mika, Finland‡ (Topic lead)	HEINONEN Mikko, Finland* (Topic lead)
MCLEAN Kyle, Canada	BURTA John, Canada
SCHNEIDER Matthias, Germany*	EL_GHALBZOURI Redouane, France
BOOH In Hyoung, Korea	WATANABE Nobumichi, Japan‡
GALINDO RODRÍGUEZ José, Spain‡	HELLMICH Mario, Germany
HELLBERG Henrik, Sweden	WARDLE Stephen, United Kingdom‡
MCKAY Kevin, Canada	KELLEY Sean, United States
MANNING Lisa, United States	DESBIENS Patrick, Canada
FOURNIER David, Canada	HARBER John, Canada

*WGIP members ‡WGDIC members

4.3. Pre-workshop questionnaire

For preparation of the workshop, participants were invited to supply their national inspection approaches used according to the questionnaire contained in the addendum (NEA/CNRA/R(2018)6/ADD1).

4.4. Opening presentation

To provide the two discussion groups with a common basis for discussing the topic, Mr Johansson made a presentation summarising the different responses that he had received to the pre-workshop questionnaire.

Twelve countries provided responses to the pre-workshop questionnaire and a review of the answers provided the following observations:

- All countries have an approach for qualifying COTS products, either using a formal commercial-grade dedication process, or using the qualification process used for nuclear grade products.
- Inspections of COTS manufacturers are rarely performed.
- Embedded digital devices are used in almost all countries, mainly to replace old or obsolete components.

In addition to the questionnaire, Mr Johansson had collected several specific challenges based on STUK's experience. These included treatment of SIL (IEC 61508) certificates and other third party qualification documentation and having access to the source code of product.

4.5. Group discussion summary

The group discussions were carried out in two sub-groups and identified the following areas for in-depth discussion:

- Treatment of SIL certificates, or SIL analyses, and whether these should be given by an accredited body (meaning that national accreditation service has accredited the company based on ISO/IEC 170xx standards) or any company.
- The SIL capability level versus national safety classification, since it was known that approaches in each country vary.
- Inspection of COTS products and, if the inspections are done, which life cycle phase is appropriate to get good evidence of the quality of the product.
- The plant level design, or allocation of EDDs.
- Licensee personnel competence on COTS products.
- Licensee processes to prevent inadvertent introduction of equipment utilising software or firmware into the nuclear power plant.
- Identification of critical characteristics of COTS products.
- Access to manufacturing data of COTS products.

The group wanted to discuss also some technical topics, but since they were not inspection practices, these were left out.

The exchange of experience and practices among participants was informative. The sub-groups met on a few occasions to discuss the results of each group. Generally, the sub-groups shared similar opinions and the participants agreed with the results of each group.

In addition to identifying some commendable practices, ideas of how to implement them were also discussed and can be found in the closing presentation as well as the section below.

4.6. Conclusions and closing presentation

The following CPs emerged from discussions during the workshop. It is important to note that these CPs are based on workshop discussions and do not reflect a consensus NEA opinion. Nevertheless, they can be utilised as a benchmark for basic comparisons of issues shared by inspectors from participating countries.

Although the discussions in the two discussion sub-groups were different (reflecting the individual experiences of the participants and the different emphasis on aspects of the workshop topic within the groups), both groups agreed on the CPs, as well as the justification for each, during a joint group meeting held before the closing presentation by Mr Johansson (see complete presentation in Annex I).

CPs for how to inspect commercial upgrade are listed below; the sub-bullets provide guidance on how to implement the proposed CPs.

CP 1: The RB should verify that the licensee has sufficient organisational competence to determine the acceptability of commercial equipment and components utilising software or firmware.

The verification process by the RB should include, but not be limited to:

- review of the licensee's reports and reviews on commercial upgrade;
- confirm the licensee's process for establishing and maintaining training and qualification of employees;
- confirm the licensee's procedures are robust enough to drive good work.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- The RB must have confidence that system reliability is maintained over time and that the licensee periodically demonstrates that devices are able to perform their intended functions (criterion one); and,
- Several RBs have requirements that licensees maintain organisational competencies, including in the area of commercial products that utilise software or firmware (criterion two).

CP 2: The RB should confirm that the licensees have acceptable/adequate processes in place to prevent the inadvertent introduction of equipment utilising software or firmware into a nuclear power plant.

The confirmation process by the RB should take into account at a minimum the following licensee processes:

- development and verification of specifications;
- equipment inspection upon receipt;

- procurement and supply chain management;
- quality control;
- training.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- Inadvertently introducing equipment utilising software or firmware into nuclear power plant systems and components may cause the reactor to operate outside the analysed state (criterion one); and,
- Several RBs require licensees to maintain configuration management (criterion two).

CP 3: The RB should verify that the licensee has established an acceptable process for the qualification of commercial equipment and components containing software/firmware.

The verification process by the RB should include, but not be limited to:

- The ability to determine the acceptability of changes and identify when requalification is required.
- Confirmation that the licensee has adequate access to manufacturing data.
- Verification that the licensee has a process to ensure that the manufacturer notifies the licensee of any issues that affect qualification, including errors or failure modes (defects or non-compliances).
- Verification that the licensee qualification process consider:
  - the development process for equipment and components;
  - independent verification and validation to the extent possible;
  - the role of the device in the system and the impact of failure (graded approach can be applied).

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- Software/firmware increases the complexity of systems and components and introduces new failure modes that need to be assessed. In addition, review of the development process is critical to determine the quality of the software/firmware (criterion one).
- Several RBs perform reviews of licensee qualification processes of commercial equipment (criterion two).

CP 4: The RB should have guidance and/or a strategy that shows how product certifications not done using nuclear standards (for example, Safety Integrity Level [SIL] Capability Certification based on International Electrotechnical Commission [IEC] 61508) can support the commercial dedication process.

The guidance and/or strategy should, at a minimum, look at the following points:

- Is there a fixed mapping between nuclear safety classes and SIL capability levels, or is it case by case?

- Is further evidence and testing required in addition to the certificate?
- Is the certifying organisation required to be accredited by a national accreditation service?
- It should be determined when additional environmental, seismic or EMI qualification will be required.

The SIL capability level specifies the capability of a single piece of equipment to be used in a system.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- Third party certification is a proven methodology to ensure that products fulfil their functional requirements. Certification is based on clear criteria and increases transparency (criterion one).
- Some RBs have this explicitly in written regulation; for some this is acceptable in whole, for others only in part of the safety justification (criterion two).
- Harmonisation of treatment of third party certificates, especially SIL capability certificates, has been under discussion in many working groups both on an international and national level (criterion four).

CP 5: The RB should ensure that licensees have considered protection against common cause failures (CCF) concerning embedded digital devices (EDDs).

The inspection process by the RB should factor in the following:

- For increases in uncertainties in the design of the EDDs, it is expected that the level of diversification increase (as far as reasonably achievable).
- Diversity and independence of EDDs should be considered in multiple layers and trains.

The discussion group determined this was a CP based on the rationale discussed below, which provides the technical justification for meeting the criteria from the "Guidance on Developing and Approving Commendable Practices", version one:

- CCFs threaten multiple layers of protection (criterion one).
- Some RBs have this explicitly in written regulation, while for others this is done implicitly (criterion two).

Observation one: The RB should develop a graded approach (e.g. related to safety significance) to inspect commercial off-the-shelf (COTS) products. Guidance for items that should be considered are:

- The stage at which the inspection should be conducted (feasibility study, before factory acceptance testing [FAT] or site acceptance testing [SAT], before additional type testing, in operation)?
- The methods of inspection (QA programme review, records review, witnessing tests, etc.).
- Scope of supplier inspections (for example, in which extent the supply chain should be inspected).

This was made into an observation because it is a rare practice among RBs.

5. General workshop conclusions

The discussions between participants were extensive, both in discussion group sessions and throughout the workshop. Participants exchanged ideas and practices regarding regulatory inspection activities on digital instrumentation and control (DI&C) and these ideas can be expected to provide improved expertise when applied in the future.

The members of the Nuclear Energy Agency (NEA) Working Group on Inspection Practices (WGIP) and the Working Group on Digital Instrumentation and Control (WGDIC) agreed that: "The workshops held by the NEA Working Groups continue to provide a unique opportunity for participants and inspection managers of nuclear power plants to meet and share and exchange information."

The topic chapters include the conclusions and commendable practices (CPs) that evolved from the group discussions. CPs were derived from the topics and discussed by the workshop participants. They are viewed as neither international standards nor guidelines but as references for member countries when they improve their inspection practices. Each country should determine its inspection practices while considering its own historical, social and cultural background.

6. Workshop evaluation

6.1. Evaluation form results

All participants at the workshop were asked to complete an evaluation form. The results of this questionnaire summarised below will be utilised by the Working Group on Inspection Practices (WGIP) in setting up future workshops and to look at key issues in the programme of work over the next few years.

Of the 50 participants, 36 completed and returned the evaluation form.

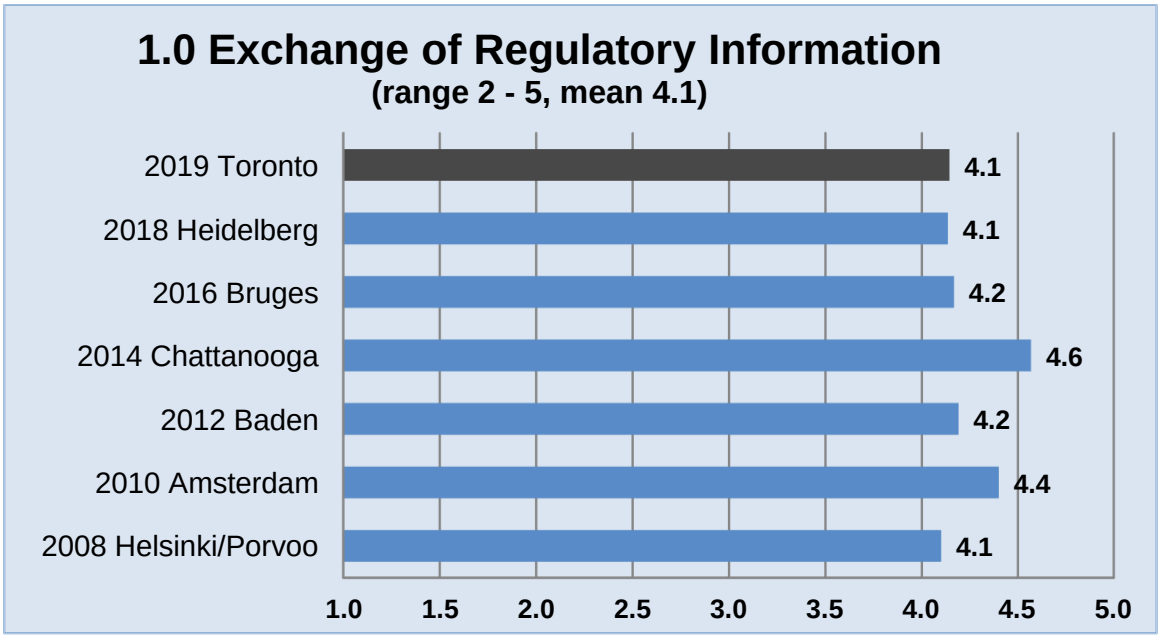
The form, which was identical to those issued at previous workshops, asked questions in four areas: general, workshop format, workshop topics and future workshops.

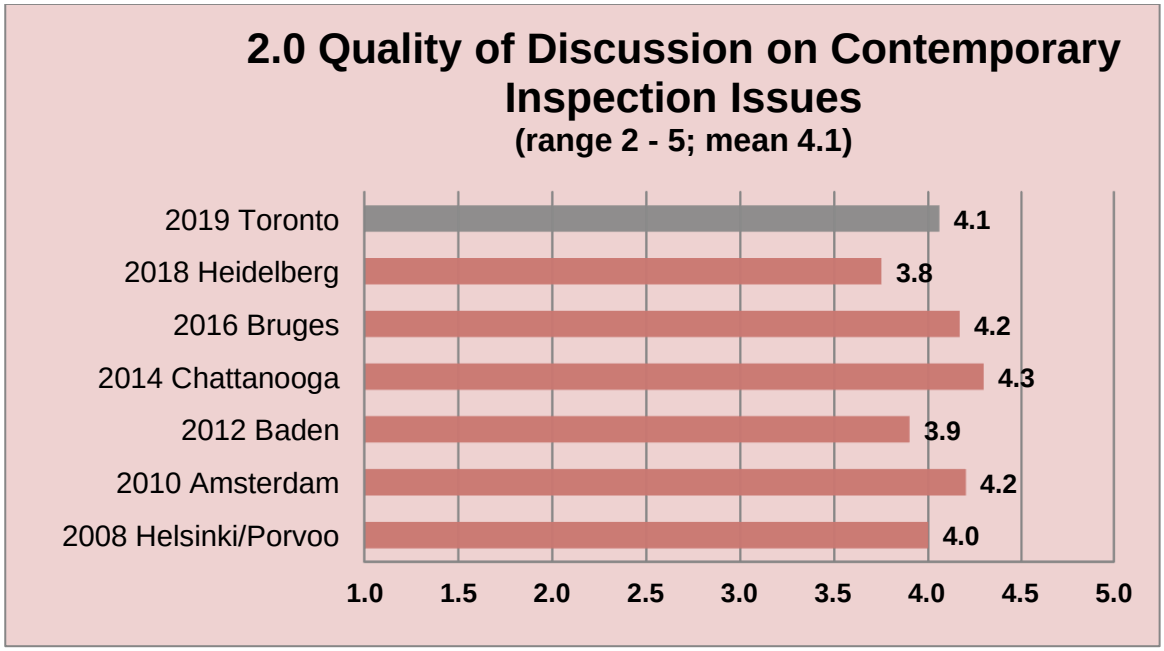
Participants were asked to rate the various questions on a scale from one to five, with one being a low (poor) score and five being a high (excellent) score. Results are provided in the following charts (which also reflect scores from the previous workshops – for comparison purposes) along with a brief written summary.

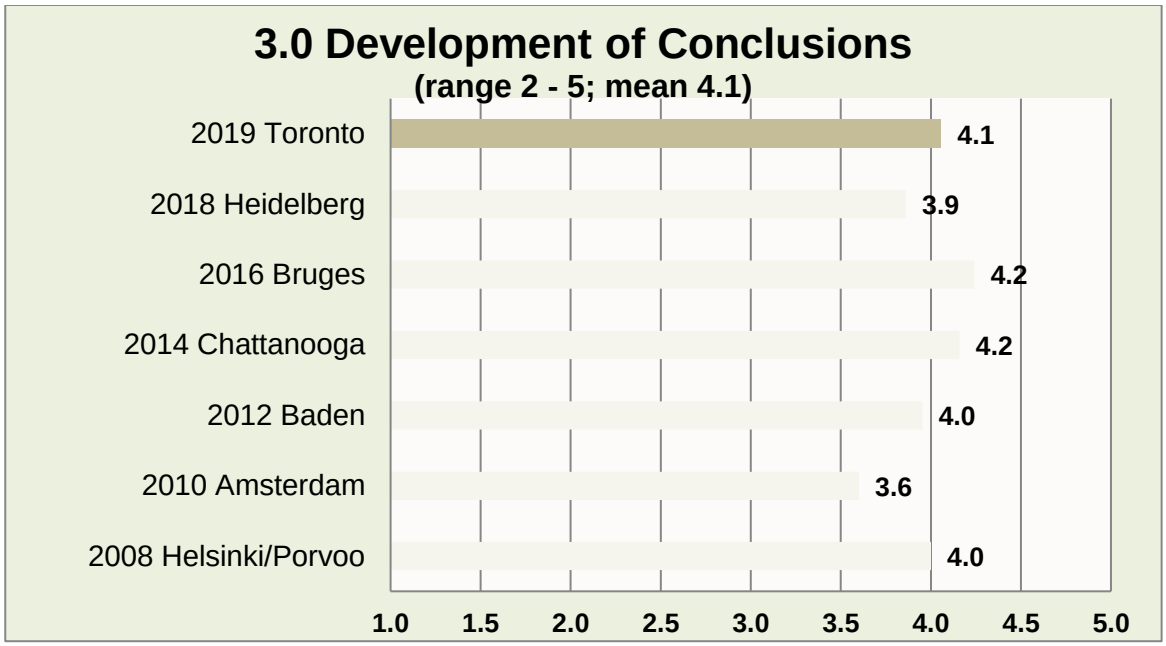
General

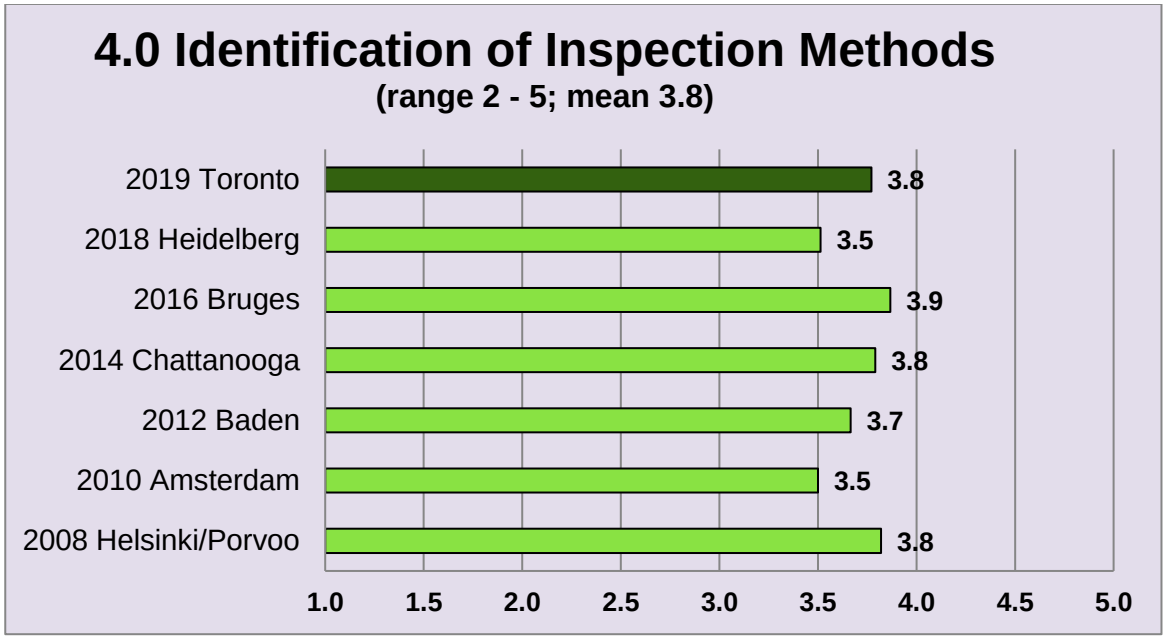
Each of the following charts depicts a specific objective of the workshop and the participant's responses on how well it was met.

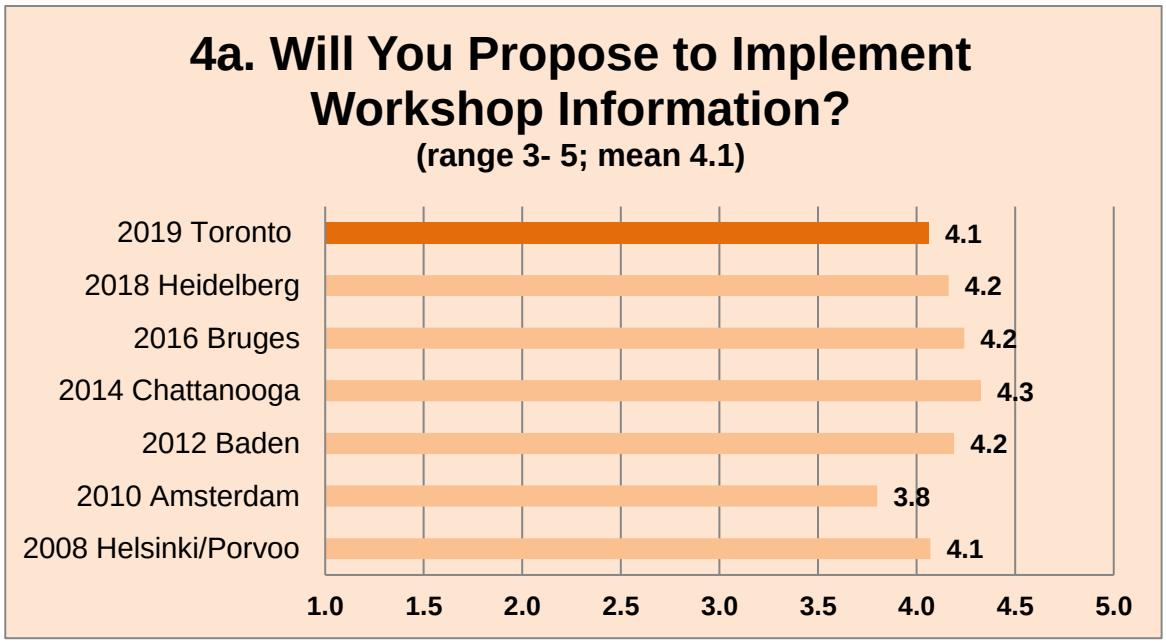
The results are comparable with the last six workshops, when the responses to questions one, two, three, four and five show that not only do participants find the exchange of information valuable, but they were able to identify methods to improve their own inspection programmes.

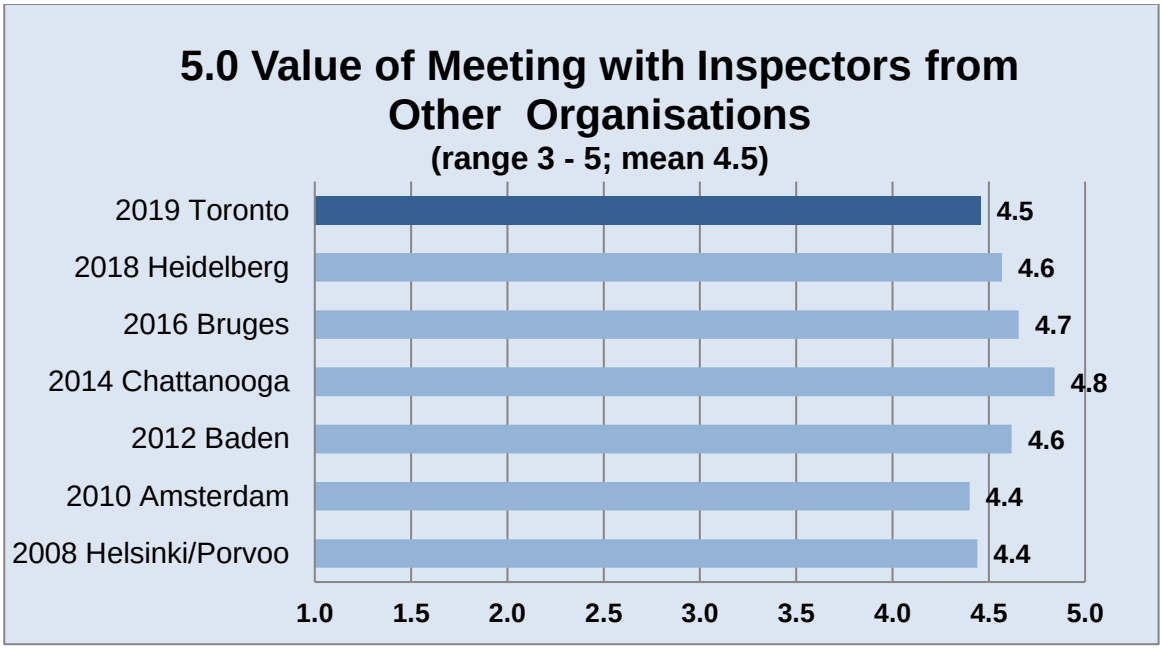



2.0 Quality of Discussion on Contemporary Inspection Issues
(range 2 - 5; mean 4.1)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.1
3.8
4.2
4.3
3.9
4.2
4.0
1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0


3.0 Development of Conclusions
(range 2 - 5; mean 4.1)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.1
3.9
4.2
4.2
4.0
3.6
4.0
1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0


4.0 Identification of Inspection Methods
(range 2 - 5; mean 3.8)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
3.8
3.5
3.9
3.8
3.7
3.5
3.8
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0

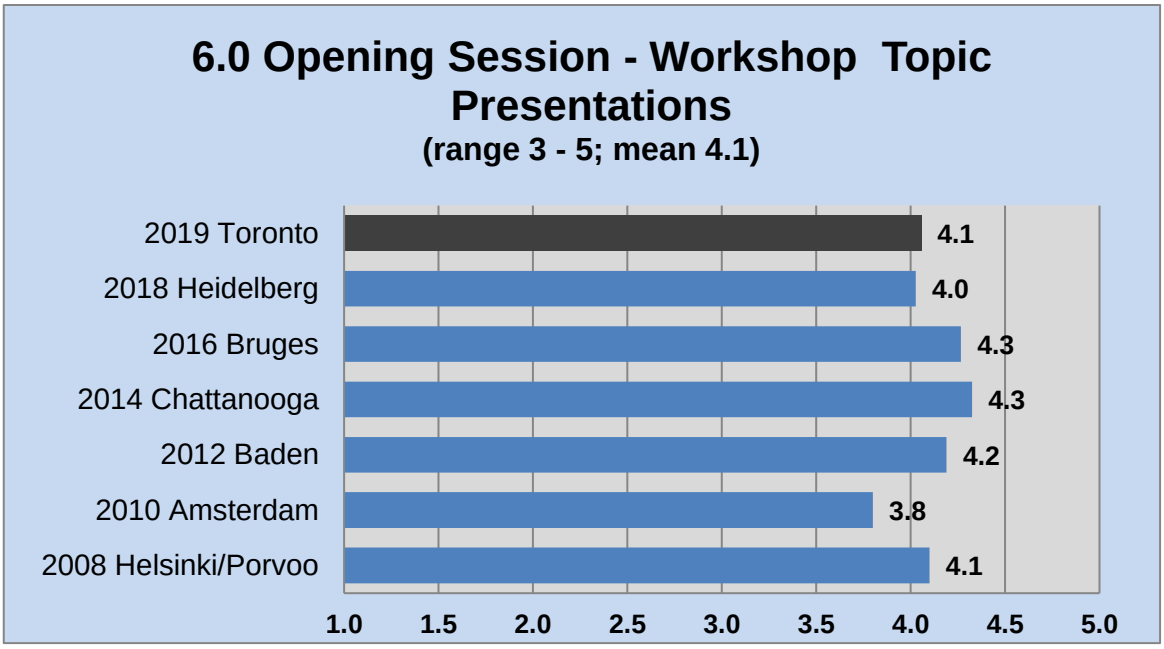

4a. Will You Propose to Implement Workshop Information?
(range 3- 5; mean 4.1)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.1
4.2
4.2
4.3
4.2
3.8
4.1
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0

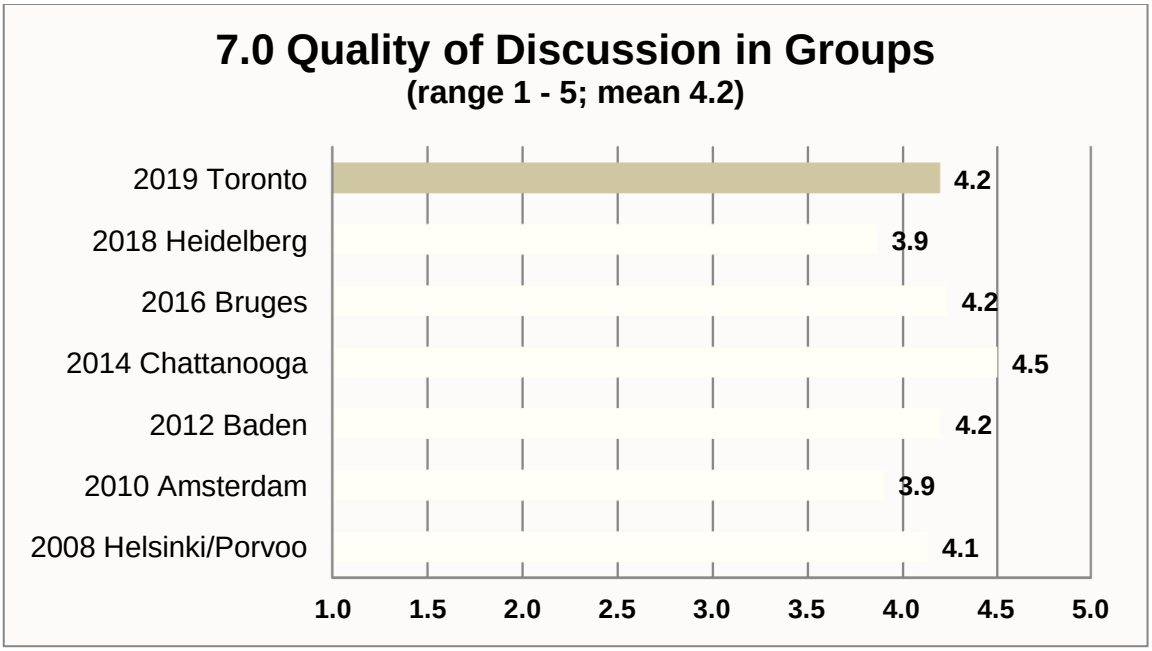

5.0 Value of Meeting with Inspectors from Other Organisations
(range 3 - 5; mean 4.5)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.5
4.6
4.7
4.8
4.6
4.4
4.4
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0

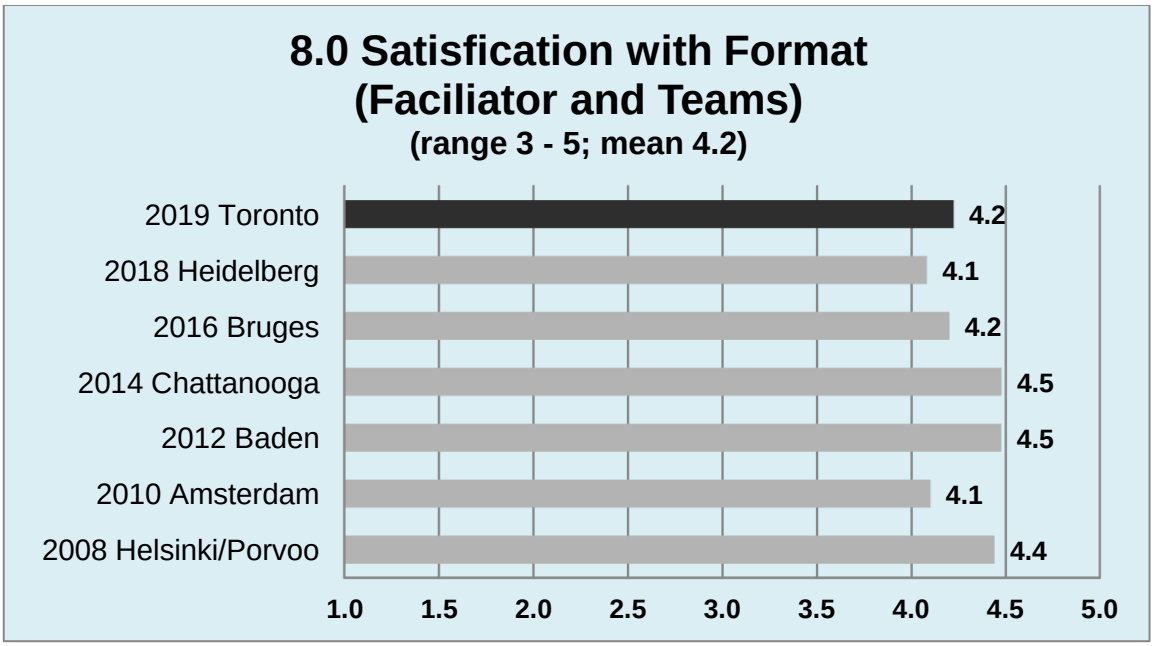
Workshop format

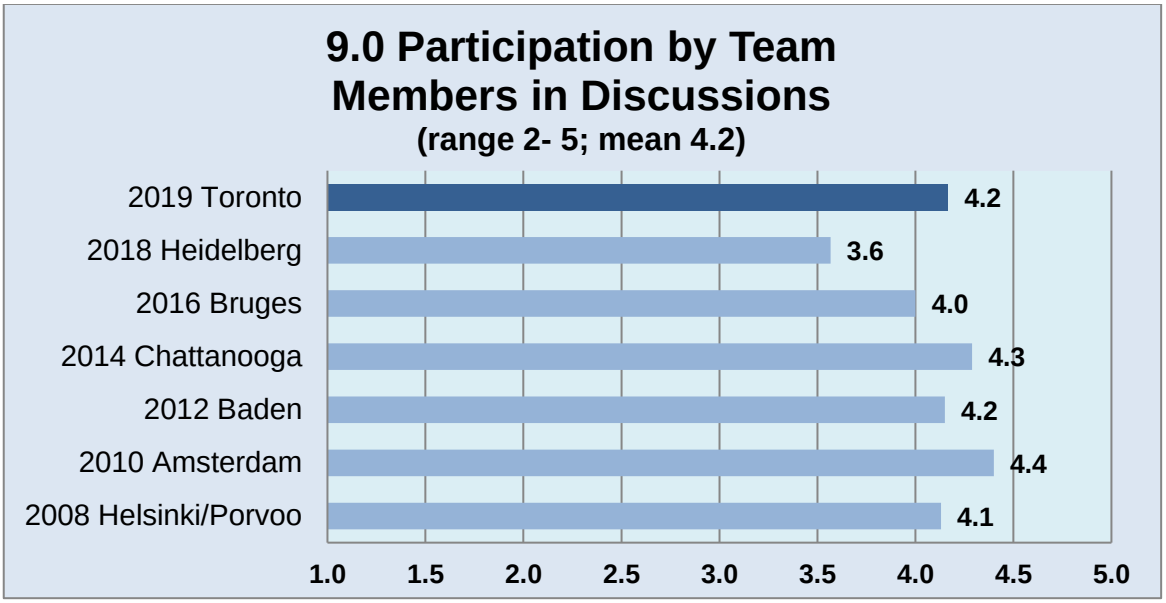
This part of the questionnaire examined the effectiveness of the sessions, with a focus on the way they were conducted.

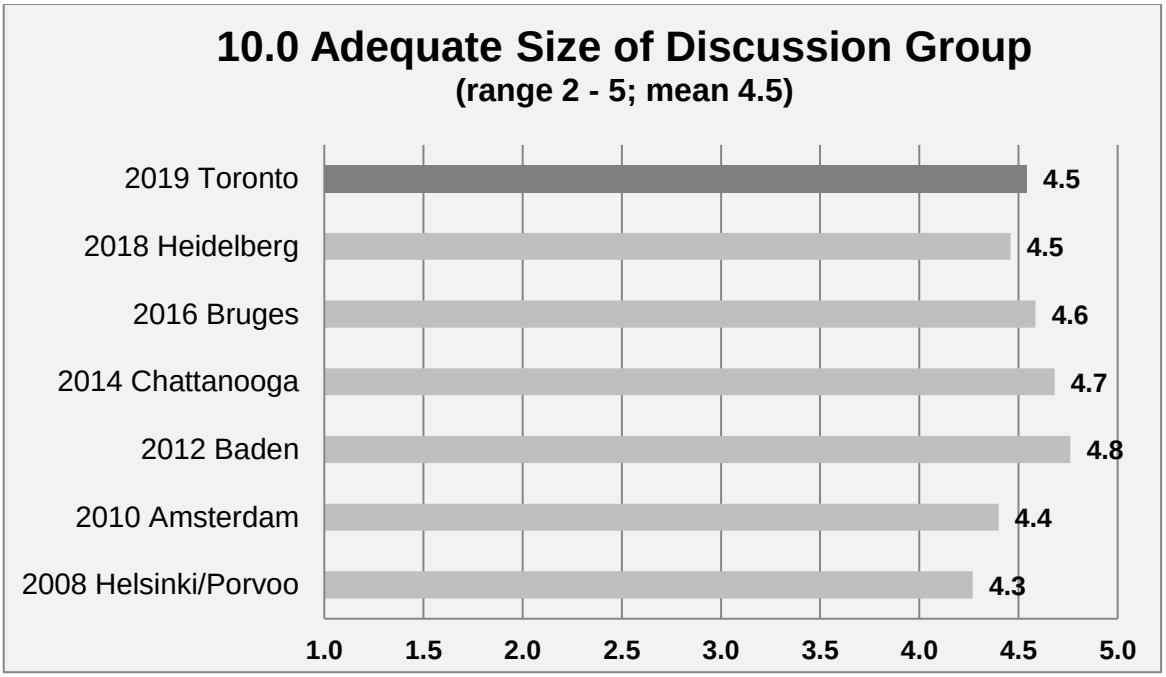
The responses provide key information to WGIP in their preparation and planning for future workshops. The results from this workshop confirmed that WGIP members have become more efficient in preparing and running the workshop. The success of each workshop depends on good preparation by the WGIP and co-ordination between the facilitators and recorders for each topic. As discussed in previous proceedings, social interaction and informal directions outside the workshop sessions enhance the discussions.

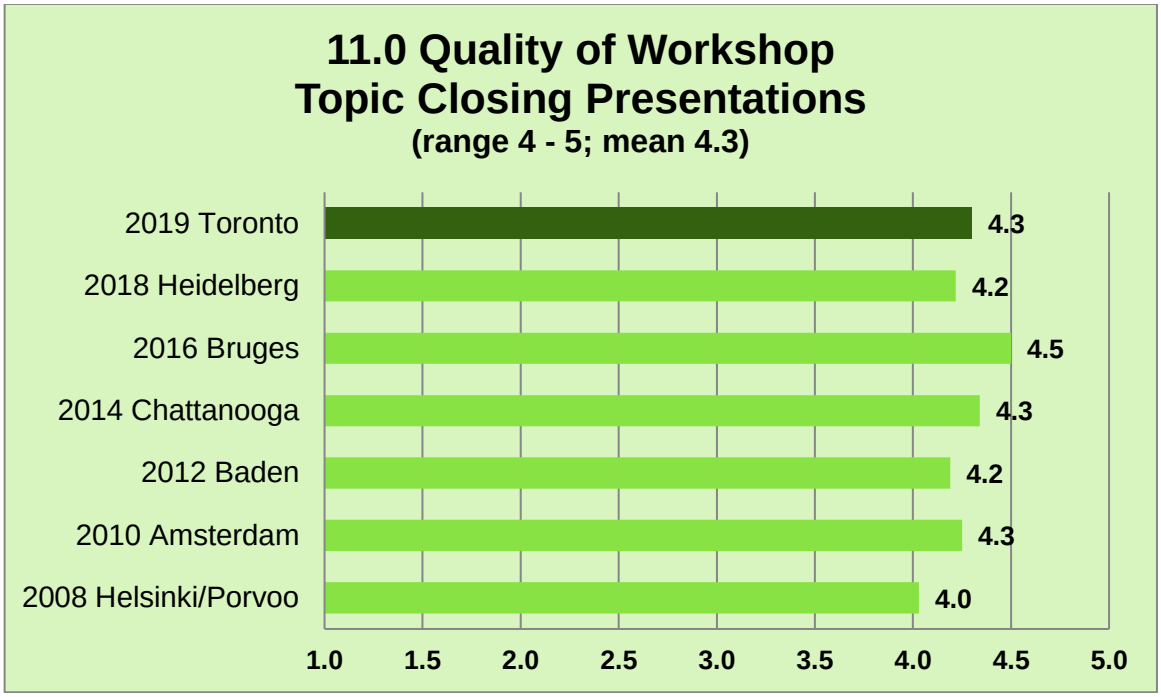



7.0 Quality of Discussion in Groups
(range 1 - 5; mean 4.2)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.2
3.9
4.2
4.5
4.2
3.9
4.1
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0


8.0 Satisfication with Format
(Faciliator and Teams)
(range 3 - 5; mean 4.2)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.2
4.1
4.2
4.5
4.5
4.1
4.4
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0


9.0 Participation by Team Members in Discussions
(range 2- 5; mean 4.2)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.2
3.6
4.0
4.3
4.2
4.4
4.1
1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0

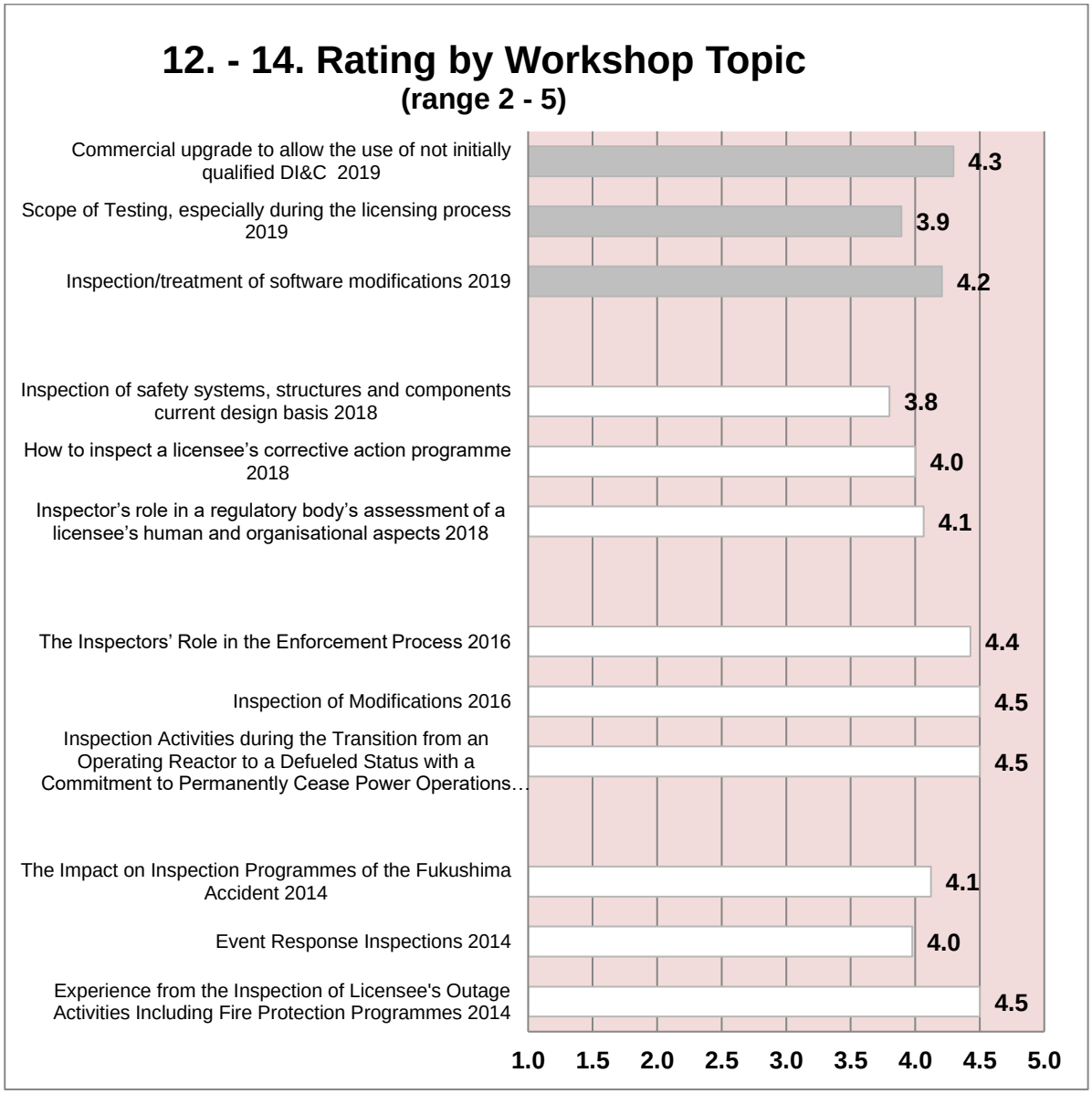

10.0 Adequate Size of Discussion Group
(range 2 - 5; mean 4.5)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.5
4.5
4.6
4.7
4.8
4.4
4.3
1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0


11.0 Quality of Workshop
Topic Closing Presentations
(range 4 - 5; mean 4.3)
2019 Toronto
2018 Heidelberg
2016 Bruges
2014 Chattanooga
2012 Baden
2010 Amsterdam
2008 Helsinki/Porvoo
4.3
4.2
4.5
4.3
4.2
4.3
4.0
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0

Workshop topics

In order to assess how well the topics were addressed, participants were asked to give a rating on whether they thought the topics were covered adequately.

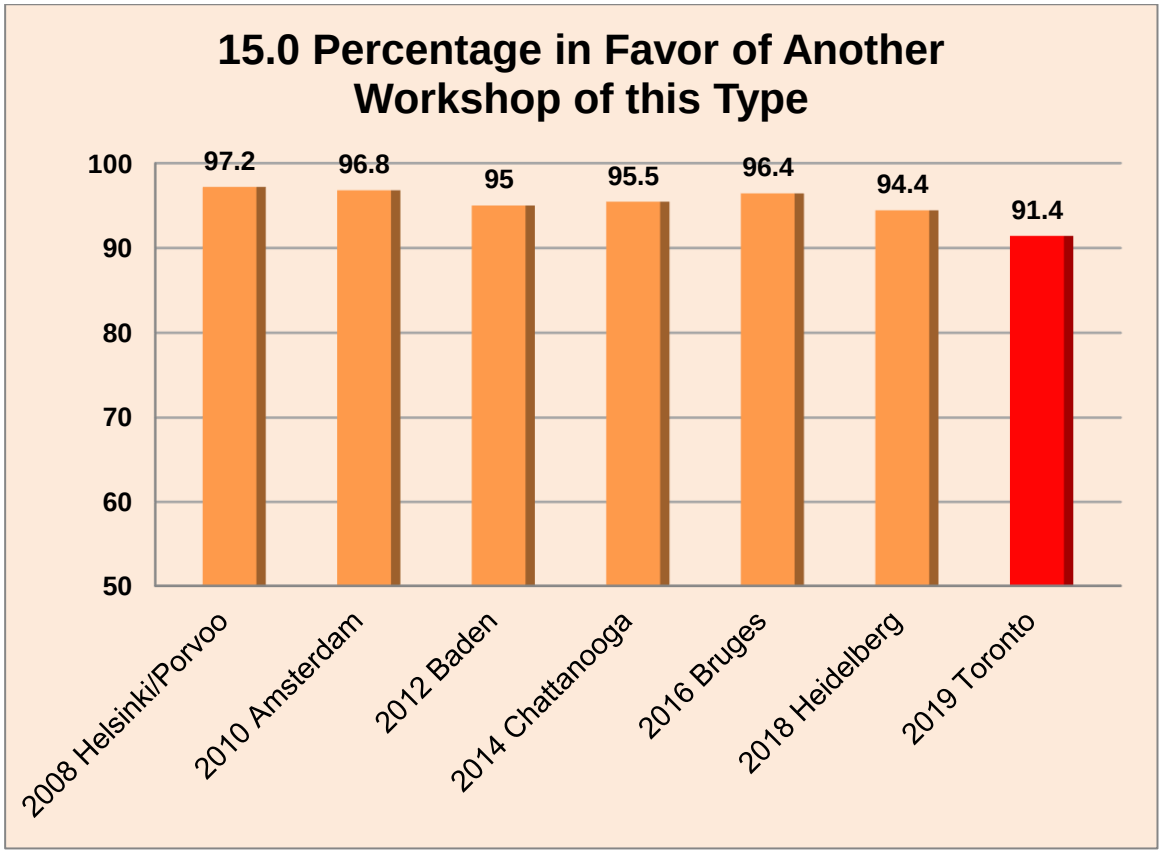
Workshop participants were generally satisfied with the selection of topics and how they were addressed.

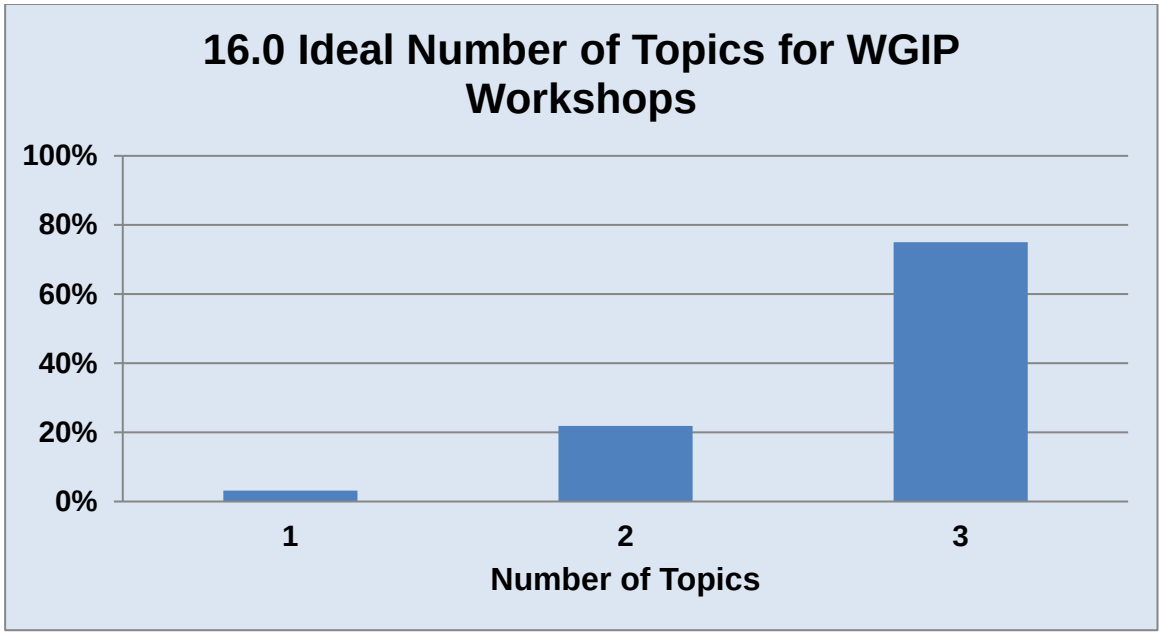


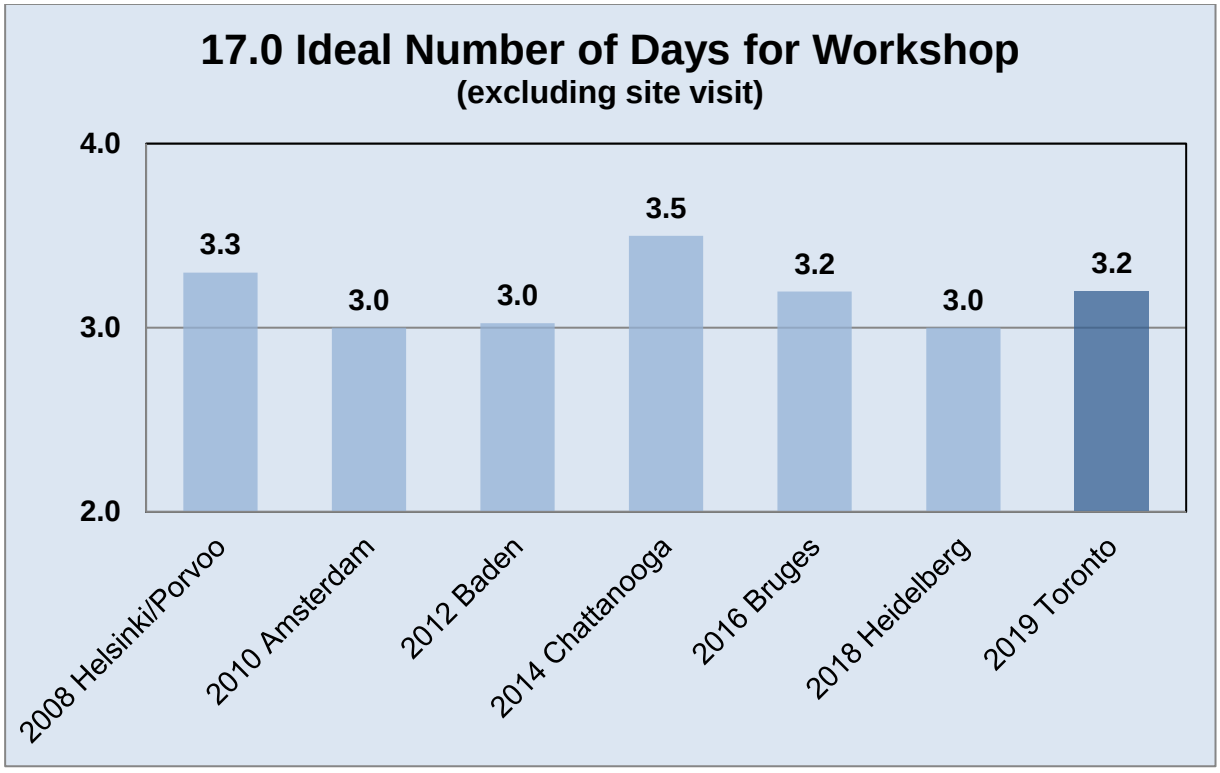
Future workshops

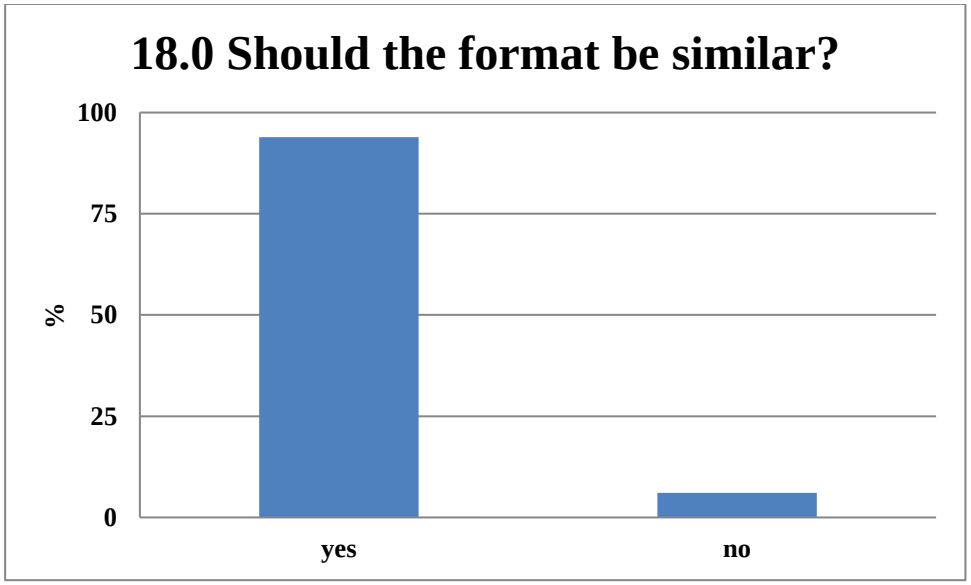
This section provides a perspective of the type of format, the overall value of having workshops and how they can be improved.

Workshop participants who responded showed strong support for future workshops. The results show that most participants also agree with the existing format regarding the number of topics and the length of the workshop.




16.0 Ideal Number of Topics for WGIP Workshops
100%
80%
60%
40%
20%
0%
1
2
3
Number of Topics


17.0 Ideal Number of Days for Workshop
(excluding site visit)
4.0
3.0
2.0
3.3
3.0
3.0
3.5
3.2
3.0
3.2
2008 Helsinki/Porvoo
2010 Amsterdam
2012 Baden
2014 Chattanooga
2016 Bruges
2018 Heidelberg
2019 Toronto


18.0 Should the format be similar?
100
75
50
25
0
%
yes
no

Annex A: List of participants

CANADA

BURTA, John
Canadian Nuclear Safety Commission
280 Slater Street
PO Box 1046, Station B
Ottawa, ON, KIP 5S9
Tel.: +1 613 996 2193
E-mail: john.burta@canada.ca

CHUN, Gilbert
Canadian Nuclear Safety Commission
280 Slater Street
PO Box 1046, Station B Ottawa, ON, K1P 5S9
Tel.: +1 613 995 2509
E-mail: gilbert.chun@canada.ca

DEMMONS, Scott
New Brunswick Power
61 Peat Drive
Quispamsis
New Brunswick
Tel.: +1 506 849 2877
E-mail: sdemmons@nbpower.com

DESBIENS, Patrick
Bruce Power
177 Tie Road
Tiverton ON
N0G 2T0
Tel.: +1 519 386 1955
E-mail: patrick.desbiens@brucepower.com

DESGAGNE, Eric
Canadian Nuclear Safety Commission
410 Laurier Avenue West, Leima Building
Ottawa, Ontario, K1R 1B7
Tel.: +1 613 991 3333
E-mail: eric.desgagne@canada.ca

FAIRWEATHER, Michael
New Brunswick Power
122 County Line Rd
Maces Bay, NB
E5J 1W1
Tel.: +1 506 650 4694
E-mail: mfairweather@nbpower.com

GORDON, Tyra
Canadian Nuclear Safety Commission
280 Slater Street
PO Box 1046, Station B
Ottawa, ON, KIP 5S9
Tel.: +1 613 947 2369
E-mail: tyra.gordon@canada.ca

HARBER, John
Candu Energy Inc.
2251 Speakman Drive
Mississauga, Ontario L5K 1B2
Tel.: +1 905 301 0551
E-mail: john.harber@snclavalin.com

FOURNIER David
EXIDA
452 Aqua Drive
Mississauga, Ontario L5G 2B6
Tel.: +1 647 838 3377
E-mail: dfournier@exida.com

LEBLANC, Alexandre
Canadian Nuclear Safety Commission
280 Slater Street
P.O. Box 1046, Station B
Ottawa, ON, K1P 5S9
Tel.: +1 613 947 7681
E-mail: alexandre.leblanc@canada.ca

MCKAY, Kevin
Ontario Power Generation
619 Cognac Crescent
Tel.: +1 289 923 2367
E-mail: kevin.mckay@opg.com

MCLEAN, Kyle
Canadian Nuclear Safety Commission
177 Tie Rd.
Tel.: +1 519 361 3002
E-mail: kyle.mclean@canada.ca

MULLIN, Daniel Richard
Canadian Space Agency
6767, route de l'Aéroport
Saint-Hubert (Québec) J3Y 8Y9
Tel.: +1 450 926 4472
E-mail: danielrichard.mullin@canada.ca

NGUYEN, Duc
Canadian Nuclear Safety Commission
1675 Montgomery Park Road
Tel.: +1 905 831 8195
E-mail: ducdavid.nguyen@canada.ca

ZENG, Charles
Canadian Nuclear Safety Commission
280 Slater Street
P.O. Box 1046, Station B
Ottawa, ON, K1P 5S9
Tel.: +1 613 996 0023
E-mail: zhaochang.zeng@canada.ca

CZECH REPUBLIC

JAKES, Miroslav
State Office for Nuclear Safety (SUJB)
Senovážné nám. 9
110 00 Prague 1
Tel.: +420 385 735 033
E-mail: miroslav.jakes@sujb.cz

NEKUŽA, Miloš
State Office for Nuclear Safety (SÚJB)
Senovážné náměstí 9,
110 00 Prague 1
Tel.: +420 221 624 273
E-mail: milos.nekuza@sujb.cz

FINLAND

HEINONEN, Mikko
STUK – Radiation and Nuclear Safety Authority
PL 14, Laippatie 4,
00881 Helsinki
Tel.: +358 40653 87 60
E-mail: mikko.heinonen@stuk.fi

JOHANSSON, Mika
P.O. Box 14
FI-00881 Helsinki
Tel.: +358 40 17 95 865
E-mail: mika.johansson@stuk.fi

FRANCE

CAZALET, Cécile
15 rue Louis Lejeune CS70013
92541 Montrouge Cedex
Tel.: +33 146164299
E-mail: cecile.cazalet@asn.fr

EL GHALBZOURI, Redouane
15 rue Louis Lejeune
92541 Montrouge Cedex
Tel.: +33 146164103
E-mail: redouane.elghalbzouri@asn.fr

GUANNEL, Yves
15 rue Louis Lejeune
CS 70013
92541 Montrouge Cedex
Tel.: +33 (0) 1 46 16 42 91
E-mail: yves.guannel@asn.fr

GERMANY

HELLMICH, Mario
Willy-Brandt-Str. 5
38226 Salzgitter
Tel.: +49 (0) 30 18 333 1033
E-mail: mario.hellmich@bfe.bund.de

SCHNEIDER, Matthias
Federal Office for the Safety of Nuclear Waste Management - Nuclear Safety and Supervision of Disposal Department
P.O. Box 10 01 49
D-38201 Salzgitter
Tel.: + 49 3018 333 1561
E-mail: matthias.schneider@bfe.bund.de

STRATMANN, Simone
Ministerium für Umwelt, Klima und Energiewirtschaft
Baden-Württemberg
Postfach 103439
D-70029 Stuttgart
Tel.: +49 7111262623
E-mail: simone.stratmann@um.bwl.de

JAPAN

KASAGAWA, Yusuke
Nuclear Regulation Authority (NRA)
1-9-9 Roppongi, Minato-ku,
Tokyo, 106-8450
Tel.: +81 3 5114 2122
E-mail: yusuke_kasagawa@nsr.go.jp

KATAOKA, Kazuyoshi
Nuclear Regulation Authority (NRA)
1-9-9 Roppongi-First Bild.
Roppongi, Minato-ku, Tokyo
Tel.: +81 3 5114 2109
E-mail: kazuyoshi_kataoka@nsr.go.jp

WATANABE, Nobumichi
1-9-9 Roppongi-First Bild
Roppongi Minato-ku, 15F
Tokyo 106-8450
Tel.: +81 3 5114 2223
E-mail: nobumichi_watanabe@nsr.go.jp

KOREA

BOOH, In Hyoung
62 Gwahak-ro,
Yuseong-gu, Daejeon
Tel.: +82 42 868 0250
E-mail: k307bih@kins.re.kr

HUH, Chang Wook
Div. of Nuclear Inspection
Korea Institute of Nuclear Safety (KINS)
62 Gwahak-ro, Yusong-gu
Daejeon
Tel.: +82 42 868 0571
E-mail: k401hcw@kins.re.kr

KIM, Hyungtae
62 Gwahak-ro, Yuseong-gu
Daejeon 34142
Tel.: +82 42 868 0804
E-mail: k719kht@kins.re.kr

NETHERLANDS

SCHREURS, Erik
Koningskade 4
2596 AA Den Haag
Tel.: +31 646368877
E-mail: erik.schreurs@anvs.nl

POLAND

DULNY, Karol
ul. Bonifraterska 17
00-203 Warszawa
Poland
Tel.: +48 225562870
E-mail: dulny@paa.gov.pl

GLOWACKI, Andrzej
National Atomic Energy Agency (PAA)
Bonifraterska 17
00-203 Warsaw
Tel.: +48 22 556 2805
E-mail: glowacki@poczta.paa.gov.pl

SLOVENIA

SAVLI, Sebastjan
Slovenian Nuclear Safety Administration
Litostrojska cesta 54
1000 Ljubljana
Tel.: +386 1 472 11 75
E-mail: sebastjan.savli@gov.si

SPAIN

GALINDO RODRÍGUEZ, José
Pedro Justo Dorado Dellmans, 11
28040 Madrid
Tel.: +34 913302023
E-mail: jgr@csn.es

YAGUE, Jorge
Calle Pedro Justo Dorado Dellmans, 11,
28040, Madrid, SPAIN

Tel.: +34 913460134
E-mail: jjym@csn.es

SWEDEN

HELLBERG, Henrik
Swedish Radiation Safety Authority
Solna strandväg 96
SE-171 16 Stockholm

Tel.: + 46 8 799 41 81
E-mail: henrik.hellberg@ssm.se

UNITED KINGDOM

KHAN, Mahtab
Redgrave Court
Merton Road
Liverpool
L20 7HS

Tel.: +44 2030280248
E-mail: mahtab.khan@onr.gov.uk

MCDONALD, Kulvinder
Office of Nuclear Regulation
4NG Redgrave Court
Merton Road
Bootle, Merseyside L20 7HS

Tel.: +44 0203 028 0217
E-mail: kulvinder.mcdonald@onr.gov.uk

WARDLE, Stephen
Principal Inspector, Nuclear Safety
Office for Nuclear Regulation (ONR)
Redgrave Court
Merton Road, Bootle
L20 7HS

Tel.: +44 (20) 3028 0395
E-mail: stephen.wardle@onr.gov.uk

UNITED STATES

DUMONT, Louis
US Nuclear Regulatory Commission (NRC)
Region I
2100 Renaissance Blvd
Suite 100
King of Prussia, PA 19406

Tel.: +1 610 337 5183
E-mail: louis.dumont@nrc.gov

DURKOSH, Donald
1000 Westinghouse Drive
Cranberry Township, Pennsylvania 16066
Tel.: +1 412 374 3753
E-mail: durkosde@westinghouse.com

GALLETTI, Greg
US Nuclear Regulatory Commission (NRC)
Office of Nuclear Reactor Regulation
11545 Rockville Pike
Rockville, MD 20852
Tel.: 301 415 1831
E-mail: gsg@nrc.gov

GARCIA, Ismael
US Nuclear Regulatory Commission (NRC)
Office of Nuclear Reactor Regulation
11545 Rockville Pike
Rockville, MD 20852
Tel.: +1 301 415 2495
E-mail: ismael.garcia@nrc.gov

JOHNSON, Gary
1255 Higuera Ct.
Livermore, California 94551
Tel.: +1 925 605 6263
E-mail: kg6un@mac.com

KELLEY, Sean
1370 Mountclaire Drive
Cumming, GA 30041
Tel.: +1 6786549354
E-mail: s.kelley@sunport.ch

MANNING, Lisa
Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066
Tel.: +1 412 374 3332
E-mail: manninla@westinghouse.com

INTERNATIONAL ORGANISATIONS

BUCKENMEYER, Thomas
Division of the Nuclear
Safety Regulation and Technology
OECD Nuclear Energy Agency
46, quai Alphonse Le Gallo
92100 Boulogne-Billancourt
Tel.: +33 1 45 24 10 57
E-mail: thomas.buckenmeyer@oecd-nea.org

CHANIAL, Luc
Acting Head, Division of the Nuclear
Safety Regulation and Technology
OECD Nuclear Energy Agency
46, quai Alphonse Le Gallo
92100 Boulogne-Billancourt

Tel.: +33 1 45 24 10 55
E-mail: luc.chanial@oecd-nea.org

NIIOKA, Terumasa
Division of the Nuclear Safety
Regulation and Technology
OECD Nuclear Energy Agency
46, quai Alphonse Le Gallo
92100 Boulogne-Billancourt

Tel.: +33 145241151
E-mail: terumasa.niioka@oecd-nea.org

Annex B: Q& A from all organisations

Canada

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Canada: Yes. DI&C systems/components important to safety are used in all CANDU plants. For example, DNGS (Darlington Nuclear Generating Station) is fully digitalised in Shutdown System No. 1 and Shutdown System No. 2, ECIS (Emergency Coolant Injection System), Containment System, plant control system including reactor control system, plant monitoring system and display system. PLNGS (Point Lepreau Nuclear Generating Station) is partially digitalised in Shutdown System No. 1 and Shutdown System No. 2, fully digitalised in plant control system including reactor control system, plant monitoring system and display system. PNGS (Pickering Nuclear Generating Station) and BNGS (Bruce Nuclear Generating Station) are digitalised in plant control system including reactor control system, plant monitoring system and display system.

[note] systems/components important to safety means safety systems/components and safety-related systems/components based on plant equipment in IAEA Safety Glossary.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Canada: For existing operating CANDU plants and new plants, CNSC (Canadian Nuclear Safety Commission) authorises the installation and use of DI&C systems through the following activities:

a) Comprehensive assessment of the information required by the CNSC;

b) Resolution of any outstanding issues from the licensing stage;

c) Conclusions and recommendations from a and b above are submitted to the Commission, which makes the final decision on the issuance of the operating licence.

The standards listed in the Licence Conditions Handbook are used as acceptable criteria (for example, REGDOC-2.5.2, CSA N286, CSA N290 series). In addition, the assessment of other applicable documents supports the licensing criteria. The examples of other applicable documents are previous CMD (Commission Member Document), Periodic safety report, Regulatory oversight report, Quarterly performance indicator report, and Inspection report.

2.2. Describe how DI&C is captured in the licensee technical basis.

Canada: DI&C is captured in the safety report submitted to CNSC. The safety report demonstrates how it meets the DI&C requirements in regulatory documents (e.g. REGDOC) and national standard (i.e. CSA standards). In addition, licensee incorporated the DI&C requirements stated in national standard into the licensee procedure documents and industry-licensee standard (e.g. CE-1001-STD, Standard for software engineering of safety critical software).

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Canada: Yes. CNSC staff inspect the DI&C systems in the area of software maintenance. CNSC staff select a few target systems and collect all the relevant maintenance records and review the records whether the records are in compliance with the national standards (e.g. CSA N286-12 for Management system) and CNSC requirements. As an example, CNSC staff use the Type II Inspection guide – Software Maintenance.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Canada: No. CNSC staff inspect design stage and operational stage. Design stage for safety critical software includes all phases of design from computer system requirements to validation testing of product. Operational stage inspection is performed on software every five years. There has been no inspection on the hardware and software at manufacturer site and installation site. But the inspection during manufacturing and installation is not excluded. For example, CNSC staff participated in the software validation test at manufacturer site as a witness.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Canada: The scope of the inspection covers the areas under CSA N286-12 (Management system requirements), e.g. management system, human performance, operating performance, fitness for service. For each area, the inspection is focused on the maintenance of digital I&C system and components. The inspector is designated from the inspection division and the staff in technical branch support the inspection.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

Canada: CNSC has no specific training programme to inspect DI&C systems/components. CNSC inspectors and subject matter experts (e.g. technical specialists) participate in the mandatory internal inspection course. Trainees learn how to perform the field inspection. The additional method is to participate in the inspection as an on-the-job participant.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

Canada: It depends on the type of inspection. For example, software maintenance inspection is a separate inspection because of unique characteristics of software. In SOE (Safe Operating Envelope) inspection, the inspection of DI&C is a part of SOE inspection.

CNSC I&C staff rarely participated in the vendor site inspections. However, CNSC QA staff performs the vendor inspection as required, e.g. design process inspection, qualification test inspection.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Canada: Yes. Licensees use the embedded digital devices (EDDs) in a limited area. EDDs are applied in, for example, engine control valve drive unit and generator protective relay

which are classified as category II system. In Canada, to date, EDDs (e.g. smart transmitter) are not applied to safety system, nor category I system.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

Canada: EDDs applied to CANDU plants are limited to Category II and III systems. Recently CNSC staff assessed sampled EDDs against CSA N290.14 (Qualification of digital hardware and software for use in I&C application). In addition, CNSC staff consider the Generic Common Position DICWG NO7 (Common position on selection and use of industrial digital devices of limited functionality) as for additional criteria (see http://www.oecd-nea.org/mdep/common-positions/).

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Canada: The qualification activities stated in CSA N290.14 are to be applied to qualify EDDs by the licensee. For example, the activities are to (1) identify and classify EDDs, (2) assess the qualification concerns, and (3) qualify the software and hardware using the methods in CSA N290.14.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Canada: CNSC staff inspect the modification procedure and software program of licensee during Type I inspection and inspect the modification outcome during the Type II inspection using the CNSC inspection guide on software maintenance. The relevant documents of licensee are, for example, Engineering Change Control, Modification Process, Software Program, Maintenance of Real-time Process Computing Systems.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Canada: Yes. In the computer hardware development plan, licensee describes the approach to obtain reasonable assurance that commercial-off-the-shelf components used as basic components will perform the intended safety functions.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Canada: CNSC staff request the relevant documents produced during the dedication process and review and approve the documents for use. One of the documents is, for example, Shutdown System Platform Qualification against CSA N290.14.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

Canada: CNSC staff use the qualification activities specified in CSA N290.14 in the aspects of qualification. For example, CNSC staff review and approve the predeveloped software in accordance with recognised standards, and make sure that the hardware is assessed in environmental tolerance, seismic tolerance, and electromagnetic immunity and emissions.

7. Equipment Qualification (electromagnetic, environmental and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

Canada: Licensee qualifies the DI&C systems according to licensee qualification test procedure which includes environmental, seismic and electromagnetic test procedure. Vendor supports the licensee with vendor's qualification test procedures.

CNSC staff perform compliance verification with applicable national standards, for example, CSA N290.13 (Environmental qualification of equipment).

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Canada: CNSC staff use the maintenance qualification requirements in CSA N290.14 (Qualification of Digital Hardware and Software for use in I&C application). When there is a software version change, CNSC staff evaluate the documents for new software version to determine the effect on existing qualification.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Canada: CNSC staff use the maintenance qualification requirements in CSA N290.14 (Qualification of Digital Hardware and Software for use in I&C application). When there is a hardware version change, CNSC staff evaluate the documents for new hardware version to determine the effect on existing qualification.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Canada: CNSC staff use regulatory document REGDOC-2.5.2 (Design of Reactor Facilities) Clause 7.6.1.3 (Independence) and CSA N290.0-11 Clause 4.6 (Separation and independence), which requires the separation between different safety systems, safety system and process systems. CNSC staff also use the Generic Common Position DICWG NO4 (Common position on principle on data communication independence) as for additional criteria (see http://www.oecd-nea.org/mdep/common-positions/).

In addition, there is limited communication between systems and components, and the communications are mainly for collecting data and display in CANDU plants.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Canada: CNSC requires the event reporting by REGDOC-3.1.1 (Reporting requirements). CNSC has internal procedure for event review of DI&C systems/components, which typically is conducted by a group of related specialists. Similar events will be trended, and if necessary, reactive inspection may be triggered for adverse trending or repeated events depending on the safety significance of the events.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

Canada: No. CNSC staff has not evaluated DI&C events in the digitalised control system to identify CCFs (common cause failures) because there is no requirement to identify CCFs in the control system. In the safety system, there were no DI&C events that need to identify CCFs. However, potential CCFs are identified in the software code FTA (Fault Tree Analysis), which causes more than one parameter trip failure.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

Canada: Designer identifies the potential failure modes of DI&C system in the System FMEA (Failure Mode and Effect Analysis). The typical failure mode is stated in the Failure Mode column in the FMEA table which is a part of hazard analysis report. Failure modes are based on the failure of assigned function. One example is the failure of receiving calibration/link enable signal.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

Canada: CNSC has no special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

11.2. What kind of functional tests does your RB inspect? Please describe.

Canada: For the safety system software, CNSC staff reviews the all the functional test reports required in the design stage. For example, functional tests include the software module test, software integration test based on software design description and software requirements specification. During the operating stage, CNSC staff review the functional tests in the surveillance that are periodically conducted.

China

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Answer: Yes they do. DI&C systems applied in Chinese nuclear power plants are:

1. RPS & ESFAS based on TXS DI&C platform in Lingao Nuclear Power Plant, Taishan Nuclear Power Plant, Tianwan Nuclear Power Plant, Fuqing Nuclear Power Plant (Unit 5&6).
2. RPS & ESFAS based on Meltac DI&C platform in Yangjiang Nuclear Power Plant, Hongyanhe Nuclear Power Plant, Ningde Nuclear Power Plant, Fangchenggang Nuclear Power Plant.

3. RPS & ESFAS based on FirmSys DI&C platform in Yangjiang Nuclear Power Plant (Unit 5&6), Hongyanhe Nuclear Power Plant (Unit 5&6) and Tianwan Nuclear Power Plant (Unit 5&6).
4. RPS & ESFAS based on Common Q DI&C platform in Sanmen Nuclear Power Plant and Haiyang Nuclear Power Plant.
5. RPS & ESFAS based on Tricon DI&C platform in Fuqing Nuclear Power Plant, Fangjiashan Nuclear Power Plant and Hainan Nuclear Power Plant.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Answer: First, any one (vendor) who want to use DI&C System/Equipment/Component in nuclear power plants for safety important system should obtain nuclear safety design and/or manufacture licence from the NNSA. EQVV

Second, before deployed into the nuclear power plant, the whole process which contains design, verification, implement, validation, integration and installation stages of DI&C System/Equipment will be supervised and inspected.

Third, when a DI&C System/Equipment is put into operation, the regulatory body will periodically inspect the performance of DI&C System/Equipment operation.

The criteria mainly include HAF003, HAF102, HAD102/14, and HAD102/16. Also some international standards such as SSR-2/1, SSG-39, IEEE 7-4.3.2, IEC 60880 may be referenced in regulatory activities.

2.2. Describe how DI&C is captured in the licensee technical basis.

Answer: This is the responsibility of the licensee.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Answer: Yes. They perform technical review on DI&C systems/components design, equipment qualification and software V&V reports, and also inspect the DI&C systems/components installation and operation.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Answer: Yes.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Answer: The scope of the inspection includes: design, equipment qualification, software V&V, installation, commissioning and operation.

The types of staff expertise are I&C, computer, communication engineer, and so on.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

Answer: The inspectors are trained periodically or when they need, and their capabilities were evaluated for the inspector mission.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

Answer: Yes, we think that I&C system/components is very important, so we have a separate I&C department.

The type and scope of vendor inspections include annually audit, specific inspection for equipment qualification, V&V, system integration, factory test and quality assurance.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Answer: Yes, in many control modules, AD/DA convert modules and display units, CPUs, MCUs and FPGA/CPLDs are used.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

Answer: The RB uses some Chinese standards, and RCC-E，IEEE 603, IEEE 7-4.3.2, IEC 60880 may be referred to.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Answer: Equipment qualification and software V&V are helpful to qualify embedded digital devices.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Answer: In inspection, the modifications and maintenance procedures and their implementation will be checked. Any intended modifications related to safety system must be reported to RB in advance.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Answer: Yes, some of them have the vendor make CGD process for DI&C.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Answer: The RB usually performs special review for CGD.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

Answer: The RB use HAD 003/03 and HAD 102/16 to review, approve, and inspect the use of commercial grade DI&C components. In specific CGD process and its inspection and review, EPRI NP-5652, TR-102260 and TR-106439 may be referred to.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C

systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

Answer:

1. Conducted the environmental tests.

   Confirmed they satisfy criteria value, including temperature/humidity Test, vibration test, long-term operation test and so on.

2. Conducted EMC tests.

   Equipment suppliers usually use RG 1.180 or IEC 61000 series to satisfy the EMC test. Besides, we also ask emission and sensitivity tests greater than 1 GHz.

3. Conducted seismic tests.

   The licensees use GB/T13625 which is similar to IEC 60980 or IEEE 344.

   The RB reviews the EQ Plan, the EQ procedures and EQ Report/record. Besides the RB inspect and witness some testing such as seismic and EMC on testing-site.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Answer: HAD102/16 is used for accept software CM. IEEE 828-2005 may be referred to.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Answer: HAD 102/16 is also used for evaluate hardware version control.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Answer: HAF102, HAD102/16 and GB/T13629 are used for accept communication designs between independent/different systems. One-way communication is usually used to achieve communication independence.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis and the dissemination of any applicable lessons learnt.

Answer: For an event, a root cause analysis is usually performed according to the procedure. If there are large number of events, trend analysis is performed after the summary.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

Answer: No.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

Answer: Typical failure modes include equipment failures and personnel factors.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

Answer: During the on-site inspection, we will pay special attention to the design changes of I&C system and its subsequent V&V and re-qualification results.

11.2. What kind of functional tests does your RB inspect? Please describe.

Answer: Response time tests, priority tests, trip tests, etc.

Czech Republic

1. A use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Dukovany Nuclear Power Plant I&C Replacement:

a) Safety Systems (IEC 61226 Category A, triple-redundant):

RPS	Reactor protection System: Reactor Trip System RTS (including EX-Core) and Engineered Safety Features Actuation System ESFAS
ELS	Emergency Load Sequencer (Diesel Generator Sequencer)
PAMS1	Post Accident Monitoring System (RG 1.97 Category 1 parameters)

b) Safety-Related Systems (IEC 61226 Category B, double or triple redundant:

RLS	Reactor Limitation System (Reactor power limitation)
RCS	Reactor Control System (Reactor power control)
RRCS	Reactor Rod Control System (Rod drives control)
PAMS2	Post Accident Monitoring System (Category 2 parameters)

c) Other Systems Important for Safety (IEC 61226 Category C):

PCS	Process Computer System

d) Main Control Room (MCR) and Emergency Control Room (ECR) - displays and controls.

e) Distributed Controls of Individual Component (Primary Circuit System Interlocks and Controls, Secondary Circuit System Interlocks and Controls, Turbine and Generator Control and Protection):

ESF Controls (cat. A per IEC 61226): Implemented on HW platform, supported by digital surveillance and diagnostic subsystems.

Other Controls (cat. B/C/not classified): 3 different digital platforms.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

In relation to the project of the I&C systems renovation at Dukovany Nuclear Power Plant important for the nuclear safety, SÚJB reached the following position:

The implementation of the renovated I&C systems important for the nuclear safety based on digital software systems is an acceptable solution assuming that the following general conditions will be met:

- design, accomplishment, installation, testing, commissioning and operation of the systems will meet all relevant requirements of the applicable Czech legislation , i.e. in particular:
  - The Act on Peaceful Use of the Nuclear Energy and of the Ionizing Radiation and on the change and amendment of some acts.
  - Decrees of SÚJB on requirements on nuclear facilities to ensure the nuclear safety, radiological protection and emergency preparedness.
  - Decrees of SÚJB on assuring the quality at activities relating to the use of the nuclear energy and at activities leading to irradiation and on determination of criteria for inclusion and classification of selected facilities into safety classes.
  - Decrees of SÚJB on providing nuclear safety and radiological protection of the nuclear facilities at their commissioning and operation.
- proposal and accomplishment of the renovated I&C systems important for the nuclear safety will meet the SÚJB requirements, specified in the chapters of *Set of SÚJB Positions to Selected Aspects of the I&C Renovation of the Dukovany Nuclear Power Plant*;
- proposal and accomplishment of the renovated I&C important for the nuclear safety will meet the relevant SÚJB requirements and recommendations for the field of ensuring nuclear safety and quality assurance, given in corresponding IAEA documents, IEC standards and industrial standards (CSN, ISO or complementarily IEEE).

2.2. Describe how DI&C is captured in the licensee technical basis.

Regulatory review process and guidance for evaluating the safety of a plant modification based on digital technology:

I&C Licensing Documentation

Dukovany I&C Innovation licensing assessment was based on a set of licensing and supporting documentation, prepared by licensee (Dukovany Nuclear Power Plant) and/or supplier (Consortium Škoda JS, FRA, SEI, ZAT), continuously updated in accordance with I&C development and SÚJB requirements.

The documentation set included:

- Supplement of Pre-Operational Safety Analysis Report (POSAR-PpBZ), with structure corresponding RG 1.70, mainly:
  - Chapter 7 (I&C)

  - Chapter 15 (Accident Analyses)
  - Chapter 16 (Limits and Conditions)
  - Chapter 18 (Quality Assurance)
- Transverse Topical Reports for
  - Classification of I&C Systems
  - Acceptability of Digital Computer-Based I&C (Systems Important to Nuclear Safety)
  - SW Development (Systems Important to Nuclear Safety)
  - SW Verification and Validation
  - Defence against SW CMF
  - Communications
  - Testability
  - Single Failure Criterion
  - Qualification
  - Reliability
  - Test Strategy
- Individual Topical Reports for
  - I&C Architecture of the Modernised Systems
  - Protection System (Reactor Trip System + Engineered Safety Features Actuation System + Emergency Load Sequencer)
  - Post Accident Monitoring System (PAMS)
  - All other Instrumentation Systems required for Safety (Supporting Action System + Reactor Limitation System)
  - Safety-Related Control System
  - Reactor Control System
- Specialised Quality Assurance Plans and Reports
- Programmes and Protocols from On-site I&C Installation (required for SÚJB Approval)
- Additional Documentation
  - Supplier's Position Papers to specific Issues
  - Detail Design Documentation (selected parts)
- Licensing Procedure

Regulatory body Approval Process was formerly guided by the Standard Review Plan NUREG 0800, transformed to Database of Licensing Issues. The Database included:

  - Issue specification, referencing to applicable standards
  - References to information sources

- Result of the Issue evaluation (Findings) and its status
- Specification of open problems in findings and actions for their solution (Request for Additional Information)

Database was organised in three levels:

- Sections of assessment criteria for digital I&C Subsystems (General, DRPS, ESFAS, ELS….)
- Accomplishment of the Review Topics (completeness, design criteria adequacy, defence-in-depth, SW life cycle...)
- Accomplishment of detail criteria for each Review Topic.

It means, the criteria were selected to groups from third to first level. Each criterion was assessed individually as an issue, the result of this evaluation (finding), the status of the issue ("open" - "closed") and the action for resolution (RAI) was be recorded to the database.

The results of the communicative RAI Process between SÚJB and Licensee were finished by completing of the RAI and adequate responses to separate licensing document. If necessary, the results had to be implemented to next revisions of the SAR or Topical Reports and (generally) to Design, Workshop and Assembly documentation.

Documents Issued by SÚJB

- Set of SÚJB Positions to Selected Aspects…

was issued on the basis of preliminary information about the Licensee intentions

- SÚJB Statements to Safety and Design Documentation

were issued to each set of documentation, handed over to SÚJB for each step of the Dukovany Nuclear Power Plant I&C Innovation Project

- SÚJB Decisions
  - Reconstruction Licence were issued on the basis of the "Licensee Application for the Reconstruction Licence…", handed over to SÚJB with enclosures corresponding to demands of the Atomic Act.
  - "Licence for re-start of a nuclear reactor to the critical condition after refuelling", handed over to SÚJB with enclosures corresponding to demands of the Atomic Act, were issued after receiving of documents proving the equipment and personnel to be ready for re-start of the nuclear reactor to the critical condition, including assessed evaluation of in- service inspections. All conditions of the Reconstruction Licence had to be accomplished.
- SÚJB Safety Evaluation Reports
- Database - ISSUES to Chapter 07
- RAI Status Record

These documents were used as supporting documents for demonstration of independent licensing (assessment and inspections) of innovated I&C System.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

In the independent licence documents, the following had to be clearly and sufficiently shown:

- For the area of control aspects:
  - V&V process general description
  - organisation aspects
  - rights and responsibilities
  - methods for management of risks related to the V&V activities
- For the area of implementation aspect:
  - assessment of the V&V process
  - specification of individual V&V tasks, procedure specification, specification of necessary inputs and required outputs from each task, necessary sources, work schedule, discrepancy addressing methods
  - documentation on V&V activities
- For the area of sources aspects:
  - description of methods, HW and SW tools for the V&V activities in individual stages of the life cycle
  - description of the methodology to carry out testing at the level of basic software components and at various levels of the software integration, methodologies to testing for the implementation of software modifications
  - summary of standards and other regulations that will govern the process

Audits - at the prime contractor and significant subcontractor to verify processes for the design and manufacturing of the I&C equipment.

FAT tests

SAT tests

Inspection during outages

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Yes

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Assessment a set of licensing and supporting documentation, prepared by licensee and/or supplier, continuously updated in accordance with I&C development and SÚJB requirements.

As observer during audits, which were performed at the various stages in the upgrade process:

- Design Requirements Audit
- Hardware and Software Design Audit
- Manufacture and Test Audit

Witnessing FAT tests SAT tests

Inspection of Installation during outages:

- Equipment Qualification documentation
- Configuration Management
- Updating of related documentation
- Impact assessment of the modification on human factor
- Protocols of installation tests, including operational tests

These types of inspections were performed by staff of RB (I&C and electro) with support by TSO.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

OJC316 project: "Licensing Related Assessment of Digital Computer Based Technology for I&C Important for Safety", within which experience of EU supervisory bodies was transferred to countries preparing themselves for joining EU (CR, Hungary).

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

SÚJB Statements to Safety and Design Documentation were issued to each set of documentation, handed over to SÚJB for each step of the Dukovany Nuclear Power Plant I&C Innovation Project

SÚJB Decision - Reconstruction Licence were issued on the basis of the "Licensee Application for the Reconstruction Licence…", handed over to SÚJB with enclosures corresponding to demands of the Atomic Act.

Corrective actions identified in previous audits were assess and inspect.

Licence for re-start of a nuclear reactor to the critical condition after refuelling", handed over to SÚJB with enclosures corresponding to demands of the Atomic Act, were issued after receiving of documents proving the equipment and personnel to be ready for re-start of the nuclear reactor to the critical condition, including assessed evaluation of in-service inspections. All conditions of the Reconstruction Licence had to be accomplished.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

It means for examples digital sensors, firmware, …

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

Individual I&C systems are of varying importance from the nuclear safety point of view. The higher importance a system is for the nuclear safety, the more demanding criteria are required to apply to grant licences for design, realisation and operation. Therefore, logically, the licensing process focuses on most important systems and relatively less attention is devoted to less important systems. This corresponds to classification of I&C systems per their importance for nuclear safety that has been applied to grade requirements on design and quality assurance of these systems.

Specific criteria

- description and justification, which shall ensure the fulfilment of design function of that equipment, where there is a risk of breach;

- use, especially in nuclear power plant/military/aviation applications;
- operation assessment;
- diagnostics, monitoring of failures;
- impact assessment on nuclear safety, radiological protection, technical safety, radiation situation monitoring, radiological emergency management and security, including this impact assessment reasoning;
- quality assurance;
- methodology of carrying out and demonstrating the I&C equipment qualification;
- results of the qualification activities and documentation of the fulfilment of qualification requirements;
- maintenance;
- functional tests.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Must be clearly and sufficiently shown at least the following:

- methodology of carrying out and demonstrating the I&C equipment qualification in the following areas:
  - qualification for the conditions of the surrounding environment (climatic conditions, mechanical conditions, radiation);
  - seismic qualification;
  - electromagnetic compatibility;
  - results of the qualification activities and documentation of the fulfilment of qualification requirements.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Generally for the lifecycle of SW safety systems of I&C Category A important for the nuclear safety (that means development, installation, operation and maintenance) that this must be well-structured process, during which the three following groups of activities are performed:

a) Planning

Outputs of these activities are documents used for the purpose of control and check during the whole software lifecycle. It is required for SW lifecycle to plan and describe items described in the following documentation:

- Software Project Management Plan
- Software Quality Assurance Plan
- Software Verification & Validation Plan
- V&V Software Configuration Management (CM) Plan
- Software Safety Plan

- Software Development Plan
- Software Integration Plan
- Software Installation Plan
- Software Training Plan
- Software Operations Plan
- Software Maintenance Plan

b) Development and Operational Activities

These activities include: SW requirements specification, SW design specification, programming activities, SW integration and SW-HW integration, validation activities, installation in the location of user, maintenance, operation and maintenance by user. Output documentation on products of the development process and documentation needed to perform operational activities is generally contained in the following complex of documents:

- Software Requirements Specification
- Software Requirements Specification
- Code Listings
- System Build Documents
- Installation Configuration Tables
- Operations Manuals
- Maintenance Manuals
- Training Manuals

c) Cross-Sectional Activities

These activities cover V&V, configuration maintenance and risk analyses fields. Performance of these activities is an integral part of each phase of SW lifecycle; completions and results must be appropriately documented. The subject-matters of these activities and associated procedures are specified in pertaining plans, see item a). Outputs of these activities are contained in the following documentation:

- Safety Analysis Reports
- V&V Reports
- CM Reports

This complex documents realisation and results of cross-section activities performed in the following phases of SW lifecycle: requirements specification, design specification, design implementation, integration, validation, installation, operation and maintenance.

The above-mentioned principles apply for the newly developed SW. For the SW developed earlier, already licensed, and used, only relevant requirements will apply for the purpose of the EDU I&C renovation project.

In relation to the project of renovation of EDU I&C Category B safety-related systems, SÚJB has arrived to the following position (applies in the case when renewed systems will be realised on the basis of freely programmable means of digital technology).

Category B safety-related systems must meet SW requirements applicable to high-quality industrial control and monitoring systems.

In relation to the project of renovation of EDU I&C Category C safety-related systems, SÚJB has arrived to the following position (applies in the case when renewed systems will be realised on the basis of freely programmable means of digital technology).

Requirements on development process and subsequent lifecycle phases of SW, which provides or participates in providing of Safety Category C functions must be the same as those applied to high-quality industrial control and monitoring systems.

In the independent licence documents (having the form of topical reports with revisions issued as the need may arise, extending and amplifying the provided information), at least the following has to be clearly and sufficiently shown:

- Structure specification and pertinent content of the SW development process for meeting the functions of the safety categories A, B and C, including the definition of the format and contents of the documentation that has to be produced in individual stages of the SW development process.
- Specification of the pertinent content of the following stages of the SW life cycle and of the documentation that will belong to the stages.

In addition to that, the following is required for the needs of the approval process:

- Participation of SÚJB staff in audits of the SW development process in the role of observers.
- Submission of information on some outputs of the activities carried out during the development process (in the course of performed audits).
- Submission for review of summarising reports on V&V activities, CM activities and activities from the areas of risk analyses (hazards) carried out during the SW development process, providing for or participating on the ensuring of the safety category A functions(in compliance with the schedule of the licensing process for the systems that will be installed and commissioned or put into permanent operation within the given renovation stage).

Requirements for V&V software:

- For the complete development process and the following stages of the SW life cycle of the renovated I&C safety category A systems, the implementation of the V&V process meeting requirements of the IEC 880 standard is required.
- Not required is the implementation of V&V activities by a so called third independent organisation assuming that the group carrying out the activities at the manufacturer's is in no way interested in the development process of the verified software.
- From the first moment of the commencement of the SW development process on, carrying out V&V process audits is required.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

The documentation to be provided where the activity to be licensed is the carrying out of modifications affecting nuclear safety, technical safety and physical protection of a nuclear installation is as follows:

1. management system programme;
2. description and justification of the modification;
3. timetable for the implementation of the modification;
4. draft update of the documentation for other licensed activities, if affected by the modification;
5. assessment of the effect of the modification on nuclear safety, technical safety and security;
6. document demonstrating that safe radioactive waste management has been ensured, including the financing thereof, if radioactive waste is generated.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Individual I&C systems are of varying importance from the nuclear safety point of view. The higher importance a system is for the nuclear safety, the more demanding criteria are required to apply to grant licences for design, realisation and operation. Therefore, logically, the licensing process focuses on most important systems and relatively less attention is devoted to less important systems. This corresponds to classification of I&C systems per their importance for nuclear safety that has been applied to grade requirements on design and quality assurance of these systems.

A licence/statement from the Office shall be required for the carrying out of modifications affecting nuclear safety, technical safety and physical protection of a nuclear installation

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

General:

The platform was developed using the recognised nuclear standards, practices and regulatory framework applicable in the country in which it is to be used, or any deviations from the recognised nuclear standards, practices and regulatory framework are identified and justified.

Specific criteria:

- demonstration of an accredited quality management system;
- assessment of necessary resources to support the qualification;
- access to all artefacts necessary to complete the qualification, including those from sub-suppliers and certification bodies;
- confirmation of the continued support of the platform;
- a justification of the method or combination of the methods used for the qualification:

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

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

Equipment important for the nuclear safety for which the qualification is required are:

1. Safety I&C systems equipment for which maintenance of the functional ability is required under conditions of the design basis accidents and seismic events as well as after their fading out to provide for safety functions (e.g. reactor trip and providing for the subcriticality, reactor cooldown and ensuring the residual heat removal, providing for the primary circuit integrity, providing for the secondary circuit integrity in the scope necessary for the cooldown, prevention of leakage of the radioactive substances into the outer environment).
2. I&C equipment that is not a part of the safety systems but the damage of which under conditions of the design basis accidents and seismic events could prevent satisfactory fulfilment of the above shown safety function.
3. Equipment of the system for the unit monitoring during and after the accident conditions occurrence.

The nuclear power plant operator has to have a programme for the determination and maintenance of the equipment qualification important for the nuclear safety that should include:

a) I&C equipment qualification for the defined operation conditions in places of their location.

b) Seismic I&C equipment qualification.

The required qualification programme of equipment important for the safety is a process including activities in three stages:

1. preparation of the programme and of its design inputs;
2. performance of the qualification;
3. maintenance of the qualification till the end of the nuclear power plant life.

All activities of Following information has to be available for individual pieces of equipment of the list:

- specification of the characteristic equipment activities necessary to fulfil the system safety functions and period for which those activities will be required during the specified operational conditions;
- environmental conditions, in particular pressure, temperature, radiation, chemical influences, potential of flooding, seismic acceleration of the location at which the equipment has to perform the required activities;
- working conditions, in particular electric power supply, mechanical stress and electromagnetic interference.

The equipment qualification programme must include the assessment of effects of the following conditions:

1. Temperature and pressure. It is necessary to start from the temperatures and pressures in the course and after the fade off of the design basis accidents for a period of the required functional ability.
2. Humidity It is necessary to determine and consider the effect of humidity that can occur during the design basis accidents.
3. Chemical effects. The chemical composition of the environment media used for the qualification has to be at least equally aggressive as the media that may occur under worst operation and accident conditions of the nuclear power plant (e.g. sprinkling of the hermetic zone, emergency cooldown, make-up and let-down mode).
4. Radiation. The radiation environment should be determined by the radiation type, dose rate, total expected dose at normal operation from the equipment installation and at the maximum design basis accident during which the equipment should stay functional.
5. Ageing. For the equipment located in harsh environment with identified important ageing mechanism, qualified life should be determined. The ageing mechanism is considered significant from the point of view of qualification if it leads under normal and abnormal operation conditions to increasing damage that considerably increases its susceptibility to failure at accident conditions.
6. Flooding (if the equipment can be flooded).
7. Seismic load.
8. Mechanical load (by a medium jet).
9. Co-operant effects. It is necessary to take into account mutually influencing effects if they can have a significant impact on the equipment performance.
10. Working conditions such as electric power supply, electric loads, electromagnetic interference.
11. Safety reserves. Safety reserves have to be used at type tests so that they include the unquantified uncertainties such as the effects of the manufacturing tolerances and inaccuracies of the measuring devices.

Equipment subject to qualification must be qualified by one of the following methods:

type tests, operational experience, analysis or combination thereof.

It is recommended to develop a programme that includes:

- maintenance;
- spare parts and their procurement;
- conditions monitoring (surrounding environment);
- diagnostics, monitoring of failures;
- operation assessment;
- quality assurance;
- maintenance of the documentation;
- personnel training.

All activities related to the preparation, performance and maintenance of the qualification must be performed in accordance with plans of quality assurance

From the point of view of acknowledging the certificates on performed qualification, a certificate will be considered acceptable issued by a peer authorised or accredited organisation or person certifying that the given equipment fulfils all qualification requirements. the required programme must be carried out in compliance with an introduced quality system.

In these "licence" documents (with revisions issued as needed, that extend and deepen the provided information), it must be clearly and sufficiently shown at least the following:

- methodology of carrying out and demonstrating the I&C equipment qualification in the following areas;
- results of the qualification activities and documentation of the fulfilment of qualification requirements.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Individual I&C systems are of varying importance from the nuclear safety point of view. The higher importance a system is for the nuclear safety, the more demanding criteria are required to apply to grant licences for design, realisation and operation. Therefore, logically, the licensing process focuses on most important systems and relatively less attention is devoted to less important systems. This corresponds to classification of I&C systems per their importance for nuclear safety that has been applied to grade requirements on design and quality assurance of these systems.

Configuration Management (CM) Plan

This document specifies organisational aspect and authorisations and responsibilities in the field of CM activities, identifies CM activities, (identifies configuration items, configuration management, method of presentation of requests for changes, approval of such requests, implementation and check of changes, configuration audits, check of subcontractors, etc.), methods, procedures and tools to perform CM activities, and also required CM activity documentation.

Configuration Tables

These documents define SW/HW configuration installed at user's place. They must assure that such configuration is a complete, correct, consistent, traceable and verifiable implementation of requirements on the subject and does not inject new risks and possibilities of unauthorised interventions.

Inspection activities:

- which results in the removal of the non-conformity identified on selected equipment, which shall ensure the fulfilment of design function of that equipment, where there is a risk of breach or where there is a breach of the Limits and Conditions or any non-conformity is identified in the course of planned maintenance, prior to start of the modification;

- impact assessment of the modification on nuclear safety, radiological protection, technical safety, radiation situation monitoring, radiological emergency management and security, including this impact assessment reasoning;
- management system programme;
- description and justification of the modification;
- timetable for the implementation of the modification;
- draft update of the documentation for other licensed activities, if affected by the modification;
- assessment of the effect of the modification on nuclear safety, technical safety and security;
- impact assessment of the modification on human factor.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

An extremely important part of digital I&C systems is the data transfer equipment within divisions of protection systems (i.e. between subsystems of a division), between redundant divisions, between protection systems and other SS, and between SS and systems of lower safety classification.

The principle requirement for the communication equipment design is to prevent its activities (data transfer, data receipt acknowledgement, transfer error detection) from loss of capability to provide assigned safety functions. In this respect, a special attention must be paid to a correct method of detecting and restoring any communication errors.

Ensuring the communication independence

SÚJB, as a minimum, require for the communication links an adequate proof of meeting the following basic requirements:

- A failure of the protection system or of its subsystem **within a single division** (i.e. both the corresponding HW and SW) must not affect the performance of safety functions in the **redundant divisions**.
- The communication loss between the divisions must not cause an interruption of the performance of the target division (e.g. due to waiting for a valid input signal).
- Possible data sharing (including the input signals) must not violate the functional separation of the individual redundant divisions.
- Performance of the safety functions in any division of the protection system must not be affected by a failure in any other SS or in a system of a lower safety classification with which the protection system communicates.

It has to be added to the above shown that SÚJB does not consider a violation of the functional divisions separation if:

- each of them has an access to all redundant input signals;

- at the signal input to the divisions, such selection algorithm of the resulting signal is individually implemented that eliminates the influence of the potential single failure of the preordered modules (e.g. of an analogue/digital converter).

SÚJB is conscious of certain advantages of such arrangement (it makes it possible for the system to deal with the sensor failures more easily).

Implementation On-line Diagnostics (OLD) in the area of communications

SÚJB requires that all communication links implemented in the SS and in the I&C systems important for the safety to be equipped by adequate OLD means (including the so called Deadman Timers) that continually check the operability of the connection and, if they detect its failure, actuate the proper corrective actions of the systems and alarms.

Application of the "fail-safe design principle" in the design of the communication links

At all places where practically feasible, the protection systems must respond to the loss of communication or to the worsening of its quality by an accurately defined action that will be in compliance with the requirements for the nuclear safety applicable for the system in question (RTS and ESFAS).

Specific documentation required in the frame of the licensing process:

- Lucid diagrams of communication links and description of their tasks. In the diagrams, all links important for the data transfer should be marked in the frame of the divisions of the protection systems, between the redundant divisions, between the protection systems and other SS, and, finally, between the SS and the systems with a lower safety classification.
- Furthermore, it is necessary to describe the make of those links (e.g. show that they are optical or electrical buses with properties), and to characterise the data they transfer.
- Basic information on OLD of the communication links.
- If purposeful, describe the methods of OLD performance and types of the applied Deadman Timers generally and, then, identify the procedures applied here for the individual links.
- The summary information on the use of the "fail-safe design principle".
- Here, it is necessary to describe in sufficient detail the "fail-safe" method by the response of the protection systems to individual failures of the communication links detected by the OLD in particular from the point of view of fulfilling the requirements of the single failure criterion.
- Results of the analysis of the fulfilling the requirements given in the part "Ensuring the communication independence".

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Full operability of the SS, and to a lesser extent of the systems of the safety category B by IEC 61226, must be verified so as to be in time identified their potential failures that could prevent their performance of the safety important functions.

Operational manuals - specify all activities required from the I&C system operators under all operational modes including recovery after a failure or substitutional action. Each function is described in terms of its purpose, performance, and interface to other functions and its user. They specify also environment for such I&C to be operated and provide explications for each system error report and instructions to handle such situation.

Maintenance Plan - specifies methods, procedures, and tools to detect and remove errors of the installed I&C, record findings and their solutions, protocol regressive tests.

Maintenance manuals - specify all activities required from the I&C system maintenance personnel. They describe procedures for performance of corrections of errors.

Every day Systematic information on correction actions initiated due to detection of various failures (if any) are sent to RB. For evaluation are use:

Limits and Conditions (Technical Specifications); I&C related part.

Corrective actions

Trending analysis

Possibility of CMF.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

NO

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

Typical failure modes for example: input/output connector, interior of cabinet cooling.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

Full operability of the SS, and to a lesser extent of the systems of the safety category B by IEC 61226, must be provably and comprehensively verified so as to be in time identified their potential failures that could prevent their performance of the safety important functions.

In principle, this requirement may be implemented by a combination of several various overlapping activities:

- By a continual automatic performance of the so called on-line diagnostics (OLD) of the HW SS state (including the communications means). OLD may be implemented in a larger scope only in digital, freely programmable SS.
- Continual “manual” or automatic monitoring of the consistency of the redundant signals by which SS sensors and their transfer routes statuses are checked in the first place.
- By means of an automatic (or manual with the non-digital SS) periodic testing (PST) under unit operation conditions that is usually performed with a period of about 1 month per one redundant SS division.
- By manual testing of the remaining SS parts (e.g. means of the manual control, Reactor Trip Breakers (RTB), control circuits of the ESF components, etc.). If any

of these tests may not be performed under power operating conditions of the unit, they can be limited to the period of reactor shutdown.

All periods of the above shown tests must be specified in the Technical Specifications and have to be substantiated by the results of the SS reliability analyses that have to prove that the potential existence of the shown failure for a maximum possible time interval (prior to its detection) will not endanger keeping the target values of the SS preparedness.

Possibility and necessity of the installed SW functions correctness verification at reactor operation.

- SÚJB does not expect that SW functions correctness of any digital system may be in some significant way verified at routine PST, and, therefore, does not require meeting of such goal by the PST.
- On the other hand, SÚJB has to persist that the intactness of memory areas where SW is stored (including all necessary data) should be checked in the frame of the OLD, and, hereby, it should be verified that no its damage occurred due to HW failure (which is not the only possible mechanism of the SW degradation).

Note:

If a doubt exists about the installed SW correctness it will be addressed by an additional V&V, including its extended testing carried out under corresponding "laboratory" conditions.

Required OLD concept and tasks.

SÚJB expects that OLD will consist of three parts:

- Complete diagnostics of the HW functions and status correctness and **the configuration** of the inserted SW at the SS commissioning and restarts.
- Continual diagnostics functions and HW status, carried out in batches in each processor basic operating cycle so that the complete HW status (i.e. processor functions correctness, intactness of all memories, etc.) is verified within ca. 10 minutes.
- OLD of the communication means carried out on the basis of diagnostic information included in the messages transferred by them, and in a maximum possible extent supported by the implementation of the so called Deadman Timers (registering the connection interruption etc.).

Furthermore, it has to be proved that the SS will respond to detected problems immediately in an automatic manner in compliance with the requirements for the operations safety and in accordance with the extent of the arisen risk and, of course, without unacceptable frequency increase of the false protection actuations

PST tasks and conditions of its complete omission.

The SÚJB requirements for PST are as follows:

- PST has an obligation to test only those HW components of the SS itself (in the narrower sense, i.e. except for sensors, RTB and connection to ESF) that participate on carrying out individual protection functions **and OLD**, and the status of which is not provably fully verified by OLD or is not tested fully in manual).
- If it will be demonstrated that such HW components do not exist (i.e. OLD is complete without any justifiable exception), then the automatic PST may be completely cancelled.

Requirement to meet the criteria of the single failure (SFC) during the PST.

Decree SÚJB does not permit unfulfilment of the SFC in any operating conditions, and, therefore, neither during the PST. However, SÚJB accepts that functional diversity implemented in the Primary Protection System should be used for the prove of meeting SFC during the PST. The SS and its PST proposal have as well fulfil the requirement of the decree since the injection of the testing signals at PST means, as a matter of fact, putting the tested channel out of operation.

Measures for provision for correct SS transfer between PST and the mode of normal operation (should the PST be implemented).

SÚJB requires that the switch-off of real SS input signals and their replacement by injected testing signals and vice versa necessary for the PST accomplishment does not require manipulation with the sensors connected to the SS and with links between its redundant divisions.

An extraordinary attention should be paid at it to measures ensuring the correct SS return to normal operation after completion of the PST.

Specific documentation required in the frame of the licensing process

- Description of the proposed OLD and PST concept (if the PST is considered necessary), from which will proceed the designer.
- SÚJB does not principally exclude the possibility of deviations from their position, formulating the concept in an as early as possible project stage is necessary for the timely review of its acceptability.
- Detailed description of the OLD and PST means and methodology (including diagnostics of communication links and means used at PST). Its integral part must be (if applicable) :
    - Sufficiently detailed analysis of the completeness of the HW components status and functions verification by means of OLD, PST and other tests that will possibly prove the possibility of cancelling the PST.
    - Systematic information on correction actions initiated due to detection of various failures at OLD.
    - Proof of meeting the requirements of the SÚJB Decree and confirmation of the sufficiency of the measures related to transitions between the normal operation and PST.
    - Documentation with a description of the methodology and results of the accident analyses, carried out in the frame of proving the meeting of SFC in the course of PST (if such additional analyses will be necessary).

The corresponding parts of the Technical Specifications then will determine and, together with the documentation of the reliability analyses, adequately justify the frequency of all performed tests of the I&C operability

11.2. What kind of functional tests does your RB inspect? Please describe.

Inspection are provided by inspection manual for I&C, or inspection manual for modifications. Inspections are focused on most important systems (by IEC 61226):

Assessment of Periodic test reports

Selection of periodic tests for witnessing during operation and/or outage

Tests after some modification

Finland

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes. For OL3, almost all I&C systems are digital. For operating plants, some I&C systems have been refurnished to software-based ones, e.g. reactor protection systems, turbine I&C, auxiliary process I&C systems.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

All I&C systems must be qualified. Qualification process must address applicable standards, design process, manufacturing, different levels of tests, organisation performing the qualification (licensee, supplier, 3rd party), analysis and when applicable, operating experience. Criteria are based on IEC standards. Suitability to the specific plant must be demonstrated.

After final suitability analysis is approved (IEC class 1) or reviewed (IEC class 2) by RB, I&C can be delivered to the site and installed. After RB has approved the commissioning test results, the I&C system or component can be taken to nuclear operation.

2.2. Describe how DI&C is captured in the licensee technical basis.

We do not understand the question.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

RB inspects all systems independent of the technology.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

RB has possibility to inspect all stages of I&C systems. Typically manufacturer/designer management system audits performed by licensee are observed. System design stage may be inspected and factory acceptance tests are observed. On-site testing is also observed.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

See 3.2. Inspections are lead and/or performed by I&C inspectors. Management system inspectors may be used for large management system inspections.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

Inspections are lead and/or performed by I&C inspectors. RB uses internal training programme to qualify inspectors.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

System level and system functions are inspected separately from component level. System level inspection is based on system's pre-inspection documentation. Component level inspection is based on preliminary and final suitability analysis. I&C platforms are inspected like components.

Systems and components are inspected separately because they are inspected by different experts and they are defined in different life cycle phases.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Yes. For example flow metres, temperature transmitters, protection relays, time relays.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

Licensee's are required to perform installation inspection by regulatory guides. RB does not inspect installation. Storage of configuration data and cyber security aspects are inspected as licensees' management system processes, but not related directly to any single digital device.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Same regulation about suitability analysis applies for all devices. If device is software based or programmable logic based, the programme part must comply to relevant international standards and its suitability must be evaluated. For highest safety class, 3rd party type approval organisation performs the evaluation as part of type approval, and for other safety classes licensee must perform the evaluation.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

RB inspects licensees' change and configuration management, maintenance and ageing management processes. Related cyber security methods are also inspected.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Commercial grade equipment are handled as other equipment. There are no different qualification requirements.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

RB does not have to authorise commercial grade dedication process, but licensees may ask RB's informal comments to the process before applying it. See 6.1. Software qualification is based on IEC standards, e.g. IEC standards 60880/62138, or 61508.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

See 6.1 and 6.2.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

All safety classified I&C systems and components must be qualified. Qualification process must address applicable standards, design process, manufacturing, different levels of tests, organisation performing the qualification (licensee, supplier, 3rd party), analysis and when applicable, operating experience.

System level and system functions are qualified separately from component level. Licensee must demonstrate system level suitability in system's pre-inspection documentation.

Component level qualification is based on preliminary and final suitability analysis. Component selection and possible additional testing are documented in preliminary suitability analysis. Quality and performance of the component are demonstrated in the final suitability analysis.

Environmental, EMC and seismic conditions must be tested by accredited independent laboratories. RB reviews the test reports which are part of the final suitability analysis.

Software evaluation is part of final suitability analysis.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

For highest safety class (IEC Cat A) compatibility is assessed by accredited type approval organisation. RB reviews type approval report which is part of the final suitability analysis. For other safety classes, licensee is responsible to perform or to buy the verification work. Verification results are part of the final suitability analysis.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

For highest safety class (IEC Cat A) compatibility is assessed by accredited type approval organisation. RB reviews type approval report which is part of the final suitability analysis. For other safety classes, licensee is responsible to perform or to buy the verification work. Verification results are part of the final suitability analysis.

RB requires that hardware components must be re-evaluated if:

- the performance values of the spare part related its safety function have deteriorated;
- the spare part deviates in terms of the way of function, any software part or structural characteristics from the original;
- the spare part does not match the original part in terms of environmental condition endurance;
- the quality management level of the spare part does not fulfil the original level;
- the manufacturer of the spare part has changed.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Inspection criteria depends mainly on safety classification. Communication features do not have effect on inspection criteria but they are reviewed as part of I&C architecture review.

Review criteria are presented in YVL B.1 chapters 4 and 5.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

All events are processed in same way. So far events related to DI&C have been so rare, that special analysis methods have not been applicable.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

A few:

- Floating point variables were used to handle time. Rounding errors led to diverging times in different parts of the system.
- Use of wrong type of memory elements led to latch up of redundant parts of control rod drive system.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

RB evaluates loss-of and spurious actuation type failure modes.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

DI&C systems must support periodical testing (self diagnostics and/or manually performed periodical testing).

See also 5.1.

11.2. What kind of functional tests does your RB inspect? Please describe.

RB observes most important functional tests during outages.

France

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

I&C's architecture can be divided in three levels. The level 0 is composed of sensors and actuators. Level 1 is dedicated to the treatment process, and is basically composed of acquisition systems, algorithms and logic calculations. Level 2 is dedicated to human-

machine interfaces. The digital technology is largely used in French nuclear power plants I&C systems at every level, except at the level 0 where only a few embedded equipment are digital. The EPR of Flamanville uses several DI&C systems/components important to safety such as:

- PS system, which ensures the automatic functions of protection and safeguarding (automatic reactor protection system, automatic control of safeguarding functions);
- SAS system, which manages the installation after an accident. PWR of the 2nd generation use also DI&C systems/components, for instance:
  - The CP0 and CPY (900 MW series) neutronic instrumentation system is in digital technology (34 reactors).
  - The P4 and P'4 (1 300 MW series) reactor protection system (performing reactor trip and ESFAS) is in in digital technology (20 reactors).
  - The N4 (1 450 MW series) reactor protection system (performing reactor trip and ESFAS) is in in digital technology (4 reactors).

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

The installation and use of DI&C systems should respect the decree of authorisation of creation and reach the objectives fixed by safety rules.

Amongst the criteria on which ASN authorises or not the installation and use of DI&C systems, we have:

- the classification of the systems;
- the impossibility for a system to influence a system with a higher classification;
- the diversity and redundancy in safety systems;
- the three main principles for the conception of calculators in safety systems, which are the prevention of bias errors, the clearance of errors and the tolerance of defaults;
- the predictability of the results;
- the determinism of working parameters for DI&C systems (calculation time, memory needed);
- the robustness of the solution;
- the guarantee of having a long term documentation, which stays complete and usable.

In France, for pressurised water reactors, RFS II.4.1.a [Basic Safety Rule II.4.1.a, safety software] deals with the requirements that apply to software, in particular those relating to determinism and predictability that play a key role in the design of safety software. RFS I.3.a [Basic Safety Rule I.3.a, single failure criterion] deals with the use of the single failure criterion and RFS IV.2.b [Basic Safety Rule IV.2.b, electrical systems] with the requirements that apply to safety-classified electrical equipment.

More precisely, we define a computation as deterministic only if its outputs (values and dates):

- are computed in a repeatable and known way;
- depend only on the specified inputs.

Requirements are detailed in:

- IAEA SSG-39 safety guide;
- IEC/45A standards such as:
  - IEC61513 for I&C architecture and main requirements;
  - IEC60880 for class 1 software;
  - IEC62340 for common cause failure.

In practice, the licensee has to communicate all design documents to ASN and IRSN, following a schedule fixed by ASN. For each classified DI&C system, these documents concern both I&C platform and application system. Amongst the requested documents, we can find:

- the system quality plan;
- the software quality plan;
- the functional diagrams;
- the specifications;
- the requalification programme;
- the test programme;
- the report of the system validation review;
- the reliability analysis of the software;
- the synthesis of the actions and results of the surveillance over the subcontractors.

2.2. Describe how DI&C is captured in the licensee technical basis.

For each nuclear installation, the Safety Analysis Report is the main licensee technical document where the chapter 7 is related to the I&C. The I&C architecture as well as safety objectives are described. All other documents issued from the development and validation process may be used by licensees to demonstrate objectives achievement.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

I&C systems constitute an inspection topic identified by ASN. This topic includes both digital and analogue I&C.

Before giving an authorisation to the licensee, the conception of DI&C is analysed, to make sure that the criteria listed at the question 2.1 are respected. In order to do that, ASN, with the technical support of IRSN, performs a technical detailed design review, based on documents listed in 2.1.

Once the licensee is authorised to implement a DI&C system in its installation, ASN can inspect on nuclear power plants the installation, test, use, maintenance and condition of the system. Inspections are usually divided into two parts. The first one is more about

documentary control. Inspectors question the licensee and evaluate the documentary basis to control:

- the test execution statements;
- the analysis and treatment of deviations encountered;
- the maintain of qualification;
- the integration of modifications;
- the risk analyses;
- the contracts with clients and external providers;
- the surveillance programmes and statements.

The second part of the inspection is in the facilities where DI&C systems are located. Inspectors control the smooth running of the tests, the respect of security requirements. Moreover, inspectors pay attention to the environment of DI&C systems (temperature, humidity…).

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing)?

Every stage, except the off-site manufacturing abroad, can be controlled by ASN. If necessary, ASN can have access to the results of the tests and quality controls made by the manufacturer.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

The way the licensee is inspected is described in 3.1. The inspection can be focused on particular points which are evaluated on several systems, or the inspection can be focused on a particular system where several points are evaluated. For example, half of an inspection can:

- have a large scope, by doing sampled analysis on documents related to DI&C;
- be dedicated to a specific modification of a DI&C system;
- be dedicated to the tests in progress at the day of the inspection.

The inspection team is usually composed by 2 to 4 persons, ASN inspectors are usually supported by IRSN experts. For example, IRSN helps ASN to understand recent events analysis or periodic test results. ASN decides which requests they will do to the licensee.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

There is no specific train for inspectors to inspect DI&C systems/components. However, it is possible for inspectors to apply for specific trainings which can be offered by schools or companies. The favoured ways to learn how to inspect DI&C components remain the review of previous inspections, and the companionship. Also, being supported by an expert from IRSN reinforces the ability to inspect DI&C systems/components.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

In France, inspections on a specific technical field last generally one day. I&C is one of these technical fields and for a nuclear site, it has to be covered at least every 3 years.

During the day, we generally cover a maximum of I&C systems whatever if they are digital, analogue or relay based.

The inspection team can chose to inspect DI&C systems/components separately or not. Even though ASN can inspect vendors (as subcontractors of the licensee), ASN would rather inspect the licensee because, according to the regulation, the licensee is responsible for the safety of its installation, and has to oversee the manufacturing process of the components composing its nuclear power plant.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

In France, for operating reactors, digital devices with limited functionalities are not used for the highest classification (C1, CEI classification). They are more and more used for systems classified C3, and carefully on C2 systems. They are used in replacement of analogue devices that become unavailable on the industrial market.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

As they will be used soon for the highest classification for EPR, IRSN reviewed the qualification of these devices. The requirements are similar to those related to DI&C systems, in particular on the process, (design, verification, validation), the design principles, the operating experience, the use in the reactor. However, one model of digital devices has a very limited role in the realisation of safety functions. The safety requirements are thus adapted and for the Flamanville EPR, the licensee provided a supplement qualification file covering the related requirements for each model.

For the future projects or replacements, licensee want to use the industrial standard CEI61508 for its process review with a classification equivalence (C1=SIL3, C2=SIL2, C3 = SIL1) supplemented by vendor inspections. This process is still under discussions and the role of ASN and IRSN in these inspections is not yet defined.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

The process of modification and maintenance of software can be divided in two phases. The first one is before the authorisation of modification/maintenance of the DI&C system/component software. The second one is between the authorisation and the implementation of the updated DI&C system/component software.

The licensee has to apply two years before the scheduled date of implementation, by sending a background note to the regulator. Then, following a schedule fixed by ASN, the licensee should communicate specific documents to ASN. Among the requested documents, we can find:

- the system quality plan;
- the software quality plan;
- the impact assessment to identify the necessary tests to the validation of the version and its “non-regression”;

- the functional diagrams;
- the specifications;
- the requalification programme;
- the test programme;
- the report of the system validation review;
- the reliability analysis of the software;
- the synthesis of the actions and results of the surveillance over the subcontractors.

Licensees have to demonstrate they follow the same process than for the design and for this purpose send technical documents to IRSN premises and meet IRSN reviewers.

ASN inspects the licensee to make sure of the good traceability of the modifications/maintenances. Also, the implementation of the modifications/maintenances can lead to an inspection.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

In France, commercial grade dedication may be used for digital devices with limited functionalities (certification according IEC61508, see answer 4.3), but not for software used in protection systems.

The SPPA-T2000 is a DI&C platform used on the EPR which ensures important to safety functions. Initially, this system was not developed for the nuclear industry. ASN asked the licensee to demonstrate the ability of the SPPA-T2000 to satisfy the requirements indicated in question 2.1. Hence, the licensee made a big effort to modify the platform and to translate the documentation in French.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

ASN doesn't inspect the commercial grade dedication process for DI&C. ASN makes sure that the criteria are met by the licensee's solution.

In the case of digital devices with limited functionalities, IRSN requires the certification reports and may ask supplementary justifications. IRSN can participate to vendor inspections lead by licensee or lead independent vendor inspections, but the exact role of IRSN is not yet defined (see answer 4.3).

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

ASN doesn't inspect the commercial grade dedication process for DI&C, and authorises the use of DI&C systems/components according to the same criteria whether it's a commercial grade equipment or not.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment

qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

The requirements of qualification depend on the place in the installation of the equipment and its role. Depending on the criteria, the qualification can be obtained by using calculus, state of the art, but also by doing tests at the factory or on site.

ASN controls the equipment qualification. In order to do that, ASN does, with the support of the IRSN, sampled analysis, to evaluate:

- the respect of the qualification requirements;
- the sufficiency of the criteria chosen to prove the qualification of the equipment.

IRSN does not use to inspect licensee or vendor for this purpose, but only assess the report files supporting this qualification during reactor design or in case of component replacement. Qualification is guaranteed by the standard followed (usually IEC standards), but for some specific points, the qualification demonstration may be made by equivalence that is justified by the vendor/licensee.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Configuration management review is a part of the process review and IRSN mainly assesses it during design review with technical documentation. During an inspection, the vendor shall be able to show that the software modifications are clearly identified by comments in the source code. Some modifications are chosen during inspection and the vendor shall be able to trace their specifications. All modifications shall be justified. Also for each version, all files and functions that are impacted since previous version shall be identified with a brief description of the cause(s).

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

The criteria are the same as software, but the term “software function” is replaced by “hardware module/component/card/…”.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Data communication shall follow the requirements related to DI&C systems described in answer to question 2.1.

An ideal architecture would avoid any communication between different levels of defence and between different safety classes, and would use diversified solutions for the different levels of defense. However, this ideal is not achievable because of the functional constraints imposed on instrumentation and control and the limited opportunity for technological diversification. There are only very few industrial solutions that can actually be safety-classified; in addition, having more technologies (and therefore tools and design and operation procedures, as well as interfaces with users) makes design and operation more complex, which can affect safety.

The designer shall therefore make choices and justify them, particularly in relation to the objective of preventing CCFs between redundant systems or sub-systems, or between systems implementing independent functions.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

When a licensee reports a significant event related to DI&C systems, ASN, with the support of IRSN, analyzes it to:

- determine if this event can affect other systems or nuclear power plants;
- evaluate the consequences of this event;
- evaluate the quality of the measures adopted by the licensee.

Then, this report feeds a database which can be used to define the priorities for the ASN inspection programme. It can also be used to emphasise a trend.

IRSN capitalises events reported by licensees in creating its own data base with its own assessment on how to use the lesson learnt from each event. IRSN also uses this data base for statistical purposes on component family (reactor series, system, etc.).

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

There is no record of DI&C event which led to an identification of CCF. For each analysed event, IRSN tries to determine if CCF due to DI&C defect is the cause.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

Some examples of typical failure modes expected by the manufacturer are:

- failure of electrical distribution;
- failure of the system monitoring;
- failure of communication between systems.

During I&C inspections, ASN and IRSN evaluate reported events that have impact on safety and that need further justifications or evidences on actions realised in response to the event.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

For a maintenance operation, the licensee has to identify the activities important for the protection (AIP) of the interests mentioned in article L. 593-1 of the Environmental Code. These AIP are subject to an appropriate technical control performed by the licensee. AIP can be made by subcontractors, on whom the surveillance exercised by the licensee is subject to traceability. This point is often inspected.

Maintenance operations can imply a renewal of the qualification, which can be subject to inspection as well.

11.2. What kind of functional tests does your RB inspect? Please describe.

The inspected periodic test reports are not necessarily functional tests. The procedures are defined and assessed by IRSN during the reactor design. The periodic tests are partially manual and automatic. During on-site inspection, ASN and IRSN analyse the periodic test reports of the safety-classified systems and the licensee justifications in case of any deviations, with the actions taken to prevent and solve the issues.

Germany

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

The licensees of nuclear power plants in Germany employ DI&C systems/components important to safety to a rather small extent. Typically, these are systems/components designed to prevent that anticipated operational occurrences lead to accident conditions, or that have even less safety relevance.

Examples for DI&C in systems important to safety in German nuclear power plants are:

- digital reactor power control and limitation system (not: the part of the protection system that is needed to control design basis accidents);
- ex-core neutron flux measurement system;
- digital relays for line protection in the emergency power system;
- process computer system (no process control functions, only additional monitoring functions);
- speed transmitters of reactor coolant pumps;
- transmitters related to the equipment protection of the emergency diesel control system;
- fail-safe programmable logic controllers (PLC) e. g. for crane controls;
- earthquake monitoring system;
- loose parts monitoring system/vibration monitoring system.

It should be noted that there is a modern research reactor in Germany which is designed with DI&C systems/component important to safety, also including the protection system needed to control design basis accidents. In principle, the respective inspection practice differs not very much and is taken into account. The German nuclear rules and regulations for nuclear power plants will be applied correspondingly to research reactors. However, the focus of the questionnaire and the answers given is on nuclear power plants.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

According to the Atomic Energy Act, a licence is required for i) the erection of nuclear power plants (which is no longer granted since 2002), ii) the operation of nuclear power plants and iii) essential modifications to nuclear power plants. Before any licence is granted, it has to be proven that all potential risks and hazards have been considered, that the necessary precautions of the identified risks and hazards have been taken and that the

analysis and the precautions to prevent damage comply with the state of the art in science and technology.

Modifications that are not essential in the sense of the German Atomic Energy Act, but that have an effect on systems/components important to safety or the safety documentation of the nuclear power plant, are subject to modification procedures under the supervision of the RB.

The German Atomic Energy Act as well as the modification procedures provide requirements and guidance for the planning and implementation of the modifications for all involved parties: the licensee, the RB and its authorised experts. The RB and its authorised experts review the modification for compliance with nuclear rules and regulations, in particular the German "Safety Requirements for Nuclear Power Plants" and their "Interpretations"[1] as well as the German safety standards of the Nuclear Safety Standards Commission "KTA"[2]. These regulations include requirements for the design, installation, operation and maintenance of I&C systems in the analogue as well as in the digital technology sector.

2.2. Describe how DI&C is captured in the licensee technical basis.

The design basis of items important to safety in German nuclear power plants has been analogue I&C (see also 1.1). DI&C is installed only in the course of modifications. As part of the modification process, the documentation of the technical basis is adapted accordingly.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Not specifically. Generally, the inspection procedures of the RB (e.g. the processes within the RB's practice to inspect modifications or in-service inspections) do not distinguish between analogue and digital technology.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing)?

Yes. As for any other type of systems or components important to safety, DI&C systems/components are subject to regulatory supervision. This includes e. g.

- modifications (assessment of design and quality assurance in manufacturing, accompanying control during installation and commissioning);
- operations (accompanying control of in-service inspections, and (preventative) maintenance, assessment of ageing management reports);
- operational events/experience (assessment of reportable events in each nuclear power plant, evaluation of information notices on the consequences from events in other nuclear or non-nuclear installations).

Within these processes, the RB mandates authorised experts with the detailed technical assessment. The authorised experts review all systems/components that are important to safety in a detailed manner. Scope and methods of these reviews are specified by the German safety standards of the Nuclear Safety Standards Commission (KTA). Concerning

[1] Available within the Handbook on Nuclear Safety and Radiation Protection, chapter 3, at https://www.bfe.bund.de/EN/bfe/laws-regulations/hns/3/3.html.

[2] The KTA standards are available at http://www.kta-gs.de/common/regel_prog1.htm.

I&C systems/components important to safety, these are especially the standards No. 3501, 3502, 3503, 3505, 3506, 3507 and 3904. Within these KTA standards, the requirements concerning the work of manufacturers, licensees and authorised experts are specified for analogue as well as for digital I&C systems/components. In this way, supervision takes place at any stage of the system's/component's lifecycle.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

As part of the modification procedure it has to be proven that new I&C systems/components important to safety meet the functional, performance and quality requirements of the existing equipment and the state of the art in science and technology.

For this reason, the authorised experts first review the technical specifications of the modification request provided by the licensee.

Additionally, it is an important requirement that only qualified equipment is to be used for I&C systems/components important to safety. Therefore, the authorised experts also inspect the type testing of electrical modules, measuring sensors and transducers. The goal is to evaluate whether the modules/devices are in accordance with the data sheet specifications and the specified characteristics. The inspection deals with theoretical examinations as well as physical tests. Concerning theoretical examinations, engineering documents (including software documents), reliability data, the critical load analysis and test instructions are reviewed. For measuring sensors and transducers, additionally the strength analysis for pressurised parts and material certifications are reviewed. Concerning physical tests, the authorised experts review the test programme and witness critical tests, also in the manufacturers' premises.

The authorised experts also assess the suitability of the quality measures applied within the framework of the manufacturing or post-repair tests. Typically, this is done on the basis of the licensee's quality audit reports concerning the manufacturer or the repair service. If repeated quality defects have occurred, the authorised experts may extend their inspection to assess the performance of the licensee's quality audits. On request, the licensee provides the authorised expert with the report on the test during manufacturing and on the final product. In some cases, the authorised expert is also present when the manufacturer performs important software tests (module or integration tests, also in the manufacturers' premises).

When a new or modified I&C system is installed in the nuclear power plant, the authorised experts review the commissioning programme and the commissioning instructions and they inspect important steps of the commissioning on-site.

For the licensee's in-service inspections during operation, the situation is similar. The authorised experts review the programme and the instructions before they are introduced, and they participate in the in-service inspections on-site to a predetermined extent.

The authorised experts that perform these type of inspections are mostly staff of big technical support organisations (e.g. the German technical inspection agencies called "TÜV"). These technical support organisations are obliged by contract to provide a sufficient number of experts with the required expertise.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

The German licensees of nuclear power plants use digital I&C systems/components only to a small extent (see 1.1). As a consequence of the nuclear phase-out in Germany, big projects like changing the complete protection system (including the part that is needed to

control design basis accidents) from analogue to digital technology were stopped at early stages or not even started. Therefore, currently there is no need any more for a specific training of RB inspectors, especially as technical experts from the support organisations are available.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

The authorised experts perform a close accompanying control with respect to the licensee's modification process. This involves a review of the suitability of the quality measures at the manufacturer as well as being present when important hard- and software tests are performed at the manufacturer or at the plant (see answer 3.3 for more details). The inspections at the manufacturer and at the plant deal with the whole range of safety features of systems/components important to safety. This includes the manufacturing of single DI&C modules/devices as well as the commissioning of a whole system in the plant.

Apart from that, there are no inspections at the manufacturer that are performed "separately" in the sense that they are completely independent from the manufacturer's or licensee's processes.

(Note that all vendors are required to have a quality management system that meets the requirements of the German safety standards of the Nuclear Safety Standards Commission (KTA). For this purpose, the association of the German nuclear power plant licensees (VGB) certifies and audit their vendors on a regular basis. This process is also subject to RB inspections.)

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Yes. Examples of embedded digital devices for systems/components important to safety include

- digital transmitters;
- digital neutron flux power range channels;
- digital protection relays;
- crane controls.

(see also answer 1.1).

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

The criteria for the assessment of embedded digital devices realising functions important to safety are specified by the German "Safety Requirements for Nuclear Power Plants" and their "Interpretations" as well as the German safety standards of the Nuclear Safety Standards Commission (KTA) for I&C components, especially in the KTA standards No. 3501, 3503 und 3505.

In particular, the requirements deal with

- the suitability and quality of the devices including hardware and software aspects;
- the system design;
- environmental testing;

- the separation of redundant facilities;
- final inspection and acceptance testing.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

The requirements for embedded digital devices to be applied by the licensee are the same as for any DI&C component and can be found in the German requirements and standards that are mentioned in answer 4.2.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Depending on the safety impact, modifications important to safety require either a licence/an approval from the RB or a positive statement from its technical support organisation. This applies also to software modifications of DI&C systems/components important to safety (see also answers 2.1, 3.2 and 3.3).

The licensee's internal instructions that describe the relevant processes for modifications, for component replacements or for quality assurance in the field of I&C (including digital components) are reviewed by the RB with support of its authorised experts. The compliance with these internal regulations is inspected during on-site inspections on a random basis and within the modification procedure.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

The same qualification process as described above (see answer 3.3) must be applied to commercial grade DI&C systems/components if they are to be used in the items important to safety of the plant.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

See answer 6.1.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

See answer 6.1.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

The qualification of DI&C equipment consists of a plant independent certificate of suitability and an application specific suitability verification.

The plant independent part is covered by the type testing procedures that are specified in the German safety standards KTA 3503 and 3505. The type tests are subdivided into

theoretical examinations (including the software and its quality characteristics) and physical tests.

Depending on the environmental conditions to which the equipment may be exposed, the physical tests include

- electromagnetic compatibility tests;
- climatic tests;
- tests with mechanical loadings;
- behaviour of the test object upon plugging procedures;
- tests for resistance to radiation from specified normal operation;
- tests under ambient conditions of the corresponding design basis accidents.

The type testing is inspected by the RB's technical support organisation as described in answer 3.3.

The application specific part involves a gap analysis of the existing qualification against the specific operational conditions, factory acceptance and commissioning tests. Depending on the gap analysis a supplementary type test may be required.

The RB's inspection of the modification process that includes an assessment and approval of the planned modification as well as inspections during and after the implementation of the modification shall ensure that only adequately qualified equipment is used. After the modification is completed (including the necessary changes of corresponding documentation), the technical support organisation writes a final report for the RB that documents its inspection activities and that confirms that the modification process has been completed properly.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Questions 8.1 and 8.2 are answered together:

Any modification of software or hardware that is important to safety is subject to the modification procedure with the corresponding inspections described above (see answers to 2.1, 3.2 and 3.3).

For replacements of technical obsolete DI&C equipment, the inspection practice follows a graded approach depending on the specification, qualification and vendor of the spare parts. The detailed procedure is specified in an instruction of the licensee that is established in accordance with the German safety standard KTA 3507. This instruction as well as any update to it are reviewed by authorised experts.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Note: The I&C architecture of German nuclear power plants is based on analogue I&C technology and does not include dedicated systems for the data communication between systems important to safety. Data transfer between the systems is part of the output interface of the systems. Due to the nuclear phase-out in Germany, no modifications affecting the existing architecture by employing DI&C systems are planned.

For the design of the I&C systems, the German nuclear safety standard KTA 3501 specifies the following criteria:

I&C systems performing category A functions should not include functions of category B and C. The same applies to the independence of category B functions from category C functions. Furthermore, systems performing category A or B functions must be independent of other systems with lesser safety relevance so that the realised functions are not compromised in the event of failures in such systems.

According to this framework, data communication of I&C systems performing category A/B functions is usually limited to

- bidirectional communication with dedicated digital test devices;
- unidirectional communication to systems with lesser safety relevance.

For the internal communication, it is necessary that data used for evaluation of category A/B functions are subject to a voting logic.

Also, the design of mechanical or electrical components important to safety that are triggered by I&C systems of category A must include a priority control to ensure that systems of lesser safety relevance cannot spoil or even prevent the execution of the safety function.

Additionally, the software design of DI&C systems important to safety shall include a signal validation to prevent failure propagation and an exception handling to ensure the correct execution of the programmes regardless of how their input signals change over time.

Further principles in the design of the DI&C systems' communication to prevent common cause failures are

- avoiding direct communication between (redundant) processing units to guarantee independence;
- realising communication links as point-to-point connection;
- reducing data-technical interaction by unidirectional traffic;
- testing the data integrity at the receiver;
- automatic cyclic test of connections.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

According to the German "Nuclear Safety Officer and Reporting Ordinance", the operators of nuclear power plants are under obligation to notify the RB in case of accidents, incidents or any other safety-relevant events. On behalf of the German nuclear authority, the

technical support organisation “GRS” analyses this information as well as information on special events in other countries. If the analysis indicates, that an event may be of significance for German nuclear power plants, GRS issues a so-called information notice that is distributed to all operators. In response to the information notice, the operators report on their investigations and consequential planned measures. With the support of authorised experts, the RB analyse the information notice and the operators’ reports and make an assessment whether the measures taken by the operator are adequate.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

There were no DI&C related events identified that had the potential for common cause failures.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

The assessment of DI&C systems/components important to safety is based on the German “Safety Requirements for Nuclear Power Plants” and their “Interpretations” as well as the German safety standards of the Nuclear Safety Standards Commission “KTA”. A selection of the most important requirements is given in the list below. The requirements given in the regulations and standards correspond to typical failure modes, expected by DI&C vendors and designers.

- The I&C installations have to be suitable to prevent operational occurrences from leading to accident conditions.
- The potential for common-cause failures of safety equipment that is needed to control design basis accidents shall be analysed. For this equipment, provision shall be taken that a multiple failure need not be assumed. Redundant safety equipment for which common cause failures have been identified, shall be installed in diverse manner as far as technically reasonable.
- The reliability and effectiveness shall be ensured under all conditions to be assumed for the relevant design basis accidents, in the case of event-induced consequential failures and for loss of functions or unavailabilities according to the single-failure concept.
- To ensure reliability, the safety equipment that is needed to control design basis accidents shall be designed according to the following principles:
    - redundant design;
    - diversity;
    - physical separation of equipment corresponding to the impact range of possible postulated initiating events;
    - automatic failure monitoring;
    - adaption of the components to the possible ambient conditions;
    - simple software structure;
    - limitation of the functional scope of the hardware and software to the necessary safety-related degree;
    - use of fault-preventing, fault-detecting and fault-controlling measures and equipment.

- Manual reactor scram shall be possible at any time, even in case of a postulated systematic failure of computer-based I&C equipment including systematic software failure.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

A general requirement is that maintenance activities shall not impair the safety functions of the plant in such a way that the effectiveness of the safety system is no longer ensured. Moreover, interventions on I&C systems/components during the operation of the reactor may only be carried out at pre-installed and tested intervention points and according to pre-planned instructions.

To identify and document functional and technical properties of I&C systems and to record any changes, there has to be a configuration management. For this purpose, the operator has to define appropriate technical and administrative instructions. The configuration management has to be used as a basis for all maintenance activities. With its help, it must be possible for example to verify that the valid (type tested) version of the hardware and software is used.

A specific requirement for DI&C is that maintenance activities shall neither unintendedly alter nor erase data.

Failures identified during maintenance work, their causes and the type of repair shall be documented. The operating experience from maintenance shall be evaluated systematically.

The programmes and instructions of planned maintenance are subject to assessment by authorised experts. The programmes also specify how often the authorised experts are present during the maintenance procedures.

11.2. What kind of functional tests does your RB inspect? Please describe.

Having finished maintenance or modification activities, functional tests shall ensure that the corresponding safety functions are available. Apart from that, functional tests are performed on a regular basis in the framework of in-service inspections to prove at fixed intervals that the I&C systems/components still meet their requirements.

The programmes and instructions of planned maintenance and in-service inspections for items important to safety are subject to assessment by authorised experts. The programmes also specify how often the authorised experts are present during the maintenance or testing procedures.

Hungary

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes. Examples: Reactor Protection System, Rod Control System.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

The criteria are defined in the Nuclear Safety Codes (NSC). The list of criteria are too long to introduce here. You can read the English version of the NSC on our website (www.oah.hu). Guidelines include recommendations on how to meet the requirements of NSC. The preliminary version of guideline is final status for I&C systems.

2.2. Describe how DI&C is captured in the licensee technical basis.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

No we doesn't have a special inspection method for the inspection of DI&C systems. The inspection processes are ordinary, but we apply special requirements.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Yes of course.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

During the inspections we take into consideration the safety and the security aspects as well. These two areas (security and safety) are the responsibility of two different organisational units. It is therefore necessary to co-ordinate the work of the two areas during the inspections. If needed, we involve professionals from both professions in the work and in the inspections.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

There is no special training courses for the inspectors. Inspectors have normal higher education studies in this area. The training of supervisors is carried out using international experience.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

For DI & C systems there is no specialised supplier control. Manufacturers need to have nuclear supplier certification. Primarily, the licensee is investigating the suppliers' compliance. It is valid for three years. During the establishment of the individual equipment, factory acceptance testing is carried out in which the RB participates.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Usually our licensees do not use embedded digital devices. Exception is the power control at the research reactors. Measuring instruments may include embedded systems. They do not perform any independent control functions.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

The normal criteria are applied. The same as for programmable systems. The guidance (referred to in point 2) deals with the way how the fulfilments of the criteria.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Verified hw and sw tools must also build embedded systems. Verification should extend to hardware components, firmware, and if applicable, user software.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Verifiable development tools must be used for software modifications. The development process must be in accordance with a fixed procedure. The authority usually carries out checks during the tests.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

The requirement is the following:

NSC 3a.4.5.5100. When a commercial product is applied, it shall have specific and type identification and an appropriate qualification from an appropriate, accredited testing organisation to demonstrate that the product meets the requirements derived from the design basis.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Verification of commercial product ratings is similar to checking standard programmable devices. Instead of controlling production and software development, focus is on licences.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

There are no specific criteria.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

The licence holder is the primary responsible for nuclear safety in Hungary. There shall be procedures in place for the solvents modified by the licensee. In the case of programmable devices originating from a supplier, the licensee is responsible for the existence of ratings. The verifications must be complete (environmental and software, hardware verification). In addition to the environmental and earthquake rating, the protection against electromagnetic effects must be demonstrated. Electromagnetic Impact Surveillance Review in the Processing of Fukushima Experience (stress test). (It is important from the point of view of nuclear safety that failures of overvoltage arresters may reduce the availability of safety systems.)

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

The requirement is the following:

Configuration management of instrumentation and control shall also cover the following areas:

a) documentation of the system and components, also in the case of commercial products;

b) hardware documentation;

c) all forms of software documentation and codes, among others, specifications, design documents, source codes, executable codes, computer codes and directories;

d) development systems, including core generators, compilers, test environments and test tools;

e) test cases and results;

f) modifications and related analyses;

g) training materials.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how this is inspected.

The criteria are set out above.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

In case of communication systems, security and safety criteria must be applied. However, the security criteria are given more attention.

A good example of this is the digital radio system that is under refurbishment.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

The DI&C system events are investigated in the same way as other events. We distinguish three levels (A, B, C) depending on the effects of the event. In the simplest case (A), one person evaluates the event. In the most complex case (C) evaluation group is created.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

There is no common cause fault based event found on our database.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

The entire development process must be qualified. It is not enough to qualify the final product (software), but the adequacy of the entire development process must be presented.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

Checking the integrity of software is a special requirement when managing the DI&C systems.

The reactor protection system

The reactor protection system includes a central test computer. The test computer can provide physical signals to the reactor protection system and evaluate the response of the reactor protection system. This is done by testing the reactor protection systems.

In addition, specialists will pay special attention to the regular replacement of electrolyte capacitors.

11.2. What kind of functional tests does your RB inspect? Please describe.

Our RB usually inspect the functional testing of the safety systems. Examples: the gradual starting process of the pumps, tests of the valves of the safety systems.

In other area, three days before the integral leakage test the computerised data acquisition and evaluation system is checked. RB inspects this process.

India

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

DI&C systems/components are used in systems important-to-safety such as reactor protection, emergency safety feature actuation system, control systems, non-safety significant SSC etc.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

The authorisation by RB, for installation and use of DI&C systems follows the following criteria:

a) DI&C systems should meet requirements given in AERB safety code/guides on design such as AERB/NPP-LWR/SC/D, AERB/NPP-PHWR/SC/D (Rev.1), AERB/NPP-PHWR/SG/D-10, AERB/NPP-PHWR/SG/D-20, AERB/NPP-PHWR/SG/D-25 . This include aspects such as reliability, diversity, independence, common cause failure consideration, failsafe design, single failure criteria, Security considerations etc.

b) DI&C systems should be demonstrated to be safe and have a high level of integrity. Integrity should be assured by developing digital I&C following a systematic, technically appropriate, carefully controlled, fully documented and reviewable engineering process, which is suitably interfaced with V & V activities.

c) Analysis of specifications, algorithms, designs and implementation need to be carried out to demonstrate safety and integrity of digital I&C systems . The reviews of designs/analysis are required to be performed by people independent than those who designed and implemented the system/software.

2.2. Describe how DI&C is captured in the licensee technical basis.

Licensee provides information on the use of digital I&C system as part of the safety report and subsequent supplements as necessary for detail review by the RB. The information include design description of I&C systems and required analyses such as system safety analysis report, common cause failure Analysis report etc.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

RB accepts use of digital I&C for safety related systems after scrutiny of evidences/documentation submitted to RB for demonstration of criteria as mentioned in answer 2.1 above. In general, RB does not carry out inspection at supplier/developer premises. However, inspection of DI&C systems is carried out after receipt/installation at site. This inspection includes aspects such as storage/preservation, manufacturing QA reports, installation, site acceptance test, performance of DI&C systems etc.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

RB conducts regulatory inspection during installation and functional testing at plant site. RB ensures the QA during design and manufacturing by scrutiny of the QA and V&V reports.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Scope of inspection covers the compliance checking of safety requirements applicable during implementation at site such as layout, segregation, configuration management of hardware/software, storage/preservation of I&C , QA reports, installation practices, site acceptance test, performance of DI&C systems, security considerations etc.

The staffs performing the inspections possess academic background in the field of I&C/Electrical and Electronics/Computer Science. They are trained to undertake review and inspection of Digital I&C systems as explained in answer 3.4

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

RB staffs are trained through orientation course for regulatory processes, NPP systems including I&C specific training modules and on job training at NPP site. Afterwards staffs are trained as per inspector qualification programme of the RB which includes working under guidance of a senior inspector. An inspector authorisation is issued by RB after successful completion of the qualification programme.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

Generally inspection of DI&C at site is carried out as part of regular inspections by trained inspector. During commissioning/ site acceptance test, specific inspection for DI&C is carried out by RB. In general, the RB does not conduct inspection at vendor site, however manufacturing related QA records are inspected at the nuclear power plant site after shipment.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Embedded digital devices such as smart transmitters, Numerical relays, digital display modules , Uninterrupted power supply modules etc. are used in safety, safety-related and non-safety applications.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

RB, generally, does not carry out inspection at the supplier/manufacturer premises to assess the embedded devices. However, use of embedded device is accepted by RB after ensuring suitability for purpose and quality of the embedded devices. Evidences justifying the fulfilment of the above are reviewed by RB.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

The embedded devices should meet the criteria of (i) suitability and (ii) quality to be eligible for use in safety related functions. The suitability criteria should establish that the functional, performance and constraint characteristics are appropriate for system function and the embedded device does not contain any functions that are not required by the system. If it is not possible to eliminate such functions, it should be ensured and demonstrated that these extra functions will not affect the performance of safety functions of the system.

The quality criteria should establish that the embedded device development has followed well defined, controlled and technically appropriate lifecycle processes.

If complementary tests and/or documentation has been done to compensate for deficiencies in above, test results and/or documentation should confirm that deficiencies are adequately compensated.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Licensee is required to prepare a configuration management plan detailing the modification and maintenance process of DI&C systems/components software. The RB inspects the DI&C systems/components at site to verify the activities as per the configuration management plan.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Licensee is required to carry out assessment of commercial grade items to demonstrate safety and integrity of the DI&C systems. Licensee assessment of the commercial DI&C system should establish that the selected commercial DI&C system development followed a systematic, technically appropriate, carefully controlled, fully documented engineering process and V&V activities. Additional testing, analyses, operational experience(in similar safety significant applications) etc. should be used to demonstrate high level of safety and integrity. Further, a dedicated item, when integrated in the design, undergoes integrated tests with all possible test cases.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

RB reviews the process of the assessment of commercial DI&C items. However, RB does not inspect the commercial item assessment process during its execution. RB reviews the

assessment report and supporting evidences. RB may witness specific tests at the nuclear power plant site after a dedicated item is integrated in the design.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

RB reviews the assessment report and supporting evidences to verify the fulfilment of the criteria of safety and integrity as explained in answer 6.1.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

Equipment Qualification of DI&C carried out by licensee addresses aspects of electromagnetic, environmental and seismic qualification as per international standards. RB, in general, does not inspect the qualification process during execution of the process, however, qualification reports are reviewed and inspected by RB.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Licensee is required to prepare a configuration management plan (CMP) detailing the modification and maintenance process of software. The CMP details the process to be followed to execute and qualify a change in software. Licensee provides a report on the changes carried out as per the CMP to the RB which is reviewed by RB to authorise its use. During inspection at site, Configuration Management records are checked to confirm appropriate version of the software.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Similar process as described in answer 8.1 is followed.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

W.r.t use of data communication, RB uses the following criteria for authorising the DI&C system. Systems/sub-systems of higher safety class shall not depend on outputs from systems/sub-systems of lower safety class for performing their safety functions. Communication channels between systems/sub-systems of different safety class shall be designed to ensure that faults in system/ subsystem of lower safety class do not affect safety functions of system/ sub-system of higher safety class. During inspection at site, RB may inspect the compliance to the regulatory requirement.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Events which match with reporting criteria as prescribed by RB, need to be reported by Licensee to the RB, including events which may be caused by DI&C. The Licensee investigation report includes information on identification of the fault (by analysis/, simulation/ test etc.). The investigation report and corrective actions proposed by licensee is reviewed by the RB. Also, follow up of corrective actions and their performance is monitored. The RB also reviews the applicability of the lessons learnt to other plant SSCs or processes and initiate action accordingly.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

Process to identify CCFs are part of event investigation and review of significant events by RB. So far, no DI&C related CCFs were observed.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

Some of the typical failure modes that should be considered for DI&C are:

I. Power supply failure

II. Input failure (invalid /out of range, etc.)

III. Output failure (Invalid output postulated due to logic malfunction)

IV. Single random hardware failure

V. Software failure

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

Maintenance activities should be in compliance with configuration management plan. Appropriate maintenance procedures should be followed. Computer security requirements should be complied with.

11.2. What kind of functional tests does your RB inspect? Please describe.

Licensee conducts functional test of DI&C systems at factory before shipment and at site after installation. These tests are conducted as per System Validation Plan (SVP). System validation plan describes the functional tests which are needed to validate the system in compliance of system requirements defined in System Requirements Specification. Validation tests are witnessed by an V&V team. The validation reports are submitted to the RB for inspection. Additionally, RB personnel may be present during the conduct of validation of important safety systems.

12. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections

(e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

Following suggested topic may be considered:

- Graded approach to be followed for inspection of DI&C system

Japan

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

<Answer>

Digital I&C systems are applied to the safety-related system since the completion of new built ABWR power plant 1996. I&C systems for existing plants have been gradually replaced or retrofitted with digital I&C system. Reactor protection system, ESFs (Engineered Safety Facilities), Neutron monitoring system are the typical digitalised safety-related I&C systems. Digital technologies are applied to non-safety systems such as: Reactor Pressure Control System, Feed Water Control systems, EHC (Electro Hydraulic Control), AVR (Automatic Voltage Regulator), etc. Also digital Annunciator system are also treated as non-safety system. Each switch for an equipment and a manual controller for process manipulations are replaced with touch operations on the display screen.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

<Answer>

In Japan, there are specific requirements for Reactor Protection System as regulatory requirements concerning digitalised I&C system (There is no specific regulatory requirements for non-safety systems). For the Reactor Protection system, NRA (Nuclear Regulation Authority) reviews the actuation signals, the voting logic and the design policy of diversity and independence, etc. in the basic design phase, and reviews the concrete control method (such as Digitalized or Hardwired) at the detailed design stage.

The criteria for conformance review and inspection for safety-related digital I&C system is described on the NRA ordinance.

Industrial codes and guidelines, these are called as JEAC 4620 (Japan Electric Association Code) and JEAG 4609 (Japan Electric Association Guideline) have been endorsed by NRA and are quoted on the part of regulatory guide of the NRA ordinance.

So, in the past example, as the voting logic was changed from “2 out of 3” to “2 out of 4” in the digitalisation for a nuclear power plant control board replacement, NRA reviewed the logic change in the licensing of Installation Permit change application. And NRA reviewed the design of control board replacement, at the stage of the Construction Planning Permit for the detailed design review. And the final inspection was conducted as the pre-service inspection after installation to ensure that the actual system and equipment has due functions being designed.

Licensee is required to submit the supplemental explanation document for application of RPS (Reactor Protection System) with digitalised control system with the Construction Planning Permit application documents, in case the licensee hope to adopt digitalised RPS.

The supplemental document is required to include the overall structure of I&C system, the design policy of digitalised RPS such as system structure, independence, diversity, response time and adequacy of compliance to the regulatory requirements. NRA reviews these design documents for the confirmation that the design requirements are satisfied.

2.2. Describe how DI&C is captured in the licensee technical basis.

<Answer>

Technical basis of the licensee in Japan are mainly influenced by the overseas information such as IEEE Std. (Institute of Electrical and Electronic Engineers), IEC Std. (International Electrotechnical Commission) and website information of NRC, EPRI and IAEA, etc. More concrete method and deep part of technical basis may be obtained from the information provided by Japanese vendors.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

<Answer>

No, NRA does not specifically inspect DI&C systems. Regardless of digital or analogue, NRA conducts the pre-service inspections to confirm that I&C systems have due functions being designed in the approved construction plans.

When applying the digital reactor protection system, in addition to the main content (excluding 5. Notes), Guides of the "Code of Application of Digital Computers to Safety Protection Systems for nuclear power plants" (JEAC 4620-2008) of the Japan Electric Association and the main content and Guide of the "Guidelines for Verification and Validation of Digital Safety Protection Systems of nuclear power plants" (JEAG 4609-2008), the following requirements should be satisfied;

(1) The operational settings of the reactor protection system should be determined so that, in the event of an Anticipated Operational Occurrence or in the case where the operation of power reactors is hindered due to an earthquake, the device can function, together with the reactor shutdown system and other systems, to avoid exceeding the Damage Limit of Fuel Elements.

(2) Preservation of documents prepared upon implementation of the Verification and Validation should be prescribed in a configuration management plan according to JEAC4620 and such documents should be properly managed.

(3) Their design should take into account environmental conditions, such as anticipated power disturbances, surge voltages, and external disturbances and noise (including electromagnetic waves), and the adequacy of measures taken based on such a design should be verified.

(4) The digital reactor protection system should not receive information from the instrumentation or control system except the initiation signals from facilities for ATWS (Anticipated Transient without Scram) measures. When it does so, measures should be taken to ensure that the digital reactor protection system is not affected by a failure of the instrumentation or control system. When the digital RPS shares a transmission line with the instrumentation and control been found to have the same or lower trip failure rate and trip error frequency than the previous one.

(5) Equipment that ensures it is not susceptible to external influences.

(6) Having a high reliability that is equivalent to the reactor protection system in JEAC4620 should mean that, as a result of evaluation, the digital reactor protection system has been

found to have the same or lower trip failure rate and trip error frequency than the previous one. The digital reactor protection system's reliability evaluation should include detection of abnormalities in hardware components, transmission of detection signals, processing of input and output signals, operation processing, transmission of trip signals, tripping operations, and other necessary evaluation components.

(7) When the integrity of digital computers used in the reactor protection system cannot be evaluated, separately prepare a means to do so by employing a different principle in order to ensure the performance of reactor protection functions.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

<Answer>

NRA reviews the designs of DI&C systems to confirm the compliance to the regulatory requirements which are defined on the NRA ordinance. NRA inspects the features of DI&C system and confirms the management conditions of the licensees during manufacturing and installation stage of DI&C system in aspect of QA (Quality Assurance). Function of DI&C is inspected through the pre-service inspection as is designed.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

<Answer>

The inspection is limited in the range of RPS licensed through the construction plan permit. The main target is to confirm the RPS main function described on the first item for the guidance of NRA ordinance related to the RPS, that is "The operational settings of the reactor protection system should be determined so that, in the event of an Anticipated Operational Occurrence or in the case where the operation of power reactors is hindered due to an earthquake, the device can function, together with the reactor shutdown system and other systems, to avoid exceeding the Damage Limit of Fuel Elements." For this confirmation in detail, the scope of inspections would be to check that the requirements described above in the item 3.1(2) to (7) should be satisfied.

These types of inspections must be performed by generally qualified inspectors and there is no particular expertise for the inspections of DI&C systems.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

<Answer>

NRA inspectors are not specifically trained to inspect DI&C systems/components.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

<Answer>

No, NRA does not inspect DI&C systems/components separately. Usually NRA does not carry out inspection of suppliers. On the other hand, NRA has the option to conduct reactive inspections as necessary in response to events or failures. During these inspections, NRA staff may enter the offices or business establishments of licensees and inspect documents, records, and other articles, as well as questioning the personnel there. These inspections include inspections of manufacturers etc. NRA may directly inspect those involved in the design or construction of nuclear facilities, as well as those involved in the manufacture of equipment for such facilities.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

<Answer>

The Licensees may be using the EDDs (Embedded Digital Devices) already. The licensees may not aware of EDDs existences in nuclear power plants, because such embedded device is latent as a portion of plant equipment. Especially, sensors, indicators, recorders, protection relay, annunciators, etc. are deemed as same of conventional analogue devices.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

<Answer>

NRA currently does not distinguish the item of EDD. But once the device is admitted as the item important to safety, the evidences derived V&V (Verification and Validation) process are requested to be submitted for review.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

<Answer>

Japanese nuclear licensee requests the vendors to fulfil the nuclear quality assurance processes base on the JEAC4111 quality assurance standard (Nuclear Standards Committee of the Japan Electric Association: a quality assurance standard for the safety for reactor facilities) and JEAG4121 guidelines. These are developed for Nuclear Power Plants, but are not intended to qualify the EDDs.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

<Answer>

Licensee is obligated to conduct the periodic self-inspection to confirm the compliance with Technical Standards for Commercial Power Reactors Facilities. For digitalised Reactor Protection System, licensee maintains and checks its status of the software version control thorough the periodic self-inspection, and NRA checks the licensee's implementation status of the software version control through the periodic facility inspections.

If the modification of the DI&C systems/components software results in the change of basic design described in the reactor installation permit application document, the licensee shall submit the "Amendment of Installation Permit Application" documents to the NRA as the regulatory authority. If it does not relate to the change of basic design, the licensee shall start from the next licensing application procedure for the detail design. After the Installation Permit Change Application was approved, the licensee shall submit the "Construction Plan Approval" application to the NRA for review of the detail design. After the "Construction Plan Approval" application was approved, the NRA confirms that the modification is completed in accordance with the design requirements described in the approved "Construction Plan" documents through the pre-service inspection.

On the other hand, a change of matters not described in the construction plan is acceptable without the licensing and inspection procedures.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

<Answer>

There is no commercial grade dedication process for DI&C.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Not applicable

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

Not applicable

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

<Answer>

With confirming the quality inspection results provided by vendors and various standards such as IEEE standards, IEC standards, JEAC 4111 (Quality Assurance Code for Safety in NPPs) and JEAC 4121 (Application Guide to Quality Assurance Code for Safety in NPPs), the licensees are trying to maintain the level of quality of DI&C system.

In approval of the construction plans, the NRA reviews the compliance of procurement management methods with the NRA Ordinance on Quality Management System, in the stage of construction order, assemble and installation of components, and checks for the licensee's management is being carried out according to the approved construction plans through the inspections.

Licensees formulate their management systems based on the JEAC 4111 quality assurance standard, which was revised while taking into account ISO 9001 and so on. Licensees should conduct procurement procedures having clearly identified the requirements for product approval procedures, processes and equipment; personnel competence checks, and quality management systems. Moreover, the standard stipulates that procured items must be inspected on the premises of the supplier if possible to ensure that they meet set standards. In procurement management, it is common for licensees to conduct audits of suppliers directly, to ensure that the suppliers satisfy the specification sheet requirements. Such specification sheets are given to the supplier at the time of ordering and products are then checked upon delivery. If checks are required during the product manufacturing process, licensees can directly check that process. NRA checks the licensee's implementation status of procurement control through the inspections.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

<Answer>

Regarding to the RPS software program, algorithms have not experienced to be changed. Validity of the change of set point value is confirmed through the pre-in-service inspection. It is confirmed through this inspection whether activation performed as scheduled or the signal was output when the process reached the designated value or timing.

Functional sustainability of SSCs of which software and/or hardware are modified is self-confirmed by the licensees through the periodic facility inspection. NRA also confirms the performance of the safety related system during this periodic facility inspection.

Function of the DI&C system which is amended on the construction plan will be confirmed through the pre-service inspection.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

<Answer>

Same as above answer in the item 8.1

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

<Answer>

The NRA ordinance regulate the communication system to be independent electrically and functionally between safety grade and non-safety grade, as well as between the other safety divisions.

Basically the unidirectional data flow direction from safety to non-safety is preferable. For application of reversal direction data flow special technical considerations and evaluation of system reliability are required.

Regarding the independence of communication system between non-safety grade and safety grade, JAEC4620 which is endorsed by NRA ordinance is referred.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

<Answer>

The licensee in Japan is obliged to make precisely described report to NRA the events which have adversely affected plant safety based on NRA Commercial Reactor Ordinance.

On this report the result of RCA (Root Cause Analysis) and Measures to prevent recurrence are required to be written.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

<Answer>

Have no experience.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

<Answer>

The NRA ordinance requires the licensees “Prepare equipment and procedures for estimating necessary plant data in the event that difficulties arise to get the necessary plant data due to the malfunction of some normal and emergency instrumentation devices caused by BDBA”.

Plant status information that shall be collected in order for licensees to implement successful core damage prevention measures and containment vessel failure prevention measures.

a) Clarify the capability of instruments to understand plant status in case of beyond design basis accidents. (Maximum measurable temperature, etc.)

b) Preparation of measures for estimating plant status in the event that situations exceed the ability to grasp the plant conditions.

    i. Preparation of measures for estimating temperature, pressure and water level inside the reactor pressure vessel.

    ii. Preparation of measures for estimating the amount of water injected into the reactor pressure vessel and containment vessel.

    iii. Parameters needed to make such estimates shall be prioritised in advance considering the accuracy among multiple parameters.

c) Parameters required to manage beyond design basis accidents, such as temperature, pressure, water level, hydrogen concentration and dose rate inside the containment vessel shall be able to be measured or monitored and recorded.

d) Preparation of measures for measuring and monitoring especially important parameters during loss of DC power (Example; testers, conversion table, etc.).

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

<Answer>

The RPS is required to implement the functions to be able to be bypassed and to be able to be tested. And the protection logic is also required to be able to work while one channel is bypassed.

11.2. What kind of functional tests does your RB inspect? Please describe.

<Answer>

NRA reviews the assessment results of digital RPS spurious actuation: failure rate will be assessed in both aspect of trip error and non-trip error. (Refer to the item of 3.1(6) in this questionnaire)

And also NRA confirms the RPS test result which is submitted by the licensee during the periodic facility inspection. The RPS test is carried out to check the logic action under the channel bye-passed condition with simulating process signals.

Refer to the item 3.1(6)

12. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections (e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

1. The scope of validation for after RPS replacement

How the output signal is technically checked?

Is plant equipment/actuator behaviour required according to these DI&C output signal?

2. Commercial Grade Items/ Smart Devices

How RB regulate the licensee to apply the COTS (Commercial off-the-Shelf)?

Does RB implement the qualification regulation for COTS (EDD, CGI, Smart Device, Operating system, Firmware and etc.)?

3. Configuration Management

How deep does RB request the licensee to perform the configuration management on I&C system including hardware and software (both of program and database)?

4. Software tools

Do your RB define the software tool? Explanation of the definition.

Does RB check the qualification of the software tools?

5. The preparation for the DIC incidents

What kind of incidents are designed and assessed on Digital I&C system?

Does RB regulate the licensee to implement the backup method for the measures to software CCF (Common Cause Failure)?

Korea

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes.

DI&C systems/components are widely used in nuclear power plants. For examples, there are Reactor Protection System (RPS), Engineered Safety Features Actuation System (ESFAS), Diverse protection system, Automatic Seismic Trip System, Reactor Regulating System, Plant Monitoring System, etc. In case of APR-14000, almost all I&C systems including safety-related and non-safety related have been fully digitalised.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Licensee who intends to do any alteration of the licence including FSAR shall obtain approval of the change from the regulatory body, as prescribed by Presidential Decree. Provided, that the alteration of any insignificant matter shall be reported. [Nuclear Safety Act Article 20 (Operating Licenses)].

If the change entails the modification of safety-related equipment or facilities including analogue and digital technology, the applicant shall submit LAR (License Amendment Report) and obtain approval of the change from the regulatory body prior to the change. [Enforcement Regulation of the Nuclear Safety Act Article 17 (Application for Change Permit), Article 18 (Report of Changes in Minor Matters)].

For new plants, KINS reviews the PSAR (Preliminary Safety Analysis Report) for Construction Permit and the FSAR (Final Safety Analysis Report) for Operating License submitted by licensee. While reviewing the SAR, KINS sends RAIs (Request for Additional Information) to licensee. In some selected areas, KINS reviews the design detailed documents and performs audits and inspection to evaluate the design processes and V&V activities.

2.2. Describe how DI&C is captured in the licensee technical basis.

Chapter 7 (Instrumentation & Control) of SAR includes the basic information of DI&C such as overall I&C architecture. In addition to SAR, KINS receives information about the vendor's documents organisation by RAI for digital I&C systems. For example, these are SPM (Software Program Manual) and listings of software documents. SPM specifies systematic approach to be used for the software engineering process of software based I&C systems. This SPM is used as a guide in writing the software development, QA, software configuration management, and Verification and Validation plans, plus other plans.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Yes.

In some selected areas, KINS performs vendor audits for digital I&C development activities (vendor process and technical documents) in the review stage of OL in order to confirm the quality of software for digital safety system. The audit is conducted by a witness on the stage of the integration test or factory acceptance test to check final product.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing)?

No.

KINS preforms the important stages such as integration test or factory acceptance test when necessary. See the response of 3.1.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Normally, KINS performs vendor audits for digital I&C development activities (vendor process and technical documents) for digital safety system. The audit includes the review of the main DI&C documents and the witness of important test stages (e.g. factory acceptance test) selected.

As experience of the inspector is important, the audit should be delegated to a more experienced staff with I&C engineering and software engineering knowledge.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

KINS training programme basically includes the topics of inspection on DI&C. According to the programme, KINS inspectors are trained in digital system, software, electromagnetic compatibility, etc.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

No.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Yes.

I&C system use embedded digital devices (EDDs) such as intelligent transmitter, digital relay, component interface module, etc. In addition to I&C systems, the safety equipment use embedded digital devices (EDDs) in emergency diesel generators, transmitters, pumps, valve, etc.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

KINS makes RAI for the information on the use of EDD. If EDDs are used in digital safety system, KINS confirms the adequacy of its quality at the stage of FSAR review. KINS performs the vendor inspection of the integration test or factory acceptance test to check final product when necessary.

Mostly, embedded digital devices shall be designed and manufactured under the required nuclear quality assurance programme to be used in safety applications.

However, the Korea regulations allow for commercial grade items that are not designed and manufactured under the required nuclear quality assurance programme to be used in safety applications if they are through a dedication process. For commercial grade items that are based on digital technology, the KINS has used the guidance in IEEE 7-4.3.2, EPRI Technical Report 106439, etc.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

EDDs shall be designed and manufactured under the required nuclear quality assurance programme to be used in safety applications. EDDs should be designed in accordance with ASME NQA-1, IEEE 7-4.3.2, EPRI Technical Report 106439, etc. See the response of 4.2.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

KINS performs vendor inspection for new plants to confirm adequacy of configuration management on the licensing basis (SAR, etc.). KINS verifies configuration item (software requirements, designs, and code, etc.) according to QAP.

Periodic inspection for operating plants are performed to verify adequacy of configuration management for DI&C systems such as reactor protection system, automatic seismic system, etc.

See the response of 8.1.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Yes.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

The Korean regulations allow for commercial grade items that are not designed and manufactured under the required nuclear quality assurance programme to be used in safety applications if they are through a dedication process. For commercial grade items that are based on digital technology, the KINS has used the guidance in EPRI Technical Report 106439, IEEE 7-4.3.2, etc. KINS performs vendor inspection on selected commercial grade items

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

For commercial grade items based on digital technology, KINS uses the guidance in EPRI Technical Report 106439, IEEE 7-4.3.2, etc.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

Section 3.10(Seismic and Dynamic Qualification of Mechanical and Electrical Equipment) of Chapter 3(Design of structures, components, equipment, and systems) in SAR provides the tests, analyses, procedures, and acceptance criteria applied to two categories (Seismic Category I/II) of electrical equipment to assure operability and structural integrity under the full range of normal, transient, seismic and accident loadings.

Section 3.11(Environmental Qualification of Mechanical and Electrical Equipment) of Chapter 3 in SAR provides the design criteria with respect to environmental effects on the electrical equipment to ensure acceptable performance in all environments (normal, abnormal, and accident) according to equipment location and function. Appendix 3.11 lists the electrical equipment for environmental qualification including electromagnetic qualification.

In addition to SAR, KINS reviews the sampled equipment qualification report (approximately 10 %) for digital I&C systems by RAI. Based on the SAR, KINS performs vendor inspection to confirm the adequacy of processes and outcomes of equipment qualification of DI&C. The inspection is conducted by a witness during EQ tests selected.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Basically, configuration management should be performed in accordance with Quality assurance programme.

KINS Regulatory Guide 8.16, “Configuration Management Plans for Digital Computer Software used in Safety Systems for Nuclear Power Plants”, which endorses IEEE 1042-1987, “IEEE Guide to Software Configuration Management” provides acceptable criteria for planning configuration management.

KINS reviews SPM including the information of software configuration management plan(SCMP). The SCMP addresses software configuration management activities

concerning the identification of software products, control and implementation of changes, and the recording and reporting of change implementation status.

KINS reviews configuration management controls for the development of software to be used in DI&C safety systems.

Based on the SAR, KINS performs vendor inspection for new plants to confirm adequacy of configuration management. Periodic inspection for operating plants are performed to verify adequacy of configuration management for DI&C systems such as reactor protection system, automatic seismic system, etc.

In addition, these inspections are conducted to confirm the controls needed over operation activities to prevent unauthorised changes to hardware, software and system parameters.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Basically, configuration management should be performed in accordance with QAP.

Based on the SAR, KINS performs vendor inspection for new plants to confirm adequacy of configuration management. Periodic inspection for operating plants are performed to verify adequacy of configuration management for DI&C systems such as reactor protection system, automatic seismic system, etc.

In addition, these inspections are conducted to confirm the controls needed over operation activities to prevent unauthorised changes to hardware, software and system parameters.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

The guidance of IEEE Std. 603 and IEEE Std. 7-4.3.2 are directly applicable to those parts of data communication systems that support safety system functions.

Where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). If a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, the review should confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the safety system.

Guidance for evaluation of physical and electrical independence is provided in IEEE Std. 384. Physical independence is attained by physical separation and physical barriers.

Electrical independence should include the utilisation of separate power sources.

KINS reviews SAR to confirm that DI&C system satisfies the requirements of the acceptance criteria and guidelines applicable to the communication system. KINS performs pre-operational inspection to confirm independence of installed system according to SAR.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

There is no specific process to evaluate DI&C related events. KINS evaluates trending analysis of events by licensee and disseminate lessons learnt if necessary.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

No.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

KINS consider hardware random failures (for example, fault of processor, memory) as the typical failure mode of DI&C system. Some software failures of non-safety DI&C system are considered as failure mode if applicable.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

KINS SRG appendix 7-13 "Guidance on software reviews for digital computer-based instrumentation and control systems" provides guideline on software maintenance plan. The maintenance phase on DI&C systems/components consists of ensuring the continued use and operation of the software as designed.

Periodic inspection is performed to verify adequacy of configuration management and the controls needed over operation activities to prevent unauthorised changes to hardware, software and system parameters. Secure operational environment inspection is also conducted to confirm the controls needed over operation activities to prevent unauthorised changes to hardware, software and system parameters.

11.2. What kind of functional tests does your RB inspect? Please describe.

KINS performs pre-operational inspection of commissioning functional tests and vendor inspection of the integration test or factory acceptance test to check final product for new plants. Also, KINS conducts periodic inspection on calibration including functional test and response time test of DI&C system.

12. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections (e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

References

IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations".

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

IEEE Std. 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits".

IEEE 1042, "IEEE Guide to Software Configuration Management".

Poland

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes. Our licensee's RR uses DI&C systems which are important-to-safety. For example:

- control system of fuel channels cooling pumps including RHR system.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

RB verifies if installed or modified systems do not have negative impact for nuclear safety because of worse quality, lower scope of measurements scale, different condition of work environmental. Afterwards RB assess reliability of this equipment and how manufacturer proves its quality.

2.2. Describe how DI&C is captured in the licensee technical basis.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Not yet. It is difficult to obtain experienced I&C specialist for RB.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing)?

There are adequate provisions in our law to inspect every stage.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

N/A

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

N/A

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

N/A

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

No.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

N/A

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

N/A

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

N/A

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

No.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

N/A

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

N/A

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

According to regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiological protection requirements which must be fulfilled by a nuclear facility design: "§ 78.4. The control and measuring devices, referred to in Section 1, shall be qualified in keeping with environmental conditions which could occur in given nuclear facility states, ensuring that these devices are appropriate for nuclear facility parameter measurements in accident conditions so as to enable the nuclear facility operator to recognise the situation at the nuclear facility and to classify the events for the purpose of emergency response".

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how this is inspected.

N/A

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how this is inspected.

N/A

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

At this moment there are no procedures on DI&C RB's inspections.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

In case of the RR we don't have any database for DI&C related events.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

In case of the RR there haven't been any DI&C events yet.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

N/A

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

There are no special requirements regarding DI&C.

11.2. What kind of functional tests does your RB inspect? Please describe.

In case of the RR the scope of application of DI&C is too small to be specifically targeted.

Russia

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes. Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, the containment, and the state of the spent fuel storage. Instrumentation shall also be provided for obtaining any information on the plant necessary for its reliable and safe operation, and for determining the status of the plant in design basis accidents. Provision shall be made for automatic recording of measurements of any derived parameters that are important to safety.

Instrumentation shall be adequate for measuring plant parameters and shall be environmentally qualified for the plant states concerned.

Computer based systems used in a reactor protection system, shall fulfil the following requirements:

- the highest quality of and best practices for hardware and software shall be used;

- the whole development process, including control, testing and commissioning of design changes, shall be systematically documented and reviewed;
- in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken;
- where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Authorises: by licensing of nuclear power plant unit siting, construction and operation.

Criteria – in the:

- Federal Rules and Regulations, e.g. NP-001-15, NP-026-16, NP-031-01.
- the state codes and standards in DI&C design, manufacturing and construction, e.g. GOST 34.201,GOST 29075.
- IEC standards, e.g. IEC 60068/ 60231/ 60780/ 60880/ 60960/ 60964/60965/ 60980/ 60987/ 61513/ 61771/ 61839.

2.2. Describe how DI&C is captured in the licensee technical basis

Special chapter in SAR (licensee technical basis) is dedicated to DI&C.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

As a rule during nuclear power plant operation they are inspected inside inspections of appropriate technological systems. But is possible goal inspection of DI&C systems or their parts.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Designers, manufacturers, vendor and operator of nuclear power plant SSC (including DI&C systems) have licences of Rostechnadzor and periodically inspected. Beside the, inspectors of RB (or specialists of Technical-Research Supporting Organisation of RB) inspect some points of manufacturing and take part in the functional or acceptance testing.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Scope of the inspections – to check licence conditions.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

Specific inspections are conducted by specialists of Technical-Research Supporting Organisation of RB.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

DI&C systems/components are inspected as separately, as together with other DI&C systems/components and SSC.

Scope of the inspections:

- to check licence conditions;
- to inspect some points of manufacturing or to take part in the functional or acceptance testing.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Yes, for example, embedded digital measuring devices of fire protection system and automatic radiation monitoring system.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

Criteria – in the state codes and standards.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Requirements – in the state codes and standards.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

By checking of appropriate verification and validation of software.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

No, for important-to-safety applications for nuclear power plants, all modifications replacements must be expertised and approved by RB (changing of licence conditions).

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

The equipment of the DI&C systems qualified in the manufacturer and then in the nuclear power plant for:

- seismic impact in accordance with NP-031-01;

- electromagnetic interference in accordance with GOST R 50746-2000.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Software must be validated.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Hardware must be certificated. Specific criteria are absent.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Criterias – in the state codes and standards and Federal Rules and Regulations.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Requirements to the process of evaluating events(including DI&C related events) – in the Federal Rules and Regulations NP-004-08 (Regulation on the procedure for investigation and accounting of nuclear power plant events).

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

Yes. Event on units No. 3 and No. 4 Leningradskaya Nuclear Power Plant 10.04.2017. Reduction of thermal power of power units No. 3 and No. 4 by 54 % of the previous power level in the BUSM-1T mode due to the disconnection of TG-5 and TG-7 by the action of emergency automation due to a short-term increase in voltage in the secondary circuits of the transformer voltage of the high-voltage line 750 kV.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

For example, periodic testing DI&C systems/components.

11.2. What kind of functional tests does your RB inspect? Please describe.

Full functional tests, partial functional tests

Slovenia

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

- Only CZ system is SR system which includes DI&C systems/components (CZ = chilled water system – MCR and battery room cooling system).
- Some NSR (but important to safety) systems includes DI&C components: PDEH (Programmable Digital Electro Hydraulic System for Turbine regulation), ICCMS (Inadequate Core Cooling Monitoring System), AMSAC (ATWS Mitigation Safeguard Actuation Circuity), RCP and TU Vibration Monitoring, regulation of HD (Heater drain system) and MSRs (Moisture Separator Reheaters), etc.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

- SNSA uses the same process as for other modifications.
- Design requirements are included in regulation JV5 (Rules on Radiation and Nuclear Safety Factors). Requirements include environmental qualification, software verification and testing, authorisation of access, etc.

2.2. Describe how DI&C is captured in the licensee technical basis.

- Licensee has in place the programme and several implementation procedures for the area of DI&C systems/components.
- Above mentioned procedures include configuration management, system design modifications, digital device inspection, cyber security, rules for human machine interface, documentation for new applications, etc.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

- Currently we do not perform regular inspections at this area. One broader topical inspection on DI&C systems/components was performed in 2016 covering design, purchasing, installation, operation, maintenance, obsolescence, NCFSI).
- We plan to incorporate topical inspection on this area into inspection plan on a two-year basis.
- We partially cover DI&C systems/components with other comprehensive inspections (EQ, modifications, testing, maintenance, vendors).

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

- As mentioned in 3.1 SNSA currently does not perform regular inspections from DI&C. In 2016 all mentioned stages were included into topical inspection review on this area.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

- For scope see 3.1 and 3.2.
- Regarding experts SNSA for that kind of inspectors uses mixed team from Inspection Division and Nuclear Safety Division (comprised of electrical and mechanical engineers).
- During outage we also use experts from authorised Technical Support Organisation.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

- SNSA does not have inspectors specifically trained to inspect DI&C systems/components.
- Currently main basis for DI&C inspections represents knowledge gained on NEA and IAEA workshops/meetings as well as personal experience of inspectors.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

- SNSA currently does not perform separate inspections in this area. See answers above.
- SNSA does not inspect vendors directly. We inspect licensee's system.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

- Licensee tries to avoid this kind of digital devices.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

- Currently we do not have specific criteria.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

- The same criteria as for other DI&C components.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

- So far, we have not inspected software modification process specifically.
- Usually we perform inspection of tests implemented after maintenance or modifications (including software modification).

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

- Yes. Requirements for DI&C commercial grade dedication are incorporated into licensee's programmes and procedures.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

- Authorisation of commercial grade dedication process for DI&C is a part of SNSA licensing process.
- Currently SNSA does not perform regular inspections of commercial grade dedication process for DI&C.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

- SNSA does not have specific criteria.
- For the authorisations SNSA uses practices of other regulators (mainly NRC).

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

- Licensee has in place programmes and implementation procedures for equipment qualification of electrical and I&C equipment (including DI&C). Qualification requirements depends on actual environment conditions (temperature, vibrations, humidity, radiation), electromagnetic compatibility, seismic requirements, etc.
- Licensee provides purchase technical specifications including requirements regarding qualification.
- Vendor needs to perform tests/analyses according to standards and specifications. Based on this vendor issues reports and certificates.
- During licensing process RB review qualification reports and certificates. Several topical inspections were performed on qualification process.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

- No specific criteria.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

- No specific criteria.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

- No detailed criteria.
- Licensee uses IEEE standards regarding this topic.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

- SNSA has in place a process to follow operating experience (including independent SNSA root cause analysis, PSA analysis where applicable, reactive inspections). This process includes also DI&C related events.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

- Up to now the licensee had no reportable DI&C events.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

- N/A.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

- SNSA does not have special requirements regarding maintenance on DI&C systems/components.

11.2. What kind of functional tests does your RB inspect? Please describe.

- During the licensing process, the SNSA reviews reports of implemented FATs and SATs.
- We are also present at some of SATs.
- For detailed evaluation of functional tests, we used authorised Technical Support organisations.

12. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections (e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

- specification requirements for DI&C modifications;
- review of RB requirements regarding licensing and inspection of DI&C systems/components;
- important DI&C inspection findings;
- important DI&C operating experience.

Spain

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes.

For example, the Solid State Protection system electronic cards can feature digital components.

Other examples would be the use of digital devices in safety related equipment such as battery chargers, inverters or breakers for class 1E electrical buses.

There are also digital components in radiation measurement equipment with associated safety-related actions.

More examples would be the use of digital devices in the:

- control of the turbine-driven pump of the AFW system;
- leakage detection system.

Digital devices are also starting to be used in air flow transmitters and process controllers.

2. Licensing to use DI&C systems/components.

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Regulation in Spain allows the use of digital systems in nuclear power plants. It is in fact specifically authorised in the generic design criterion of Spain's mandatory instruction IS-27,

Spains' RB, the CSN, worked together with the utilities (UNESA) and issued a guide that establishes a methodology for licensing digital systems for nuclear power plants.

This guide was intended to provide in a single document a global vision of the most relevant steps to introduce digital systems in nuclear power plant safety-related systems. However, the guide does not specifically address all licensing modification in nuclear power plants, but instead redirects to other documents, such as NRC's regulatory guides.

Specific requirements to be met are the ones that appear in those RG that deal with digital issues and have been incorporated to the facility's licensing basis: namely RG 1.152, RG 1.168, RG 1.169, RG 1.170, RG 1.171, RG 1.172 and RG 1.173.

2.2. Describe how DI&C is captured in the licensee technical basis.

All RGs, including the ones dealing with digital modifications or systems, are periodically incorporated into the nuclear power plants' licence basis.

3. Inspection of DI&C systems/components.

3.1. Does your RB specifically inspect DI&C systems? Describe how.

There are NOT specific periodic inspections on digital I&C systems. There have been inspections and meetings to address specific digital design modifications. Additionally, some design modifications inspections have included digital devices from time to time.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Yes, all stages are inspected, though maybe not enough in depth.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Inspections aim to understand if the digital equipment development process has been carried out following existing regulations, which would ensure an adequate quality of the final product.

Inspectors' expertise is obtained during licensing process for design modifications, with the participation in international seminars or working groups and with assistance to EPRI training courses.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

As already mentioned, inspectors' expertise is obtained during licensing process for design modifications, with the participation in international seminars or working groups and with assistance to EPRI training courses. There is no specific training, inspector's motivation and initiative are of primary importance.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

Up to now, the inspections that have been carried out have always been restricted to the licensee, who has provided the necessary vendor's documents. Therefore, digital I&C equipment has NOT been separately inspected.

However, existing regulations allow the inspection of vendors in the vendor's facilities in presence of the licensee.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Regarding CPLD, they are used in:

- 1 nuclear power plant: SSPS;
- 1 nuclear power plant: battery chargers;
- 2 nuclear power plant: inverters.

The problem is that, at least initially, licensees fail to identify the existence of embedded digital devices in the design modifications, hence they don't consider the modification to be digital and therefore do not request licence amendments.

This is creating some trouble on how to treat this design modifications, though this issue has also arisen in the United States.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

Most of the time the embedded digital devices are already installed at the facility when the RB or the licensee identify its existence.

Since the software development process was too difficult to trace, the licensee has opted to test 100% of the inputs, combinations, sequences and states. This testing is currently under development.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

The requirements would be the same as for a digital device, though some activities might be easier since the code can't usually be changed easily.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

The compliance with Regulatory Guide 1.169, related with configuration management in nuclear power plants, which is licence basis for all licensees.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Yes.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

For the authorisation, compliance with Regulatory Guide 1.152 and its reference rules is verified. This in the end means endorsing EPRI's TR-106439, at least regarding COTS equipment.

Inspections fall under the Reactor Oversight Program design modifications inspections.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

The specific criteria would be the ones exposed above and contained in EPRI TR-106439.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

The electrical and I&C department of Spain's RB carries out verifications regarding compliance with RG 1.180, regarding EMI and compatibility.

Environmental qualifications is verified by the maintenance and ageing management

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Compliance with RG 1.169 is verified, regarding configuration management. Specific criteria for software do not exist.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Compliance with RG 1.153, regarding safety and non-safety equipment separation) and RG 1.152 in specific digital. The Standard Review Plan (Nureg-0800) would also apply, specifically chapter 7.9 regarding Data communication systems, as well as Nureg-CR/6082.

CSN has not assessed communications between systems.

10. Operating Experience. Events due to modification/installation of DI&C systems/components.

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Within the CSN there is a branch that specialises in operating experience and analyzes the events occurred in all nuclear power plants. This analysis is supposed to be multidisciplinary and it makes no difference whether or not any digital equipment has been involved in the event.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

The question is not well understood.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

The question is not well understood.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

There are requirements over the existence and availability of established plant procedures to monitor and assess the error logs generated by the systems, as well as to ensure that adequate configuration control is maintained. There are also requirements on the training received by the operators of digital systems.

11.2. What kind of functional tests does your RB inspect? Please describe.

The functional tests inspected by the CSN are tests following RG 1.22, which is not specific for digital modifications but should include some specific verifications on functional aspects of software.

Sweden

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

DI&C are used for both safety and non-safety related systems. Usage of DI&C in safety related equipment is declining due to closure of the oldest nuclear power plants in Sweden.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Independently of technology, it is the responsibility of the licensees to proof that implemented equipment are compliant to its requirements according to the Swedish Radiation Safety Authority oversight process.

There are mainly two regulations, (SSMFS 2008:1 The Swedish Radiation Safety Authority's Regulations concerning Safety in Nuclear Facilities and SSMFS 2008:17 The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power Reactors) that are the basis for the assessment of I&C.

The current regulations will most likely be superseded during 2020 with new regulations. For changes in the nuclear power plants, the new regulations will place great emphasis on that both safety and security shall be demonstrated in a safety demonstration. In order to be able to assess the systems whole lifecycle the licensees shall provide a safety demonstration plan to Swedish Radiation Safety Authority in the pre-design phase.

2.2. Describe how DI&C is captured in the licensee technical basis.

DI&C included in technical basis reflects the amount of DI&C implemented by the licensee after the design phase. DI&C has mainly been implemented in technical basis for older nuclear power plants that have been shut down or are about to be shut down before the end of 2020.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

The Swedish Radiation Safety Authority is currently focusing on overseeing DI&C when implemented in Swedish nuclear power plants. However are other oversight activities also performed, especially related to processes for maintenance and changes in existing systems.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

The Swedish Radiation Safety Authority considers it is of most importance to oversee all the processes during the systems whole lifecycle. Even though current regulations not require involvement of the regulatory body in the early phases. The RB together with the licensees have been working in close contact during the DI&C projects since late 90s.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

The inspection staff is chosen on a case-by-case basis based on the expertise needed for a specific inspection. A generic inspection of DI&C includes staff expertise in maintenance, operations, DI&C and human factors.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

Inspectors at the Swedish Radiation Safety Authority are mostly senior engineers within their field of expertise. All inspectors have a personalised education plan to evolve in their field of expertise.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

No, the technology is reviewed within the scope of its implementation. The interface between different technologies is an important factor during the oversight.

An update of the Nuclear Activities Act that took place in August last year now gives SSM the possibility to perform vendor inspections, which SSM was not allowed to do before. The new regulations will give guidance on how to use it.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Our licensees use embedded digital devices in varying ways, depending on their nuclear power plants. Embedded digital devices are mostly used in non-safety related equipment. Even though it cannot be fully avoided, the licensees make great efforts to avoid embedded digital devices when replacing old analogue instrumentation.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

CCFs in embedded digital devices are specifically inspected with regard to its implications on nuclear safety. It's hard to fully prove that programmable equipment have no common failure modes, the RB normally pay attention to the consequences of CCF in the embedded digital devices and diverse means to provide the safety function.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

There are no specific requirements issued with regards to embedded digital devices in the regulations from the Swedish Radiation Safety Authority. The requirements are focused on processes and that applicable guidelines and standards are followed.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Functional changes in safety related software are reported to the Swedish Radiation Safety Authority. The focus during such inspection, except the implementation itself, is to review if there are processes that ensures that other functionality in the software is not affected. The inspection also focuses on test programmes and if the software is safe to use.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

No, not to the same extent as other electrical/electronic equipment.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

For I&C systems/components the system/components are usually qualified by a vendor which not necessarily is the original producer of the components. Therefore, it is of great importance to be able to assess the vendors processes as well. Today it's the licensees responsibility to provide the RB with the adequate documentation that are necessary to assess the qualification. The new regulations will give the RB increased authorisation to assess the vendor itself (possible due to the updated Nuclear Activities Act).

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

Normally the systems/components are classified to the extent necessary to demonstrate that they fulfils the standard for given safety class. The Swedish licensees are not bound to a specific standard. For electrical systems and components both IEEE and IEC are used. Both as a guideline for the licensees and support for the authority international common positions are used. For example, TF SCS Licensing of safety critical software for nuclear reactors.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

The requirement for equipment qualification for DI&C is identical to other electrical equipment. Fulfilment of environmental requirement shall as far as reasonable possible be verified by testing. DI&C is more likely to be affected by electromagnetic hazards therefore more attention should be laid on electromagnetic when assessing DI&C than other components/system.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

There are no specific requirements issued with regards to different software versions by the Swedish Radiation Safety Authority. The requirements are focused on processes and that applicable guidelines and standards are followed

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

There are no specific requirements issued with regards to different hardware versions from the Swedish Radiation Safety Authority. The requirements are focused on processes and that applicable guidelines and standards are followed

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Independence is required between equipment that is classified as safety equipment and not safety equipment and between redundant safety equipment. Equipment that is not safety related shall not affect safety related equipment in case of failure. There are also requirements related to independence between IT security zones.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

All events or incidents that affects nuclear safety shall be reported to the RB. There is no dedicated process for DI&C. The staff for evaluating a specific event is chosen on a case-by-case basis based on the expertise needed for the specific task.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

Yes. The most severe events have been hardware related, i.e. power supply equipment or priority modules. All of the failures have been within the MTBF reported from the vendor. However, the RB has on occasion forbid licensees to take nuclear power plants in operation, after changes in software, due to shortcomings to demonstrate that other functionality of the software has not affected.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

A typical failure is loss of function in one of four divisions due to processor failure, failure of processor power supply or failure of single IO-module. The systems are designed to have such failures without jeopardise the plant safety. In most cases, the failure rate has been less than expected.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

When assessing implementation of new DI&C, the RB have had focus on the implementation processes and that there are tools to be able to perform maintenance without affecting safety related functions or IT security in a negative way.

11.2. What kind of functional tests does your RB inspect? Please describe.

Processes and instructions that ensures safe and reliable periodic tests are assessed as a part of the total scope of assessment during implementation of new DI&C

United Kingdom

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes, we have one existing example of a licensee using a DI&C reactor protection system (Class 1 safety system) on an operating plant as well as numerous examples of DI&C control systems (Class 2/3 safety-related systems).

All four of the reactor designs that have been submitted to the ONR for Generic Design Assessment (GDA) have proposed the use of DI&C reactor protection and control systems (see www.onr.org.uk/new-reactors/index.htm for details).

All operating plants and GDA submissions in the United Kingdom use DI&C industrial devices of limited functionality in safety and/or safety-related applications.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

The overall approach to regulation adopted by ONR is described on our website at www.onr.org.uk/regulation-and-licensing.htm. Before ONR can permission key activities such as the installation and use of DI&C systems we assess licensees' safety cases, on a sample basis according to potential consequences, to ensure that the hazards have been understood and are properly controlled.

For the use of DI&C systems ONR expects the licensee to provide a justification in the safety case where such systems are fulfilling safety functions identified as Category A, B or C in accordance with IEC 61226, and the SSCs are identified as Class 1, 2 or 3 in accordance with IEC 61513.

ONR Safety Assessment Principles ECS.1 – Safety Categorisation and ECS.2 - Safety classification of structures, systems and components (www.onr.org.uk/saps/index.htm), as well as Technical Assessment Guide NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components (www.onr.org.uk/operational/tech_asst_guides/) provide further guidance regarding ONR expectations for categorisation and classification.

ONR use Safety Assessment Principle ESS.27 - Computer-based safety systems (www.onr.org.uk/saps/index.htm) and Technical Assessment Guide NS-TAST-GD-046 - Computer Based Safety Systems (www.onr.org.uk/operational/tech_asst_guides/) to determine whether the safety justification for the DI&C equipment is adequate for the intended application.

The expectation is that the DI&C equipment will be shown to conform with NS-TAST-GD-046 and the applicable IEC standards for the safety function category / SSC classification e.g. IEC 60880 for Category A functions, IEC 62138 for Category B and C functions.

2.2. Describe how DI&C is captured in the licensee technical basis.

ONR expects explicit justification of the DI&C equipment in the Licensee safety case, NS-TAST-GD-051 - The Purpose, Scope, and Content of Safety Cases (www.onr.org.uk/operational/tech_asst_guides/) provides guidance regarding safety cases. The means by which the safety justification of DI&C is captured is not prescribed however the SAPs and TAGs discussed in the response to 2.1 above will be used to assess this aspect of the safety case.

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Yes. During the design and manufacturing phases (including GDA) document reviews may be undertaken at the licensee premises or at ONR offices. Occasionally a review may take place at manufacturer premises but this is not the norm. During the installation, commissioning and operational phases, formal inspections are undertaken at the licensee site to determine compliance with the applicable licence conditions.

The site based inspections are typically undertaken either during a plant shutdown to determine readiness of the reactor to restart, or as a specific system-based inspection (SBI) during power operations. The SBI may be single-discipline or multidisciplinary e.g. the DI&C Inspector may be accompanied by Human Factors, Security or other Specialist Inspectors.

The inspection approach is common to all disciplines, technical assessment guides (www.onr.org.uk/operational/tech_asst_guides/) and technical inspection guides

(www.onr.org.uk/operational/tech_insp_guides/index.htm) are used as the basis for specific aspects of the inspections.

For DI&C systems technical assessment guide NS-TAST-GD-046 - Computer Based Safety Systems applies throughout, for site-based inspections the following technical inspection guides also apply:

- NS-INSP-GD-019 - LC19: Construction or Installation of New Plant;
- NS-INSP-GD-020 - LC20: Modification to Design of Plant Under Construction;
- NS-INSP-GD-021 - LC21: Commissioning;
- NS-INSP-GD-022 - LC22: Modification or Experiment on Existing Plant;
- NS-INSP-GD-027 - LC 27 Safety Mechanisms, Devices and Circuits; and
- NS-INSP-GD-028 - LC28 Examination, Inspection, Maintenance and Testing (EIMT).

In addition, the UK legal requirement to reduce risk as low as reasonably practicable (ALARP) applies to all ONR assessment and inspection activities. Technical assessment guide NS-TAST-GD-005 - Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable) provides further information in this regard.

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Yes, see 3.1 above.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

All design, development, installation, commissioning, modification and operational records fall within the scope of the inspections, the specific documents selected depend upon the phase of the lifecycle at which the inspection takes place. A sampling approach is taken to the inspections. The sample is typically focused on areas of uncertainty, risk (safety and project), low confidence or high safety significance.

For site-based inspections an assessment of the physical condition of the equipment is undertaken.

The inspections are carried out by ONR Specialist Inspectors, typically Chartered Engineers, supported by technical support contractors where necessary. All regulatory decisions are taken by the ONR Specialist Inspectors who are also warranted Nuclear Safety Inspectors.

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

ONR Specialist Inspectors undertake an extensive technical, behavioural and regulatory training programme within ONR. Where necessary, external training is provided for novel or highly technical topics e.g. the safety justification of FPGAs.

Specialist DI&C Inspectors are members of the ONR Electrical, Control and Instrumentation (E,C&I) Professional Group. The group is run by a dedicated Professional Lead who is responsible for maintaining a DI&C capability within the organisation.

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

DI&C inspections are undertaken as part of an integrated intervention strategy. Each division of the ONR e.g. New Reactors, Operating Reactors etc. will develop an intervention plan that covers all aspects of regulatory inspections for the division, including those focused on DI&C. Occasionally an inspection may be initiated following the identification of significant or repeated operational issues.

The DI&C inspections are typically undertaken separately due to the specialist nature of the activity. As mentioned in 3.1 above, the inspections may be undertaken by DI&C Specialist Inspectors only, or may also address multidisciplinary aspects such as Human Factors or Security.

ONR has not yet undertaken formal vendor inspections for DI&C on operational plants. Reviews of supplier's design and development documentation have taken place at their premises as part of the GDA process.

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Yes. Embedded digital devices have been found in package plant such as mechanical handling equipment and HVAC systems. Devices range from sensors and actuators to programmable logic controllers.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

The inspection criteria for these devices are the same as those described in 3.1 above.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

The qualification criteria are the same as those described in 3.1 above for protection and control systems i.e. those defined in NS-TAST-GD-046 - Computer Based Safety Systems.

A significant concern regarding embedded digital devices is the ability of the licensee to identify where they have been used. The procurement of package plant such as those described in 4.1 above is typically the responsibility of other disciplines. These other disciplines often do not recognise that embedded digital devices have been used in safety applications within the package plant and therefore do not engage DI&C specialists in their substantiation.

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

The approach, technical assessment guides and technical inspection guides identified in the response to 3.1 are applied. In particular, the following guides are used:

- NS-TAST-GD-046 - Computer Based Safety Systems;
- NS-INSP-GD-020 - LC20: Modification to Design of Plant Under Construction;
- NS-INSP-GD-022 - LC22: Modification or Experiment on Existing Plant;
- NS-INSP-GD-028 - LC28 Examination, Inspection, Maintenance and Testing (EIMT).

It should be noted that ALARP considerations may influence the approach and acceptability of aspects of modifications to operational systems as opposed to new designs (see NS-TAST-GD-005 - Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable).

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

The licensee processes for the safety justification of commercial grade items (commercial-off-the-shelf (COTS) items in the United Kingdom) are largely the same as for bespoke systems.

For industrial devices of limited functionality the safety justification approach has been informed by research undertaken by the Licensees. This research has resulted in the development of the 'EMPHASIS' tool that is used to assess conformance with applicable standards.

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

As a non-prescriptive regulator ONR does not authorise or approve the commercial grade dedication process for licensees. ONR does seek to influence the licensees to follow relevant good practice as defined in technical assessment guides and international standards during the development of their processes.

Each application of the commercial grade dedication process is assessed on its own merits. The inspection typically involves a review of the licensee safety case and a sample of the documentation provided by the system/component manufacturer. The inspection may be undertaken at ONR premises, licensee premises or at the manufacturer's premises if intellectual property concerns are raised.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

ONR does not approve the use of a system or component. The implementation of the licensee process described in 6.2 above is assessed for specific applications. The assessment criteria are the same as those defined for bespoke systems i.e. those defined in NS-TAST-GD-046 - Computer Based Safety Systems.

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects).

ONR does not prescribe the details of relevant standards, certification and/or qualification criteria for nuclear plants and facilities as this is deemed to be the responsibility of the site licensee.

The ONR regulatory expectations regarding equipment qualification are captured in the safety assessment principles (http://www.onr.org.uk/saps/index.htm), in particular the following apply:

- EQU.1 - Qualification Procedures;
- ECS.3 – Codes and Standards;

- ESS.11 – Demonstration of Adequacy.

ONR guides on aspects of this topic include NS-TAST-GD-013 - External Hazards, NS-TAST-GD-015 - Electromagnetic compatibility and NS-TAST-GD-019 - Essential Service.

ONR are currently drafting a technical assessment guide for the qualification of equipment. The scope of the guide extends beyond DI&C systems. In principle, the approach taken by ONR aligns with the recommendations made on this subject in IAEA Safety Standard SS-2/1.

A key element of ONR's approach to assessing the suitability of DI&C systems and equipment that have a role in supporting SSCs important to safety is to ensure that that these are designed, manufactured, constructed, etc. to appropriate codes and standards. For DI&C systems and equipment this typically refers to relevant international and European standards, which have been transposed into BS EN or BS IEC standards by the British Standards Institution (BSi), and particular attention should be given nuclear sector specific standards published by BSi technical committee NCE/45. In addition, there is a regulatory expectation that DI&C systems and equipment be subject to qualification procedures to confirm that they will perform their allocated safety and/or support function(s) in all operational, fault and accident conditions identified in the licensees safety case and for the duration of the operational lifetime of the plant or facility. The qualification process is intended to ensure, as necessary, that the DI&C systems or equipment will withstand the effects of external (e.g. seismic, shock, adverse temperatures) and internal (e.g. flooding, fire) hazards.

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

ONR expect the licensee to establish and apply adequate modification and configuration management arrangements such that changes between software versions may be controlled, verified and validated. ONR safety assessment principle ESS.15 - Alteration of configuration, operational logic or associated data and technical assessment guides NS-TAST-GD-003 - Safety Systems and NS-TAST-GD-046 - Computer Based Safety Systems provide further guidance in this regard.

The inspection arrangements for this topic are the same as those described in 3.1 above.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

The expectations for hardware configuration management are identical to those for software as described in 8.1 above.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

ONR safety assessment principle ECS.2 expects that SSCs that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety. Paragraph 167 of the safety assessment principles further explains that appropriately designed interfaces should be provided between (or within) SSCs of different classes to ensure that any failure in a lower class item will not propagate to an

item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

DI&C events are evaluated in a similar manner to all events that are reported to ONR. ONR guidance ONR-OPEX-GD-001 - Notifying and Reporting Incidents and Events to ONR (www.onr.org.uk/operational/inspection/onr-opex-gd-001.pdf) assists licensees in relation to notifying events to ONR. Once notified to ONR the nominated ONR site inspector will identify suitable specialisms (e.g. Electrical, Control and Instrumentation (E,C&I)) for further notification. The specialisms will consider the totality of events submitted for review via quarterly, and yearly, intelligence reviews. The internal ONR guidance for undertaking Specialism Regulatory Intelligence Reviews states:

"The purpose of the event and intelligence review is to identify intelligence signals and evidence that are either sufficient in their own right in terms of substantiation or which may be used with further analysis to provide corroborated evidence to derive actionable intelligence."

Input to the reviews is decided by the E,C&I Professional Lead but includes a wider scope than just notifications from the licensees, for example; licensee follow up reports, inspection ratings, issues database, licensee internal regulator data, and also INES and IRS reports etc.

The data is presented at a facilitated workshop supported by sufficient SQEP to identify actionable OPEX. Actionable OPEX will be reviewed to determine if it is appropriate for further follow up, for example further intervention plans, OPEX brief, themed inspections across a licensees' sites etc. This would feed into the yearly planning discussions which would determine the Integrated Intervention Strategy (IIS).

As part of the ONR Regulatory Intelligence (RI) process external OPEX is also directed to the E,C&I Professional Group on a monthly basis by the RI team to assist in identifying relevant information to feed into OPEX reviews.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

ONR safety assessment principle EDR.4 - Single failure criterion; expects that during any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. ONR assessments explicitly evaluate that this criterion is met for those systems that are the principal means of fulfilling Category A safety functions.

In addition, for safety and safety-related DI&C systems, the requirements of IEC standards such as IEC 60880, IEC 62138 and IEC 60987 regarding the systematic evaluation of failure modes form the basis of ONR inspection programmes.

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

UK Site Licence Condition LC28 requires that the licensee shall make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all plant which may affect safety (www.onr.org.uk/documents/licence-condition-handbook.pdf).

ONR technical inspection guide NS-INSP-GD-028 - LC28 Examination, Inspection, Maintenance and Testing (EIMT) and technical assessment guide NS-TAST-GD-046 - Computer Based Safety Systems provide further guidance to ONR Inspectors in this regard.

11.2. What kind of functional tests does your RB inspect? Please describe.

It is not usually the case that ONR Inspectors witness functional tests, rather, the records of such tests are reviewed during inspections. Under LC28 the ONR expectation is that safety functions performed by DI&C SSCs are subject to an EIMT regime that ensures that the nuclear plant remains capable of performing its safety functions, with the required level of reliability.

Wherever possible, it is the preference that an end to end test of the safety function is performed whereby the input to the DI&C system is manipulated while the output is monitored to ensure that the safety function is performed as and when required. It is acknowledged that it is not always possible to complete an end to end test as this may require the licensee to drive the plant to a potentially unsafe state. In such circumstances the licensee must present and justify their arrangements that allow partial tests to demonstrate the adequacy of the whole circuit.

12. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections (e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

The ONR expectation is that DI&C inspections would be undertaken by suitably qualified and experienced DI&C specialists (N.B. ONR DI&C specialists are also warranted Nuclear Safety Inspectors). It has been suggested previously that non-specialists may be involved in such inspections. If so, we would appreciate clarification on the role of non-specialists in such activities.

12. Use of DI&C systems/components in nuclear power plant applications,

12.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Yes, US licensees use DI&C systems/components to various degrees in both safety related and non-safety-related applications.

Beginning in the early 1990s, several US installations installed versions of the Westinghouse Eagle 21, 808286 based system, as for portions of the primary protection system functions and a couple use it for the primary protection system, and Allen-Bradley programmable logic controllers (PLC) as the emergency diesel generator sequencers. More recently, licensees developed and installed core calculator systems based on the Westinghouse Common Q CPC system and AREVA Teleperm as a reactor safety system. The scope of the safety functions DI&C has been integrated into ranges from a couple of

protection system functions to entire safety systems as well as variable low temperature over pressure (VLTOP), various systems for anticipated transient without scram (ATWS), GE NUMAC based nuclear instrumentation systems, to post accident monitoring systems.

Non-safety related functions include Digital Rod Control and Position systems (Framatome Triconex upgrade to B&W Diamond rod control system, main turbine control systems (e.g. GE Mark 6 and Mark 6e systems, Ovation Turbine Controls), feedwater controls, (Lovejoy Control systems, Ovation controls, Woodward turbine control systems, GE Fanuc, Triconex), rod control systems (GE NUMAC), and plant computer systems.

For new reactors, all the applicants and those planning on becoming licensees use or plan to use digital systems to control their safety-related (important to safety, per the context of the question stated above) and non-safety related (no safety significance per the context of the question stated above). I&C systems are approximately 90 percent digital (best estimate). The reactor protection system is digital and there is also embedded digital technology in many of the plant systems (e.g. inverters). This is the case for the AP1000 as shown below. New reactors under construction such as Vogtle Units 3 and 4 use the Common Q based platform for its safety I&C systems and a FPGA based platform for its DAS:

AP1000 – Safety Related – Common Qualified (Common Q) [microprocessor-based] along with the Component Interface Module subsystem [FPGA-based] for component control of Safety related components

Non-Safety Related – Ovation based system

Many of the instruments (particularly those in a harsh environment) are still not digital. For the Gen III+ and Gen IV plants, the scope of important-to-safety systems is reduced.

United States

1. Licensing to use DI&C systems/components

1.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Our RB currently authorises the use of digital technology primarily through the use of guidance that typically provides one method acceptable to the Commission, however other methods can be utilised if they can be shown to be acceptable via analysis and evaluation. Currently, from a regulatory standpoint, regulations concerning I&C systems do not differentiate between digital and non-digital systems.

The plants must submit a combined license (COL) application if using 10 CFR Part 52[3] or a construction application/operating licence application if using 10 CFR Part 50[4]. Once the staff has reviewed the DI&C system design and determined that it meets applicable NRC regulations, the plant can install and use the DI&C systems. The staff may conduct audits and inspections to verify the correct implementation of the DI&C system design during development of the system, Factory Acceptance Testing, or Site Acceptance Testing.

Licensees have the authority modify their facilities under the criteria of 10 CFR 50.59[5]. Using the 10 CFR 50.59 criteria, the licensee can determine if a modification would or

[3] Part Licenses, certifications, and approvals for nuclear power plants.

[4] 10 CFR Part 50 Domestic licensing of production and utilisation facilities.

[5] § 50.59 Changes, Tests and Experiments.

would not require prior NRC review and approval. The criteria require qualitative and quantitative analyses to determine if a more than minimal increase in various risk indicators would occur given the modification details. NRC Region-based inspectors, on a cyclic basis, inspect the licensee 10 CFR 50.59 determinations and modifications to determine if a licence amendment would have been required.

If a licence amendment is requested, the potential modification is reviewed to verify if the design satisfies the general design criteria in Appendix A[6] of 10 CFR Part 50, the facility applicable requirement in 10 CFR 50.55a(h)[7] (e.g. IEEE-279 or IEEE-603). A licensing review uses NUREG 0800[8] (SRP), for guidance on performing safety evaluations. Chapter 7 of the SRP and its appendices include review guidance for I&C systems including I&C systems that use digital technologies.

The SRP provides the following inspection guidance:

SRP Chapter 7.0 Section V, Page 7.0-14

For digital licence amendment activities associated with operating reactors, the I&C technical reviewer should contact the region to see if they would like specific items for inspection follow-up to be identified during the licensing process and included in the Safety Evaluation Report (SER). Consider aligning, if possible, inspection follow-up items to inspection areas outlined in Inspection Procedure 52003, "Digital Instrumentation and Control Modification Inspection".

For digital licence amendment activities associated with operating reactors, the I&C technical reviewer should ensure that the licensee commits to completion periods for implementing documents (e.g. testing, surveillance, and maintenance procedures) and Office of Nuclear Reactor Regulation (NRR) should include a reference to these commitments dates in the SER.

Identify as early as possible regional, licensee, and licensing project managers to facilitate timely status of licensing, construction, and installation activities. The appropriate Regional office should be kept informed as much as possible in the licensing process (i.e. RAIs [Requests for Additional Information], issues, site audits). A SharePoint (or similar) site for information exchange between NRC headquarters and the Regional office is recommended as one way to ensure rapid and continuing availability of applicable information.

For digital licence amendment activities associated with operating reactors, installation inspection may require expertise in several areas (e.g. electrical power, digital systems, operations, cyber security and software architecture). NRR should contact region staff to identify NRR staff input on required expertise early, to enable the additional training or acquisition of necessary expertise.

For licence amendments involving DI&C system upgrades, the NRC has published several Branch Technical Positions within the Standard Review plan to address DI&C related

[6] Appendix A to 10 CFR 50 General Design Criteria for Nuclear Power Plants.

[7] § 50.55a Codes and Standards, paragraph (h) Protection and Safety Systems.

[8] NUREG-800, Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition.

topics and a variety of guidance documents. Below is a list of Branch Technical Positions which provide guidance for performing safety evaluations of DI&C systems:

- BTP 7-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems;
- BTP 7-18 - Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems;
- BTP 7-19 - Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems;
- BTP 7-21 - Guidance on Digital Computer Real-Time Performance.

The following is a list of NRC regulatory guides (RGs) for use of DI&C:

- RG 1.173 – Developing Software Lifecycle Processes;
- RG 1.152 – Criteria for use of Computers in Safety Systems of Nuclear Power Plants;
- RG 1.168 – Verification, Validation, Reviews and Audits for Digital Computer Software;
- RG 1.169 – Configuration Management Plans for Digital Computer Software;
- RG 1.170 – Software Test Documentation for Digital Computer Software;
- RG 1.171 – Software Unit Testing for Digital Computer Software;
- RG 1.172 – Software Requirements Specifications for Digital Computer Software.

1.2. Describe how DI&C is captured in the licensee technical basis.

The licensing basis is described the facility's Final Safety Analysis Report (FSAR). The FSAR describes the regulations the facility meets and how it meets them. Aside from the regulations, the other requirements include the licence (which includes technical specifications) and orders. Written commitments by the licensee to the NRC are also considered part of the licensing basis.

When DI&C systems are installed as upgrades to operating nuclear power plants, a licensing basis review is performed to determine what if any changes to the licensing basis are required. Licensing basis changes typically involve changes to plant Technical Specifications (TS), Safety system setpoints, revisions to the plant specific Updated Final Safety Analysis Report (UFSAR), changes to the TS basis descriptions, and changes to the plants Technical Requirements Manual. In some cases, the digital systems are functionally equivalent to the systems they are replacing and licensing basis changes may be minimal.

In addition, title 10 CFR 50.71(e)[9] requires licensee's to periodically update UFSAR to assure that it contains the latest information developed. This includes the effects[10] of all changes made in the facility or procedures as described in the FSAR; all safety analyses and evaluations performed by the applicant or licensee either in support of approved licence amendments or in support of conclusions that changes did not require a licence amendment in accordance with § 50.59(c)(2); and all analyses of new safety issues performed by or on

[9] 50.71 Maintenance of records, making of reports.

[10] Effects of changes includes appropriate revisions of descriptions in the FSAR such that the FSAR (as updated) is complete and accurate.

behalf of the applicant or licensee at Commission request. The updated information shall be appropriately located within the update to the FSAR.

For new reactors, the DI&C systems important to safety and certain balance of plant I&C systems are included in the FSAR or in technical/topical reports that have been incorporated by reference into the FSAR.

Before approving such an application for consideration, the NRC staff reviews this FSAR, and its secondary references, to ensure a reasonable assurance finding can be made in its final safety evaluation report. However, from an everyday operability and testability standpoint, the requirements of those systems are described in the plant's TS.

2. Inspection of DI&C systems/components

2.1. Does your RB specifically inspect DI&C systems? Describe how.

Yes. Inspections of DI&C systems are performed either as part of the NRCs Regulatory Oversight Process inspections such as design basis assurance inspections (DBAI) and 10 CFR 50.59 inspections, or as part of a targeted audit in support of a licence amendment review. This usually occurs in conjunction with a plant implementation of a specific DI&C system. In both cases, inspection plans are developed and used to facilitate activities as determined by the inspection team.

For vendor inspection, we select approximately 20 vendors per year for inspection. The selection is based on risk-importance of their products or services and operating experience. If the vendor provides a DI&C system or a product with embedded digital technology, then the NRC staff would assign an inspection team of approximately four persons (some having DI&C expertise) to conduct a week-long inspection. Following the inspection, an inspection report would be issued to the vendor with any findings during the inspection.

The staff inspects DI&C systems in a multi-pronged approach. It utilises a developmental stage or phased approach (see the list of Typical Phased Approach to Testing in answer to question 3.2 below), however it also contains an over-arching quality control programme that contains many high level aspects, one of which is inspections itself. This high-level approach, primarily found in Appendix B[11], of 10 CFR Part 50, applies to many characteristics (e.g. design control and configuration management (CM), etc.).

2.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

For operating reactors, not all stages of a DI&C system lifecycle are audited or evaluated for each application. However, any phase or combination of phases of a project can be subjected to audit at the discretion of the NRC staff. The NRC regulatory infrastructure contains guidance for evaluating all phases of a typical lifecycle. Inspections of modification performed without NRC review and approval are typically conducted after the modifications have been completed. Samples of the design and implementation lifecycles are inspected. These inspections focus on the various risk indicators affected by the modification to determine if a licence amendment would have been required.

For new reactors, all stages from planning and procurement through operation are inspected. As a function of preparing for the vendor inspection, the vendor is contacted to determine where in the design/manufacturing process they currently are, so we can attempt

[11] Appendix B of 10CFR Part 50 Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

to observe particular lifecycle activities in progress, such as testing (see typical phased approach to testing below), requirements development, fabrication, etc.

Typical Phased Approach to Testing

Planning Phase

Requirements Phase

Design Phase

Implementation Phase

Integration Phase

Pre-Operational Phase

Start-Up Phase

Pre-existing Operational Reactor Inspection Program takes over at the point of operation

2.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

The scope of DI&C system inspection activities varies widely and is largely determined by the type, scale and scope of the system modification being inspected. As an example, detailed audits and regional inspections may include oversight of the site acceptance and installation tests, review of operator training programmes, review of operating procedures prior to system startup, and completion of recommended inspection items which were provided in the system safety evaluation that supported the licence amendment.

The level and type of staff expertise needed to complete inspection activities is typically determined during inspection planning. For at least one of the NRC inspections, the inspection teams were augmented by headquarters staff who performed the systems safety evaluation. The NRC has also augmented its audit and inspection teams with personnel with specialised experience in vendor inspections, cyber security and quality assurance.

For vendor inspections, the NRC staff has inspected the AP1000 reactor protection system and products with embedded digital technology (two digital inverter suppliers, an instrument supplier, and an electrical breaker vendor that commercially grade dedicates its equipment). Staff involved in the inspections have expertise in the IEEE standards, Electric Power Research Institute (EPRI) guidelines endorsed in NRC regulations, and guidance. The inspection teams are typically augmented with staff that have particular expertise in DI&C systems.

2.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

There has not been a formal training programme, but inspectors are selected based on their DI&C knowledge and experience. The agency hires individuals with DI&C background and contractors when needed. The inspections are normally led by regional specialists and supplemented by HQ experts.

Most of the training to date has been on-the-job training. NRC has staff that are trained and qualified inspectors. Under them are DI&C staff that are more knowledgeable about such systems. The NRC staff has held knowledge management seminars to transfer DI&C expertise to inspectors and other technical members. In some instances, inspectors and technical staff have participated in industry training activities or taken additional topic-specific university training.

2.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

The DBAIs and 10 CFR 50.59 inspections generally inspect modifications after they have been completed and put into service. These inspections assess the integrated systems including human machine interfaces and samples of specific components.

The staff typically inspects safety-related systems or those with augmented quality. In other words, the staff inspects those systems whose failure may not rise to the level of a failure of a safety-related system, but would reasonably impact the plant's Probabilistic Risk Analysis response. For a 10 CFR Part 52 plant, the staff inspects via ITAAC (or Inspections, Tests, Analyses and Acceptance Criteria). This type of inspection would occur in addition to a generic type of vendor inspection that might focus on overall vendor quality. For example, if the DI&C system is a stand-alone system (e.g. reactor protection system), the NRC staff would conduct a vendor inspection specifically targeted to that system. If there is embedded digital technology in a component (e.g. inverter, electrical breaker, or instrument), then inspection of the DI&C portion would be a part of a bigger inspection of the other portions of the component. For example, other parts of the vendor inspection may look at electrical design, qualification, and mechanical/material aspects.

Regarding audits, the NRC staff does evaluate DI&C platform components separately from the systems because the plant specific systems are not designed or available for review during these evaluations. The License Topical Report safety evaluations include plant specific action items which identify activities that need to be performed when a plant specific system is developed using the subject platform.

3. Embedded Digital Devices

3.1. Do your Licensees use embedded digital devices? Please describe how and where.

Yes. Embedded Digital Devices (EDDs) have been installed in a variety of systems at many operating plants. Examples of plant modifications performed that include use of EDDs are relay replacements, breaker replacements (including scram breakers), control panel indicator replacements, protection relays, time delay relay replacements and discrete controller replacements. Most embedded DI&C device installation resulted from modification that were not submitted for licence amendment NRC review and approval.

EDDs are generally appearing in new and replacement components that did not have such technology 30 years ago. Examples include reactor trip breakers, inverters, electrical breakers, instruments, skid-mounted systems (air compressors, chillers, etc.). In some cases, such devices are integral to sub-components of the system that are procured for use. Specifically, more multiple components and devices are designed and come pre-packaged as EDDs. Aside from its typical increased reliability and subsequent lower operating costs, comes the potential negative impact to the device being digitally-based, and potentially less robust than its former analogue counterparts; there also exists the need to implement a tiered approach to the potential cybersecurity issues associated with digital devices. Also, the whole issue of information awareness arises in that sometimes devices contain digital technology but the sales representative for the company in question may not even be aware of the EDD within the given device and the associated implications that entails. Therefore, if the salesperson is not aware and the sales literature of the EDD and does not explain that an EDD exists within the "updated" component, there may exist situations where the potential issues associated with EDDs have not been addressed at all. In such cases additional scrutiny of those sub-components may be needed to fully understand the potential impact to the overall system.

3.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

The regional inspectors identify most of these types of modifications during DBAI and 10 CFR 50.59 inspections. The NRC has a generic DI&C inspection plan template. This template can be used and customised to support plant and system specific inspection activities as needed.

Additionally, the SRP provides guidance, for the NRC staff performing licence amendment reviews, to include recommended inspection items in safety evaluations performed for DI&C systems. These recommended inspection items can optionally be used by inspection teams to support inspection planning and execution activities. It is also a common practice for NRC inspectors to include HQ staff on inspection teams to provide technical expertise or to provide review support for inspections of DI&C modifications.

3.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Regulatory requirements for digital devices are no different than those for non-digital devices. The NRC regulations are performance-based and are technology-neutral. Guidance on acceptable means of meeting regulatory criteria is technology-specific and is provided in the RGs and SRP references provided above.

For vendors, it is the responsibility of the licensees to pass down requirements in their purchase orders for components containing EDDs. Licensees are required to pass down quality assurance and notification requirements (10 CFR Part 50, App. B and 10 CFR Part 21[12]). They may pass down IEEE standards for overall I&C development and qualification. Generally, the only qualification requirements the NRC staff sees passed down are the Electromagnetic Interference (EMI)/ Radio Frequency interference (RFI) and seismic qualification requirements since digital technology is generally not used in harsh environments. Licensees are also passing down cyber security requirements (10 CFR 73.54[13] and associated Reg. Guides).

For safety-related system, the staff issued a Regulatory Issue Summary (RIS) 2016-05, "Embedded Digital Devices in Safety-Related Systems". This RIS provides clarification to licensees and applicants on the NRC's technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with EDDs. This RIS states, "Although I&C cabinets and components usually operate in a mild environment, some commercial components may operate in harsh or potentially harsh environments. The one unique difference in the nuclear facilities, such as nuclear power reactors, is the potential for some equipment and components to operate in a radiation environment either normally or during an accident condition. Commercial products intended to operate in a nuclear facility's potentially harsh environment should be qualified to meet the applicable requirements of NRC regulations (e.g. 10 CFR 50.49[14], for nuclear power plants) and recommendations of guidance regarding environmental qualification, which includes criteria addressing radiation in addition to temperature and humidity extremes."

[12] 10 CFR Part 21 Reporting of defects and noncompliance.

[13] 10 CFR Part 73.54 Protection of digital computer and communication systems and networks.

[14] 10 CFR Part 50.49 Environmental qualification of electric equipment important to safety for nuclear power plants.

4. Process to control modifications and maintenance of software

4.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Regional DBAI and 10 CFR 50.59 inspections assess these modifications in consideration of each site's licensing basis. As guidance in the assessments, the inspectors can reference inspection procedures as informed by the same guidance documents that may be used for licence amendment reviews. BTP 7-14 includes guidance for evaluation of planning, implementation and design product aspects of the DI&C system for compliance with regulatory criteria. A BTP 7-14 evaluation typically involves an evaluation of plant or vendor development processes which include processes used maintaining DI&C hardware and software. The NRC evaluates vendor processes during platform evaluations and performs confirmatory evaluations of design products by performing vendor audits when a licensee implements such a system. For inspections, the inspectors may review the design basis documents that control the processes at the licensee site and correlate those instructions to what is observed during the inspections.

5. Use of Commercial Grade DI&C systems/components

5.1. Do your licensees have a commercial grade dedication process for DI&C?

Though it is possible for a licensee to perform commercial grade dedication of a commercial digital I&C system for use in safety-related applications, this approach is generally used for small-scale digital components. Typically they, or the vendor, hires a separate entity to perform a system, subsystem or component upgrade who possesses some form of a commercial grade dedication programme. These components are dedicated for use in nuclear power plants by the vendors under 10 CFR 50 Appendix B programmes and therefore, do not require commercial grade dedication by the licensees themselves.

For safety-related DI&C systems, the platforms are designed developed and manufactured by and supplied to the licensee by vendors who maintain 10 CFR 50 Appendix B compliant Quality Assurance programmes such as Westinghouse, AREVA, Schneider Electric, etc. Some of these platforms were reviewed and approved by the NRC and thus specifically reviewed modules do not require commercial grade dedication.

5.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Yes, the NRC has the ability to inspect the commercial grade dedication (CGD) of DI&C systems. The NRC has developed inspection procedures for the inspection of both Licensee and Vendor CGD processes.

The CGD process is specifically assessed during regional DBAI and 10 CFR 50.59 inspections. The NRC inspects domestic and foreign vendors that supply basic components to US commercial nuclear power plants and perform inspections at the vendor sites inside and outside the United States. In addition, the vendor commercial grade dedication processes, when applicable, are reviewed and evaluated by the NRC staff when a DI&C platform evaluation is performed. These evaluations include review of the CGD plans, processes and methods as well as associated documentation. The NRC also performs audits of the vendors as needed to establish a basis for acceptability. During an audit NRC only issues recommendations, which the vendor is not obligated to fix the issue nor answer the NRC.

5.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

The overall requirements for CGD are outlined in 10 CFR Part 21 (defined there) and the process is controlled in 10 CFR Part 50, Appendix B, Criterions III and VII. The NRC has Regulatory Guide 1.164 that describes one acceptable means to perform general CGD. There are EPRI guides that have been accepted by the NRC that provide more specific direction for DI&C CGD. In addition the NRC has developed inspection procedures for use at licensee and vendor facilities for the inspection of CGD programmes. These inspection procedures provide guidance used by the inspection team to formulate their inspection activities.

The SRP includes guidance for qualification of existing commercial computers. This guidance states the following:

"EPRI TR-106439, as accepted by the NRC safety evaluation dated 17 July 1997, provides guidance for the evaluation of existing commercial computers and software to comply with the criteria of Sub-Clause 5.4.2 of IEEE Std. 7-4.3.2. The guidance of SRP BTP 7-14 may be applied to the evaluation of vendor processes described in EPRI TR-106439.

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," as accepted by the NRC safety evaluation dated 30 July 1998, provides more specific guidance for the evaluation of existing PLC.

6. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

6.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity and radiation effects),

The NRC has both regulations (those criteria that "shall" be followed) and guidance (one acceptable means to accomplish the requirements set forth in the regulation) to satisfy equipment qualification. The licensee is expected to conform to NRC guidance for qualifying safety-related DI&C systems and components to address EMI and RFI, environmental, and seismic conditions. For example, RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems" states "The design and installation practices described in IEEE Std 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," are endorsed for limiting EMI/RFI subject to the conditions stated in the Regulatory Position. Electro Magnetic Compatibility testing practices from military and commercial standards are endorsed to address electromagnetic emissions, EMI/RFI susceptibility, and power surge withstand capability. Selected EMI/RFI test methods from MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," and the IEC 61000 Series are endorsed to evaluate conducted and radiated EMI/RFI phenomena for safety-related I&C systems." RG 1.180 provides the test methods and operating envelopes in Regulatory Positions 3, 4 and 6 of this guide. Similarly, RG 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants" and RG 1.100, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants" provide guidance on qualifying DI&C systems and components for environmental and seismic conditions.

The inspections are typically handled by inspection personnel with support from technical personnel when requested. The DI&C equipment we have seen installed in facilities is in a mild environment (i.e. the electromagnetic, environmental and seismic conditions are not expected to be greatly different from normal, abnormal and accident conditions). It seems to be difficult to qualify DI&C equipment for harsh environments. EMI/RFI qualification is the most challenging for DI&C equipment. Seismic is typically not too challenging since there are no moving parts (as with electromechanical relays) provided that the components are properly braced. For vendor inspections, NRC staff would perform vendor inspections to verify (and observe to the degree possible) the EMI/RFI and seismic tests. NRC staff will inspect digital inverters for the AP1000 and have done so for portions of the AP1000 Protection and Safety Monitoring System and sub-systems.

Typically, a licensee or a 10 CFR 50, Appendix B supplier develops a representative test system which is subjected to various bounding environmental conditions. Environmental conditions considered are: Temperature, Humidity, Radiation, EMI compatibility, RFI compatibility, Electrostatic Discharge susceptibility and Seismic. These bounding conditions establish a qualification envelope for the equipment to be installed in a plant. This Environmental Qualification testing is usually performed at special laboratory facilities that have resources needed to establish conditions specified in the applicable standards or specified for a specific installation. Test Systems are placed into operation and performance is monitored before, during and after EQ test level conditions are established in order to demonstrate satisfactory system performance up to the established qualification levels.

Once equipment qualification levels are established, a licensee must evaluate the expected environmental conditions at the installation location to determine if equipment qualification levels are sufficient to support operational requirements for all expected normal and abnormal operating conditions. If site specific qualification requirements exceed the qualification levels established for the DI&C system to be installed, then additional EQ testing or redesign of the equipment may be necessary.

The processes and outcomes are assessed during regional DBAI and 10 CFR 50.59 inspections. Review Guidance for evaluating Environmental Qualification is provided in SRP Chapter 7.1-D Section 5.4, “Equipment Qualification.” NRC evaluation of DI&C equipment qualification is normally performed as part of a DI&C platform Licensing Topical Report review. Subsequent inspections of DI&C system compliance with EQ requirements may also be performed as part of the regulatory oversight inspection programme.

7. Configuration management

7.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

This criteria would be accounted for generically via 10 CFR Part 50, Appendix B (design control (Criterion III)) and specifically would be accounted for in staff guidance, particularly regulatory guidance. Some of the guidance occurs in Chapter 7 of the SRP NUREG 0800, Chapter 7 for I&C systems, that, points to BTPosition 7-14, which in turn points to RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” This RG endorses IEEE Stds. 828, and 1042 as acceptable means of meeting regulatory requirements.

As inspectors look at samples of functions carried out by the DI&C system, they would review the configuration control practices. Also, as work is performed and inspectors observe, they would ask questions regarding CM of software. Often Vendors will perform

a regression analysis to confirm that changes to the software versions have been evaluated to determine potential impacts on testing. The inspectors would review the regression processes and sample results from those processes to confirm that differences were adequately evaluated. Inspectors would also take a critical look at the Independent V&V activities performed to assess the impact on version changes to the design of the system.

7.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Hardware CM for DI&C systems is not treated any differently than CM of non-digital nuclear power plant components. The regulatory basis for establishing and maintaining design CM of structures, systems and components of a nuclear power plant is contained in 10 CFR 50 Appendix B, Criterion III, "Design Control." This regulation states the following:

"Measures shall be established for the identification and control of design interfaces and for coordination among participating design organisations. These measures shall include the establishment of procedures among participating design organisations for the review, approval, release, distribution and revision of documents involving design interfaces.

The design control measures shall provide for verifying or checking the adequacy of design, such as by the performance of design reviews, by the use of alternate or simplified calculational methods, or by the performance of a suitable testing program."

From a software standpoint and how the implementation of that software must occur on hardware, IEEE Std. 828-2005 does state that the associated hardware and its CM is within scope of the document. When looking at samples of functions carried out by the DI&C system, inspectors would question any design control issues, such as changes in hardware and how those changes are controlled to not have consequences. For instance, significant changes to the system hardware may require additional EMI/RFI and seismic evaluations as well as revisions or evaluations of previously conducted hardware tests.

8. Communication systems

8.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Besides the aforementioned references, DI&C Interim Staff Guidance (ISG) – 04, "Highly Integrated Control Rooms and Digital Communication Systems," includes communication between redundant safety divisions, between safety and non-safety systems, and for multi-divisional control and display stations. ISG - 04 provides NRC guidance for digital communication interfaces. This guidance document provides detailed criteria which is used by the NRC staff to evaluate and determine acceptability of communication interfaces either between different safety divisions or between safety and non-safety systems.

The staff also uses the guidance in RG 1.152, "Criteria for Use of Computer in Safety system of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2-2003, "Standard Criteria for Use of Computer in Safety system of Nuclear Power Plants" to evaluate communication between redundant safety divisions and between safety and non-safety systems. Again, as this information is guidance, following it is not a requirement but a suitable alternative must be proposed by the applicant/licensee and approved by the staff.

Note: Much of the criteria of ISG-04 has been incorporated into the newer versions of IEEE 7-4.3.2, however, RG 1.152 has not been updated to provide endorsement of the newer versions of that standard.

If there are particular requirements for a vendor in the design requirements of the purchase order, the inspectors would observe how those requirements are carried out by the vendor. For such system interfaces testing is performed to confirm the integrity of communications between systems including signal priority control, signal isolation, and fault detection and isolation.

9. Operating Experience. Events due to modification/installation of DI&C systems/components

9.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Significant industry events including those involving DI&C systems are monitored and tracked by the NRC. However, not all events have a significance level which requires NRC notification.

For significant issues that are identified, the NRC and the US nuclear industry have several mechanisms for communication. First, vendors and licensees are required to submit a report to the NRC any deviations in DI&C systems that could result in a substantial safety hazard. When these notifications are made, the vendors also communicate to the affected licensees. The NRC has a generic communication group that identifies significant issues and communicates them to the industry through generic communications (e.g. information notices). One example is a timer relay that originally did not contain embedded digital technology, but was discovered at a licensee to have embedded digital technology without any indication otherwise. Both a notification from the licensee and vendor were submitted to the NRC, and the NRC issued an information notice.

Within the Division of Inspection and Regional Support (DIRS) of the NRC, there is an operating experience branch with a mission to systematically collect, communicate, and evaluate operating experience, and apply the lessons learnt. Information derived from operating experience is regularly distributed to the NRC staff in order to keep them informed of current industry events, and is evaluated to determine whether follow-up actions such as initiation of generic communications to license holders should be taken.

Additionally, the NRC maintains a database of industry operating experience. This database is available to all NRC staff by means of a share point website that is maintained by the operating experience branch.

9.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

To date, no significant events involving DI&C safety systems have been attributed to software CCF, however, the NRC has identified several instances where a potential for software CCF existed and was not adequately addressed by licensee in their design control processes.

In one case, a licensee installed a digital rod control system, which was a generic design, which had the capability of moving more than one control rod at a time. Because the plant was not licensed for multiple simultaneous rod motion, this function was disabled via a software configuration switch. The function, however, as an integral part of the system was installed into the plant via a 10 CFR 50.59 modification without a corresponding analysis of the potential condition presented when multiple rod motion is initiated due to a software error.

In another example, several licensees installed digital circuit boards, provided by a vendor as an upgrade to address obsolescence issues with the older analogue circuit boards, into the logic portion of reactor protection systems. The licensees used the 10 CFR 50.59 process without adequately addressing the potential for CCF of the upgraded components introduced to the system or evaluating the effects of such a CCF on the plant accident analysis.

Another example had to do with replacing diesel output relays with digital descendants that resulted in a CCF due to the EMI/RFI environment. The older analogue relays were not susceptible to that environment, while their digital replacements were vulnerable to surrounding environment.

9.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

The following are the some failure mechanisms we inspect:

- Incorrect/incomplete requirements – we would trace requirements and question why they are structured the way they are; (by the way it is the number one reason for software failures).
- Incorrect implementation – inspectors would observe and review design analyses and testing to verify completeness and how issues are resolved.
- Improper changes – inspectors would assess CM and regression analyses/testing to ensure changes did not create new problems and solved the old ones.

The following is a list of typical failure modes evaluated by DI&C vendors:

- hardware failures of input circuitry (Analogue, digital, RTD, etc.);
- hardware failures of output circuitry (Analogue, digital, RTD, etc.);
- circuit faults of components or modules within the platform;
- power supply failures;
- input sensor failures;
- output relay or interfacing device failures;
- input device failures (e.g. hand switch contact fault);
- data communications errors;
- communications interface faults;
- data corruption errors;
- memory errors / faults;
- self-diagnostic errors / faults.

During inspections or audits, the vendor or licensee failure modes and effects analysis documents are reviewed and assessed for adequacy. If apparent failure modes are not included of considered in the documented Failure Modes and Effects Analyses then inspectors will ask the licensee to explain how such faults are addressed. If they are not addressed, then the licensee will be asked to provide justification for the omission.

10. Maintenance

10.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

BTP 7-14 Section B.3.1.6 contains guidance for evaluating software maintenance plans associated with DI&C systems. It includes criteria for management, implementation and resource characteristics expected for a maintenance plan. This section also includes review guidance for the software maintenance plan which describes records that should be reviewed and activities that should be performed by the reviewer to determine adequacy of the maintenance planning and implementation processes. Section B.3.1.6 includes guidance for evaluating maintenance plan implementation.

For vendor inspections, we would go back to Criterion III (Design Control) and Criterion XI (Test Control) of 10 CFR Part 50, Appendix B. These two requirements would address the CM and prevention of inadvertent change issues.

10.2. What kind of functional tests does your RB inspect? Please describe.

The NRC has performed audits and inspections of several test activities performed during digital system development including:

- Unit Testing at Factory;
- Integration Testing;
- Validation Testing;
- Simulation based testing of software / logic design;
- Factory Acceptance Testing;
- Site Acceptance Testing;
- Installation Testing at site.

The NRC is not required to provide oversight of these test activities, but may do so at the discretion of the lead reviewer or inspection team to support a safety evaluation or as a means of determining if a DI&C system meets regulatory requirements.

Functional testing required by TS surveillances and preventative maintenance can be reviewed and observed by site resident inspectors at any time. In addition, regional inspectors may review and observe activities during engineering inspections like DBAIs and 10 CFR 50.59 inspections.

For vendor inspections, we can observe any type of testing that may occur at the vendor's facility, so long as we know and plan to observe such testing. This includes elemental, unit (module), sub-system (channel or critical sub-component), system, and factory acceptance tests. Generally, since we don't have endless resources to inspect a vendor, we would observe the more critical tests such as factory acceptance testing on critical functions.

11. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections (e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

There is one observation we have made as we conduct vendor inspections of DI&C systems, particularly at vendors that supply embedded digital technology. The regulatory guidance documents are voluminous and difficult for vendors whose primary business is supplying a component, not digital technology. For example, we inspected a long-time supplier of inverters and battery chargers to the nuclear industry. This company has approximately 300 employees, which includes engineers, manufacturing technicians, managers, sales/marketing, and administrative staff. They have a line of commercial digital inverters and battery chargers they supply to other industries for several years. They embarked on creating a digital inverter for the nuclear industry and spent two years just learning the various DI&C requirements and guidance documents. They only have three to four engineers that work on this project as a medium-sized company. While they developed a high quality digital inverter, they spent much time trying to understand the regulatory documents and then produce subsequent documentation versus engineering work on the product. It would be beneficial for the group to discuss ways to streamline guidance documentation and resulting documentation during the development lifecycle so companies whose primary function is not creating DI&C components can take advantage of digital technology in a safe manner. In other words, with their limited resources, they should be focusing more on the technical aspects of the embedded digital technology while using a quality development process.

Similarly, RBs have limited inspection resources and time at a vendor or licensee facility. It is not practical evaluate the vast amounts of documentation that may be generated. We are interested in coming up with an inspection strategy that will focus on the important aspects of DI&C safety, engage in real technical issues hidden in a product (versus process issues), and do all of this realising the limits on staff and time. It is always easy to gravitate to the process issues during an inspection because it is easy to evaluate, but the real safety benefit is reaching the hidden technical issues. This requires knowledgeable and expert staff that are disciplined in inspection techniques.

I wholeheartedly agree with the above comments regarding identifying what regulatory guidance is really most critical to developing an acceptable system, and what we can glean from these guidelines to specifically influence the conduct of our inspections to be efficient, effective, and provide meaningful inspection activities focused on the technical and quality aspects of these complex systems. From my experiences at vendor facilities designing and fabricating Safety-Related D I&C systems, the documentation is voluminous. We need to better understand what is really critical (to inspect) and what we should be focused on. System architecture, requirements development, software and hardware configuration control, Independent Verification and Validation activities, and testing are in my opinion all very critical to developing such systems and gaining adequate confidence that they will perform their safety functions when necessary.

WNA DICTF feedback to questionnaire

(Version of 10 April 2018)

INTRODUCTION

This paper includes the WNA DICTF feedback on OECD Questionnaire from 10th of April 2018 on **Digital Instrumentation & Control Inspection** provided by five different DICTF experts. It includes the experiences / practice and processes in place for the country (respectively RB) and approaches applied by the industry (supplier & operator). To assign the feedback to the supplier / operator the text is labelled by different colours.

Responding country: *Germany / International*

China

Korea

France

United States

I&C Expert (company): *PICKELMANN Johannes (Framatome)*

ZHENG Wei (SNERDI)

YUN Jea Hee (Kepco)

DOUTRE Jean Luc (EDF)

Mark Burzynski (NewClear Day, Inc.)

Important Note: *Most of the questions are purely directed to Regulator Bodies (RBs). Replies from Framatome (as a supplier for DI&C) would lead to the point that most of the questions would be kept open. But to provide OECD feedback the subsequent answers provide information how Framatome deals with the different subjects in general for TELEPERM® XS I&C safety applications. As inspection requirements differ from RB to RB, the inspection activities itself, the stakeholders and the responsibilities need to be adapted to the country specific needs. The described methodologies, documentation and V&V activities are to be adjusted accordingly.*

Best regards,

Johannes PICKELMANN

WNA CORDEL DIC Task Force - Chairman

Questionnaire

Instructions - Please answer to the best of your knowledge the following questions related to DI&C systems/components (both hardware and software) used in important-to-safety applications for nuclear power plants**.**

1. Use of DI&C systems/components in nuclear power plant applications

1.1. Do your licensees use DI&C systems/components important-to-safety (e.g. reactor protection system, no safety significant SSC)? If so, provide some examples.

Framatome:

Since 1998, SIEMENS KWU / AREVA / Framatome has installed its nuclear power plant safety class 1 digital I&C platform TELEPERM® XS in more than 80 units of 17 countries for 18 different nuclear island designs.

Table .1. Facts on TELEPERM® XS nuclear power plant installations / I&C systems (status Feb.2018)

	Commissioned	*Ongoing Projects*
Reactor Protection	26	21
Reactor Limitation	20	11
Reactor Control	22	10
Neutron Flux Measurement	15	13
Diesel Load Sequencer	8	6
Core Cooling Monitoring	14	9

The following list provides some view examples of Reactor Protection, Limitation and Control systems of the past 20 years:

Table .2. Examples of Reactor Protection, Limitation and Control systems of the past 20 years

Plant	***Country***	***Type***	***Design***	***Function(s)***	***Operation***
Fuqing 5 & 6	China	ACP (PWR)	CNNC 1 080 MW	Reactor Protection / Reactor Control	design phase
Leningrad II-1/2	Russia	VVER (PWR)	ROSATOM 1 170 MW	Reactor Protection / Reactor Limitation	in operation / in commissioning
Taishan 1 & 2	China	EPR (PWR)	AREVA 1 750 MW	Reactor Protection / Reactor Control	in operation / in commissioning
Olkiluoto 3	Finland	EPR (PWR)	AREVA 1 720 MW	Reactor Protection / Reactor Control and Limitation	in commissioning
Oconee 1-3	United States	PWR	B&W 891 MW	Reactor Protection	in operation 2011 / 2012 / 2013
Beznau 1 & 2	Switzerland	PWR	WH 380 MW	Reactor Protection and Control Systems	in operation 2000 / 2001
Paks 1-4	Hungary	VVER (PWR)	AEE 500 MW	Reactor Protection / Reactor Limitation	in operation 1999 / 2000 / 2001 / 2002

For the nuclear power plants Unterweser (Germany), Forsmark 3 (Sweden), Beznau 1&2 (Switzerland) and Paks 1-4 (Hungary – ongoing) software and hardware upgrades have been performed to extend the lifetime of the installed digital applications.

SNERDI:

Yes, e.g. Protection Systems in Sanmen Nuclear Power Plant, Haiyang Nuclear Power Plant and QINSHAN I Nuclear Power Plant in China

Kepco:

*The safety I&C system for **APR1400** is based on a common Programmable Logic Controller (PLC) platform which has been dedicated for nuclear safety systems. The safety I&C systems implemented on the common PLC platform consist of the Plant Protection System (PPS), Engineered Safety Features – Component Control System (ESF-CCS), Core Protection Calculator System (CPCS) and Qualified Indication and Alarm System – P (QIAS-P).*

EDF:

Yes, DI&C systems important to safety are used in our plants:

- 1 300 MW: protection system (controlled state) and safety related systems (safe state);
- 1 400 MW and EPR : same + computerised HMI.

NewClear Day

Yes. Some examples are reactor protection systems and inadequate core cooling monitoring systems.

2. Licensing to use DI&C systems/components

2.1. Please explain how your regulatory body (RB) authorises the installation and use of DI&C systems. What are the criteria?

Framatome:

For I&C projects of new builds and plant modernisation the main criteria's under inspection of the RB are:

- *software CCF of DI&C;*
- *N+2 (deterministic) criteria (for main line of defence – e.g. protection system);*
- *categorisation of I&C functions / Classification of I&C systems & components;*
- *independence between DiD levels / safety classes (secured by means for diversity and separation);*
- *operation & maintenance features (self-monitoring, maintainability, verifiability).*
- *fault behaviour regarding*
  - *sensor fault;*
  - *communication fault;*
  - *component fault (safety-oriented failure behaviour).*
- *Quality Assurance / Qualification / V&V / Configuration management / Requirements management (typically separated between I&C system engineering and I&C platform development incl. HW + SW).*

SNERDI:

Nuclear and Radiation Safety Center performs review of the applications for nuclear reactor licences, including the DI&C portions. National Nuclear Safety Administration (NNSA, China RB) authorises or rejects the applications depending on the review conclusion and opinions from Nuclear and Radiation Safety Center

During the review of DI&C, HAD 102/16 (Chinese version of IAEA Safety Standards No. NS-G-1.1) issued by RB and industry standards contained in the licensee basis provide the main criteria.

Kepco:

The Regulatory Body (RB), Korea Institute of Nuclear Safety (KINS) uses Evaluation Guideline for Light Water Reactor prepared by KINS, which is correspondent with NRC safety review plan.

The RB reviews the APR1400 design to determine if the quality standards requirements of GDC 1 are adequately addressed. Additionally, the RB reviews the application to determine if IEEE Std 603-1991, Clause 5.3 has been adequately addressed. IEEE Std 603-1991, Clause 5.3, requires components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance programme.

The evaluation guideline requires that the application should confirm that the quality assurance provision of 10 CFR Part 50, Appendix B is applicable to the safety system.

For digital computer-based systems, the evaluation guideline points to guidance provided by IEEE Std. 7-4.3.2-2003. The software topics are areas of focus for the review of digital computer systems quality design.

EDF:

The main criteria is the qualification according to the safety class requirements which globally correspond to the IEC standards: 61513 for the architecture, 60880 for class 1 software, 62138 for class 2 & 3 software ; plus hardware qualification including seism.

In addition there is a specific French rules (equivalent to the law) asking for specific behaviour of DI&C system:

- *Class 1 system must have a deterministic behaviour;*
- *Class 2 system must have a predictable behaviour.*

All the documentation concerning this qualification must be provided to our RB.

NewClear Day

The first criteria in the United States is the evaluation to determine if the proposed change to the plant can be made without NRC approval. The governing criteria are found in 10 CFR 50.59 (see https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0059.html). Some recent NRC guidance on making these evaluations for digital I&C changes can be found in NRC Regulatory Issue Summary 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems (see https://www.nrc.gov/docs/ML1814/ML18143B633.pdf). If the criteria in 10 CFR 50.59 are not met, then the licensee must submit a licence amendment request to the NRC and receive approval prior to implanting the change. Guidance regarding licence amendment requests for digital I&C topics can be found in NRC Draft Interim Staff Guidance DI&C-ISG-06, "Licensing Process," Revision 2 (see https://www.nrc.gov/docs/ML1811/ML18114A383).

2.2. Describe how DI&C is captured in the licensee technical basis.

Framatome:

Requirements to be implemented by the supplier such as Framatome, are derived from procedural/quality, operational, functional, technical and safety requirements and plant constraints as specified by the contract and codes & standards to be applied for the respective project. These requirements are documented by the I&C system requirement specification in the first phase of the engineering lifecycle. For the management of the comprehensive number of requirements it is essential to install a process for requirements engineering and management. (RE&M). The RE&M process focuses on activities related to the fulfilment of requirements. Each requirement is linked to one or more design element(s) which itself is (are) linked to the validation.

SNERDI:

Some key topics for digital technology should be captured in the licensee technical basis, including:

- *qualifications of the safety digital I&C platforms;*
- *software verification & validation;*
- *configuration management;*

- *testing;*
- *common cause failure;*
- *communication.*

Kepco:

KINS/RG-N08.13, "The Application of DI&C for Safety Systems" prepared by KINS requires the application should confirm that the safety system shall meet the requirements of IEEE Std. 603 and IEEE Std. 7-4.3.2.

Licensee describes the design features to show how the DI&C for APR1400 safety systems meet the requirements in the Design Control Documents such as Prelimiary Safety Analysis Report (PSAR) and Final Safety Analysis Report (FSAR)

EDF:

Until now all the documentation is provided on paper but computerised exchanged will be used in the future.

NewClear Day

Licensees are required update the final safety analysis report (FSAR) for the plants to assure that the information included in the report contains the latest information developed (see https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0071.html). The periodic updates are required to incorporate the effects (i.e. appropriate revisions of descriptions in the FSAR) of all changes made in the facility or procedures as described in the FSAR and all safety analyses and evaluations performed in support of approved licence amendments or in support of conclusions that changes did not require a licence amendment in accordance with 10 CFR 50.59(c)(2).

3. Inspection of DI&C systems/components

3.1. Does your RB specifically inspect DI&C systems? Describe how.

Framatome:

The development process of a safety I&C platform is planned and controlled by documents such as Quality Assurance Plan, V&V Plan, Configuration Management Plan. Compared to hardware components of a safety I&C platform, the software development process is much more an area of interest and inspected by the RB. The process for engineering and development of software components for safety DI&C is quite precisely described – such as IEC 60880 / IEC 62138 / IEEE 1012.

Note: For IEC / IEEE standards it is necessary to be aware which of the identified requirements are related to platform / component development and which are related to DI&C system engineering.

Additional specific inspection issues are derived nowadays e.g. from cybersecurity threats and the more intensified discussion on Defence-in-Depth and Diversity.

The following provides an overview of the typical inspection activities being performed during the I&C lifecycle. The RB determines with the plant operator to which inspections the RB participates, or not.

Since the first TELEPERM® XS projects in 1998 the lifecycle considers several types of inspection such as:

- *supplier audits (by operators);*

- *type Approval (by third party assessment – as requested by RB);*
- *manufacturing follow up (by operators / regulators – as requested by RB);*
- *factory Acceptance Test – Cabinet Manufacture (by operators / third party);*
- *factory Acceptance Test – Testbay (by operators / regulators – as requested by RB);*
- *site Acceptance Test – On site (by operators / regulators – as requested by RB).*

Supplemented by single document review (by operator) and third party assessment. Details are typically provided by the codes & standards of the national regulator.

For the equipment qualification of the safety I&C components Framatome performs a comprehensive generic qualification programme, with generally TÜV (Germany) as the independent body involved along the qualification of the component from the start – as a third party.

For the case of project specific qualification activities (beyond the requirements covered by the generic platform qualification) dedicated inspection are initiated as defined by the Equipment Qualification Plan – to be inspected by the RB.

Kepco:

The RB inspects DI&C via the following review process:

- *review the Topical Report for DI&C Platform;*
- *audit for Software Life Cycle process and documents;*
- *audit for supplier;*
- *site inspection for integration testing and pre-operational testing;*
- *request for Additional Information (RAI) for PSAR and FSAR;*
- *request for presentation of Pending items.*

EDF:

Yes, the source code of the protection system is provided to our RB who analyses it with their own tools. Test coverage is also checked.

Specific audits are also organised to check the development process (documents, traceability, miles stones….). Our RB can ask for all documents: some are directly sent; other are only accessible in our offices

NewClear Day

NRC has guidance to audit digital I&C modifications during the review of a licence amendment request. The guidance is found in NRC Standard Review Plan Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems" (see https://www.nrc.gov/docs/ML1601/ML16019A085.pdf). NRC also has inspection procedures for digital I&C modifications. These inspections can be performed during or after installation. The inspection method is described in Inspection Procedure 52003, "Digital Instrumentation and Control Modification Inspection" (see https://www.nrc.gov/docs/ML0808/ML080800048.pdf)

3.2. Do you inspect all the stages (i.e. design, manufacturing, installation, functional testing?

Framatome:

The participating stakeholders might differ from project to project. By use of the Quality Assurance Plan (QAP - in combination with the V&V Plan) and the Equipment Qualification Plan, the inspections are harmonised between the stakeholders at an early stage of the project lifecycle.

Typical, the DI&C system engineering plans are to be inspected by the RB (respectively by assigned third part). The RB can inspect the implementation of the measures by the inspections as listed in 3.1.

Kepco:

The RB inspects and audits the documents for all stages.

EDF:

Yes all stages are inspected either by our internal teams or by RB.

NewClear Day

The NRC inspection and audit guidance can be used to cover all the stages.

3.3. Please provide a short description of the scope of the inspections and the types of staff expertise that perform these types of inspections.

Framatome:

The subsequent listing provides some more details on the typical inspection activities as described in chapter 3.1. The scope of inspection and the staff might change:

- *Supplier audits*
  - *Scope: Verification of the implementation of the described quality assurance process (according QAP)*
  - *Types of staff: Quality people + project manager + technical worker (on demand)*
- *Type approval*
  - *Scope: Independent verification of the I&C component qualification (according Equipment Qualification Plan)*
  - *Types of staff: Third party assessment (by IEC17020 inspector)*
- *Manufacturing follow up – Manufacturer*
  - *Scope: Check of the specified manufacturing sequence and the required tests to be performed on certain stages*
  - *Types of staff: Quality people + I&C experts + project manager*
- *Factory Acceptance Test (FAT) – Cabinet Manufacture:*
  - *Scope: Verification of the implementation of the manufacturing processes incl. handling of tools, components, etc. Check of the assembling quality of the components / I&C cabinets, etc.*
  - *Types of staff: Quality people + Manufacturer + project manager*
- *Factory Acceptance Test (FAT) – Test field:*
  - *Scope: Validation of the functional requirements (open-loop / closed-loop simulation), the technical requirements (e.g. response time, accuracy, fault*

behaviour), operation and maintenance requirements (service tools / maintenance) and cyber security requirements (e.g. unidirectional connection / access control)

- *Types of staff: Quality people + Process experts + I&C experts + cyber security experts + operation and maintenance staff*

- *Site Acceptance Test (SAT) - I&C System Commissioning*
  - *Scope: Validation of the I&C system integration into the plant (interface check) – supplemented by additional technological tests (I&C signal chain test / priority testing / etc.)*
  - *Types of staff: I&C commissioning experts + add. I&C specialists (on demand)*
- *Site Acceptance Test (SAT) – Process System Commissioning*
  - *Scope: Cold / Hot Functional Commissioning Tests with the plant (by use of I&C applications)*
  - *Types of staff: Process System Commissioning engineers + I&C experts (supporting)*

The "inspection" of the engineering documentation should be selective according to the related topics. In addition to the single document review, by use of the "Phase Reviews" the set of documents is verified by quality people to finalise a design phase.

Design changes could request to step back in the engineering lifecycle of the I&C system. The process how to V&V or inspect the modifications shall be specified by the Configuration Management Plan.

<u>Kepco:</u>

The RB inspects DI&C including the following specific items.

- *Equipment Qualification*
- *QA plan and process*
- *Configuration Management*
- *Factory Acceptance Testing*
- *Commercial grade dedication process*
- *System Design documents*
- *Component Design documents*
- *Site test including MMIS Integration Testing*
- *Software Life Cycle process and documents*
- *Analysis report review such as setpoint analysis, response time analysis, FMEA, unavailability analysis, S/W V&V for DI&C*

<u>EDF:</u>

Inspection could be focused on:

- *the documentation (specification, design, integration, test...);*
- *the behaviour of the system (from an input to the output of the system);*
- *the programming rules;*

- *the hardware tests;*
- *the manufacturing.*

The competences of the our teams covers "quality assurance", "software development", "hardware development" and "functional behaviour".

3.4. Describe how RB inspectors are specifically trained to inspect DI&C systems/components.

Framatome:

No comment.

Kepco:

The RB inspectors are trained to inspect DI&C via education, lessons learnt and inspection experience. The RB exchanges licence experience with abroad RBs.

EDF:

Our RB is used to our qualification process which is described in RCC-E (AFCEN document). Our RB has his own R&D capacity to develop specific methods or tools. Specific way to inspect a DI&C system is called "tread audit" (from an input to the output of the system).

3.5. Does your RB inspect DI&C systems/components separately and why? Describe the type and scope of vendor inspections.

Framatome:

AREVA/Framatome applies a "two-stage" licensing approach for the safety I&C platform TELEPERM® XS concerning:

1. *Generic qualification of the system platform (components and system properties)*
2. *Application-specific design of the architecture and implementation of the individual I&C system*

The main advantage of this approach is that the suitability of the hardware and software components of the system platform for safety-related tasks and the essential aspects of platform integration have already been verified in a generic way and are thus available to all projects as a feature of TELEPERM® XS. The documentation provided by Framatome follows the "two-stage" approach by differentiating between "platform documentation" and "application related documentation". In practice this approach has been successfully applied for licensing of DI&C in relation with many RBs.

Kepco:

The RB reviews the Topical Report for DI&C platform for applying nuclear power plants. The review for PSAR for construction permit and FSAR for operating permit is performed in the aspect of inherent system design but the systems based on the same platform are reviewed and inspected together.

EDF:

Our RB could inspect preferably the supplier of the protection system and safety-related system to access to specific internal information

4. Embedded Digital Devices

4.1. Do your Licensees use embedded digital devices? Please describe how and where.

Framatome:

To a small scale, embedded digital devices are (and probably will be more frequently) used for field control devices, sensors and actuators – layer 0 and 1[15] (components of limited functionality / complexity) It is mainly driven by the need to increase the functionality of the component (e.g. regarding self-testing / monitoring / data communication) and the fact that the supplier (industry) has mainly turned towards digital since years.

For safety class 1 components, embedded digital devices are avoided today as far as reasonable. For safety class 2 and 3 components the situation is different and assessed case by case. Issued certification from other RBs or certification according to e.g. IEC 61508 (SIL level) could be credited but need to be assessed / analysed according to the RB requirements.

Note: The situation for electrical devices is – compared to safety I&C – a bit more complicated, as electrical non-software components are quite rare on the market. By that reason, Framatome electrical department already considered own development of components critical to safety. Another strategy is to rely on component diversity to manage the weaknesses of the off-the-shelf components software qualification (accepted by German RB).

The project related Equipment Qualification Plan lists all components of the I&C systems for which a confirmation of certification is required. For first of a kind application of embedded digital devices, the measures to provide evidence have to be specified. Subsequent projects could benefit from the available certification.

Note: For the safety I&C platforms for the process control systems of layer 2 (Reactor Protection System / Reactor Control and Limitation System, Diverse Actuation System, etc.) Framatome relies on own components developed by / under control of the company.

Kepco:

Two types of common Programmable Logic Controller (PLC) platform such as Common-Q and POSAFE-Q are used for safety I&C system for APR1400.

The base software for POSAFE-Q platform is pCOS which is operating system.

The POSAFE-Q base software contains such programmes as diagnostic routines and communication interfaces to the I/O backplane, the SDN communication interface and the SDL interface. The TASK scheduler which schedules the execution of all TASKs based on the pre-defined priorities is included.

The base software for Common-Q platform is VRTX which is operating system.

EDF:

Embedded digital device are used in a limited number in safety and safety-related systems: for example for conditioning of signal. The use of the same kind of embedded devices in two different lines of defence for the same functions is not allowed

NewClear Day

Yes, typically end device components like recorders, circuit breakers, etc.

4.2. If so, describe the specific inspection criteria used by the RB to assess its installation.

[15] See upcoming IAEA paper, "Approaches for overall instrumentation and control architectures of Nuclear Power Plants".

Framatome:

The inspection criteria strongly depend on the use case and the related safety classification, the country specific requirements (e.g. regarding application software, failure behaviour, EMC, earth quake) and plant specific requirements. Details to be specified by the Equipment Qualification Plan.

Kepco:

EPRI TR-106439, "Guideline on Evaluation and Acceptance on Commercial Grade Digital Equipment for Nuclear Safety Application" and TR-107330, "Evaluating Commercial Digital Equipment for High Integrity Application" is used as the criteria for inspection and review.

EDF:

A specific qualification is performed based on IEC 62671

NewClear Day

See answers to item 3 above.

4.3. What are the requirements to be applied by the licensee to qualify embedded digital devices?

Framatome:

The dedicated approach for the embedded digital devices is oriented on the kind of the device and its performed safety class, which must be described by a qualification plan with reference of selected approach. This could be based on IEC 60880, IEC 62138, IEC 62671, IEC 60987, IEC 62566 or national specific approaches which represent adaptions of industrial qualification.

Note: The standard IEC 62671 "NPPs – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality" provides guidance for the qualification of embedded digital devices. It includes checklists with criteria to provide evidence according to the safety class of the component.

Kepco:

Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" and IEEE603 provide the requirements for digital computer.

IEEE 7-4.3.2, EPRI TR-106439 and TR-107330 is used as the criteria for inspection and review to qualify embedded digital devices.

EDF:

Same as 4.2

NewClear Day

See discussions in:

- NRC Regulatory Issue Summary 2016-05, "Embedded Digital Devices in Safety-Related Systems" (see https://www.nrc.gov/docs/ML1511/ML15118A015.pdf)
- NRC Regulatory Issue Summary 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems (see https://www.nrc.gov/docs/ML1814/ML18143B633.pdf).

5. Process to control modifications and maintenance of software

5.1. How does your RB inspect the licensee processes and outcomes of said processes used to modify and maintain DI&C systems/components software?

Framatome:

The following provides information on how the control of modifications is managed by Framatome. The application of the described process is inspected during supplier audits (as requested by RB).

The process for the control of modifications and maintenance of software is following the "two-stage" approach and is subdivided into control of:

- *application Software (plant specific I&C functions – for protection and control of the nuclear power plant);*
- *system Software (safety platform specific operating software).*

Both shall be designed / developed (incl. V&V) in accordance with IEC 61513 and IEC 60880 (Cat A) or IEC 62138 (Cat. B and C).

IEC 61513 requires preparing a "System Configuration Management Plan (CMP)" (see section 6.3.2.3) covering the action of configuration identification and configuration control. For configuration control IEC 61513 requires: "… - the status of each controlled item shall be tracked; this includes information on the initial approved version, the status of requested changes and the implementation of approved changes;"

The CMP provide the process for:

- *management of the baselines;*
- *version management and version planning process;*
- *management, structure and control of the Configuration Identification Document (CID);*
- *management of issues leading to a formal or technical change request;*
- *specification of the roles and responsibilities.*

All project related modifications of the I&C system (incl. application software – but not system software) are managed by the I&C system CMP.

The cause for a modification is different, starting from technical / design changes initiated from the operator / regulator or process and safety engineers, lessons-learnt / improvement derived from the I&C system design up to anomalies detected during testing / inspections / etc.

Depending on the issuing discipline and the phase of the project lifecycle the responsible group of inspectors (process & safety / I&C design experts, V&V experts) vary. In principle the later the lifecycle phase, the more comprehensive the inspection, as passed test of previous phase are credit as independent brick stones for the overall demonstration.

For the engineering of an DI&C system, Framatome's main practice for the inspection of modification is to focus on the complete verification and validation of the modification influencing the structure and components of the I&C system (and its interfaces to others – if affected). Therefore, one of the main actions is to assess the influence and consequences the modification will have for the system regarding safety, operation and maintenance, fulfilment of requirements, etc.

For control of the system (platform) software modifications, Framatome has implemented a rigorous change procedure for all DI&C platform software components: Every change to the platform requires a formal change request workflow. Change requests are first analysed with respect to their impact on other platform components and on installed systems prior to their implementation and subsequent testing. The entirety of all changes with respect to the previous baseline constitutes a new software version, which is presented to the RB. The RB or a third party reviews these change requests, the corresponding development and test documentation and audits Framatome's conformance to codes & standards before issuing a type approval.

Kepco:

V&V including regression testing is performed when the software for safety system is modified for design change. The affected software design and V&V documents are revised. The RB reviews and inspects all process and documents when the licensee submits the design change package for licensing.

EDF:

For each safety qualified system, there is a reference file identifying all the components of the system (hardware and software). All the modification managed on the system after its qualification are registered in this file. In case of "simple" modification, the supplier is only obliged to inform EDF, in case of "complex" modification, the supplier is obliged to ask for EDF acceptance. All software modifications are considered as "complex".

NewClear Day

No specific criteria or guidance.

6. Use of Commercial Grade DI&C systems/components

6.1. Do your licensees have a commercial grade dedication process for DI&C?

Framatome:

Framatome performs dedication based on IEEE acc. to internal procedures, and well oriented on the approach of cross-qualification or combined method which is oriented on IEC60780.

SNERDI:

Not yet, but RB is researching and establishing the process.

Kepco:

The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B programme.

The process for commercial grade dedication (CGD) is prepared according to EPRI TR-106439 by Compoent Designer.

NewClear Day

Yes. Regulatory Guide 1.164, "Dedication of Commercial-Grade Items for Use in Nuclear Power Plants," provides general guidance for commercial grade dedications (see https://www.nrc.gov/docs/ML1704/ML17041A206.pdf).

6.2. If so, how does your RB authorise/approve and inspect the commercial grade dedication process for DI&C?

Framatome:

The inspection during projects is linked to the dedicated Equipment Qualification Plan.

Kepco:

The RB reviews if the CGD process identifies the critical characteristics of the commercial grade digital equipment based on the safety-related technical and quality requirements, and selects appropriate methods to verify the critical characteristics to enable dedication of the digital equipment.

The commercial grade dedication process is described briefly in PSAR and FSAR. The RB reviews the requirements and processing for CGD based on the design control documents.

The commercial grade computer and software is applied for safety systems through the following process:

- *Technical evaluation is performed if the CGD items meet the functional and performance requirements of the safety systems.*
- *The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function.*

NewClear Day

See answers to items 2 and 3 above.

6.3. If so, describe the specific criteria used by the RB to review, approve, and inspect the use of commercial grade DI&C systems/components.

Framatome:

This task is strongly linked to the country of the RB, equipment kind and complexity of performed safety function.

Kepco:

EPRI TR-106439 identifies the categories of critical characteristics in terms of physical, performance, and dependability attributes. These characteristics correspond to the categories identified in IEEE Std. 7-4.3.2.

The RB reviews the CGD according to EPRI TR-106439 which adapts four acceptance methods to establish an approach to verify the characteristics for digital equipment.

NewClear Day

NRC has two documents that outline the methods and criteria for the commercial grade dedication of digital I&C equipment:

6.3.1.1.1. NRC, Review of EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," (see https://www.nrc.gov/docs/ML1220/ML12205A284.pdf)

- *NRC, Safety Evaluation by Office of Nuclear Reactor Regulation of Electric Power Research Institute (EPRI) Topical Report, TR-107330, Final Report, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants" (see https://www.nrc.gov/docs/ML1220/ML12205A265.pdf)*

7. Equipment Qualification (electromagnetic, environmental, and seismic) of DI&C

7.1. Describe how a licensee qualifies DI&C systems. Describe how the RB inspects licensee processes and outcomes of said processes to ensure that DI&C systems/components are adequately qualified (Note: Environmental equipment qualification includes, but it is not limited to, temperature, pressure, humidity, and radiation effects).

Framatome:

The qualification evidence is performed by a plant specific suitability analysis. This analysis builds the link between the requirements and the evidence demonstration by test or analysis.

Kepco:

The objective of equipment qualification is to demonstrate that the safety I&C system equipment is capable of performing its designated safety functions during and following a DBE. Equipment qualification is composed of three major components: environmental, seismic and electromagnetic compatibility (EMC) qualification. The licensee describes that Equipment testing and analysis are performed to meet the requirements of IEEE Std. 603, IEEE Std. 323, IEEE Std. 344, EPRI TR-107330, EPRI TR-102323 and RG 1.180 in the DCD documents

The RB reviews the qualification plan and reports through RAI and audits to confirm that the safety I&C system is fully qualified and capable of performing its designated safety functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions, as required

EDF:

Qualification is based on RCC-E code which is based on IEC standards

NewClear Day

Three sets of guidance are available to licensees to use to qualify digital I&C equipment:

- *Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants (see https://www.nrc.gov/docs/ML0701/ML070190294.pdf)*
- *Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems (see https://www.nrc.gov/docs/ML0327/ML032740277.pdf)*
- *NRC staff accepted the Electric Power Research Institute (EPRI) topical report TR-102323, "Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants," in a Safety Evaluation Report (SER) by letter dated 17 April 1996, as one method of addressing issues of EMC for safety-related digital I&C systems in nuclear power plants.*

8. Configuration management

8.1. Describe any specific criteria used by your RB to verify acceptance compatibility between different software versions and how is this inspected.

Framatome:

The following provides information on how Framatome handles the version management for software considering the "two-stage" approach (application software vs. system software – see chapter 5).

As described in chapter 5.1, Framatome puts focus on the impacts of the related modification. Regarding software it is essential to assess the differences between two versions of the software. The application software of a TELEPERM® XS DI&C system is based on a unique / I&C system specific database covering all relevant data required for the application. This database contains the entire software specification of a DI&C system and all aspects of the hardware specification as far as they also affect the software.

Next to tools required for the engineering (e.g. function diagram editor) TELEPERM® XS provides tools for analysis of the implemented modifications between two different versions of the database. The generated output is used to demonstrate that only those function diagrams have been modified which were intentionally affected by the modification.

SNERDI:

Changes between different software versions must be identified and reflected in the configuration status accounting reports, which are required to submit to the RB to review.

Kepco:

The Software Configuration Management Plans (SCMP) are prepared in accordance with RG 1.169, which endorses IEEE Std. 828. The design team is responsible for the implementation of adequate measures to manage and control the software configuration in accordance with the SCMP. The librarian maintains all controlled software items as well as all control records.

The SCMP describes seven functions of software configuration management activities: configuration identification, configuration control, status accounting, configuration audits and reviews, interface control, subcontractor/vendor control, and release management and delivery.

APR1400 application software baseline is established at the implementation phase and changes are documented and approved as described in this SCMP. The software tool is used for software configuration management.

The RB reviews the requirements for Software Configuration Management Plan to verify its compliance with applicable regulatory requirements. Based on the applicant's description of how the development of the SCMP will conform to RG 1.169 and SRP BTP 7-14, the staff inspects that the requirements for Software Configuration Management Plan meet the relevant. The RB inspects how configuration management is maintained though audit.

EDF:

The main criteria is the qualification (hardware or software)

NewClear Day

No specific criteria or guidance.

8.2. Describe any specific criteria used by your RB to verify acceptance compatibility between different hardware versions and how is this inspected.

Framatome:

The following provides information on how Framatome handles the version management for hardware.

Analogue to the question on software, hardware needs to be portioned into project / system specific hardware functionality and hardware (components) provided by the platform (e.g. TELEPERM® XS).

Modification on the DI&C are managed by the CMP (as described in 5.1). This includes an assessment of the modifications between two versions of the DI&C system (CID). One set of the data to be identified by the CID is the listing of all modules (incl. type / version / serial number) and its location (incl. room, cabinet, installation location within the cabinet). In case if an updated version of some module (version 1.3 instead of 1.2) shall be installed, the CMP requests to analyse the impacts on the DI&C system.

The hardware modules are explicitly identified by their order number incl. version number. For each hardware module version, a RMD (Register of Manufacturing Documents) is available to identify the module and the relevant documents like Bill of Material, schematics etc. Any changes are analysed according the impact on the qualification status.

If there is an impact on the qualification status (the change has potential impact on seismic, climatic, EMC or technical behaviour of the qualified product), an update of qualification with the independent inspector is necessary. According to the Framatome processes, the order number of the modified component will be changed if technical data of a hardware module have been changed and the compatibility between the versions is not ensured. If the compatibility is ensured, only the version number of the hardware module will be increased.

SNERDI:

Same requirements like software.

Kepco:

The RB inspects that the configuration management for hardware, software and tools is performed by the appropriate documents.

EDF:

Same as 8.1

NewClear Day

No specific criteria or guidance.

9. Communication systems

9.1. Describe any particular criteria used by the RB to review, accept, and inspect DI&C systems that communicate between independent/different systems and between systems of different safety classes.

Framatome:

The following gives information on how Framatome provides evidence for communication independence.

During the system basic design phase of a DI&C system the system's interfaces / communication with I&C systems belonging to different DiD levels or Safety Classes (within Layer 2), to the supervisory control and information systems (Layer 3) and to field control devices (Layer 1) are specified and assessed regarding the necessity and the postulated initiating events. Depending on the type of interface (hardwired / network) different means are applied to secure independence. The selection of the right independence means secures non-propagation of subsequent fault of components of a lower safety class towards components of a higher safety class. Main independence criteria are derived from the defence-in-depth concept and the role of the interfaces / communication.

As an example, to improve the operation and monitoring of a nuclear power plant, modern reactor protection DI&C systems consist of network interfaces to the supervisory control and information system. To secure the independence between the safety system and the non-safety system, a unidirectional interface solution is considered in the design. This communication independence feature is validated by analysis (assessed by RB – as requested by RB), and tests (e.g. during test bay / test setups).

The abstract of the interface assessment is provided by an I&C system suitability analysis, by which each interface (according to the I&C System Specification) is analysed.

SNERDI:

The Chinese national standard of applicable criteria for digital computers in safety systems of nuclear power plants (GB/T 13629-2008) which modifies and adopts IEEE Std 7-4.3.2-2003 provides some criteria about communication, e.g. data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function.

Kepco:

KINS/RG-N08.28, "Communication Independence" prepared by KINS provides the criteria for the communication between safety channels and between safety and non-safety system. The guide refers IEEE Std. 7-4.3.2

EDF:

Communication between systems belonging to the same safety class are allowed. In case of communication between different safety classes, specific justifications are needed: one-exchange or functional non-pollution can be used.

NewClear Day

NRC uses DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc) Interim Staff Guidance," to evaluate communication independence (see https://www.nrc.gov/docs/ML0833/ML083310185.pdf).

10. Operating Experience. Events due to modification/installation of DI&C systems/components

10.1. Describe the process followed by your RB for evaluating DI&C related events reported by licensees including the use of analytical techniques, such as trending analysis, and the dissemination of any applicable lessons learnt.

Framatome:

The following identifies the process on how non-conformances are managed by Framatome.

The "Non-Conformance-Process" is regulated by a work instruction and installed dealing with any kind of findings resulting from product activities and projects (worldwide). By application of industrial methodologies the root cause, the impact on product(s) and project(s) is analysed, its safety relevance determined, and measures for the implementation specified (incl. lessons-learnt). The operator (and the RB) can review the process in the frame of an audit.

Kepco:

The RB requires the operating experience for each module of DI&C when the licensee tries to modify the testing interval or design change. The licensee submits the failure mode and effects analysis (FMEA) and unavailability analysis report which analyzes the probability to fail the RPS and ESFAS function. The unavailability analysis report is prepared based on the failure rates which are generated based on the calculation by the MIL Stds and updated by Basian Update with operating experience.

EDF:

Each year, an annual feedback of experience is send to our RB.

10.2. Have any DI&C events that have occurred been evaluated by your RB to identify CCFs? Please provide some examples.

Framatome:

There has been no DI&C event that have occurred related with CCF.

Framatome internal findings with the potential of becoming a CCF for nuclear power plants are classified as safety related. Under consideration of the use case (plant applications) and the overall design, impacts regarding the safe operation of the plant are assessed by process & safety and I&C experts. Dependent on the results, concerned customers are promptly informed by the supplier including a statement regarding potential impact on safety, a description of the cause (analysis) and the measures to be applied (recommendation – if necessary).

This process is in place at Framatome covering any kind of findings with potential impact on plants running with components of TELEPERM® XS. Beyond the direct communication, operators have direct access to a customer portal with all published TELEPERM® XS Service Letters.

Assumed I&C CCF design weaknesses identified during the lifecycle of a project are managed by the review process of the engineering documentation, e.g. through validation by use of a simulator(s) or by analysis (CCF Analysis / Defence-in-Depth Analysis / etc.). Results are to be assessed by the customer and the regulator (on demand).

Kepco:

There has been no DI&C event that have occurred related with CCF. The analysis for CCF and unavailability is performed by assuming the postulating concurrent failures of the same software block (bistable processor, LCL processor, communication processor) in all redundant divisions.

EDF:

No CCF have already been identified

10.3. Describe the typical failure modes, expected by DI&C vendors and designers that your RB´s inspection programmes evaluate.

Framatome:

Framatome's work instruction for the "Performance of Failure Mode and Effects Analysis (FMEA) for the Hardware Structure of I&C Systems" provides guidance for such analysis.

For safety I&C systems, Failure Mode and Effect Analysis (FMEA) is requested to be provided (and be assessed by the customer and the regulator (on demand). The FMEA report includes a system description, the hardware features including fault behaviour, a description of the functions, the interface analysis and the results. For each type of module the function, failure modes, the potential causes, means of detection, counter measures, effect on the I&C safety function and the failure rate (FIT) is given.

Kepco:

There are two primary failure modes to be considered in the analysis:

a. *The postulated software failure in all redundant channels results in the failure to generate a trip or actuation signal when a trip or actuation signal is required by plant conditions.*
b. *The postulated software failure in all redundant channels results in the generation of a spurious trip or actuation signal when a trip or actuation signal is not required by plant conditions.*

There are many failure modes that the RB evaluates. Among them, the RB's inspection focuses on the power failures in the view of fail-safe design.

EDF:

Typical failure modes are due to the hardware components

11. Maintenance

11.1. Describe any special requirements necessary to perform maintenance on DI&C systems/components that are included in an inspection programme.

Framatome:

Following the request from IEC 61513 (2011), a system operation and maintenance plan (see IEC 61513 chapter 6.3.7 and 6.3.8) shall be prepared during the engineering lifecycle of the project. During I&C system basic design, measures for e.g. parameter management, periodic testing, module replacement should be considered (for requirements – see IEC 61513).

Kepco:

Channel check is performed periodically for confirming the diagnostic results according to Tech Spec.

EDF:

Maintenance of DI&C are made division per division and not globally to avoid error propagation

NewClear Day

Specific controls may exist on the use of maintenance laptops that are used for digital assets are controlled to expectations described in Section C.4 of Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (see https://www.nrc.gov/docs/ML0903/ML090340159.pdf).

11.2. What kind of functional tests does your RB inspect? Please describe.

Framatome:

The I&C system Operation and Maintenance Plan identifies or links to the concept for periodical testing of the DI&C system. DI&C systems realised by the safety I&C platform TELEPERM® XS take benefit from the self-surveillance features of the platform and the available monitoring possibilities.

The demonstration for periodic testing coverage of TELEPERM® XS DI&C systems can be split up into online monitoring and periodic tests. The online monitoring, which runs cyclically in each CPU and I/O board, can be divided into the self-monitoring and engineered monitoring functions (e.g. measurement monitoring). As the DI&C functions are realised in software by components under surveillance of the online-monitoring, no additional need for periodic functional test is given. This conclusion is strongly related to the fact of absence of ageing effect of software. Nevertheless, the number of regulators who request to install measures for periodical demonstration of the correct and fault free function block execution and data communication is growing.

Note: For functions performed on non-digital I&C equipment additional means for periodic testing shall be considered in the design, including the functional tests.

Kepco:

The RB inspects that the periodic testing and diagnostic features for DI&C for safety systems meet the requirements of RG1.22, RG1.118, and RG1.153 through RAI.

The RB inspects the MMIS integration testing, pre-operational testing, periodic functional testing, channel calibration, and response time testing.

NewClear Day

No specific criteria or guidance.

12. Other

Please add any other questions/topics of interest to potentially consider for the workshop (Note: There may be other questions/topics that are important to DI&C inspections (e.g. cyber-security) but these topics have not been specifically mentioned herein as they might be too broad in scope for the workshop).

Framatome:

By introduction of digital I&C the topic of "cyber security" becomes important. Past incidents on cyber security attacks (such as Stuxnet) and the increased awareness on the vulnerabilities gets the standard design organisations to specify requirements and guidance to manage cyber security for nuclear power plants.

Based on the known threats / vulnerabilities, design measures and platform features are designed / developed to control them.

Regarding the inspection of the applied cyber security measures more specific approaches for analysis and testing need to be applied. As a hacker tries to find new (yet undetected) vulnerabilities of some installed DI&C system, the inspectors need to have a high level of knowledge in that area. For the verification and validation of the cyber security means, different test methods are applied by Framatome. In the frame of the I&C System V&V Plan a dedicated test plan for cyber security is issued. As an example, Framatome introduce penetration testing of the safety I&C systems for f projects.