Nuclear Regulation
NEA/CNRA/R(2014)7
June 2014

www.oecd-nea.org

Report on the Survey of the Design Review of New Reactor Applications

Volume 1: Instrumentation and Control

Working Group on the
Regulation of New Reactors

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Unclassified **NEA/CNRA/R(2014)7**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **28-Jul-2014**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

NEA/CNRA/R(2014)7
Unclassified

CNRA Working Group on the Regulation of New Reactors

Report on the Survey of the Design Review of New Reactor Applications Volume 1: Instrumentation and Control

JT03360764

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

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

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

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 31 countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, the Republic of Korea, the Russian Federation, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

– to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as

– to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management, 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. In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

The Committee on Nuclear Regulatory Activities (CNRA) shall be responsible for the programme of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. The Committee shall constitute a forum for the effective exchange of safety-relevant information and experience among regulatory organisations. To the extent appropriate, the Committee shall review 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 shall review current management strategies and safety management practices and operating experiences at nuclear facilities with a view to disseminating lessons learnt. In accordance with the NEA Strategic Plan for 2011-2016 and the Joint CSNI/CNRA Strategic Plan and Mandates for 2011-2016, the Committee shall promote 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 shall promote transparency of nuclear safety work and open public communication. The Committee shall maintain an oversight of all NEA work that may impinge on the development of effective and efficient regulation.

The Committee shall focus primarily on the regulatory aspects of existing power reactors, other nuclear installations and the construction of new power reactors; it may also consider the regulatory implications of new designs of power reactors and other types of nuclear installations. Furthermore it shall examine any other matters referred to it by the Steering Committee. The Committee shall collaborate with, and assist, as appropriate, other international organisations for co-operation among regulators and consider, upon request, issues raised by these organisations. The Committee shall organise its own activities. It may sponsor specialist meetings and working groups to further its objectives.

In implementing its programme the Committee shall establish co-operative mechanisms with the Committee on the Safety of Nuclear Installations in order to work with that Committee on matters of common interest, avoiding unnecessary duplications. The Committee shall also co-operate with the Committee on Radiation Protection and Public Health and the Radioactive Waste Management Committee on matters of common interest.

FOREWORD

The Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency (NEA) is an international committee composed primarily of senior nuclear regulators. It was set up in 1989 as a forum for the exchange of information and experience among regulatory organisations and for the review of developments which could affect regulatory requirements. The Committee is responsible for the NEA programme concerning the regulation, licensing and inspection of nuclear installations. In particular, the Committee reviews current practices and operating experience.

The CNRA created the Working Group on the Regulation of New Reactors (WGRNR) at the Bureau meeting of December 2007. Its Mandate was to "be responsible for the programme of work in the CNRA dealing with regulatory activities in the primary programme areas of siting, licensing and oversight for new commercial nuclear power reactors (Generation III+ and Generation IV)".

At its second meeting in 2008, the Working Group agreed on the development of a report based on recent regulatory experiences describing; 1) the licensing structures, 2) the number of regulatory personnel and the skill sets needed to perform reviews, assessments and construction oversight and 3) types of training needed for these activities. Also the Working Group agreed on the development of a comparison report on the licensing processes for each member country. Following a discussion at its third meeting in March 2009, the Working Group agreed on combining the reports into one, and developing a survey where each member would provide their input to the completion of the report.

During the fourth meeting of the WGRNR in September 2009, the Working Group discussed a draft survey containing an extensive variety of questions related to the member countries' licensing processes, design reviews and regulatory structures. At that time, it was decided to divide the workload into four phases: General, Siting, Design and Construction. The General section of the survey was sent to the Working Group at the end of the meeting with a request to the member countries to provide their response by the next meeting. The *Report of the Survey on the Review of New Reactor Applications* NEA/CNRA/R(2011)13[1] which covers the members' responses to the General section of the survey was issued in March 2012.

At the tenth meeting of the WGRNR in March 2013, the members agreed that the report of the responses to the Design section of the survey should be presented as a multi-volume text. As such, each volume will focus on one of the eleven general technical categories covered in the survey. It was also agreed that only those countries with design review experience related to the technical category being reported are expected to respond to that section of the survey.

The reports of the survey on the design review of new reactor applications are to serve as guides for regulatory organisations to understand how technical design reviews are performed by member countries. It therefore follows that the audience for these reports are primarily nuclear regulatory organisations, although the information and ideas may also be of interest to other nuclear industry organisations and interested members of the public.

[1] Follow this link to download the report: https://www.oecd-nea.org/nsd/docs/2011/cnra-r2011-13.pdf

ACKNOWLEDGMENTS

This report, prepared by Dr Steven Downey (NRC, United States), is based on discussions and input provided by members of the CNRA Working Group on the Regulation of New Reactors listed below. Mr Steve Gibson (ONR, United Kingdom) and Ms Aurélie Lorin (NEA Secretariat) chaired the meetings and supervised the work carried out by the group.

– Philip Webster, CNSC, Canada
– Ken Lafrenière, CNSC, Canada
– Janne Nevalainen, STUK, Finland
– Thomas Houdré, ASN, France
– Philippe Joyer, ASN, France
– Jaharlal Koley, AERB, India
– Atushi Ui, JNES, Japan
– Walter Kim, KINS, Korea
– Seon Ho Song, KINS, Korea
– Mikhail Lankin, SEC NRS, Russia
– Jozef Kubanyi, UJD, Slovak Republic
– Ladislav Haluska, UJD, Slovak Republic
– Andreja Persic, SNSA, Slovenia
– Lovisa Wallin Caldwell, SSM, Sweden
– Andrea Valentin, NRC, United States
– Steven Downey, NRC, United States

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At the tenth meeting of the CNRA Working Group on the Regulation of New Reactors (WGRNR) in March 2013, the members agreed to present the responses to the Second Phase, or Design Phase, of the Licensing Process Survey as a multi-volume text. As such, each report will focus on one of the eleven general technical categories covered in the survey. The general technical categories were selected to conform to the topics covered in the International Atomic Energy Agency (IAEA) Safety Guide GS-G-4.1. This report, which is the first volume, provides a discussion of the survey responses related to Instrumentation and Control (I&C).

The Instrumentation and Control category includes the twelve following technical topics: Reactor trip system, actuation systems for Engineered Safety Features (ESF), safe shutdown system, safety-related display instrumentation, information and interlock systems important to safety, controls systems, main control room, supplementary control room, diverse I&C systems, data communication systems, software reliability and cybersecurity. For each technical topic, the member countries described the information provided by the applicant, the scope and level of detail of the technical review, the technical basis for granting regulatory authorisation, the skill sets required and the Level of effort needed to perform the review. Based on a comparison of the information provided in response to the survey, the following observations were made:

- Among the regulatory organisations that responded to the survey, there are similarities in the design information provided by an applicant. In most countries, the design information provided by an applicant includes, but is not limited to, a description of the I&C system design and functions, a description of the verification and validation programmes, and provisions for analysis, testing, and inspection of various I&C systems.
- In addition to the regulations, it is a common practice for countries to make use of guidance documents and consensus standards to provide the technical basis for acceptability.
- Most of the technical topics covered in the survey are reviewed in some manner by all of the regulatory organisations that provided responses. Some perform separate design reviews related to each topic, while others address several topics as part of a broader I&C system design review.
- It is common to consider emerging issues, operating experience and lessons learned from the current fleet during the review process.
- Design review strategies commonly used to confirm that the regulatory requirements have been met include document review, onsite audit, inspection and independent verification of analyses performed by the applicant.
- The most commonly and consistently identified technical expertise needed to perform the I&C related design reviews is Electrical or I&C engineering. Other technical disciplines are identified on a less consistent basis.

The complete survey inputs are available in the appendices.

INTRODUCTION

During the five decades of commercial nuclear power operation, nuclear programmes in NEA countries have grown significantly. Over the years, communication among member countries has been a major reason for the steady improvements to nuclear plant safety and performance around the world. Member countries continue to learn from each other, incorporating past experience and lessons learned in their regulatory programmes. They consult each other when reviewing applications and maintain bilateral agreements to keep the communication channels open. This has been vital and will continue to be extremely important to the success of the new fleet of reactors being built.

The Design Phase Survey Reports will continue along these lines by providing detailed information on the design-related technical topics that are reviewed by the regulatory organisation as part of the regulatory authorisation process. This document, which is the first report on the results of the Design Phase Survey, focuses on Instrumentation and Control (I&C).

SURVEY

The second phase, or Design Phase, of the licensing process survey conducted by the CNRA Working Group on the Regulation of New Reactors (WGRNR) covers eleven general technical categories that are based on IAEA Safety Guide GS-G-4.1. Under these eleven general categories, there are a total of 69 specific technical topics to be addressed. For each technical topic, a member country is asked to answer seven survey questions. At the March 2013 meeting, the working group agreed that the report of the responses to the design section of the survey should be presented as a multi-volume text. As such, each volume will focus on one of the eleven general technical categories covered in the survey. This volume, which focuses on Instrumentation and Control, is the first of several reports that will present the results of the Design Phase Survey.

The following pages present high level summaries provided by the members and a discussion of the survey results. Complete survey responses are presented in the appendices.

HIGH LEVEL SUMMARIES

Canada

The information provided applies to the licensing review of a new nuclear power plant in Canada. It is also used in pre-project Vendor Design Reviews (VDR). Pre-licensing VDR is:

- not a licensing discussion,
- a technical conversation between the Canadian Nuclear Safety Commission (CNSC) and the vendor,
- a proven and standardized process to evaluate, in principle, whether there are fundamental barriers to licensing the vendor's reactor design in Canada.

The outcome of a VDR is not a detailed review of the entire design; it is a broad sample of key safety related topics. As such, the Level of effort needed to review a VDR is less than that of a licensing review.

The review of the Instrumentation and Control (I&C) area is based on guidance provided in the applicable sections of the following CNSC regulatory documents:

- RD/GD-369, License to Construct a Nuclear Power Plant;
- RD-337, Design of a New Nuclear Power Plant;
- GD-385, Pre-licensing Review of a Vendor's Reactor Design.

CNSC staff will also use various applicable codes and standards in the evaluation of I&C topics (such as Canadian Standards Association (CSA) and Institute of Electrical and Electronics Engineers (IEEE) standards).

CNSC staff will examine the design approach for I&C pertaining to all SSC of the plant. We will also review the various design rules that the applicant has followed to implement the design approach and to ensure that the reliability of the systems meets design targets. Particular attention should be given to explaining common cause and cross-link effects arising from the various events considered in the safety case, and the equipment diversity and independence that have been incorporated into the design to deal with these eventualities. Interfaces (including independence and separation between safety and all other instrumentation and control systems) should be addressed.

The description of I&C systems should include failure end-states for key instrumentation and control devices, taking into account the implications of these failure states for the safe operation of the plant. General expectations for instrumentation and control are given in section 7.9 of RD-337. Specific expectations concerning the following topics are provided in subsections 6.7.1 to 6.7.4 of RD/GD-369:

- safety system I&C,
- information systems important to safety,
- all other instrumentation systems important to safety,
- control room I&C.

As part of the review, CNSC staff also consider emerging issues, operating experience and lessons learned from the current fleet.

Electrical, electronics and computer engineering are the primary expertise needed to successfully perform I&C-related design reviews. In some areas, human factors engineers and reactor systems engineers are also needed to completely review the technical topic. The review of cybersecurity requires additional expertise in the area of information technology and cybersecurity.

Finland

Finnish regulatory guidance (Radiation and Nuclear Safety Authority – STUK – YVL Guides) for instrumentation and control systems is specified in the following guides: YVL 1.0 (general requirements), YVL 1.4 (managements system and Quality Assurance (QA)), YVL 2.0 (systems), YVL 2.7 (analysis) and YVL 5.5 (I&C). Requirements concerning the system descriptions contained in the Preliminary Safety Analysis Report are specified in Section 3.2 of the Guide YVL 2.0. The issues to be included in the conceptual design plan for each system are listed in Section 6.2 of the Guide YVL 5.5. Content requirements for these points are specified in Chapter 2 and 3 of the Guide YVL 5.5 in particular.

In addition to STUK YVL Guides, the design and implementation of the instrumentation and control system are intended to be carried out according to international nuclear power standards (IEC, IAEA and IEEE, etc.) and European Commission report EUR 19625 *Common Position of European Regulators for the Licensing of Safety Critical Software for Nuclear Reactors*. In addition to the nuclear power standards, international European standards (EN) and ISO standards, and other national standards (e.g. standards from the German Nuclear Safety Standards Commission (KTA)) are also commonly used.

The inspected area in the Olkiluoto 3 nuclear power plant (NPP) construction licence review includes the main instrumentation and control system (logic and control systems) of the plant unit as well as separate measurement systems. In the case of the Olkiluoto 3 NPP review, the following documentation was reviewed:

The instrumentation and control system is discussed in Chapter 7 of the PSAR and in topical reports. The most important topical reports are listed below:

- The topical report entitled “I&C Architecture Concept Independence and Diversity” describes independence, principles of separation and diversity, and common cause failure via I&C architecture.
- The topical report entitled “Implementation of the Fail Safe Principle” describes the implementation of the fail-safe principle in the reactor protection system (PS).
- The topical report entitled “Functional Design and Safety Classes of Automation System” describes the various system functions primarily from a process perspective.
- Topical report: Provision for hardware back-up system in case of total loss of computerised I&C.
- The Teleperm XS platform used in the system PS is discussed in section 7.6.2 of the PSAR. This includes the preliminary suitability analysis and the suitability analysis documentation for the plant independent TELEPERM XS System Platform.
- The diversity of the Teleperm XS and XP platforms is discussed in a topical report entitled “Diversity between TELEPERM XP and TELEPERM XS”.
- Equipment qualification, in particular, is described in the topical report entitled “Classification, Qualification and Quality Assurance for Instrumentation and Control Systems”.
- Requirements concerning accidental environmental conditions are described in the topical report entitled “Qualification Curve of Electrical and I&C Equipment against Increased Ambient Conditions”.

- Equipment compliance with the requirements concerning accidental environmental conditions is described in the topical report entitled “Qualification to Accident Conditions (accidental environmental conditions)”.
- Compliance with the requirements of YVL 5.5 is described in topical report entitled “Fulfilment YVL 5.5 – Instrumentation Systems and Components at Nuclear Facilities”.

Other chapters of the PSAR and topical reports were also used in connection with the inspection.

France

In France, the review of NPPs with extensive use of digital I&C systems, and in particular an integrated digital protection system performing both reactor trip and actuation system for emergency safeguard functions (ESF), started about 30 years ago with EDF’s 1300 MW_e series (20 units in operation). Digital control rooms were introduced in the mid 90’s with the N4 reactor series (4 units in operation). At the present time, the EPR is being reviewed based on the experience of those two previous reactor series.

The review is based on the fact that digital technology can be considered as reliable for the performance of safety functions, provided that:

- Really strong design principles are applied (in this respect the French basic safety Rule on software puts forward the principle of “determinism”);
- Adequate recognised standards are fully enforced (e.g. standards from IEC 45A: 60513, 60880, 62138, etc.);
- A specific and thorough technical review is performed, including some analysis of the source code itself.

A significant research effort is made to promote assessment techniques that rely on a strong mathematical basis (e.g. static analysis, proof of program, formal measurement of test coverage, etc.). Assessment techniques that do not rely on a strong mathematical basis are considered only as a complement (e.g. diversity) or not considered (quantitative software reliability).

Based on our experience the most important and most technical part is the assessment of the digital platforms. Indeed, from a computer science point of view the functions to be performed by the platform are overall more complex than the application functions themselves (e.g. reactor trip functions, etc.). Provided those platforms have the appropriate algorithmic properties and quality of design, the development of the target systems is then quite bounded.

Commercial dedication may also lead to difficulties in the assessment in particular to obtain sufficient documentation and proper justifications.

India

AERB Safety guide No. AERB/NPP&RR/SG/G-1, “consenting process for nuclear power plants and research reactors”, specifies the relevant information to be submitted by the applicant for review and assessment during various stages of consenting/licensing of a NPP. This document along with AERB/SG/G-7, “regulatory consents for nuclear and radiation facilities: contents and formats”, is meant to provide information on the methods of review and assessment to be carried out by the Atomic Energy Regulatory Body (AERB). The design description part of safety analysis report should bring out the design criteria/bases, functional requirements, and how these are met in the detailed design of I&C systems.

The staff of AERB (1) conduct initial checks for adequacy of information submitted and conducts preliminary reviews of the information provided, and then (2) the AERB asks for additional information as necessary. (3) detailed reviews are conducted in a specialist group (SG) or working group (WG) constituted for the purpose and (4) the SG or WG resolves technical issues with utility. (5) The unresolved issues and recommendations of specialist groups are then brought to the Project Design Safety Committee (PDSC) of the AERB. (6) specific issues are referred to AERB standing committee on I&C and computer based systems. The same committee also reviews the operating experience feedback on I&C systems. (7) The PDSC makes its recommendation to the advisory committee of project safety review (ACPSR) for the final disposition. (8) after its review, the ACPSR makes the necessary recommendation to the board of AERB.

The scope and level of detail of the safety review is based on the guidance of applicable codes and guides of AERB. In specific areas where AERB documents are not prepared, relevant IAEA or other codes/standards acceptable to AERB are used. During the review AERB committees also consider emerging technical and construction issues, operating experience, and lessons learned related to this category. Confirmatory analyses are performed, if necessary, on a case-by-case basis by the technical service organisation or at the designated division of AERB. The commonly performed confirmatory analyses are to verify the adequacy of the submissions related to Failure modes and effects analysis.

The review is carried out based on general design principles relevant to assuring safety as enunciated in AERB safety code AERB/NPP-PHWR/SC/D and guides AERB/NPP-PHWR/SG/D-1, AERB/NPP-PHWR/SG/D-10, AERB/NPP-PHWR/SG/D-20 and AERB/NPP-PHWR/SG/D-25. For Indian NPPs, safety related I&C are classified as IA, IB and IC and as seismic category 1 or 2. Special attention is given to computer based systems through an elaborate audit of software V&V (verification and validation).

Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. The regulatory staff are also trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the technical support organisations (TSOs) that work in specialised areas.

Japan

The information provided is based on the licensing review process of establishment/permit for existing Japanese nuclear power plants before the Fukushima Daiichi nuclear power plant accident. The requirements and guides were established by the nuclear safety commission (NSC). The nuclear and industrial safety agency (NISA) staff had reviewed the design of Instrumentation and Control (I&C) based on the examination guide for safety design of light water power reactor facilities.

After the Fukushima Daiichi nuclear power plant accident, a new nuclear regulatory body, the nuclear regulation authority (NRA) was established to improve its nuclear safety management and regulation in 2012. On 8 July 2013, the new regulatory requirements for commercial nuclear power plants went into force. In the sense of a “back-fit”, the new regulations are applied to the existing nuclear power plants. The NRA staff review the safety design of I&C in terms of design-basis events and severe accident conditions.

Republic of Korea

The information provided applies to the licensing review of the implementation of digital I&C and full scope modernisation of the main and supplementary control rooms, at Shin-Kori units 3 and 4 (APR1400), in 2003-2014.

The modernisation of Shin-Kori units 3 and 4 (APR1400) is a total exchange of all I&C systems. The Korea Institute of Nuclear Safety (KINS) reviewed the PSAR (preliminary safety analysis report (SAR)) for CP (Construction Permit) and is reviewing the FSAR (Final SAR) for OL (operating licence) submitted by the Korea hydro and nuclear power (KHNP). while reviewing the SAR, KINS sends RAIs (Request for Additional Information) to KHNP. In some selected areas, KINS evaluated the design information documents and performed audits and inspection visits to evaluate the design processes and V&V activities.

I&C subject areas of SAR are the following:

- 7. I&C system;
- 7.1 Introduction;
- 7.2 Reactor Protection System (RPS);
- 7.3 Engineered Safety Features Actuation System (ESFAS);
- 7.4 Safety Shutdown System;
- 7.5 Safety Related Display Information;
- 7.6 All other instrumentation system required for safety (Interlock system);
- 7.7 Systems not required for safety;
- 7.8 Diverse Instrumentation And Control systems;
- 7.9 Data communication system;
- 18 Human Factor Engineering;
- 18.1 Main control room;
- 18.2 Remote shutdown room.

In addition to SAR, for digital computer safety systems, KINS performed an audit of software life-cycle processes implementation in the review stage of Operating Licence (OL) in order to confirm the quality of software for digital computer protection system. The audit was conducted by a witness on the stage of the integration test or factory acceptance test. Also, the audit of software life-cycle process design outputs was conducted by reviewing the design documents or walking-through in the OL stage.

The regulatory body uses a qualitative approach for determining software reliability. Such qualitative approach is typically based on strong requirements on the deterministic behaviour of the software to allow full V&V and gives a high confidence in the reliability of the software.

Regulations require a diverse protection system (DPS) to address the requirements for reduction of risk from an anticipated transient without scram (ATWS) event. The DPS utilises independent and diverse logic to initiate reactor trip and auxiliary feedwater actuation.

The regulatory body requires that the applicant shall assess the defence-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. The hardwired manual control is required as a means to cope with a postulated common cause failure (CCF) that could disable the digital RPS and ESFAS.

For cybersecurity of I&C system, an I&C security policy and security plan were submitted to and reviewed by KINS. The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system life-cycle.

Russian Federation

In the Russian Federation, Rostekhnadzor’s regulatory activity in the area of I&C systems is based on the following regulations:

- OPB-88/97 General Safety Provisions for NPPs (Sections 4.4, 4.5);
- NP-082-07 Nuclear Safety Rules for Reactor Installations of NPPs (chapter 3);
- NP-026-04 Requirements to Control Systems Important To Safety of NPPs;
- NP-006-98 Requirements to the Content of the Safety Analysis Report for VVER-type NPPs (chapter 7).

For those areas which are not covered by national regulations in due details, the provisions of internationally recognised documents (such as IAEA standards) are considered. Digital I&C implementation can act as an example of such areas.

A licensee shall submit a NPP Safety Analysis Report to the regulatory body. Among other issues to be addressed, this report shall contain information on all safety related I&C systems within the scope of requirements of chapter 7 of the federal rules and regulations NP-006-98.

The report is subject for regulatory review which is carried out by Rostekhnadzor's TSO in the scope of the licensing procedure.

Slovak Republic

The information provided is based on the Slovak legal framework which accommodates the Western European Nuclear Regulators' Association (WENRA) reference levels and IAEA standards. The requirements are common for the new reactors, as well as in the case of the modernisation or exchange of existing I&C systems. The fulfilment of these requirements is reported via safety analysis report, technical and quality documentation.

The applicant has to demonstrate that the safety principles were applied in I&C systems. These principles include single failure protection, graded approach, diversity, redundancy and quality. It has to also be demonstrated that I&C systems were validated and verified. The main goal of all submitted documentation is to ensure that all legislative requirements are fulfiled, that a nuclear facility will be operated safely and that the public will be protected against undesirable effects of nuclear facility.

Review of the applicants´ submitted documentation is usually performed by regulatory body employees with the support of a TSO. When support services from a TSO are used, there is a condition of TSO independence. This condition results from the fact that the Slovak Republic is small and there are not many organisations with relevant skills in this field. Therefore, we have to prevent the possibility that the same TSO will provide support services for a nuclear facility and for the regulatory body.

Slovenia

The information provided is based on the review of a licensing process for I&C systems design approval. The most extensive review of I&C is performed at the design certification stage. During the operation stage, in case of the systems changes, the licensing system is carried out in the same way, only less intensive. Description of the systems and their operation is given in the Safety Analysis Report (for Krško NPP it follows the requirements of NRC RG 1.70, revision 3).

The basic I&C systems design basis requirements are set in the Regulation. The Instrumentation shall allow measurement of all the main variables of the nuclear power plant and allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived. The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested, and an additional degree of conservatism shall be taken into account in their analyses. I&C systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems. I&C shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible. Any unauthorised access or ingress to I&C systems shall be prevented by appropriate physical, technical and administrative measures.

The information provided by applicant is based on detail system description and design basis, system logic, system specification including setpoints, time delays, uncertainties, the interfaces with other systems. The safety analyses are normal part of applications. Additionally, the Slovenian Nuclear Safety Administration (SNSA) verifies that the applicant has provided complete information to demonstrate that the design, materials, fabrication methods, inspection techniques used conform to all applicable regulations, industrial codes and standards. The review of the results of testing, inspection and surveillance is also performed.

During the licensing process it is necessary to confirm that:

- The I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions;
- The implementing systems and equipment have been properly classified to identify their importance to safety;
- Commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction, and testing of I&C systems and equipment commensurate with the importance of the safety functions performed.

Electrical engineer, computer engineer, nuclear engineer are the primary expertise needed to successfully perform I&C related design reviews. In some areas, human factors engineers and reactor systems engineers are also needed to completely review the technical topic. For cybersecurity of I&C the Krško NPP prepared the cyber security program, which was submitted to SNSA for review. This requires additional expertise in the areas of information technology and of cybersecurity.

Sweden

The information provided applies to the licensing review of the implementation of digital I&C and full scope modernisation of the main and supplementary control rooms, at Ringhals Unit 2 (project TWICE), in 2004-2011. SSM is a relatively small organisation with limited resources. Because of these limitations SSM licensing reviews are often process oriented reviews with focus on the quality assurance and control within the licensee organisation and the vendors. It should also be noted that Sweden has no TSO.

The modernisation of Ringhals 2, the twice project, was a total exchange of all I&C systems. A discussion started between the regulatory body (SKI/SSM) and the utility concerning the utility strategy for licensing of the new I&C system. As a result of the discussions the utility proposed a “Plant Safety Assurance and Demonstration Plan” (PSADP). The plan has it background and inspiration from the Safety Case activities in UK and a European Union research project (CEMSIS) which SKI participated in and where Safety Justification was a part of the project.

An attachment to the PSADP was a Total Safety Case where the areas that is presented below are break down in claims and sub-claims. The strategy on how to show fulfilment and responsible organisation is also presented.

The strategy was that several plant safety assurance and demonstration reports (PSADR) should be presented and delivered to the regulator at different phases in the project. These reports can be seen as summarizing a safety case covering a total of fourteen different safety subject areas (SSAs). The safety subject areas are the following:

SSA 1: Scope Capture, Safety Categorization And System Definitions;
SSA 2: Quality Assurance (QA/QC);
SSA 3: Processes, Strategies And Plans;
SSA 4: Assumptions, Preconditions, Design Basis and Requirements (APDB&R) Identification;
SSA 5: Regulations, Codes, Standards and Guidelines (RCS&G);
SSA 6: Solution, System Architecture, Functional Design, System Design and Detail Design;
SSA 7: HFE; MCR, SCR and general HIS;
SSA 8: Verification and Validation Of Plant I&C;
SSA 9: Base Product Qualification;
SSA 10: Plant Installation;
SSA 11: Plant Documentation;
SSA 12: Organization and Competence Assurance;
SSA 13: Integration in Plant;
SSA 14: Operation, Maintenance and Modifications.

In the final PSADR the utility concluded that the main intents with the definition of the Total Safety Case (TSC), i.e. completeness and correctness of the defined SSAs and the claims formulated, are deemed fulfiled. The 14 SSAs with claims and sub claims have been confirmed sufficient by this PSADR, after addressing requirements qualification, process/project qualification, design qualification and corresponding evaluation of the PSAR, TS/TR and PLS representation respectively. Minor improvements/clarifications in formulations of claims as well as a few additional sub claims have been defined or proposed for agreement with WEC during the previous PSADP phases. Both the clarifications and addition of sub claims have been made to make them clearer and easier to understand. The changes performed or proposed do not impact negatively on the TSC intents – on the contrary, the clarifications improve it.

The regulatory assessment of these reports was performed at two stages. In the early reports review, the plans and the result in the early phases are reviewed. Then before start-up, the total report is reviewed. In some selected areas, detailed reviews and inspections were performed to low level.

United States

The information provided in response to the survey is based on the technical review of a new reactor design certification application, but is also applicable to the review of applications for new reactor design approvals and combined licences issued under 10 CFR Part 52. Typically, the most extensive review of I&C is performed at the design certification stage. New reactor combined licence (COL) applicants prefer to incorporate the I&C design by reference to a certified standard plant design. As such, the staff's review of Instrumentation and Control at the COL application stage would focus on site-specific information and departures from the approved standard design. Therefore the level of effort needed to review a COL application is significantly less than what is required to review a design certification application.

Regardless of the type of application, the fundamental purpose is for the applicant to demonstrate that the facility and equipment, the operating procedures, the processes to be performed and other technical requirements described in the SAR offer reasonable assurance that the plant will comply with the regulations and that public health and safety will be protected. Design information provided by the applicant in this technical category should emphasise those instruments and associated equipment that constitute the protection and safety systems. The applicant should also provide analysis of control systems, with particular consideration of transients induced by the control system, which, if not terminated in a timely manner, could result in fuel damage and subsequent fission product release to the environment. The regulations related to I&C require applicants to address fundamental I&C safety design principles. These principles include single failure protection, independence, redundancy, diversity and quality. Several I&C regulatory guides have been developed to provide guidance to applicants and licensees on acceptable approaches to meet the regulatory requirements. The Nuclear Regulatory Commission (NRC) staff have also endorsed industry guidance in the area of cybersecurity.

Once an application has been formally accepted, NRC staff review the information provided for compliance with the regulatory requirements and performs confirmatory analyses, as necessary, to make a reasonable assurance finding. The scope and level of detail of the staff's safety review of I&C is based on the guidance provided in the applicable sections of The Standard Review Plan (SRP), NUREG-0800. As part of the review, the staff also consider emerging issues, operating experience and lessons learned from the current fleet.

Electrical, electronics and computer engineering are the primary expertise needed to successfully perform I&C-related design reviews. In some areas, human factors engineers and reactor systems engineers are also needed to completely review the technical topic. The review of cybersecurity requires additional expertise in the area of Information Technology and cybersecurity.

DISCUSSION

Under the category of Instrumentation and Control, there were twelve technical topics to be addressed in the survey. These topics were selected to conform to the topics covered in IAEA Safety guide No. GS-G-4.1. For each of the twelve technical topics under this category, the member countries were asked seven questions in order to gather some insights on the level of detail needed for regulatory authorisation. In responding to these questions, each member country described the following:

- The design information provided by the applicant;
- The analysis, reviews and/or research performed by the regulatory organisation's reviewer(s) and the scope of the review;
- The types of confirmatory analyses performed (if any) by the regulatory organisation;
- The technical basis (standards, codes, acceptance criteria) for regulatory authorisation;
- The skill sets required to perform the review;
- The specialised training, experience, education and/or tools needed to perform the regulatory review;
- The Level of effort needed for the regulatory organisation to perform the review.

Design information provided by the applicant.

Among the regulatory organisations that responded to the survey, there are similarities in the design information provided by an applicant. In general, most countries responded that the applicant provides a description of the I&C system design, design bases, functions and requirements. In most countries, applicants are also required to provide information on verification and validation (V&V) programmes as well as provisions for analysis, testing and inspection of various I&C systems. Human Factors and Human Machine Interface (HMI) were also mentioned by multiple countries when describing the information provided by the applicant related to the main control room and the supplementary control room.

In Canada, Finland, India, Korea, Slovenia and the United States, a cybersecurity programme or plan is provided by the applicant. In addition to the cybersecurity plan, in Finland, the applicant also provides risk assessment plans and results. On the other hand, in Slovakia, the applicant addresses cybersecurity by providing a change control programme for all life cycle phases. It is noted that France, Japan, Russia and Sweden currently do not review cybersecurity as part of granting regulatory authorisation. However, Russia is currently developing regulations with plans to review this topic in the future.

Analysis, reviews and/or research performed.

Most of the technical topics covered in the survey are reviewed in some manner by all of the regulatory organisations that provided responses. Some regulatory organisations perform separate design reviews related to each survey topic, while others address several of the I&C topics as part of a broader I&C system design review. For example, in Japan and Sweden, safety related display instrumentation is reviewed as part of the design review of the main control room. Also, in Finland and France, the information and interlock systems important to safety are reviewed as part of the design review of the actuation systems for ESF and the safe shutdown systems.

All countries review the information provided by the applicant for compliance with the applicable regulatory requirements. In addition to document reviews, some countries use onsite audits and inspections to confirm that the regulatory requirements have been met. For example, in Finland, India, Korea, Sweden and the United States, audits or inspections are used in the review of various I&C related technical topics. In Korea, audits or inspections are used as part of the review of nine of the twelve technical topics covered in the survey. These inspections are primarily related to the evaluation of design processes and V&V activities. In Finland and Sweden, audits and inspections are used as part of the review of actuation systems for ESF, safe shutdown systems and diverse I&C systems. In India, an audit of system development life cycle documents (including V&V and QA documents) is performed as part of the review of software reliability. In the United States, inspections are used to evaluate the implementation of a licensee's cybersecurity programme.

Most countries also responded that some type of confirmatory analyses is performed as part of the design review of Instrumentation and Control.

Technical basis.

In all cases, the technical basis for regulatory authorisation is provided by a combination of country-specific regulations and regulatory guidance. In addition to the regulations and guidance documents, most countries make use of either national or international consensus standards related to Instrumentation and Control.

Canada, Korea, Sweden and the United States refer to the IEEE standards as part of the technical basis for regulatory authorisation. IEEE Standard 603 *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations* and IEEE Standard 7-4.3.2 *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* were most consistently identified as part of the technical basis.

Finland, India, Russia, Slovenia and Sweden all identified the use of IAEA standards related to their review of instrumentation and control. Finland and Sweden consistently listed IAEA Safety Standards/Safety Requirements No. GS-R-3 *The Management System for Facilities and Activities* while Slovenia consistently identified IAEA Safety guide No. NS-G-1.1 *Software for Computer Based Systems Important to Safety in Nuclear Power Plants*, as well as other general IAEA standards. In Russia, IAEA Safety guide No. NS-G-1.3 *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants* and IAEA Draft Safety Guide DS-431 *Design of I&C Systems for Nuclear Power Plants* provide part of the technical basis for granting regulatory authorisation in several technical topics. Also, in India, IAEA standards, or other acceptable codes, are used to review specific areas where AERB documents have not been prepared.

Another commonly used consensus standard is the International Electrotechnical Commission (IEC) Standards, which were identified by Canada, Finland, France, Russia, Slovakia and Sweden as part of the technical basis for granting regulatory authorisation. The most commonly identified IEC standards were IEC 60880 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, IEC 61513 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems and IEC 62138 Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.

Skill sets required to perform review.

Electrical and I&C engineering were the most consistently identified skill sets needed to perform the reviews related to Instrumentation and Control. Other technical experts that were identified on a less consistent basis by the member countries were nuclear engineers, computer engineers, health physicists, human factors engineers, inspectors, mechanical engineers, quality engineers and reactor systems engineers.

Computer engineers were consistently listed as an expertise needed to perform I&C related design reviews in Canada, Finland, France, Korea and Slovenia. In Slovakia, computer engineers are used in the review of software reliability.

Nuclear engineers are used by Finland, Korea, Slovakia and Slovenia. Finland listed the need for this expertise in the review of all I&C topics. In Korea and Slovenia, nuclear engineers are used in the review of the reactor trip system and control systems. Korea also uses nuclear engineers in the review of safety related display instrumentation and information and interlock systems important to safety. In Slovakia, nuclear engineers are used in the review of the actuation systems for ESF.

Human factors engineers are used by Canada, Korea, Slovenia, Sweden and the United States. Canada identified the need for human factors engineering expertise in the review of most technical topics covered in the survey. Korea, Sweden and the United States listed the need for this expertise in the review of the main and supplementary control room. Korea and the United States also use human factors engineers in the review of safety-related display instrumentation.

Mechanical engineers are used by Korea, Slovakia and Slovenia. In Slovakia and Slovenia, mechanical engineering is the expertise needed to perform main control room and supplementary control room reviews. Korea listed the need for mechanical engineers in the review of systems not required for safety (control systems).

Reactor systems engineers are used by Canada, India, Korea, Slovenia and the United States. For example, India identified the need for reactor systems engineers in the review of all technical categories covered in the survey. Korea and the United States use reactor systems engineers in the review of diverse I&C systems. The United States also uses reactor systems engineers in the review of the reactor trip system and the main control room, while Korea uses this expertise in the review of actuation systems for ESF.

The specific skill sets needed to review each technical topic are provided in the summary tables located on the first page of each appendix.

Specialised training.

All countries have indicated that experience related to the technical review topic is important. Finland, India, Japan, Korea and the United States offer formal training programmes for technical reviewers responsible for Instrumentation and Control.

Level of effort.

The estimated total Level of effort required for each member country to review the Instrumentation and Control category is provided in the table below. It is noted that, in Japan and India, resources (hours) are not set up for each individual review area. Also, in Slovakia, the Level of effort allotted for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved. For each technical topic, the estimated Level of effort is presented in the summary table located on the first page of the appropriate appendix.

Country	Total estimated level of effort for I&C	Basis for Estimate
Canada	3 000 hours.	Construction licence application review.
Finland	2 505 working days (20 040 hours).	Olkiluoto 3 NPP review.
France	5 man-years, 6 man-months and 25 working days. (11 160 hours).	Review of NPPs with digital I&C systems.
India	–	Resources (hours) are not set up for each individual review area.
Japan	–	Resources (hours) are not set up for each individual review area.
Korea	1 610 working days (12 880 hours).	Review of digital I&C and control room modernisation at Shin-Kori 3 and 4.
Russia	32-48 man-months (5 120-7 680 hours).	Current review experience and planned future activities.
Slovakia	–	Level of effort defined by regulation and dependent upon the activity to be approved.
Slovenia	3 540 hours.	Review of a licensing process for Instrumentation and Control (I&C) systems design approval.
Sweden	675 working days (5 400 hours).	Review of digital I&C and control room modernisation for Ringhals Unit 2.
United States	27 180 hours.	Standard Design Certification review.

Table 1: Total estimated Level of effort for Instrumentation and Control category

Note:

The total level of effort is only listed for those countries that provided hours for all technical topics. The Level of effort for each specific technical topic is located in the summary table of the corresponding appendix.

CONCLUSION

This report focused on the results of the design survey related to instrumentation and control. Based on a comparison of the information provided in response to the survey, the following observations were made:

- Among the regulatory organisations that responded to the survey, there are similarities in the design information provided by an applicant. In most countries, the design information provided by an applicant includes, but is not limited to, a description of the I&C system design and functions, a description of the verification and validation programmes, and provisions for analysis, testing and inspection of various I&C systems.
- In addition to the regulations, it is a common practice for countries to make use of guidance documents and consensus standards to provide the technical basis for acceptability.
- Most of the technical topics covered in the survey are reviewed in some manner by all of the regulatory organisations that provided responses. Some perform separate design reviews related to each topic, while others address several topics as part of a broader I&C system design review.
- It is common to consider emerging issues, operating experience and lessons learned from the current fleet during the review process.
- Design review strategies commonly used to confirm that the regulatory requirements have been met include document review, onsite audit, inspection and independent verification of analyses performed by the applicant.
- The most commonly and consistently identified technical expertise needed to perform the I&C related design reviews is electrical or I&C engineering. Other technical disciplines are identified on a less consistent basis.

Additional reports will be issued by the working group in order to discuss the results of the Design Phase survey in other technical areas. In addition to the design phase reports, the working group will also issue a report that will deal with a survey on the review of new reactor applications, focusing on questions related to the construction stage.

APPENDIX A
REACTOR TRIP SYSTEM

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factors engineering.	500 hours.
Finland	Yes.	Yes.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	615 working days (4 920 hours).
France	Yes.	Yes.	I&C engineer, computer engineer.	2 man-years (4 000 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[1]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10-year experience are taken on the task.	–[1]
Korea	Yes.	Yes.	I&C engineer, electrical and electronics engineering, computer engineering, nuclear engineer.	180 working days (1 440 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	4-6 man-months (960 hours).
Slovakia	Yes.	No.	Electrical engineer.	–[2]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer, nuclear engineer.	360 hours.
Sweden	Yes.	Yes.	I&C engineer.	10 working days (80 hours).
United States	Yes.	Yes.	Electrical engineer, reactor systems engineer.	4 000 hours.

Notes:

1. In Japan and India, resources (hours) are not set up for each individual review area.
2. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Reactor trip system	Canada CNSC
Design information provided by applicant.	Section 6.7.1 of the CNSC licence application guide RD/GD-369 "licence to construction a nuclear power plant" specifies information to be provided by applicant for safety system instrumentation and control. Specific information to be provided for this technical area includes: – Design basis requirements for individual actuation parameters (physical measurements used to trigger safety system action), including a list of the postulated initiating events for which each parameter is credited; – Identification of the interfaces with other systems, including the provisions to ensure the proper isolation of electrical signals, the means used to ensure the physical separation of redundant actuation system channels and the means used to generate coincidence signals from redundant independent channels; – A description of the hardware and software quality assurance programmes and the software development process (including software requirements, design, implementation, verification, computer system integration, computer system validation, commissioning and configuration control). The description for software is needed when digital computers are used for safety systems; – Specification of actuation system setpoints for safety systems, the time delays in system operation, the measurement uncertainties and how these relate to the assumptions made in chapter 7, Safety Analyses of RD/GD-369; – Provisions for manually initiating safety systems from the main control room and the secondary control room; – Relevant remote operator and/or automatic control, local control, on-off control or modulating control considered in the design and credited in the safety analysis; – Elementary logic diagrams of the safety systems from the sensors to the end devices; – Provisions of a secure development and operating environment for the protection of digital computer-based safety system I&C.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC guidance document GD-385 "Pre-licensing Review of a Vendor's Reactor Design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area are as follows: – Focus Area 2: Classification of structures, systems, and components (SSCs); – Focus Area 5: Control system and facilities; – Focus Area 6: Means of reactor shutdown. The scope and level of detail of the staff's safety review is based on the guidance of the CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.7 "How to Assess the Instrumentation and Control". The following sections are applicable to reactor trip system: – Part A – Overall Instrumentation and Control; – Part B – Safety System Instrumentation and Control. During the Pre-Licensing Vendor Design Review process, the review for digital computer-based I&C systems might be limited to a detailed review at the function block level. More detailed reviews will be performed when reviewing

	construction and operation licence application.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmation analysis to verify: – Separation of reactor trip system with process control systems; – Separation of reactor trip system with other safety systems; – Completion of the intended sequence of trip action when initiated; – Strategies to address software common cause failure; – Fail-safe design.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the Reactor trip system: – Section 5.3 Quality assurance program; – Section 5.4 Proven engineering practices; – Section 5.7 Design documentation; – Section 6.1 Application of defence-in-depth; – Section 6.2 Safety functions; – Section 6.3 Accident prevention and plant safety characteristics; – Section 7.1 Classification of SSCs; – Section 7.3 Plant states; – Section 7.4 Postulated initiating events considered in the design; – Section 7.6 Design for reliability; – Section 7.6.1 Common cause failure; – Section 7.6.2 Single failure criterion; – Section 7.6.3 Fail-safe design; – Section 7.6.4 Allowance for equipment outage; – Section 7.6.5.1 Shared instrumentation for safety systems; – Section 7.8 Equipment environmental qualification; – Section 7.9 Instrumentation and control; – Section 7.13 Seismic qualification; – Section 7.14 In-service testing, maintenance, repair, inspection, and monitoring; – Section 7.17 Ageing and wear; – Section 7.21 Human factors; – Section 7.22 Robustness against malevolent acts; – Section 8.4 Means of shutdown; – Section 8.4.1 Trip parameters; – Section 8.4.2 Reliability; – Section 8.4.3 Monitoring and operator action; – Section 9.3 Hazard analysis. The main codes and standards relevant to this technical area include: – CSA N290.0 "General requirements for safety systems of nuclear power plants"; – 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 computer in safe systems of nuclear power generating stations".

Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Methodology for determination of trip set point; – Reactor reactivity control.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience with operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering; – Preferably higher education in electrical and electronics engineering or computer science.
Level of effort in each review area.	500 person-hours for construction licence application review.

Reactor trip system	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification and its independent assessment; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – Failure Mode Effects Analysis (FMEA); – Reliability analysis; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of all design information documents; – Independent model checking to evaluate correct functionality of selected reactor trip functions (by TSO); – Audits and inspection visits to evaluate design processes, staff competencies and interface between different design organisations.
What type of confirmatory analysis (if any) is performed?	– See design information; provided by supplier; – Safety assessment by licence holder; – Safety assessment by designer.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Government decree on nuclear safety; – Regulatory guidance (YVL guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 60880); – KTA standards for I&C platform; – For quality management: ISO 9001, IAEA GS-R-3, KTA 1401; – Acceptance criteria: same safety level must be demonstrated as required by YVL guides and main standards.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – TSO: computer engineer, quality engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – SPICE (ISO/IEC 15504) training; – Plant specific training; Tools and methods: – Document management system; – Model checker tools; – ISO/IEC 15504 for auditing; Experience: – I&C (hardware, software); – Process and safety design; – Testing methods; – Quality management.
Level of effort in each review area.	– Regulator review: 555 working days. – Consultants' time: 30 working days. – TSO's review time: 30 working days.

Reactor trip system	France ASN
Design information provided by applicant.	The applicant has to provide the complete set of the development documentation. In particular, the source code of the platform's system software and of a sample of the application software has to be provided. (The environmental qualification results for the hardware equipment is also provided and reviewed separately.)
Analysis, reviews and/or research performed by the reviewer and scope of review.	A detailed technical review of the whole development documentation against the relevant IEC 45A standards, the French basic safety rules, and previously accepted projects is performed. This type of review is performed for both the I&C platform and the system build upon this platform and including the application software. Significant research activities have been performed during the last 20 years in order to influence the state in the art in the field of safety critical software. This research focuses on functional test coverage and on static analysis.
What type of confirmatory analysis (if any) is performed?	Experiments using the tools issued from the above research activities are performed using the actual source code.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Relevant IEC 45A standards (mainly IEC 61513, IEC 60880), French basic safety rule II.4.1a.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	I&C engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Extensive knowledge in computer science and more specifically real time software; – Extensive experience with safety critical digital systems.
Level of effort in each review area.	As a rough estimate: – 1 man-year for the platform; – 1 man-year for architecture and the application software.

Reactor trip system	India AERB
Design information provided by applicant.	The requirements are elaborated in AERB document on "Consenting Process For Nuclear Power Plants And Research Reactors" AERB/NPP&RR/SG/G-1. The design description part of safety analysis report should bring out design criteria/bases and functional requirements and how these are met in the detailed design of I&C systems. Following topics should be addressed with respect to reactor trip/shutdown system: – The instrumentation and controls (I&C) associated with the reactor trip system design should include for example redundancy, reliability, diversity, separation among protective channels, separation between protection and regulating function, testability and calibration, etc.; – Design criteria and design bases; – Special requirements for instruments; – Computer systems used and provisions for protection against faults in hardware/software; – Operator information systems and operator aids; – An instrumentation plan; – Reactor Protective/Shutdown Systems (Control & Instrumentation (C & I) aspects): design objectives, system description of sensors and their range overlaps, trip logics and their instrumentation, PSS (SDS1), SSS (SDS2); – Startup instruments; – Description for trip latching system; – Description of support systems (Instrument Air/Control Power supplies and their distribution, etc.); – Instrument air. As a part of failure analysis of Safety Analysis Report (SAR), the following should be brought out: – System failure mode and effects analysis (single failure analysis); – Common cause failure analysis (diversity analysis); – Reliability analysis; – Trip setpoint uncertainty analysis and trip system response time analysis; – Consequences to the failure of support systems (instrument air, power supply, etc.); – Conformance of reactor shutdown/trip system design with applicable codes/standards.
Analysis, reviews and/or research performed by the reviewer and scope of review.	AERB safety guide No. AERB/NPP&RR/SG/G-1 "Consenting Process For Nuclear Power Plants And Research Reactors" provides the review mechanism and processes. The Atomic Energy Regulatory Body (AERB) (1) conducts initial checks for adequacy of information submitted and conducts preliminary reviews of the information provided, (2) AERB asks for additional information as necessary, (3) detail review is conducted in specialist group (SG) or working group (WG) constituted for the purpose. (4) The SG or WG resolves technical issues with utility, and (5) The unresolved issues and recommendations of specialist groups are brought to the Project Design Safety Committee (PDSC) of AERB. (6) PDSC makes its recommendation to the Advisory Committee of Project Safety Review (ACPSR) for the final disposition. (7) ACPSR after its

	review makes the necessary recommendation to the board of AERB. The scope and level of detail of the safety review is based on the guidance of applicable codes and guides of AERB. In specific areas where AERB documents are not prepared relevant IAEA or other codes/standards acceptable to AERB are used. During the review AERB committees also considers emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis by the technical service organisation or at the designated division of AERB. The commonly performed confirmatory analysis is to verify the adequacy of the submissions related to failure modes and effects analysis.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	AERB safety guide No. AERB/SG/G-7, Regulatory Consents for Nuclear and Radiation Facilities: Contents and Formats provides the basis for review and issuance of regulatory consents. Trip coverage is given in table-2 of AERB document on “Safety Systems for Pressurised Heavy Water Reactors” AERB/NPP-PHWR/SG/D-10. The review is carried out based on general design principles relevant to assuring safety as enunciated in AERB safety code AERB/NPP-PHWR/SC/D and guides AERB/NPP-PHWR/SG/D-1, AERB/NPP-PHWR/SG/D-10, AERB/NPP-PHWR/SG/D-20 and AERB/NPP-PHWR/SG/D-25. Standards are referred in the above guiding documents.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or first of a kind (FOAK)), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Reactor trip system	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, the following design information of the safety protection circuit is provided in the application: – Type of reactor shutdown circuit. Design information of reactivity control system is provided, including functions of reactor shutdown system, in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Technical bases established by legislation and regulation. The guides employed by the Nuclear Safety Commission are listed below: – Examination guide for nuclear reactor siting and criteria and its application guide for dose objectives around light water power reactor facilities; – Evaluation guide for dose objectives around light water power reactor facilities; – Guide for measurement of released radioactive materials from light water power reactor facilities; – On the “Matters that has to be Safety Assurance Measures of our country”; – Examination guide for fire protection of light water power reactor facilities; – Evaluation guide for emergency core cooling system performance of light water power reactors; – Evaluation guide for seismic design of light water power reactor facilities; – Examination guide for radiation measurement during accident of light water power reactor facilities; – Evaluation guide for dynamic loads on BWR, Mark-II suppression system; – Items to be considered or principles of safety examination on radioactive liquid waste treatment facilities; – Meteorological guide for safety analysis of nuclear power reactor facilities; – Evaluation guide for reactivity insertion event of light water power reactor facilities; – Examination guide for safety design of light water power reactor facilities; – Review guide for safety evaluation of light water power reactor facilities, and; – Examination guide for classification of importance of safety functions of light water power reactor facilities. The reports compiled by “the Special Committee on Examination of Reactor Safety” of the Nuclear Safety Commission are listed below: – On 8×8 lattice type fuel assembly to be used for boiling water type nuclear reactors facilities;

	– On the core thermal design method and decision method of limiting values for thermal operation of boiling water type nuclear reactors facilities; – Reloaded Core Investigative Committee report; – Guidance of safety examination for geology and ground of nuclear power plants facilities, and; – Guidance of safety examination of active faults and others. The reports compiled by "Special Committee on Nuclear Reactor Standards" of the Nuclear Safety Commission are listed below: – Clarification of interpretation that "fuel cladding tubes are not damaged mechanically"; – On the fuel design method of light water nuclear power reactors; – On the radiation dose evaluation for general public at the safety review of light water nuclear power reactor facilities; – Radiation energy used in exposure calculation; – "Design consideration against internal missiles" associated with piping break; – 9×9 lattice type fuel assembly used in boiling water type nuclear power reactor facilities; – Handling of highly burned-up fuel in the reactivity insertion event of light water nuclear power reactor facilities. The following internal rules were established by the Nuclear and industrial safety agency: – Evaluation basis for aircraft crash probability onto nuclear power reactor facilities and others.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Reactor trip system	Korea KINS
Design information provided by applicant	– Safety analysis report chapter 7.2 Reactor Protection System; – Overall I&C architecture; – System requirements (including functional requirements) specification; – System description; – FMEA; – Reliability analysis; – System test plan, test specifications; – System test results; – Setpoint methodology; – Testability; – EQ documents; – Software documents; o Software quality assurance plan; o Software V&V plan, V&V report; o Software configuration management plan; o Software management plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluation of all design information documents; – Audits and inspection visits to evaluate design processes and V&V activities. For Digital System: – Software plan; – Life-cycle (computer system development process) planning; – Review and audit (if necessary) of software life-cycle process implementation; – Review and audit (if necessary) of software life-cycle process design outputs.
What type of confirmatory analysis (if any) is performed?	– Safety assessment by regulator; – Third party review or analysis is carried out in case of the implementation of new platforms or technology.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Regulation on technical standards for nuclear reactor facilities: o (Article 19) Suppression of reactor power and power distribution oscillations; o (Article 20) Instrumentation and control system; o (Article 26) Protection system; – Notice of NSSC (Nuclear safety and security commission): o (Reactor. 15) Regulation on safety classification and applicable codes and standards for nuclear reactor facilities; o (Reactor. 21) Guidelines of application of Korea electric power industry code (KEPIC) as technical standards of nuclear reactor facilities; – KINS Standard Review Guides: o (App. 7-13) Review Guide on Software of Digital-based I&C; o (7.2) Reactor trip system; – KEPIC ENB 1100(IEEE 603), KEPIC ENB 6370(IEEE 7-4.3.2); – KEPIC ENB 3000(IEEE 379); – KEPIC ENB 2000(IEEE 384).

Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer. – Junior: I&C engineer, computer engineer, nuclear engineer.
Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and system design.
Level of effort in each review area.	Regulator review: 180 working days (1 440 hours).

Reactor trip system	Russia SEC NRS
Design information provided by applicant.	A Safety Analysis Report (SAR) is to be submitted. Among other issues, this report contains information on the reactor control and protection system (including the reactor trip system) that is within the scope of the requirements of Chapter 7 of the federal rules and regulations NP-006-98 “Requirements to the Content of the Safety Analysis Report for Nuclear Power Plants (NPPs)”. The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to the reactor control and protection system. In particular, observance of the requirements of OPB-88/97 “General Safety Provisions for NPPs” (Sections 4.4, 4.5) and NP-082-07 “Nuclear Safety Rules for Reactor Installations of NPPs” (Section 2.3) shall be confirmed.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Requirements of the federal rules and regulations: – OPB-88/97 General Safety Provisions for NPPs (Sections 4.4, 4.5); – NP-082-07 Nuclear Safety Rules for Reactor Installations of NPPs (Section 2.3); – NP-006-98 Requirements to the Content of the Safety Analysis Report for VVER-Type NPPs (Chapter 7); – NP-026-04 Requirements to Control Systems Important to Safety of NPPs; Provisions of the IAEA Standards: – IAEA Safety Standards Series. Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011; Provisions of the national standards: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems); – GOST 26843-86. Nuclear Power Reactors. General Requirements to Control and Protection System; – GOST 27445-87. Neutron Flux Monitoring Systems for Control and Protection of Nuclear Reactors.

Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	Industry-specific education in the field of I&C systems for NPPS.
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	4-6 man-months.

Reactor trip system	Slovakia UJD
Design information provided by applicant.	– System description and functions (purpose of the system, technical solution, power supply, layout); – Analysis of the system performance and reliability (incorporation in the defence-in- depth, resistance to a single failure, resistance to a common cause failure, requirements for redundancy, requirements for diversity and independence, maintainability, testability); – Requirements for classification and qualification; – Requirements for Hardware (HW) and Software (SW); – Resistance to the environment (environment conditions, Electro Magnetic Compatibility (EMC) requirements, seismic resistance); – Verification and validation by the independent organisation; – Technical report about fulfilment of quality requirements; – Response analyses of the system to postulated trigger events, including system failure or incorrect operator procedures, in order to specify all internal events that can have an impact on nuclear safety.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the Reactor Trip System (RTS) fulfils the requirements for functionality, performance, reliability, resistance to the environment and quality.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	IEC standards, Slovak technical standards, regulatory guidance.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Reactor trip system	Slovenia SNSA
Design information provided by applicant.	– System description and design basis; – The design bases for each individual reactor trip parameter with reference to the Postulated Initiating Events (PIEs) whose consequences the trip parameter is credited with mitigating; – The specification of reactor trip system setpoints, time delays in system operation and uncertainties in measurement, and how these relate to the assumptions made in the chapter of the report on safety analyses; – Any interfaces with the actuation system for engineered safety features; – Any interfaces with non-safety-related instrumentation, control or display systems, together with provisions to ensure independence; – The mean employed to ensure the separation of redundant reactor trip system channels and mean by which coincidence signals are generated from redundant independent channels; – Provisions for the manual actuation of the reactor trip system from both the main control room and the supplementary control room; – Where reactor trip logic is implemented by means of digital computers, information of the software design, QA programme, the software verification and validation programme are provided.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques used conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety and; – That commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction, and testing of I&C systems and equipment commensurate with the importance of the safety functions performed. Confirmatory analysis of the predictions and calculations.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	General aspects of design standards including: – IAEA, "Safety of Nuclear Power Plants: Design", Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, "Site Evaluation for Nuclear Installations", Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, "Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide", Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, "Safety Assessment and Verification for Nuclear Power Plants", Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", Nuclear Security Series No. 4, IAEA, Vienna

	(2007); – IAEA, "Design of the Reactor Coolant System and Associated Systems in Nuclear power plants - safety guide", safety standards series No. NS-G-1.9, IAEA, Vienna (2004). IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No.NS-G-1.1, IAEA, Vienna (2000). Regulation JV 5, Reactor trip systems: To ensure safe shutdown of the reactor, at least two diverse systems shall be provided. At least one of these systems shall be capable of autonomously bringing, within four seconds, the reactor into subcritical condition with an appropriate reactivity margin, from any state of the facility and in a design-basis event. This shall be achieved also under the assumption of a single failure. Instrumentation and control: – Instrumentation shall allow measurement of all the main variables of the nuclear power plant that may affect the fission process, the reactor-core integrity, the reactor coolant system and the containment. Instrumentation shall also allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived; – Instrumentation and Control shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible; – Any unauthorised access or ingress to the instrumentation and control systems shall be prevented by appropriate physical, technical and administrative measures; – Instrumentation and control systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems; – The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Senior: electrical engineer, computer engineer, nuclear engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer, nuclear engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	– Regulator review: 160 hours. – TSO's review time: 200 hours.

Reactor trip system	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Non-specific review.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. revision 2010, SSM rapport 2010:01, Jan 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3: The Management System for Facilities and Activities, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	Approximately 10 working days.

Reactor trip system	**United States U.S. NRC**
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe or provide the following: – The instrumentation and controls (I&C) associated with the reactor trip system design including initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defence-in-depth features and actuated devices; – Logic diagrams, piping and instrumentation diagrams, and layout drawings of all reactor trip systems and supporting systems; – System failure mode and effects analysis; – Considerations of instrumentation installed to prevent or mitigate the consequences of the following: o Spurious control rod withdrawal; o Loss of plant instrument air systems; o Loss of cooling water to vital equipment; o Plant load rejection; o Turbine trip; – Conformance of reactor trip system design with IEEE Standards.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.2, "Reactor Trip System"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff commonly perform confirmatory analyses to verify the adequacy of the following submittal(s) related to this technical area: – Failure Modes and Effects Analysis. Other confirmatory analyses may be performed, if necessary, to aid the staff in making their safety finding. This is typically on a case-by-case basis.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The following NRC regulatory requirements are applicable to this technical area: – 10 CFR 50, Appendix A, General Design Criterion (GDC); o GDC 1, "Quality Standards and Records"; o GDC 2, "Design Basis for Protection Against Natural Phenomena"; o GDC 4, "Environmental and Missile Design Basis"; o GDC 10, "Reactor Design"; o GDC 13, "Instrumentation and Control"; o GDC 15, "Reactor Coolant System Design"; o GDC 19, "Control Room";

  - o GDC 20, “Protection Systems Functions”;
  - o GDC 21, “Protection System Reliability and Testability”;
  - o GDC 22, “Protective System Independence”;
  - o GDC 23, “Protection System Failure Modes”;
  - o GDC 24, “Separation of Protection and Control Systems”;
  - o GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”;
  - o GDC 29, “Protection Against Anticipated Operational Occurrences”;
- – 10 CFR 50.34(f), “Additional TMI-Related Requirements”;
- – 10 CFR 50.36(c)(ii)(A), “Technical Specifications”;
- – 10 CFR 50.55a(a)(1), “Quality Standards”;
- – 10 CFR 50.55a(h), “Protection and Safety Systems”;
- – 10 CFR 52.47 (b)(1), “Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”;
- – 10 CFR 52.80(a), “Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”.

The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this technical area are as follows:

- – Regulatory Guide (RG) 1.22, “Periodic Testing of Protection System Actuation Functions”;
- – RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”;
- – RG 1.53, “Application of the Single-Failure Criterion to Safety Systems”;
- – RG 1.75, “Criteria for Independence of Electrical Safety Systems”;
- – RG 1.105, “Setpoints for Safety-Related Instrumentation”;
- – RG 1.118, “Periodic Testing of Electric Power and Protection Systems”;
- – RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”;
- – Staff requirements memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs”, July 15, 1993;
- – NUREG/CR-6303, “Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems”, December 1994.

Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required.

The Codes and Standards related to this technical area are as follows:

- – IEEE Std 379-2000, “IEEE Standard application of the single-failure criterion to nuclear power generating station safety systems”;
- – IEEE Std 603-1991, “IEEE Standard criteria for safety systems for nuclear power generating stations”;
- – IEEE Std 7-4.3.2-2003, “IEEE Standard criteria for digital computers in safety systems of nuclear power generating stations”.

Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	– Electrical engineer; – Reactor systems engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	4 000 hours (estimated based on the level of complexity of the design).

APPENDIX B
ACTUATION SYSTEMS FOR ESF

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	500 hours.
Finland	Yes.	Yes.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	1 230 working days (9 840 hours).
France	Yes[1].	Yes.	I&C engineer, computer engineer.	2 man-years (4 000 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[2]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[2]
Korea	Yes.	Yes.	I&C engineer, electrical and electronics engineering, computer engineer, reactor systems engineer.	180 working days (1 440 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	4-6 man-months (960 hours).
Slovakia	Yes.	No.	Electrical engineer, nuclear engineer.	–[3]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer.	360 hours.
Sweden	Yes.	Yes.	I&C engineer.	20 working days (160 hours).
United States	Yes.	Yes.	Electrical engineer.	4 000 hours.

Notes:

1. In France, the same digital system performs reactor trip and ESF. Therefore the two technical topics are reviewed concurrently.
2. In Japan and India, resources (hours) are not set up for each individual review area.

3. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

<table>
<tr><th>Actuation systems for ESF</th><th>Canada
CNSC</th></tr>
<tr><td>Design information provided by applicant.</td><td>Section 6.7.1 of the CNSC Licence Application Guide RD/GD-369 “Licence to Construction a Nuclear Power Plant” specifies information to be provided by applicant for safety system instrumentation and control. Specific information to be provided for this technical area includes:
– Design basis requirements for individual actuation parameters (physical measurements used to trigger safety system action), including a list of the postulated initiating events for which each parameter is credited;
– Identification of the interfaces with other systems, including the provisions to ensure the proper isolation of electrical signals, the means used to ensure the physical separation of redundant actuation system channels and the means used to generate coincidence signals from redundant independent channels;
– A description of the hardware and software quality assurance programmes and the software development process (including software requirements, design, implementation, verification, computer system integration, computer system validation, commissioning and configuration control).The description for software is needed when digital computers are used for safety systems;
– Specification of actuation system setpoints for safety systems, the time delays in system operation, the measurement uncertainties, and how these relate to the assumptions made in chapter 7, Safety Analyses of RD/GD-369;
– Provisions for equipment protective interlocks (e.g. pump and valve interlocks and motor protection) within the actuation system, including a demonstration that such interlocks will not adversely affect the operation of safety systems;
– Provisions for manually initiating safety systems from the main control room and the secondary control room;
– Relevant remote operator and/or automatic control, local control, on-off control or modulating control considered in the design and credited in the safety analysis;
– Elementary logic diagrams of the safety systems from the sensors to the end devices;
– Provisions of a secure development and operating environment for the protection of digital computer-based safety system I&C.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>Appendix A of the CNSC guidance document GD-385 “Pre-licensing Review of a Vendor’s Reactor Design” describes review focus areas used in the assessment of a vendor’s reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include:
– Focus Area 2: Classification of structure, systems, and components (SSCs);
– Focus Area 5: Control system and facilities;
– Focus Area 7: Emergency core cooling and emergency heat removal systems;
– Focus Area 8: Containment/confinement and safety-important civil structure.
The scope and level of detail of the staff’s safety review is based on the guidance of the CNSC Work Instruction document WI-2.01-CON-11NNNN-006.7 “How</td></tr>
</table>

	to Assess the Instrumentation and Control". The following sections are applicable to actuation systems of EFS: – Part A – Overall Instrumentation and Control; – Part B – Safety System Instrumentation and Control.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmatory analysis to verify: – Separation of ESF actuation system with process control system; – Separation of ESF actuation system with other safety systems; – Completion of the intended sequence of safety action when initiated; – Fail-safe design.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the Reactor trip system: – Section 5.3 Quality assurance program; – Section 5.4 Proven engineering practices; – Section 5.7 Design documentation; – Section 6.1 Application of defence-in-depth; – Section 6.2 Safety functions; – Section 6.3 Accident prevention and plant safety characteristics; – Section 7.1 Classification of SSCs; – Section 7.3 Plant states; – Section 7.4 Postulated initiating events considered in the design; – Section 7.6 Design for reliability; – Section 7.6.1 Common cause failure; – Section 7.6.2 Single failure criterion; – Section 7.6.3 Fail-safe design; – Section 7.6.4 Allowance for equipment outage; – Section 7.6.5.1 Shared instrumentation for safety systems; – Section 7.8 Equipment environmental qualification; – Section 7.9 Instrumentation and Control; – Section 7.13 Seismic qualification; – Section 7.14 In-service testing, maintenance, repair, inspection, and monitoring; – Section 7.17 Ageing and wear; – Section 7.21 Human factors; – Section 7.22 Robustness against malevolent acts; – Section 8.5 Emergency core cooling system; – Section 8.6 Containment; – Section 8.8 Emergency heat removal system; – Section 9.3 Hazard analysis. The codes and standards that are relevant to this area include: – CSA N290.0 "General requirements for safety systems of Nuclear Power Plants"; – CSA N290.2 "Requirements for emergency core cooling systems of Nuclear Power Plants";

	– CSA N290.3 "Requirements for the containment system of Nuclear Power Plants"; – 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 Computer in Safe Systems of Nuclear Power Generating Stations".
Skill sets (education) required by: • **senior (regulator),** • **junior (regulator),** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Methodology for determination of trip setpoint; – Thermal hydraulics; – Containment and safety-related civil structure.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of Bachelor of Engineering (B.E.) degree in electrical and electronics engineering preferably higher education in electrical and electronics engineering or computer science.
Level of effort in each review area.	500 person-hours for construction licence application review.

Actuation systems for ESF	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification and its independent assessment; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – FMEA; – Reliability analysis; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of all design information documents; – Independent model checking to evaluate correct functionality of selected reactor trip functions (by TSO); – Audits and inspection visits to evaluate design processes, staff competencies and interface between different design organisations.
What type of confirmatory analysis (if any) is performed?	– See design information; provided by supplier; – Safety assessment by licence holder; – Safety assessment by designer.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 60880); – KTA standards for I&C platform; – For quality management ISO 9001, IAEA GS-R-3, KTA 1401; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill Sets required by (education): • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – TSO: computer engineer, quality engineer.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – SPICE (ISO/IEC 15504) training; – Plant specific training; – (IEC 61508 functional safety professional training).

	Tools and methods: – Document management system; – Model checker tools; – ISO/IEC 15504 for auditing. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods; – Quality management.
Level of effort in each review area.	– Regulator review: 1 110 working days. – Consultants' time: 60 working days. – TSO's review time: 60 working days.

Actuation systems for ESF	France ASN Note: For all reactor designs in France since the 1980's, the same digital system performs reactor trip and ESF. Hence the answer to this section is identical to the answer given in the section for Reactor trip system.
Design information provided by applicant.	The applicant has to provide the complete set of the development documentation. In particular, the source code of the platform's system software and of a sample of the application software has to be provided. (The environmental qualification results for the hardware equipment is also provided and reviewed separately.)
Analysis, reviews and/or research performed by the reviewer and scope of review.	A detailed technical review of the whole development documentation against the relevant IEC 45A standards, the French basic safety rules, and previously accepted projects is performed. This type of review is performed for both, the I&C platform and the system build upon this platform and including the application software. Significant research activities have been performed during the last 20 years in order to influence the state in the art in the field of safety critical software. This research focuses on functional test coverage and on static analysis.
What type of confirmatory analysis (if any) is performed?	Experiments using the tools issued from the above research activities are performed using the actual source code.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Relevant IEC 45A standards (mainly IEC 61513, IEC 60880), French basic safety rule II.4.1a.
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	I&C engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Extensive knowledge in computer science and more specifically real time software; – Extensive experience with safety critical digital systems.
Level of effort in each review area.	As a rough estimate: – 1 man-year for the platform; – 1 man-year for architecture and the application software.

<table>
<tr><th>Actuation systems for ESF</th><th>India
AERB</th></tr>
<tr><td>Design information provided by applicant.</td><td>The design description of safety analysis report (SAR) part should bring out design criteria/bases and functional requirements and how these are met in the detailed design of I&C systems.

Following topics should be addressed with respect to Actuation systems for ESF:

– Design criteria and design bases;
– Redundancy, reliability, diversity, separation among channels/trains, testability, calibration;
– Description of sensors;
– Logics and their implementation;
– Special requirements for instruments;
– Operator information systems and operator aids;
– An instrumentation plan;
– Use of digital/computer based systems and provisions for protection against faults in hardware/software;
– Devices for measuring reactor power and their calibrations;
– Instrumentation for engineered safety features/accident mitigation systems;
– Instrumentation for Emergency core cooling systems (ECCS), small leak handling;
– Instrumentation for containment including instrumentation for accident conditions;
– Arrangement of support systems (Control power supplies and their distribution, Instrument air).

As a part of failure analysis of safety analysis report (SAR) part should bring out:

– System failure mode and effects analysis (single failure analysis);
– Common cause failure analysis (diversity analysis);
– Reliability analysis;
– Consequences to the failure of instrument air, power supply, etc.;
– Conformance of I&C system design with applicable Standards.

The requirements are elaborated in AERB document on “Consenting Process for Nuclear Power Plants and Research Reactors” AERB/NPP&RR/SG/G-1.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The Atomic Energy Regulatory Body (AERB) conducts safety review as described earlier before it makes the necessary recommendation to the board of AERB. The scope and level of detail of the safety review is based on the guidance of applicable codes and guides of AERB. In specific areas where AERB documents are not prepared relevant IAEA or other codes/standards acceptable to AERB are used. During the review AERB committees also considers emerging technical and construction issues, operating experience and lessons learned related to this category.

For example, the ECCS actuation system should meet the performance requirements given in section 3.5 of “Safety Systems for Pressurised Heavy Water Reactors” AERB/NPP-PHWR/SG/D-10 and “Primary Heat Transport System for Pressurised Heavy Water Reactors”, AERB/NPP-PHWR/SG/D-8.

For Containment Isolation Actuation System the design should meet the performance requirements given in section 3.6 of AERB/NPP-PHWR/SG/D-10 and “Safety Related Instrumentation and Control for Pressurised Heavy Water</td></tr>
</table>

	Reactor Based Nuclear Power Plants", AERB/NPP-PHWR/SG/D-20.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	AERB Safety Guide No. AERB/SG/G-7, "Regulatory Consents For Nuclear And Radiation Facilities: Contents And Formats" provides the basis for review and issuance of regulatory consents. Requirements specified in AERB safety code AERB/NPP-PHWR/SC/D and "Safety Systems For Pressurised Heavy Water Reactors" AERB/NPP-PHWR/SG/D-10 forms the primary technical basis. Other relevant safety guides are AERB safety guides AERB/NPP-PHWR/SG/D-1 and AERB/NPP-PHWR/SG/D-20. Standards are referred in the relevant code/guides of AERB.
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Actuation systems for ESF	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, design information such as structures and capabilities for the following systems is provided in the specification: i.e. emergency core cooling system, reactor containment facility, containment spray system, annulus air cleanup system, safe auxiliary machinery room air cleanup system and the like. Design information of design policy, equipment outline and main specifications is provided in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Identical with the scope provided in subsection of "reactor trip system".
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is also performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Identical with technical basis provided in subsection of "reactor trip system".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Actuation systems for ESF	Korea KINS
Design information provided by applicant.	– Safety Analysis Report Chapter 7.3 Engineered Safety Features Actuation System; – Overall I&C architecture; – System requirements (including functional requirements) specification; – System description; – FMEA; – Reliability analysis; – System test plan, test specifications; – System test results; – Setpoint methodology; – Testability; – EQ documents; – Software Documents; – Software Quality Assurance Plan; – Software V&V Plan, V&V report; – Software Configuration Management Plan; – Software Management Plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluation of all design information documents; – Audits and inspection visits to evaluate design processes and V&V activities. For Digital System: – Software Plan; – Life-cycle (Computer System development process) planning; – Review and audit (if necessary) of software life-cycle process; implementation; – Review and audit (if necessary) of software life-cycle process design outputs.
What type of confirmatory analysis (if any) is performed?	– Safety assessment by regulator; – Third party review or analysis is carried out in case of the implementation of new platforms or technology.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance).**	– Regulation on Technical Standards for Nuclear Reactor Facilities: o (Article 20) Instrumentation and Control System; o (Article 25) Control Room; o (Article 26) Protection System; – Notice of NSSC (Nuclear Safety and Security Commission): o (Reactor. 15) Regulation on Safety Classification and Applicable Codes and Standards for Nuclear Reactor Facilities; o (Reactor. 21) Guidelines of Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities; – KINS Standard Review Guides: o (7.3) ESFAS; – KEPIC ENB 1100(IEEE 603), KEPIC ENB 6370(IEEE 7-4.3.2); – KEPIC ENB 3000(IEEE 379);

	– KEPIC ENB 2000(IEEE 384).
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Senior: I&C engineer, computer engineer, reactor system engineer. – Junior: I&C engineer, computer engineer, reactor system engineer.
Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and safety design.
Level of effort in each review area.	Regulator review: 180 working days (1 440 hours).

Actuation systems for ESF	Russia SEC NRS
Design information provided by applicant.	A safety analysis report (SAR) is to be submitted. Among other issues, this report contains information on the control safety systems that are within the scope of the requirements of Chapter 7 of the federal rules and regulations NP-006-98 "requirements to the content of the safety analysis report for NPPs". The SAR shall also contain substantiation for fulfilment of the requirements of the regulations and rules related to the control safety systems. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (Sections 4.4, 4.5), NP-082-07 (Section 2.4).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance).**	Requirements of the federal rules and regulations: – OPB-88/97 (Sections 4.4, 4.5); – NP-082-07 (Section 2.4); – NP-006-98 (Chapter 7); – NP-026-04; Provisions of the IAEA Standard: – IAEA Safety Standards Series, Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011; Provisions of the national standards: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO**	– Industry-specific education in the field of I&C systems for NPPs.

Specialised training, experience and/or education needed for the review of this topic.	– Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	4-6 man-months.

Actuation systems for ESF	Slovakia UJD
Design information provided by applicant.	– System description and functions (purpose of the system, technical solution, power supply, layout); – Analysis of the system performance and reliability (system assignment to in depth protection, resistance to a single failure, resistance to a common cause failure, requirements for redundancy, requirements on independence, maintainability, testability); – Requirements for classification and qualification; – Requirements for HW and SW; – Resistance to the environment (environment conditions, EMC requirements, seismic resistance); – Verification and validation by the independent organisation; – Technical report about fulfilment of quality requirements; – Response analyses of the system to postulated trigger events, including system failure or incorrect operator procedures, in order to specify all internal events that can have an impact on nuclear safety.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the system fulfils the requirements for functionality, performance, reliability, resistance to the environment and quality.
What type of confirmatory analysis (if any) is performed?	–
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance).**	IEC standards, Slovak Technical Standards, regulatory guidance.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.

Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Actuation systems for ESF	Slovenia SNSA
Design information provided by applicant.	– System description; – System level logic; – Component level logic; – Initiating signals, logic, actuation devices and manual controls; – Design basis information; – Safety analysis; – Test and inspections.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques and load combinations used conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance. Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety, and; – That commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction and testing of I&C systems and equipment commensurate with the importance of the safety functions performed.
What type of confirmatory analysis (if any) is performed?	Confirmatory analysis of the predictions and calculations**.**
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance).**	General aspects of design standards including: – IAEA, "Safety of Nuclear Power Plants: Design", Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, "Site Evaluation for Nuclear Installations", Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, "Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide", Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, "Safety Assessment and Verification for Nuclear Power Plants", Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, "Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide", Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No.NS-G-1.1, IAEA, Vienna (2000). Regulation JV5, Instrumentation and control:

	– Instrumentation shall allow measurement of all the main variables of the nuclear power plant that may affect the fission process, the reactor-core integrity, the reactor coolant system and the containment. Instrumentation shall also allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived; – Instrumentation and controls shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible; – Any unauthorised access or ingress to the instrumentation and control systems shall be prevented by appropriate physical, technical and administrative measures; – Instrumentation and control systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems; – The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer, computer engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	– Regulator review: 160 hours. – TSO's review time: 200 hours.

Actuation systems for ESF	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Document review; – Assessment by consultant; – Inspections; – Oral presentations by the licensee.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan. 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3 The Management System for Facilities and Activities, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	– Approximately 10 working days. – Consultant approximately 10 working days.

Actuation systems for ESF	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe or provide the following: – The I&C associated with engineered safety features (ESFs), including initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defence-in-depth features and actuated devices; – I&C systems that regulate the operation of auxiliary supporting features and other auxiliary features; – Logic diagrams, piping and instrumentation diagrams, and layout drawings of all ESF and supporting systems; – Description of automatic/manual signals applications; – Description of inter/intra divisional communications; – System failure mode and effects analysis; – Considerations of (1) loss of plant instrument air systems and (2) loss of cooling water to vital equipment; – Method for periodic testing of ESF I&C equipment and effects on system integrity during testing; – Conformance of the engineered safety features systems with IEEE Standards.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.3, "Engineered Safety Features Systems"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2"; The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff commonly perform confirmatory analyses to verify the adequacy of the following submittal(s) related to this technical area: – Failure Modes and Effects Analysis. Other confirmatory analyses may be performed, if necessary, to aid the staff in making their safety finding. This is typically on a case-by-case basis.

Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance).**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General Design Criterion (GDC): o GDC 1, “Quality Standards and Records”; o GDC 2, “Design Basis for Protection Against Natural Phenomena”; o GDC 4, “Environmental and Missile Design Basis”; o GDC 10, “Reactor Design”; o GDC 13, “Instrumentation and Control”; o GDC 15, “Reactor Coolant System Design”; o GDC 16, “Containment Design"; o GDC 19, “Control Room”; o GDC 20, “Protection Systems Functions”; o GDC 21, “Protection System Reliability and Testability”; o GDC 22, “Protective System Independence”; o GDC 23, “Protection System Failure Modes”; o GDC 24, “Separation of Protection and Control Systems”; o GDC 29, “Protection Against Anticipated Operational Occurrences; o GDC 33, “Reactor Coolant Makeup”; o GDC 34, “Residual Heat Removal”; o GDC 35, “Emergency Core Cooling”; o GDC 38, “Containment Heat Removal”; o GDC 41, “Containment Atmosphere Cleanup”; o GDC 44, “Cooling Water”; – 10 CFR 50.34(f), “Additional TMI-Related Requirements”; – 10 CFR 50.55a(a)(1), “Quality Standards”; – 10 CFR 50.55a(h), “Protection and Safety Systems”; – 10 CFR 52.47 (b)(1), “Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”; – 10 CFR 52.80(a), “Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”. The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 1.22, “Periodic Testing of Protection System Actuation Functions”; – RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”; – RG 1.53, “Application of the Single-Failure Criterion to Safety Systems”; – RG 1.75, “Criteria for Independence of Electrical Safety Systems”; – RG 1.105, “Setpoints for Safety-Related Instrumentation”; – RG 1.118, “Periodic Testing of Electric Power and Protection Systems”; – RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”; – NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems”, December 1994; – Staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs”, July 15, 1993. Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required.

	The Codes and Standards related to this category are as follows: – IEEE Std 379-2000, "IEEE Standard Application of the single-Failure Criterion to Nuclear Power Generating Station Safety Systems"; – IEEE Std 603-1991, "IEEE Standard Criteria For Safety Systems for Nuclear Power Generating Stations"; – IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	4 000 hours (estimated based on the level of complexity of the design).

APPENDIX C
SAFE SHUTDOWN SYSTEM

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, process control, thermal hydraulics and human factor engineering.	200 hours.
Finland	Yes.	Yes.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	155 working days (1 240 hours).
France	Yes.	No.	I&C engineer, computer engineer.	1 man-year (2 000 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[1]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[1]
Korea	Yes.	No.	I&C engineer, electrical and electronics engineering, computer engineering.	120 working days (960 hours).
Russia	Yes.	No	Industry-specific education in the field of I&C systems for NPPs.	2-3 man-months (480 hours).
Slovakia	Yes	No.	Electrical engineer.	–[2]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer.	360 hours.
Sweden	Yes.	Yes.	I&C engineers.	50 working days (400 hours).
United States	Yes.	No.	Electrical engineer.	2 000 hours.

Notes:

1. In Japan, resources (hours) are not set up for each individual review area.
2. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Safe Shutdown System	Canada CNSC
Design information provided by applicant.	There are no systems specifically dedicated as safe shutdown systems, however, there are a number of plant systems that are available to establish and maintain safe shutdown conditions. The applicant should provide the following information: – Design basis requirements for safe shutdown; – A description of systems required for establish and maintain safe shutdown conditions; – Provision of safe shutdown capability from outside the main control room; – A description of indications and manual controls relevant to achieve and maintain safe shutdown conditions; – A description of appropriate displays in the secondary control room for monitoring the status of safe shutdown; – Evidence that the design maintain parameter indications such that the operator will access the same parameters that are being relied upon from both the main control room and the secondary control rooms; – Evidence that equipment used for safe shutdown in both the main and the secondary control rooms is designed to the same codes and standards; – Evidence that safe shutdown systems do not challenge the operation of other systems important to safety.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC GD-385 "Pre-licensing Review of a Vendor's Reactor Design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include: – Focus Area 2: Classification of structure, systems, and components (SSCs); – Focus Area 5: Control system and facilities. The scope and level of detail of the staff review is based on the guidance of the CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.7 "How to Assess the Instrumentation and Control". The following sections are applicable to this technical area: – Part D – All other Instrumentation and Control Systems Important to Safety; – Part E – Control Room Instrumentation and Control; – Part C – Information Systems Important to Safety.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmatory analyses to verify: – Provision of remote shutdown capabilities outside the main control room; – Equipment used for safe shutdown in both the main and the secondary control rooms is designed to the same codes and standards; – Provision of adequate manual controls in both the main and the secondary control rooms for safe shutdown.

Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The regulatory requirements and acceptance criteria are mainly drawn from the CNSC RD-337: – Section 5.7 Design documentation – Section 7.6.5.1 Shared instrumentation for safety systems – Section 7.9 Instrumentation and control – Section 7.11 Guaranteed shutdown state – Section 8.2.4 Removal residual heat from reactor core – Section 8.5 Emergency core cooling system – Section 8.7 Heat transfer to an ultimate heat sink – Section 8.8 Emergency heat removal system – Section 8.10.1 Main control room – Section 8.10.2 Secondary control room
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	The review requires a team with combined knowledge and experience in electrical and electronics engineering, process control, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Reactor reactivity control; – Thermal hydraulics; – Plant auxiliary systems.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering.
Level of effort in each review area.	200 person-hours for construction licence application review.

Safe Shutdown System	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – FMEA; – Reliability analysis; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of all design information documents; – Audits and inspection visits to evaluate design processes, staff competencies and interface between different design organisations.
What type of confirmatory analysis (if any) is performed?	– See Design information; provided by supplier; – Safety assessment by licence holder; – Safety assessment by designer.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 62138 cat B); – For quality management ISO 9001, IAEA GS-R-3, KTA 1401; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – TSO: computer engineer, quality engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – SPICE (ISO/IEC 15504) training; – Plant specific training. Tools and methods: – Document management system; – ISO/IEC 15504 for auditing. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods; – Quality management.
Level of effort in each review area.	– Regulator review: 140 working days. – Consultants' time: 15 working days.

Safe Shutdown System	France ASN Note: "Safe shutdown system" is understood as the "safety actuation system (SAS)" which is a cat B/F1B system used to bring the plant from the controlled state to the safe shutdown state following a Plant Conditions Categories (PCC) event.
Design information provided by applicant.	– Most of the development documentation for the platform; – Documentation necessary to substantiate the commercial dedication (including a detailed a posteriori justification of conformance to IEC 62138 and French basic safety rule II.4.1.a; – Documentation on the architecture of the system; – Development documentation for the application software; (The environmental qualification results for the hardware equipment is also provided and reviewed separately.)
Analysis, reviews and/or research performed by the reviewer and scope of review.	Review according to IEC 62138 cat B and French basic safety rule II.4.1a. Including, in particular, a detailed review of the demonstration of the predictability principle required by the French Basic Safety Rule for systems performing cat B functions.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Relevant IEC 45A standards (mostly IEC 62138), French basic safety rule II.4.1a.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	I&C engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Extensive knowledge in computer science and more specifically real time software; – Extensive experience with real time digital systems.
Level of effort in each review area.	1 man-year for the platform. (Commercial dedication process may require resource consuming exchanges with licensees and vendors.)

Safe Shutdown System	India AERB
Design information provided by applicant.	The design description of safety analysis report (SAR) part should bring out design criteria/bases and functional requirements and how these are met in the detailed design of I&C systems. Following topics should be addressed with respect to safe shutdown system I&C: – Design criteria and design bases; – Description of instruments; – The I&C associated with the safe shutdown system design should include for example redundancy, reliability, diversity, separation between protection and regulation function, testability and calibration, etc.; – Special requirements for instruments; – Operator information systems and operator aids; – Requirements for Control power supplies and their distribution. As a part of failure analysis the relevant part of safety analysis report (SAR) should bring out: – Failure mode and effects analysis; – Consequences to the failure of instrument air and power supply, etc.; – Conformance of I&C system design with applicable Standards. The requirements are elaborated in AERB document on "Consenting Process For Nuclear Power Plants And Research Reactors" AERB/NPP&RR/SG/G-1.
Analysis, reviews and/or research performed by the reviewer and scope of review.	AERB safety guide No. AERB/SG/G-7, "Regulatory Consents For Nuclear And Radiation Facilities: Contents And Formats" provides the scope and process for review and issuance of regulatory consents. The scope and level of detail of the safety review is based on the guidance of applicable codes and guides of AERB. In specific areas where AERB documents are not prepared relevant IAEA or other codes/standards acceptable to AERB are used. During the review AERB committees also considers emerging technical and construction issues, operating experience and lessons learned related to this category. For example the Shutdown Actuation Systems should be designed to add fast negative reactivity into the reactor to meet the performance requirements given in section 3.4 of AERB/SG/D-10. Any failure of services such as power shall lead to actuation of shutoff devices to ensure safe shutdown of reactor. Any actuation device performing the shutdown function should normally not be used for reactor regulation. The design shall be such that normal functioning of the process systems shall not affect the minimum performance requirements of the shutdown system as in section 3 of AERB/SG/D-10. The absorber material should be selected based on following considerations: – Macroscopic absorption cross section; – Stability against irradiation and other parameters; – Solubility and surface deposition characteristics for liquid poison, and; – Compatibility with the chemistry of moderator water.

What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Requirements specified in AERB document on "Safety Systems For Pressurised Heavy Water Reactors" AERB/NPP-PHWR/SG/D-10 forms the primary technical basis. Other relevant safety guides are AERB/NPP-PHWR/SG/D-1 and AERB/NPP-PHWR/SG/D-20. Standards are referred in the relevant code/guides of AERB.
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Safe Shutdown System	Japan NISA/JNES
Design information provided by applicant.	Design information such as design policy of reactor shutdown system, shutdown capability and design policy of residual heat removal system is provided in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Identical with technical basis provided in Subsection of "Reactor trip system".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Safe Shutdown System	Korea KINS
Design information provided by applicant.	– Safety Analysis Report Chapter 7.4 Safety Shutdown system; – Overall I&C architecture; – System requirements (including functional requirements) specification; – System description; – FMEA; – Reliability analysis; – System test plan, test specifications; – System test results; – Testability; – EQ documents; – Software Documents: o Software Quality Assurance Plan; o Software V&V Plan, V&V report; o Software Configuration Management Plan; o Software Management Plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluation of all design information documents; – Audits and inspection visits to evaluate design processes and V&V activities. For digital system: – Software plan; – Life-cycle (computer system development process) planning; – Review and audit (if necessary) of software life-cycle process implementation; – Review and audit (if necessary) of software life-cycle process design outputs.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Regulation on Technical Standards for Nuclear Reactor Facilities: o (Article 20) Instrumentation and Control System; o (Article 26) Protection System; o (Article 25) Control Room; – Notice of NSSC (Nuclear Safety and Security Commission): o (Reactor. 15) Regulation on Safety Classification and Applicable Codes and Standards for Nuclear Reactor Facilities; o (Reactor. 21) Guidelines of Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities; – KINS Standard Review Guides: o (7.4) Safety Shutdown System; o (App. 7-13) Review Guide on Software of Digital-based I&C; – KEPIC ENB 1100(IEEE 603), KEPIC ENB 6370(IEEE 7-4.3.2).

Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	–
Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 120 working days (960 hours).

Safe Shutdown System	Russia SEC NRS
Design information provided by applicant.	A Safety Analysis Report (SAR) is to be submitted. Among other issues, this report contains information on the control safety systems involved in safe shutdown. This information is within the scope of the requirements of Chapter 7 of the federal rules and regulations NP-006-98 "Requirements to the Content of the Safety Analysis Report for NPPs". The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to the control safety systems. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (Section 4.4), NP-082-07 (Section 2.4).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Requirements of the federal rules and regulations: – OPB-88/97 (Section 4.4); – NP-082-07 (Section 2.4); – NP-006-98 (Chapter 7); – NP-026-04; Provisions of IAEA standards: – IAEA Safety Standards Series, Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011; Provisions of the national standards: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems); – RD EO 0554-2005. Guideline Document. Nuclear Power Plants. Control Systems Important to Safety. Manufacturing, Upgrading and Operation. General Provisions.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the field of I&C systems for NPPs.
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	2-3 man-months.

Safe Shutdown System	Slovakia UJD
Design information provided by applicant.	– System description and functions; – Analysis of the system performance and reliability (system assignment to in depth protection, resistance to a single failure, requirements for redundancy and for diversity, requirements on independence, maintainability, testability); – Requirements for HW and SW; – Resistant to the environment; – Technical report about fulfilment of quality requirements.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the shutdown system fulfils the requirements for functionality, performance, reliability, resistance to the environment and quality.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	IEC standards, Slovak technical standards, regulatory guidance.
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Safe Shutdown System	Slovenia SNSA
Design information provided by applicant.	– System description; – Design basis; – Safety analysis; – Restrictive setpoints.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques and load combinations used conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety, and; – That commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction and testing of I&C systems and equipment commensurate with the importance of the safety functions performed. Confirmatory analysis of the predictions and calculations.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	General aspects of design standards including: – IAEA, “Safety of Nuclear Power Plants: Design”, Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, “Site Evaluation for Nuclear Installations”, Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, “Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide”, Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, “Safety Assessment and Verification for Nuclear Power Plants”, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, “Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage”, Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, “Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide”, Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). Regulation JV5, Reactor trip systems: To ensure safe shutdown of the reactor, at least two diverse systems shall be provided. At least one of these systems shall be capable of autonomously bringing, within four seconds, the reactor into subcritical condition with an appropriate reactivity margin, from any state of the facility and in a design-basis event. This shall be achieved also under the assumption of a single failure. Regulation JV5, Instrumentation and control: – Instrumentation shall allow measurement of all the main variables of the

	nuclear power plant that may affect the fission process, the reactor-core integrity, the reactor coolant system and the containment. Instrumentation shall also allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived; – Instrumentation and controls shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible; – Any unauthorised access or ingress to the instrumentation and control systems shall be prevented by appropriate physical, technical and administrative measures; – Instrumentation and control systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems; – The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Senior: electrical engineer, computer engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	– Regulator review: 160 hours; – TSO's review time: 200 hours.

Safe Shutdown System	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Document review; – Inspections; – Oral presentations by the licensee.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan. 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3 The Management System for *Facilities and Activities*, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	Approximately 50 working days.

Safe Shutdown System	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe or provide the following: – The systems that are needed for safe shutdown of the plant, including initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defence-in-depth features and actuated devices; – Logic diagrams, piping and instrumentation diagrams and layout drawings of all ESF and supporting systems; – Analyses that demonstrate how the safe shutdown system meets IEEE 603-1991 as required by the regulations; – Considerations of instrumentation installed to permit a safe shutdown in the event of the following: o Loss of plant instrument air systems; o Loss of cooling water to vital equipment; o Plant load rejection; o Turbine trip. The need for and method of changing to more restrictive setpoints during abnormal operating conditions.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.4, "Safe Shutdown Systems"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff do not commonly perform confirmatory analyses in this technical area.
Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General design criterion (GDC); o GDC 1, "Quality Standards and Records"; o GDC 2, "Design Basis for Protection against Natural Phenomena"; o GDC 4, "Environmental and Missile Design Basis"; o GDC 13, "Instrumentation and Control"; o GDC 19, "Control Room"; o GDC 24, "Separation of Protection and Control Systems"; o GDC 34, "Residual Heat Removal";

<table>
<tr><td>guidance).</td><td>o GDC 35, “Emergency Core Cooling”;
o GDC 38, “Containment Heat Removal”;
– 10 CFR 50.34(f), “Additional TMI-Related Requirements”;
– 10 CFR 50.55a(a)(1), “Quality Standards”;
– 10 CFR 50.55a(h), “Protection and Safety Systems”;
– 10 CFR 52.47 (b)(1), “Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”;
– 10 CFR 52.80(a), “Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”.

The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows:

– Regulatory guide (RG) 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”;
– RG 1.189, “Fire Protection for Operating Nuclear Plants”.

Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required.

The Codes and Standards related to this category are as follows:

– IEEE Std 603-1991, “IEEE Standard Criteria For Safety Systems For Nuclear Power Generating Stations”;
– IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers In Safety Systems of Nuclear Power Generating Stations”.</td></tr>
<tr><td>Skill sets (education) required by:
• Senior (regulator),
• Junior (regulator),
• TSO.</td><td>– Electrical engineer.</td></tr>
<tr><td>Specialised training, experience and/or education needed for the review of this topic.</td><td>All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently.

Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include:

– Experience with traditional and digital I&C systems;
– Basic knowledge of software structure and application;
– Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.;
– Basic knowledge of data communications devices;
– Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.</td></tr>
<tr><td>Level of effort in each review area.</td><td>2 000 hours (estimated based on the level of complexity of the design).</td></tr>
</table>

APPENDIX D
SAFETY-RELATED DISPLAY INSTRUMENTATION

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, accident management and human factor engineering.	200 hours;
Finland	Yes.	Yes.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	45 working days (360 hours).
France	Yes.	No.	I&C engineer, computer engineer.	1 month (160 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[2]
Japan	Yes[1].	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[2]
Korea	Yes.	Yes.	I&C Engineer, electrical and electronics engineering, computer engineering, nuclear engineer and human factors engineering.	180 working days (1 440 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	2-3 man-months (480 hours).
Slovakia	Yes.	No.	Electrical engineer.	–[3]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer.	280 hours.
Sweden	Yes[1].	–	–	–
United States	Yes.	No.	Electrical engineer, human factors engineer.	2 000 hours.

Notes:

1. In Japan and Sweden, safety related display instrumentation is reviewed as part of the design review of the Main Control Room.
2. In Japan and India, resources (hours) are not set up for each individual review area.
3. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

<table>
<tr><th>Safety Related Display Instrumentation</th><th>Canada
CNSC</th></tr>
<tr><td>Design information provided by applicant.</td><td>Section 6.7.2 of the CNSC licence application guide RD/GD-369 “Licence to construction a nuclear power plant” specifies information to be provided by applicant for information systems important to safety:
– Safety class of each information system important to safety;
– List of the measured parameters;
– Physical locations of the sensors;
– Equipment qualification envelope (defined by the most limiting conditions in operational states or accident condition);
– The duration of the time period for which the reliable operation of the sensors is required.
If the measured parameters are processed by a computer, the following information should also be provided:
– Characteristics of any computer software (e.g. scan frequency, parameter validation and cross-channel sensor checking) used for filtering, trending or to generate alarms;
– Long-term storage of data and displays and how information will be made available to the operators in the control room and the secondary control room;
– Implications of the failure of the plant computers and the mitigating strategies developed to provide operators with essential information;
– Means of achieving the synchronisation of the different computer systems if data processing and storage are performed by multiple computers.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>Appendix A of the CNSC guidance document GD-385 “Pre-licensing Review of a Vendor’s Reactor Design” describes review focus areas used in the assessment of a vendor’s reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include:
– Focus Area 2: Classification of structure, systems, and components (SSCs);
– Focus Area 5: Control system and facilities;
– Focus Area 9: Beyond design basis accidents (BDBAs) and severe accident (SA) – prevention and mitigation;
– Focus Area 18: Human Factors.
The scope and level of detail of the staff’s safety review is based on the guidance of the Work Instruction Document WI-2.01-CON-11NNNN-006.7 “How to Assess the Instrumentation and Control”. The following section is applicable to this technical area:
– Part C – Information systems important to safety.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>CNSC staff normally perform confirmatory analysis to verify that accident monitoring instrumentation meets IEEE 497 requirements.</td></tr>
</table>

Technical basis: • **standards,** • **codes,** • **acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the Reactor trip system: • Section 5.3 Quality assurance program; • Section 5.7 Design documentation; • Section 7.6.5.1 Shared instrumentation for safety systems; • Section 7.9 Instrumentation and Control; • Section 7.9.3 Accident monitoring instrumentation; • Section 8.10 Control facilities; • Section 8.10.1.1 Safety parameter display system. The codes and standards that is relevant to this area include: – IEEE Std 497 "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	The review requires a team with combined knowledge and experience in electrical and electronics engineering, computer engineering, accident management and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Human factor engineering; – Accident management.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering.
Level of effort in each review area.	200 person-hours for construction licence application review.

Safety Related Display Instrumentation	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – System test plan, test specifications; – System test results; – HMI validation plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of all design information documents.
What type of confirmatory analysis (if any) is performed?	– Safety assessment by licence holder; – Safety assessment by designer.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 62138 cat B); – For quality management ISO 9001, IAEA GS-R-3, KTA 1401; – NUREG-0711; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – Plant specific training. Tools and methods: – Document management system. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 45 working days.

Safety Related Display Instrumentation	**France** **ASN** Note: "Safety related display instrumentation" is understood as being the "Safety Information and Control System (SICS)" which, on French reactor design is a non-digital category B/F1B system.
Design information provided by applicant.	– System architecture and description; – Environmental qualification.
Analysis, reviews and/or research performed by the reviewer and scope of review.	As this system is non-digital and simple, review of the design file, in particular, on electrical schematics and wiring diagrams.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Relevant IEC 45A standards, French basic safety rule II.4.1a. (in practice few specific requirements beyond single failure criterion and environmental qualification).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	I&C engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	General skills in I&C, basic electricity skills.
Level of effort in each review area.	1 man-month at most.

Safety Related Display Instrumentation	India AERB
Design information provided by applicant.	The design description of safety analysis report (SAR) part should bring out design criteria/bases and functional requirements and how these are met in the detailed design of I&C systems. The utility should provide information to adequately demonstrate the provisions as elaborated in chapter 10 "Safety system monitoring" of AERB document on "Safety systems for pressurised heavy water reactors" AERB/NPP-PHWR/SG/D-10. Further for each safety systems, information on identified set of parameters for monitoring, which indicate that the intended safety function and safety requirements are met. Such safety systems monitoring and display should be dedicated to those systems and may not form part of the general plant operator information systems to meet the independence and reliability requirements of the safety systems.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Parameter displays mean the display of values of plant variables characteristic of the state of the plant. The displays may actually present the variable values in digital read out on, say, a visual display unit. For the sake of redundancy, additional discrete (i.e. variable specific) display modules may be optionally provided. The display design shall facilitate cross-checking between channels that bear known relationship to one another. Wherever the cross-checking is required to establish safety systems performance, the display design shall ensure immunity to common cause failures. The measurement range of instrumentation shall cover possible range of values of monitored variables during and following an accident situation. So, the range may extend well beyond the operational range of the variable. Information about the state and availability of safety systems is essential in the control room. Information must also be available on systems and parameters required to initiate manual backup action as specified. While the former belongs to the category of safety related I&C (Category I-B, ref. "Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-1), the latter shall meet the requirements of safety systems (Category I-A). Suitably designed safety systems monitoring system is therefore a required complement to the I&C of the reactor.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Requirements specified in AERB document on "Safety Systems For Pressurised Heavy Water Reactors" AERB/NPP-PHWR/SG/D-10 forms the primary technical basis. Other relevant safety guides are AERB/NPP-PHWR/SG/D-1, AERB/NPP-PHWR/SG/D-20 and for computer based system PHWR/SG/D-25. Standards are referred in the relevant code/guides of AERB. The monitoring system shall be simple in design by use of minimum amount of equipment that is adequate for its basic scope. The system should not be rendered inoperative by specific design basis events under which it is intended to perform the monitoring function. The information chain may share instrumentation provided for safety and process functions; but with adequate isolation/buffering such that failure anywhere in the system shall not affect the functionality of the systems it monitors.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor Systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Safety Related Display Instrumentation	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, design information of main control room is provided in the specification.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is also performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Identical with technical base provided in Subsection of "Reactor trip system".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Safety Related Display Instrumentation	Korea KINS
Design information provided by applicant.	– Safety Analysis Report Chapter 7.5, Safety Related Display Information; – System requirements (including functional requirements) specification; – Topical reports on specific issues in overall I&C; – System test plan, test specifications; – System test results; – EQ documents; – Software documents: o Software quality assurance plan; o Software V&V plan, V&V report; o Software configuration management plan; o Software management plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluation of all design information documents; – Audits and inspection visits to evaluate design processes and V&V activities; – Diversity and defence-in-depth, separation of protection and control systems. For digital system: – Software plan; – Life-cycle (computer system development process) planning; – Review and audit (if necessary) of software life-cycle process implementation; – Review and audit (if necessary) of software life-cycle process design outputs.
What type of confirmatory analysis (if any) is performed?	– Review design, V&V, equipment qualification documentation provided by supplier.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Regulation on Technical Standards for Nuclear Reactor Facilities: o (Article 20) Instrumentation and Control System; o (Article 26) Protection System; o (Article 25) Control Room; – Notice of NSSC (Nuclear Safety and Security Commission): o (Reactor. 15) Regulation on Safety Classification and Applicable Codes and Standards for Nuclear Reactor Facilities; o (Reactor. 21) Guidelines of Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities; – KINS Standard Review Guides: o (7.5) Information system important to safety; o (App. 7-13) Review Guide on Software of Digital-based I&C; – KEPIC ENB 1100(IEEE 603), KEPIC ENB 6370(IEEE 7-4.3.2); – KEPIC ENB 6330(IEEEE 497).

Skill sets (education) required by: • **Senior (regulator),** • **Junior (regulator),** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, mechanical engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, mechanical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 180 working days.

Safety Related Display Instrumentation	Russia SEC NRS
Design information provided by applicant.	A Safety Analysis Report (SAR) is to be submitted. Among other issues, this report contains information on the control safety systems in the part of information display systems important to safety. This information is within the scope of requirements of Chapter 7 of the federal rules and regulations NP-006-98 “Requirements to the Content of the Safety Analysis Report for NPPs”. The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to the systems mentioned. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (Sections 4.4, 4.5), NP-082-07 (Section 2.4) shall be confirmed.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Requirements of the federal rules and regulations: – OPB-88/97 (Section 4.4); – NP-082-07 (Section 2.4); – NP-006-98 (Chapter 7); – NP-026-04; Provisions of the IAEA Standards: – IAEA Safety Standards Series Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011; Provisions of the national standards: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems); – GOST 26635-85 “Nuclear Power Vessel-Type Pressurized Water Reactors. General Requirements to In-Core Instrumentation System”; – GOST 24789-81 “Instrumentation Tubes of In-Core Instrumentation System of Power Vessel-Type Pressurized Water Reactors. General Technical Requirements”. Provision of the guideline document of the operating organisation: – RD EO 0554-2005. Guideline Document. Nuclear Power Plants. Control Systems Important to Safety. Manufacturing, Upgrading and Operation. General Provisions.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the field of I&C systems for NPPs.
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	2-3 man-months.

Safety Related Display Instrumentation	Slovakia UJD
Design information provided by applicant.	– System description; – Design basis; – Requirements for classification and qualification; – Requirements for operation and reliability; – Resistance to single failure.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review includes an evaluation of the information systems design against applicable standards, guidelines and legislation requirements.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	IEC standards, Slovak Technical Standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Safety Related Display Instrumentation	Slovenia SNSA
Design information provided by applicant.	– System description; – Design basis, standards, criteria; – Regulatory conformance; – Safety analysis.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review should include an evaluation of the information systems design against applicable standards, guidelines and legislation requirements with special emphasis on independence, dependableness of computer based systems and environmental qualification when needed.
What type of confirmatory analysis (if any) is performed?	It shall be confirmed that the operator has sufficient information to perform required manual safety functions (e.g. ensuring safe control rod patterns, manual engineered-safety-feature operations, possible unanticipated post-accident operations and monitoring the status of safety equipment) and sufficient time to make reasoned judgments and take action where operator action is essential.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	General aspects of design standards including: – IAEA, "Safety of Nuclear Power Plants: Design", Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, "Site Evaluation for Nuclear Installations", Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, "Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide", Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, "Safety Assessment and Verification for Nuclear Power Plants", Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, "Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide", Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No.NS-G-1.1, IAEA, Vienna (2000). Regulation JV5, Instrumentation and control: The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer, computer engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software); – Environmental qualification.
Level of effort in each review area.	– Regulatory review time: 80 hours. – TSO's review time: 200 hours.

Safety Related Display Instrumentation	Sweden SSM
Design information provided by applicant.	See Section 6. Main Control Room.
Analysis, reviews and/or research performed by the reviewer and scope of review.	See Section 6. Main Control Room.
What type of confirmatory analysis (if any) is performed?	See Section 6. Main Control Room.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	See Section 6. Main Control Room.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	See Section 6. Main Control Room.
Specialised training, experience and/or education needed for the review of this topic.	See Section 6. Main Control Room.
Level of effort in each review area.	– Approximately 30 working days (HFE). – Approximately 5 working days (Computer system platform).

Safety Related Display Instrumentation	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe the following: – Systems that provide information to enable to operator to perform required safety functions, including; o Accident monitoring instrumentation; o Plant annunciators; o Safety parameter displays; o Information systems associated with emergency response facilities and nuclear data link. – Logic diagrams, piping and instrumentation diagrams and layout drawings of all information systems important to safety; – Analysis to demonstrate that the operator has sufficient information to perform required manual safety functions; – Analysis to demonstrate that the operator has sufficient time to make reasoned judgment and take action where operator action is essential for maintaining plant safety; – The information readouts and indications provided to the operator for monitoring conditions in the reactor, the Regulations, Codes, Standards (RCS), the containment and safety related process systems.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.5, "Information Systems Important to Safety"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff do not commonly perform confirmatory analyses in this technical area.

<table>
<tr>
<td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from accident analysis, regulatory guidance).</td>
<td>The following NRC regulatory requirements are applicable to this category:
– 10 CFR 50, Appendix A, General Design Criterion (GDC);
o GDC 1, “Quality Standards and Records”;
o GDC 2, “Design Basis for Protection Against Natural Phenomena”;
o GDC 4, “Environmental and Missile Design Basis”;
o GDC 13, “Instrumentation and Control”;
o GDC 19, “Control Room”;
o GDC 24, “Separation of Protection and Control Systems”.
– 10 CFR 50.34(f), “Additional TMI-Related Requirements”;
– 10 CFR 50.55a(a)(1), “Quality Standards”;
– 10 CFR 50.55a(h), “Protection and Safety Systems”;
– 10 CFR 52.47 (b)(1), “Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”;
– 10 CFR 52.80(a), “Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)".

The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows:
– Regulatory Guide (RG) 1.7, “Criteria for Independence of Electrical Safety Systems”;
– RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”;
– RG 1.97, Revision 4, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants”;
– RG 1.105, “Setpoints for Safety-Related Instrumentation”;
– RG 1.151, “Instrument Sensing Lines”;
– RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”;
– RG 1.189, “Fire Protection for Operating Nuclear Plants”;
– NUREG-0737 Supplement 1, “Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability”, January 1983;
– Staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs”, July 15, 1993.

Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required.

The Codes and Standards related to this category are as follows:
– IEEE Std 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations”;
– IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”;
– IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”.</td>
</tr>
</table>

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer; – Human factors engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	2 000 hours (estimated based on the level of complexity of the design).

APPENDIX E
INFORMATION AND INTERLOCK SYSTEMS IMPORTANT TO SAFETY

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	100 hours.
Finland	Yes[1].	–	–	45 working days (360 hours).
France	Yes[1].	–	–	–
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[2]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[2]
Korea	Yes.	Yes.	I&C engineer, electrical and electronics engineering, computer engineering, nuclear engineer.	60 working days (480 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	2-3 man-months (480 hours).
Slovakia	Yes.	No.	Electrical engineer.	–[3]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer.	420 hours
Sweden	Yes.	Yes.	I&C engineer.	10 working days (80 hours).
United States	Yes.	No.	Electrical engineer.	2 000 hours.

Notes:

1. In Finland and France, Information and interlock systems important to safety are reviewed as part of the design review of the Actuation systems for ESF and the Safe Shutdown System.
2. In Japan and India, resources (hours) are not set up for each individual review area.
3. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Information and Interlock Systems Important to Safety	Canada CNSC
Design information provided by applicant.	The applicant should provide the following information for interlock systems important to safety: – Description and functional diagram of each interlock systems important to safety; – Description of by-passed or inoperable status indication of interlocks important to safety; – Evidence that interlocks do not challenge the operation of other systems important to safety.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC guidance document GD-385 "Pre-licensing review of a vendor's reactor design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include: – Focus Area 2: Classification of structure, systems, and components (SSCs); – Focus Area 5: Control system and facilities; – Focus Area 6: Means of shutdown; – Focus Area 7: Emergency core cooling and emergency heat removal; – Focus Area 8: Containment/confinement and safety-important civil structure; The scope and level of detail of the staff's safety review is based on the guidance of Work Instruction Document WI-2.01-CON-11NNNN-006.7 "How to Assess the Instrumentation and Control". The following sections are applicable to this technical area: – Part C – Information systems important to safety; – Part D – All other Instrumentation and Control System Important to Safety; – Part E – Control Room Instrumentation and Control.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmatory analyses to verify: – Appropriate interlocks are provided to ensure that the safety goals are not exceeded during any conditions of normal operation; – Appropriate controls and indications are provided for interlock initiation and bypass.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the Reactor trip system: – Section 5.3 Quality assurance program; – Section 5.7 Design documentation; – Section 7.6.5.1 Shared instrumentation for safety systems; – Section 7.9 Instrumentation and control; – Section 8.4 Means of shutdown; – Section 8.5 Emergency core cooling; – Section 8.6 Containment; – Section 8.8 Emergency heat removal system; – Section 8.10 Control facilities;

	– Section 9.3 Hazard analysis. The codes and standards that are relevant to this area include: – CSA N290.0 "General requirements for safety systems of Nuclear Power Plants"; – 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 Computer in safe Systems Of Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Thermal hydraulics; – Plant process control.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering.
Level of effort in each review area.	100 person-hours for construction licence application review.

Information and Interlock Systems Important to Safety	India AERB
Design information provided by applicant.	Information and interlock systems important to safety are treated according to the safety significance. Design criteria such as redundancy, fail-safe, etc. are applied. The design description of safety analysis report (SAR) part should bring out design criteria/bases and functional requirements and how these are met in the detailed design. The SAR should provide information to adequately demonstrate that the design meets the provisions as elaborated in AERB document "Safety Related Systems For Pressurised Heavy Water Reactors" AERB/NPP-PHWR/SG/D-20.
Analysis, reviews and/or research performed by the reviewer and scope of review.	AERB safety guide No. AERB/SG/G-7 "regulatory consents for nuclear and radiation facilities: contents and formats" provides the scope and process for review and issuance of regulatory consents. Regulatory reviews are conducted as stated in AERB document on "consenting process for nuclear power plants and research reactors" AERB/NPP&RR/SG/G-1 and "safety related instrumentation and control for pressurised heavy water reactor based nuclear power plants" AERB/NPP-PHWR/SG/D-20.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	AERB document "safety systems for pressurised heavy water reactors" AERB/NPP-PHWR/SG/D-10 and safety guide on "Safety Related Instrumentation and control for pressurised heavy water reactor based nuclear power plants" AERB/NPP-PHWR/SG/D-20 form the basis for review.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.

Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Information and Interlock Systems Important to Safety	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, design information including the design policy of information and interlock systems is provided in the specification.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis result are verified. Independent evaluation is also performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Identical with technical basis provided in Subsection of "Reactor trip system".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Information and Interlock Systems Important to Safety	**Korea** **KINS**
Design information provided by applicant.	– Safety analysis report chapter 7.6 all other instrumentation system required for safety; – System requirements (including functional requirements) specification; – Topical reports on specific issues in overall I&C; – System test plan, test specifications; – System test results; – EQ documents: o Software documents; o Software quality assurance plan; o Software V&V plan, V&V report; o Software configuration management plan; o Software management plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluation of all design information documents; – Audits and inspection visits to evaluate design processes and V&V activities. For digital system: – Software plan; – Life-cycle (computer system development process) planning; – Review and audit (if necessary) of software life-cycle process implementation; – Review and audit (if necessary) of software life-cycle process design outputs.
What type of confirmatory analysis (if any) is performed?	– Review design, V&V, equipment qualification documentation provided by supplier.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Regulation on technical standards for nuclear reactor facilities: o (Article 20) Instrumentation and Control System; o (Article 26) Protection System; o (Article 25) Control Room; – Notice of NSSC (Nuclear Safety and Security Commission): o (Reactor. 15) Regulation on Safety Classification and Applicable Codes and Standards for Nuclear Reactor Facilities; o (Reactor. 21) Guidelines of Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities; – KINS Standard Review Guides: o (7.5) Information system important to safety; o (App. 7-13) Review Guide on Software of Digital-based I&C; – KEPIC ENB 1100 (IEEE 603), KEPIC ENB 6370 (IEEE 7-4.3.2).

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer. – Junior: I&C engineer, computer engineer, nuclear engineer.
Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 60 working days.

<table>
<tr><th>Information and Interlock Systems Important to Safety</th><th>Russia
SEC NRS</th></tr>
<tr><td>Design information provided by applicant.</td><td>A Safety Analysis Report (SAR) is to be submitted. Among other issues, this report contains information on the control safety systems in the part of information and interlock systems. This information is within the scope of requirements of Chapter 7 of the federal rules and regulations NP-006-98 “Requirements to the content of the safety analysis report for NPPs”. The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to the systems mentioned. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (Sections 4.4, 4.5), NP-082-07 (Section 2.4).</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>No confirmatory analysis to be performed.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from accident analysis, regulatory guidance).</td><td>Requirements of the federal rules and regulations:
– OPB-88/97 (Section 4.4);
– NP-082-07 (Section 2.4);
– NP-006-98 (Chapter 7);
– NP-026-04;
Provisions of the IAEA Standards:
– IAEA Safety Standards Series, Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008;
– IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011;
Provisions of the national standard:
– GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems);
Provision of the guideline document of the operating organisation:
– RD EO 0554-2005. Guideline Document. Nuclear Power Plants. Control Systems Important to Safety. Manufacturing, Upgrading and Operation. General Provisions.</td></tr>
</table>

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the field of I&C systems for NPPs.
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	2-3 man-months.

Information and Interlock Systems Important to Safety	**Slovakia UJD**
Design information provided by applicant.	– System description; – Safety analysis; – Requirements on quality, which producer of equipment has to fulfil; – Technical report about fulfilment of quality requirements conform to regulations, codes and standards.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the system fulfils the requirements for functionality, performance; – Reliability, resistance to the environment and quality.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	IEC standards, Slovak Technical Standards**.**
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Information and Interlock Systems Important to Safety	Slovenia SNSA
Design information provided by applicant.	– System description; – Design basis; – Safety analysis. Detail information should be provided regarding: – Interlock systems to prevent over-pressurisation of low-pressure systems; – Interlocks to prevent over-pressurisation of the primary coolant system during low-temperature operation of the reactor vessel; – Valve interlocks to assure the availability of ECCS system accumulators; – Interlocks to isolate safety systems from non-safety systems (e.g. seismic and non-seismic portions of auxiliary supporting systems), and; – Interlocks to preclude inadvertent inter-ties between redundant or diverse safety systems where such inter-ties exist for the purposes of testing or maintenance.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety, and; – That commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction and testing of I&C systems and equipment commensurate with the importance of the safety functions performed. Confirmatory analysis of the predictions and calculations.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	General aspects of design standards (see above): Regulation JV5, Instrumentation and control: – Instrumentation shall allow measurement of all the main variables of the nuclear power plant that may affect the fission process, the reactor-core integrity, the reactor coolant system and the containment. Instrumentation shall also allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived; – Instrumentation and controls shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible; – Any unauthorised access or ingress to the instrumentation and control systems shall be prevented by appropriate physical, technical and administrative measures;

	– Instrumentation and control systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems; – The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	General aspects of design standards (see above): IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No.NS-G-1.1, IAEA, Vienna (2000). – Senior: electrical engineer, computer engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	– Regulator review: 180 hours. – TSO's review time: 240 hours.

Information and Interlock Systems Important to Safety	Sweden SSM
Design information provided by applicant.	See high level summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Non-specific review.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan 2010; – IAEA safety standards/safety requirements no. GS-R-3: The management system for facilities and activities. international atomic energy agency, Vienna, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	Approximately 10 working days.

Information and Interlock Systems Important to Safety	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe or provide the following: – All other instrumentation systems required for safety that are not addressed in the sections describing the reactor trip system, ESF systems, safe shutdown systems or any of their supporting systems; – Design basis information required by IEEE Std 603; – Logic diagrams, piping and instrumentation diagrams, and layout drawings of interlock systems important to safety; – Considerations of the following interlocks: o Interlocks to prevent over-pressurisation of low-pressure systems; o Interlocks to prevent over-pressurisation of the primary coolant system during low-temperature operations of the reactor vessel; o Interlocks to assure the availability of ECCS accumulator valves; o Interlocks required to isolate safety systems from non-safety systems; o Interlocks required to preclude inadvertent inter-ties between redundant or diverse safety systems.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The nuclear regulatory commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.5, "Information Systems Important to Safety"; – SRP 7.6, "Interlock Systems Important to Safety"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff do not commonly perform confirmatory analyses in this technical area.

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, 10 CFR 50, Appendix A, General Design Criterion (GDC); o GDC 1, "Quality Standards and Records"; o GDC 2, "Design Basis for Protection Against Natural Phenomena"; o GDC 4, "Environmental and Missile Design Basis"; o GDC 10, "Reactor Design"; o GDC 13, "Instrumentation and Control"; o GDC 15, "Reactor Coolant System Design"; o GDC 16, "Containment Design"; o GDC 19, "Control Room"; o GDC 24, "Separation of Protection and Control Systems"; o GDC 28, "Reactivity Limits"; o GDC 33, "Reactor Coolant Makeup"; o GDC 34, "Residual Heat Removal"; o GDC 35, "Emergency Core Cooling"; o GDC 38, "Containment Heat Removal"; o GDC 41, "Containment Atmosphere Cleanup"; o GDC 44, "Cooling Water"; – 10 CFR 50.34(f), "Additional TMI-Related Requirements"; – 10 CFR 50.55a(a)(1), "Quality Standards"; – 10 CFR 50.55a(h), "Protection and Safety Systems"; – 10 CFR 52.47 (b)(1), "Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)"; – 10 CFR 52.80(a), "Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)". The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"; – RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"; – RG 1.189, "Fire Protection for Operating Nuclear Plants"; – Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs", July 15, 1993. Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. The Codes and Standards related to this category are as follows: – IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"; – IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	2 000 hours (estimated based on the level of complexity of the design).

APPENDIX F
CONTROL SYSTEMS

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	100 hours.
Finland	Yes.	No.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	15 working days (120 hours).
France	Yes.	No.	I&C engineer.	1 man-month (160 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[1]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[1]
Korea	Yes.	No.	I&C engineer, electrical and electronics engineering, computer engineering, nuclear engineer and mechanical engineering.	180 working days (1 440 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	4-6 man-months (960 hours).
Slovakia	Yes.	No.	Electrical engineer.	–[2]
Slovenia	Yes.	Yes.	Electrical engineer, nuclear engineer.	360 hours.
Sweden	Yes.	Yes.	I&C engineer.	10 working days (80 hours).
United States	Yes.	No.	Electrical engineer.	1 500 hours.

Notes:

1. In Japan and India, resources (hours) are not set up for each individual review area.
2. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

<table>
<tr><th>Control Systems</th><th>Canada
CNSC</th></tr>
<tr><td>Design information provided by applicant.</td><td>Section 6.7.3 of the CNSC Licence Application Guide RD/GD-369 “Licence to Construction a Nuclear Power Plant” specifies information to be provided by applicant for control systems:
– A description of control systems used for normal plant operations;
– A description of any limitation systems (e.g. control grade power reduction systems installed to avoid a reactor trip, by initiating a partial power reduction);
– Evidence that such systems do not challenge the operation of other systems important to safety.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>Appendix A of the CNSC guidance document GD-385 “Pre-licensing Review of a Vendor’s Reactor Design” describes review focus areas used in the assessment of a vendor’s reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include:
– Focus Area 2: Classification of structure, systems, and components (SSCs);
– Focus Area 5: Control system and facilities.
The scope and level of detail of the staff’s safety review is based on the guidance of the CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.7 “How to Assess the Instrumentation and Control”. The following section is applicable to this technical area:
– Part D – All Other Instrumentation and Control Systems Important to Safety.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>CNSC staff normally performs confirmatory analyses to verify that failure of control systems cannot have an adverse impact on safety system functions and will not pose frequent challenges to the safety systems.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from accident analysis, regulatory guidance).</td><td>The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the Reactor trip system:
– Section 5.3 Quality assurance program;
– Section 5.7 Design documentation;
– Section 7.6.5.1 Shared instrumentation for safety systems;
– Section 7.9 Instrumentation and control;
– Section 7.10 Safety support systems;
– Section 8.1 Reactor core;
– Section 8.2 Reactor coolant system;
– Section 8.3 Steam supply system;
– Section 9.3 Hazard analysis.
The codes and standards relevant to this section include:
– CSA N290.4 “Requirements for reactor control systems of nuclear power plants”.</td></tr>
</table>

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Plant process control.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering.
Level of effort in each review area.	100 person-hours for construction licence application review.

Control Systems	Finland STUK
Design information provided by applicant.	– System quality plan; – System requirements (including functional requirements) specification; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of selected design information documents.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 62138 cat C); – For quality management ISO 9001; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer; – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – Plant specific training. Tools and methods: – Document management system. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods; – Quality management.
Level of effort in each review area.	Regulator review: 15 working days.

Control Systems	France ASN Note: "Controls systems" is understood as being the process actuation system (PAS). Some parts of this system are classified F2 others non-safety. This system is based on the same platform as safe shutdown system.
Design information provided by applicant.	– System architecture; – Development documentation for the application software. (The environmental qualification results for the hardware equipment is also provided and reviewed separately. Note: Platform documentation is already provided for the assessment of the SAS. This is one benefit of having a safety classified platform to perform non-safety functions).
Analysis, reviews and/or research performed by the reviewer and scope of review.	Platform assessment already performed for the SAS. Simple overall architecture assessment performed.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Relevant IEC 45A standards. (In practice, few specific requirements beyond single failure criterion and environmental qualification.)
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	I&C engineer.
Specialised training, experience and/or education needed for the review of this topic.	General knowledge regarding digital I&C.
Level of effort in each review area.	About one man-month.

<table>
<tr><th>Control Systems</th><th>India
AERB</th></tr>
<tr><td>Design information provided by applicant.</td><td>The design description of safety analysis report (SAR) part should bring out design criteria/bases and functional requirements and how these are met in the detailed design of I&C systems. The utility should provide information to adequately demonstrate the provisions as elaborated in AERB guide on “Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants”, AERB/NPP-PHWR/SG/D-20. Design rules such as redundancy, reliability etc. are applied as par safety significance. Capability of control systems to maintain process variables within limits should be demonstrated.

As a part of failure analysis of safety analysis report (SAR) part should bring out:
– System failure mode and effects analysis (single failure analysis);
– loss of control analysis;
– consequences to the failure of instrument air, power supply, etc.;
– Conformance of I&C system design with applicable standards.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The design of control and monitoring systems shall be such that, in combination with stipulated operator actions, process variables are maintained within the limits used in safety analysis.

Review also to cover consequences of loss of control and the issues which may come after installation and commissioning of the I&C systems, fine tuning of various control system settings for optimal performance.

Review should focus on how the transient and steady state performance of the plant systems in maintaining the set limits affected by tuning of control system.

The dynamic performance of the control system should be assessed after such tuning to maintain the control band.

The safety-related I&C systems ensure the operation of the plant within a prescribed safe operation region. In response to initiating events, including the failure of control systems, the plant may migrate beyond the safe operation region. Thresholds are to be set in safety, or safety-related I&C systems to bring the plant back to the safe state or to initiate safety action before any significant damage is done to the plant.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from accident analysis, regulatory guidance).</td><td>AERB document “Safety Systems For Pressurised Heavy Water Reactors” AERB/NPP-PHWR/SG/D-10 and safety guide on “Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants”, AERB/NPP-PHWR/SG/D-20 forms the basis for review.</td></tr>
</table>

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Control Systems	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, design information such as types, number, structures and capabilities of the following systems is provided for instrumentation and control system in the application: – Instrumentation; – Safety protection circuit; – Control system, and; – Emergency control system. Design information including design policy of above systems is provided in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Identical with technical basis provided in Subsection of “Reactor trip system”.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Control Systems	Korea KINS
Design information provided by applicant.	– Safety analysis report chapter 7.7 systems not required for safety; – System requirements (including functional requirements) specification; – Topical reports on specific issues in overall I&C; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Safety reviews and inspections based on technical basis (standards, codes, acceptance criteria); – Separation of protection and control systems; – Inspection of selected design information documents if necessary.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	– Regulation on Technical Standards for Nuclear Reactor Facilities: o (Article 20) Instrumentation and Control System; o (Article 26) Protection System; o (Article 25) Control Room; – Notice of NSSC (Nuclear Safety and Security Commission): o (Reactor. 15) Regulation on Safety Classification and Applicable Codes and Standards for Nuclear Reactor Facilities; o (Reactor. 21) Guidelines of Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities; – KINS Standard Review Guides: o (7.7) Control Systems; – KEPIC ENB 1100(IEEE 603), KEPIC ENB 6370(IEEE 7-4.3.2).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, mechanical engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, mechanical engineer.

Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 180 working days.

Control Systems	Russia SEC NRS
Design information provided by applicant.	A safety analysis report (SAR) is to be submitted. Among other issues, this report contains information on the normal operation safety-related control systems within the scope of requirements of Chapter 7 of the federal rules and regulations NP-006-98 "requirements to the content of the safety analysis report for NPPs". The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to the systems mentioned. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (sections 4.4, 4.5), NP-082-07 (section 2.4).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	Requirements of the federal rules and regulations: – OPB-88/97 (Section 4.4); – NP-082-07 (Section 2.4); – NP-006-98 (Chapter 7); – NP-026-04; Provisions of the IAEA Standards: – IAEA Safety Standards Series. Safety Guide, Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011; Provisions of the national standard: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems); Provision of the guideline document of the operating organisation: – RD EO 0554-2005. Guideline Document. Nuclear Power Plants. Control Systems Important to Safety. Manufacturing, Upgrading and Operation. General Provisions.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the field of I&C systems for NPPs.
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	4-6 man-months.

Control Systems	Slovakia UJD
Design information provided by applicant.	– Detailed description and design basis of the control system important to safety and safety related; – Safety analysis; – Requirements for HW and SW; – Resistant to the environment.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the control system fulfils the requirements for functionality, performance; – Reliability, resistance to the environment and quality.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	IEC standards, Slovak technical standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Control Systems	Slovenia SNSA
Design information provided by applicant.	Detailed description and design basis of the following systems: – Reactor control system; – Nuclear instrumentation system; – Control rod drive mechanism control system; – Rod position indication system; – In-core instrumentation system; – Balance of plant control; – Turbine electro hydraulic governor control system; – Turbine supervisory instrumentation system; – Turbine protection control; – Electrical system control; – Radiation monitoring system; – Auxiliary equipment control system.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques and load combinations used conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety and; – That commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction and testing of I&C systems and equipment commensurate with the importance of the safety functions performed. Confirmatory analysis of the predictions and calculations.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from accident analysis, regulatory guidance).**	General aspects of design standards including: – IAEA, "Safety of Nuclear Power Plants: Design", Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, "Site Evaluation for Nuclear Installations", Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, "Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide", Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, "Safety Assessment and Verification for Nuclear Power Plants", Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, "Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide", Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004); – IAEA, "Software for Computer Based Systems Important to Safety", Safety

	Standards Series No.NS-G-1.1, IAEA, Vienna (2000). Regulation JV5, Instrumentation and control: – Instrumentation shall allow measurement of all the main variables of the nuclear power plant that may affect the fission process, the reactor-core integrity, the reactor coolant system and the containment. Instrumentation shall also allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived; – Instrumentation and controls shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible; – Any unauthorised access or ingress to the instrumentation and control systems shall be prevented by appropriate physical, technical and administrative measures; – Instrumentation and control systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems; – The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer, computer engineer, nuclear engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer, nuclear engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	– Regulator review: 160 hours. – TSO's review time: 200 hours.

Control Systems	Sweden SSM
Design information provided by applicant.	See high level summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Non-specific review.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorized technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3: The Management System for Facilities and Activities. International Atomic Energy Agency, Vienna, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	Approximately 10 working days.

<table>
<tr><th>Control Systems</th><th>United States
U.S. NRC</th></tr>
<tr><td>Design information provided by applicant.</td><td>As part of the safety analysis report (SAR), the applicant should describe or provide the following for all control systems that can, through failure of normal operation, or spurious operation, affect the performance of critical safety functions:
– Design bases for control systems, which include the necessary features for manual and automatic control of process variables within normal operating limits;
– Basic description of each control system and its functions, including information on the architecture, communications and manual/automatic signal configurations;
– The effects of control system operation on accidents;
– The effects of control system failures;
– The effects of control system failures caused by accidents;
– Detailed design information to demonstrate independence of safety system functions from the control system;
– Demonstrate that control systems are not required for safety.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows:
– SRP 7.7, "Control Systems";
– SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603";
– SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2".
The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>The staff do not commonly perform confirmatory analyses in this technical area.</td></tr>
<tr><td>Technical basis
• Standards
• Codes
• Acceptance criteria
(e.g. can come from Accident analysis, regulatory guidance)</td><td>The following NRC regulatory requirements are applicable to this category:
– 10 CFR 50, Appendix A, General Design Criterion (GDC):
o GDC 1, "Quality Standards and Records";
o GDC 10, "Reactor Design";
o GDC 13, "Instrumentation and Control";
o GDC 15, "Reactor Coolant System Design";
o GDC 19, "Control Room";
o GDC 24, "Separation of Protection and Control Systems";
o GDC 28, "Reactivity Limits";
o GDC 29, "Protection Against Anticipated Operational Occurrences";
o GDC 44, "Cooling Water".</td></tr>
</table>

<table>
<tr><td></td><td>
– 10 CFR 50.34(f), “Additional TMI-Related Requirements”;
– 10 CFR 50.55a(a)(1), “Quality Standards”;
– 10 CFR 50.55a(h), “Protection and Safety Systems”;
– 10 CFR 52.47 (b)(1), “Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”;
– 10 CFR 52.80(a), “Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”.

The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows:

– Regulatory Guide (RG) 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”;
– RG 1.151, "Instrument Sensing Lines";
– RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”;
– Staff Requirements Memorandum(SRM) on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,” July 15, 1993.

Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required.

The Codes and Standards related to this category are as follows:

– IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”;
– IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”.
</td></tr>
<tr><td>Skill sets (education) required by:
• Senior (regulator)
• Junior (regulator)
• TSO.</td><td>Electrical engineer.</td></tr>
<tr><td>Specialised training, experience and/or education needed for the review of this topic.</td><td>
All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently.

Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include:

– Experience with traditional and digital I&C systems;
– Basic knowledge of software structure and application;
– Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.;
– Basic knowledge of data communications devices;
– Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
</td></tr>
<tr><td>Level of effort in each review area.</td><td>1 500 hours (estimated based on the level of complexity of the design).</td></tr>
</table>

APPENDIX G
MAIN CONTROL ROOM

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering and human factor engineering.	150 hours.
Finland	Yes.	Yes.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	45 working days (360 hours).
France	Yes.	No.	I&C engineer.	4 man-months (640 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[1]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[1]
Korea	Yes.	Yes.	Human factors engineer, I&C engineer.	200 working days (1 600 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	2-3 man-months (480 hours).
Slovakia	Yes.	No.	Mechanical engineer.	–[2]
Slovenia	Yes.	Yes.	Mechanical engineer, health physicist.	–
Sweden	Yes.	Yes.	I&C Engineer, human factors specialist, site inspector.	95 working days (760 hours).
United States	Yes.	Yes.	Electrical engineer, human factors engineer, reactor systems engineer.	2 500 hours.

Notes:

1. In Japan and India, resources (hours) are not set up for each individual review area.
2. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Main Control Room	Canada CNSC
Design information provided by applicant.	Section 6.7.4 of the CNSC licence application guide RD/GD-369 "Licence to construction a nuclear power plant" specifies information to be provided by applicant for control room instrumentation and control. This includes: – The means of physical and electrical isolation between the plant systems and communication signals routed to the main control room and the secondary control room should be described in detail. This description should demonstrate that the secondary control room instrumentation and control equipment is redundant and fully independent from the main control room; – The mechanisms for the transfer of control and communications from the main control room to the secondary control room should also be described in detail to demonstrate how this transfer would occur under accident conditions. Communication with the emergency support centre should also be described.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC guidance document GD-385 "pre-licensing review of a vendor's reactor design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include: – Focus Area 2: Classification of structure, systems, and components (SSCs); – Focus Area 5: Control system and facilities. The scope and level of detail of the staff's safety review is based on the guidance of the CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.7 "How to Assess the Instrumentation and Control". The following sections are applicable to this technical area: – Part A – Overall Instrumentation and Control; – Part E – Control Room Instrumentation and Control.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmatory analyses to verify: – Adequate manual controls are provided in the main control rooms; – Independence between the main and the secondary control room; – Provision of reliable communication links to emergency support facilities.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the technical area of the Main control room: – Section 6.6 Facility layout; – Section 7.9 Instrumentation and control; – Section 7.20 Escape routes and means of communication; – Section 7.21 Human factors; – Section 7.22 Robustness against malevolent acts; – Section 8.10.1 Main control room; – Section 8.10.3 Emergency support facilities; – Section 8.10.4 Equipment requirements for accident conditions.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in electrical and electronics engineering, computer engineering and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Human factor engineering.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering.
Level of effort in each review area.	150 person-hours for construction licence application review.

Main Control Room	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – System test plan, test specifications; – System test results; – HMI validation plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of selected design information documents.
What type of confirmatory analysis (if any) is performed?	– Safety assessment by license holder; – Safety assessment by designer.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 62138 cat B); – For quality management ISO 9001, IAEA GS-R-3, KTA 1401; – NUREG-0711; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer; – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – Plant specific training. Tools and methods: – Document management system. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 45 working days.

Main Control Room	**France** **ASN** Notes: Applied to the EPR FA3 design, "Main Control room" is understood as being the "Primary Information and Control System" (PICS) which is the preferred man-machine interface used in all plant conditions. In French designs, this system is a digital based system safety category 2 (F2). This system is not used for the safety demonstration. The SICS (section 4) is also located in the main control room.
Design information provided by applicant.	– High level development documentation for the platform; – Documentation necessary to substantiate the commercial dedication (including a detailed a posteriori conformance to IEC 62138); – Documentation on the architecture of the system. (The environmental qualification results for the hardware equipment is also provided and reviewed separately.)
Analysis, reviews and/or research performed by the reviewer and scope of review.	Review essentially consists in the review of the commercial dedication of the platform.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Relevant IEC 45A standards (mostly IEC 61513, IEC 62138).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	General knowledge in digital I&C.
Specialised training, experience and/or education needed for the review of this topic.	None.
Level of effort in each review area.	About 4 man-month.

<table>
<tr><th>Main Control Room</th><th>India
AERB</th></tr>
<tr><td>Design information provided by applicant.</td><td>The design description of safety analysis report (SAR) part should bring out the design provisions adopted according to AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants with respect to control room.

Adequate information is necessary to review the following:

– From the control room, the plant can be safely operated in all its operational states, and can be brought and maintained in the safe state after the onset of accident conditions (ref. clauses 5.2.9.1 to5.2.10.1 of the Code mentioned above);
– Appropriate measures and adequate information provided to safeguard the occupants of the control room against postulated hazards;
– Displays in the control room will provide the operator with adequate and comprehensive information of the state and performance of the plant;
– The layout and design of the safety related instrumentation, in particular, shall ensure prompt attention of the operator. Also, if any part of the safety systems has been temporarily rendered inoperative for testing, it should amenable to be put under administrative control and the bypass shall be displayed in the control room;
– Ergonomics and human factors are taken into account in the control room design;
– Special attention is given to identifying those events, both internal and external to control room, which may pose a direct threat to its continued availability, and the design shall include reasonably practicable measures to minimise the effects of such events.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>Safety analysis and review is conducted based on Chapter 4 of the guide on “Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants”, AERB/NPP-PHWR/SG/D-20.

The review recognises that the control room is the centre where redundant safety and safety-related channels of instrumentation from the plant converge. The review also covers maintenance of independence of various channels and configuration of separate control equipment rooms close to the control room that house the associated redundant channel instrumentation.

Since the safety critical systems, safety related systems and systems not important to safety are all brought close together in the control room, the layout shall take into account the requirements for functional isolation and physical separation.

Review of control room also covers survival ventilation system for control, level of illumination in control room, control room direct access independent of other plant areas and arrangements to guard against unauthorised entry.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.</td></tr>
</table>

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants with respect to control room forms the basis of review. Further safety analysis and review is conducted based on Chapter 4 of the guide on of "Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants", AERB/NPP-PHWR/SG/D-20.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Main Control Room	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, design information of main control room is provided in the application as one item of instrumentation and control system. Design information, such as design policy, main equipment and main specifications of main control room, is provided in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Identical with technical basis provided in Subsection of “Reactor trip system”.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Main Control Room	Korea KINS
Design information provided by applicant.	– Safety Analysis Report for "Human Factors Engineering"; – The implementation plan and result document for Human Factors Program Element according to NUREG-0711; – Technical or Topical Reports for any specific design issues; – Design Specification for Man-Machine Interface Systems (MMIS) Balance of Plant (BOP); – Documents of "System Design Criteria" for each MMI; – Documents of "System Functional Descriptions" for each MMI.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Safety reviews and inspections based on technical basis (standards, codes, acceptance criteria); – Field audits of quality assurances for design and installation.
What type of confirmatory analysis (if any) is performed?	– Human Factors validations during the licence application process such as integrated system validations and operating ensemble tests.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Government decree on nuclear safety; – Regulatory standards (RS) for light water reactor (KINS/RS-N15.00); – Regulatory guidelines (RG) for light water reactor (KINS/RG-N15.01~05); – KINS Safety Review Guidelines (SRG) for Light Water Reactor (KINS/GE-N001); – (as a reference only) NUREG-0800, NUREG-0711, NUREG-1792, RG-1.62, RG-1.97, RG-1.149 (published by the U.S. NRC); – (as a reference only) ANSI/ANS-3.5, ANSI/ANS-58.8.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: human factors engineering, nuclear engineering, I&C engineering, plant operations, computer engineering. – Junior: human factors engineering, nuclear engineering, I&C engineering, plant operations, computer engineering.
Specialised training, experience and/or education needed for the review of this topic.	– Training and experiences related to the human factors aspects for human-system interfaces, based on the knowledge of human performance, capabilities and limitations, human factors tests and evaluation, and human factors principles; – Training and experiences related to the design of hardware and software aspects of control systems, based on the knowledge of the human-system interfaces including control and displays; – Training and experiences related to the plant operations based on the knowledge of operational activities including task characteristics.
Level of effort in each review area.	– Safety Review: 200 working days.

Main Control Room	Russia SEC NRS
Design information provided by applicant.	A Safety Analysis Report (SAR) is to be submitted. Among other issues, this report contains information on main control room within the scope of requirements of Chapter 7 of the federal rules and regulations NP-006-98 "Requirements to the Content of the Safety Analysis Report for NPPs". The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to main control room. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (Sections 4.4, 4.5), NP-082-07 (Section 2.4).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Requirements of the federal rules and regulations: – OPB-88/97 (Section 4.4); – NP-082-07 (Section 2.4); – NP-006-98 (Chapter 7); – NP-026-04. Provisions of the IAEA Standards: – IAEA Safety Standards Series, Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011. Provisions of the national standard: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems). Provision of the guideline document of the operating organisation: – RD EO 0554-2005. Guideline Document. Nuclear Power Plants. Control Systems Important to Safety. Manufacturing, Upgrading and Operation. General Provisions. Provision of IEC standard: – IEC 60964:1989. Design for Control Rooms of Nuclear Power Plants.
Skill sets (education) required by: • **Senior**	Industry-specific education in the field of I&C systems for NPPs.

(regulator) • **Junior (regulator)** • **TSO.**	
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	2-3 man-months.

Main Control Room	Slovakia UJD
Design information provided by applicant.	Detailed description and information which should demonstrate that control room fulfils following requirements: – A control room must be designed so that from the perspective of occupational health, it permits access and safe and healthy conditions even during emergency conditions; – The design must ensure identification of internal and outdoor events that directly threaten the control room's non-stop operation and propose measures that restrict their influence as effectively as possible; – The equipment layout and manner in which information is presented must provide an appropriate overall impression of the nuclear facility's status and operating characteristics; – All equipment needed during manual control must be located where they are accessible during normal operation, abnormal operation and design basis accidents, and to a reasonable extent also during selected severe accidents; – The design must contain facilities that effectively provide visual and audible indication of the state of operating parameters that have deviated from normal and could have an effect on nuclear safety.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submits documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the main control room fulfils all requirements for functionality, performance, reliability, resistance to the environment and quality and ability to check and control NPP operation.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	–

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: mechanical engineer. – Junior: mechanical engineer. – TSO: mechanical engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Experience with evaluation and safety analysis; – Knowledge about nuclear facilities.
Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Main Control Room	Slovenia SNSA
Design information provided by applicant.	– Detailed description and design basis; – Design of the control room ventilation system; – Control building layout and structures; – Effectiveness of shielding and structure surrounding the control room.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques and load combinations used conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance; – Verify that plant operators are adequately protected against the effects of accidental releases of toxic and radioactive gases; – Independent analyses are performed to determine the radiation doses and toxic gas concentrations.
What type of confirmatory analysis (if any) is performed?	Confirmatory analysis of the predictions and calculations.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	General aspects of design standards including: – IAEA, “Safety of Nuclear Power Plants: Design”, Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, “Site Evaluation for Nuclear Installations”, Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, “Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide”, Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, “Safety Assessment and Verification for Nuclear Power Plants”, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, “Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage”, Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, “Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide”, Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). Regulation JV5, Control room: – The control room shall allow safe operation and monitoring of the nuclear power plant in all the states of the facility. All actions necessary to keep the plant in a safe condition and the restoring of safe condition upon an anticipated operational occurrence or a design-basis event must be achievable from the control room; – The design of a control room shall follow the principles of ergonomics; – The control room shall provide appropriate visual and acoustic indications of the facility and process states that deviate from normal conditions and may affect safety; – The operator shall be provided with appropriate information necessary to manage the consequences of automatic actions; – The design shall envisage those events within and outside the nuclear power

	plant that might pose threats to the activities in the control room and minimise their potential impacts; – In an event of inaccessibility of the main control room, a supplementary control room shall be provided, physically and electrically separated from the main control room. The supplementary control room shall be fitted with instruments and controls that allow safe shutdown of the reactor, maintenance of the safe shutdown condition and removal of residual heat. The supplementary control room shall also provide for monitoring of the nuclear power plant's essential parameters.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: mechanical engineer, health physicist. – Junior: mechanical engineer, health physicist. – TSO: mechanical engineer, health physicist.
Specialised training, experience and/or education needed for the review of this topic.	– Experience in radiation analysis.
Level of effort in each review area.	– Regulator review: 120 hours. – TSO's review time: 200 hours.

Main Control Room	Sweden SSM
Design information provided by applicant.	See High level summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Document review; – Inspections; – Oral presentations by the licensee; – Research reports review: o Halden; o SKI 2005:15. Human Factors Engineering Plan for Reviewing Nuclear Plant Modernization Programs. – NUREG 0711 adapted to Swedish conditions; o SKI 2006:06. Kontrollrumsfilosofi: Principer för kontrollrumsutformning och kontrolrumsarbete (Philosophy and principles of design - control room); o SKI 2008:34. Utformning av larmsystem I svenska kärnkraftverk; o 2009 Rapport SKI. Granskning av Turbic Validering.SKI 2006:06.
What type of confirmatory analysis (if any) is performed?	– Assessments by licensee (incl. PSADR); – Baseline report (HIS); – Safety assessments by independent reviewer (HIS). SSM requested an ISV but this has not been delivered.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; – SSMFS 2008:32; SSM general advice: – U.S. Nuclear Regulatory Commission: Human Factors Engineering Program Review Model", NUREG 0711; – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3: The Management System for Facilities and Activities. International Atomic Energy Agency, Vienna, 2006; Other: – NUREG 0700; – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Human factors specialist; – Senior I&C engineers (computer system platform); – Senior site inspectors.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	– Approximately 60 working days (HFE). – Approximately 30 working days (computer system platform). – Independent expert approximately 5 working days (HIS).

Main Control Room	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe the following areas related to the main control room: Safety related display instrumentation: – Systems that provide information to enable to operator to perform required safety functions, including: o Accident monitoring instrumentation; o Plant annunciators; o Safety parameter displays; o Information systems associated with emergency response facilities and nuclear data link; – Logic diagrams, piping and instrumentation diagrams and layout drawings of all information systems important to safety; – Analysis to demonstrate that the operator has sufficient information to perform required manual safety functions; – Analysis to demonstrate that the operator has sufficient time to make reasoned judgment and take action where operator action is essential for maintaining plant safety; – The information readouts and indications provided to the operator for monitoring conditions in the reactor, the RCS, the containment and safety related process systems; – Data communication systems provided to support instruments and controls within the control room to allow actions to be taken to maintain the plant in a safe condition during shutdown, including shutdown following an accident. Control Room Area Ventilation System: – The design bases for the air handling and treatment system for the control room; – Criteria and features that ensure the performance and reliability of the system for all modes of operation; – System description; – Safety objectives of the system; – Inspection and testing requirements; – Instrumentation and controls. The Human Factors Engineering program plan: – The planning and analysis elements used to identify HFE design inputs; – The HFE standards that will be incorporated in the control room design; – Verification and Validation practices to confirm the design effectiveness; – Implementation and long term monitoring strategies.

Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.4, "Safe Shutdown Systems"; – SRP 7.5, "Information Systems Important to Safety"; – SRP 7.9, "Data Communication Systems"; – SRP 9.4.1, "Control Room Area Ventilation System"; – SRP 18.1, "Human Factors Engineering". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff inspect the following confirmatory analysis completed by the applicant: – An integrated system validation exercise that demonstrates that the control room design supports safe operation of the plant. Other confirmatory analyses may be performed, if necessary, to aid the staff in making their safety finding. This is typically on a case-by-case basis.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General Design Criterion (GDC): o GDC 1, "Quality Standards and Records"; o GDC 2, "Design Basis for Protection Against Natural Phenomena"; o GDC 4, "Environmental and Missile Design Basis"; o GDC 5, "Sharing of Structures, Systems, and Components"; o GDC 13, "Instrumentation and Control"; o GDC 19, "Control Room"; o GDC 24, "Separation of Protection and Control Systems"; o GDC 60, "Control of Release of Radioactive Materials to the Environment". – 10 CFR 50.34(f), "Additional TMI-Related Requirements"; – 10 CFR 50.54, "Conditions of Licenses"; – 10 CFR 50.55a(a)(1), "Quality Standards"; – 10 CFR 50.55a(h), "Protection and Safety Systems"; – 10 CFR 50.63, "Loss of All Alternating Current Power"; – 10 CFR 52.47 (b)(1), "Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)"; – 10 CFR 52.80(a), "Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)". The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 1.7, "Criteria for Independence of Electrical Safety Systems"; – RG 1.29, "Seismic Design Classification"; – RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems";

	– RG 1.52, “Design, Testing, and Inspection Criteria for Air Filtration and Adsorption Units of Post-Accident Engineered-Safety-Feature Atmosphere Cleanup Systems in Light-Water-Cooled Nuclear Power Plants”; – RG 1.78, “Evaluating the Habitability of a Nuclear Power Plant Control Room During a Postulated Hazardous Chemical Release”; – RG 1.97, Revision 4, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants”; – RG 1.105, “Setpoints for Safety-Related Instrumentation”; – RG 1.140, “Design, Inspection, and Testing Criteria for Air Filtration and Adsorption Units of Normal Atmosphere Cleanup Systems in Light-Water-Cooled Nuclear Power Plants”; – RG 1.151, “Instrument Sensing Lines”; – RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”; – RG 1.155, “Station Blackout”; – RG 1.189, “Fire Protection for Operating Nuclear Plants”; – Staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs”, July 15, 1993; – NUREG-0737 Supplement 1, “Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability”, January 1983; – NUREG-0711, “Human-Factors Engineering Program Review Model”, November 2012; – NUREG-0700, “Human-System Interface Design Review Guidelines”, May 2002. Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. The Codes and Standards related to this category are as follows: – ASME Code AG-1, “Code for Nuclear Air and Gas Treatment”, 1991; – IEEE Std 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations”; – IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”; – IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer; – Human factors engineer; – Reactor systems engineer.

Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Electrical engineer: o Experience with traditional and digital I&C systems; o Basic knowledge of software structure and application; o Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; o Basic knowledge of data communications devices; o Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	2 500 hours (estimated based on the level of complexity of the design).

APPENDIX H
SUPPLEMENTARY CONTROL ROOM

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	150 hours.
Finland	Yes.	Yes.	Security inspector, I&C engineer, computer engineer, nuclear engineer, quality engineer.	10 working days (80 hours).
France	Yes.	No.	I&C engineer.	10 working days (80 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[1]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[1]
Korea	Yes.	Yes.	Human factors engineer, I&C engineer.	30 working days (240 hours).
Russia	Yes.	No.	Industry-specific education in the field of I&C systems for NPPs.	2-3 man-months (480 hours).
Slovakia	Yes.	No.	Mechanical engineer.	–[2]
Slovenia	Yes.	Yes.	Mechanical engineer, health physicist.	320 hours.
Sweden	Yes.	Yes.	I&C engineer, human factors specialist.	15 working days (120 hours).
United States	Yes.	No.	Electrical engineer, human factors engineer.	500 hours.

Notes:

1. In Japan and India, resources (hours) are not set up for each individual review area.
2. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

<table>
<tr><th>Supplementary Control Room</th><th>Canada
CNSC</th></tr>
<tr><td>Design information provided by applicant.</td><td>Section 6.7.4 of the CNSC licence application guide RD/GD-369 “licence to construction a nuclear power plant” specifies information to be provided by applicant for control room instrumentation and control:
– The means of physical and electrical isolation between the plant systems and communication signals routed to the main control room and the secondary control room should be described in detail. This description should demonstrate that the secondary control room instrumentation and control equipment is redundant and fully independent from the main control room;
– The mechanisms for the transfer of control and communications from the main control room to the secondary control room should also be described in detail to demonstrate how this transfer would occur under accident conditions. Communication with the emergency support centre should also be described.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>Appendix A of the CNSC guidance document GD-385 “Pre-licensing Review of a Vendor’s Reactor Design” describes review focus areas used in the assessment of a vendor’s reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include:
– Focus Area 2: Classification of structure, systems, and components (SSCs);
– Focus Area 5: Control system and facilities;
The scope and level of detail of the staff’s safety review is based on the guidance of the CNSC work instruction document WI-2.01-CON-11NNNN-006.7 “how to assess the instrumentation and control”. The following sections are applicable to this technical area:
– Part A – Overall Instrumentation and Control;
– Part E – Control Room Instrumentation and Control.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>As a minimum, CNSC staff normally perform confirmatory analyses to verify:
– Adequate manual controls are provided in the secondary control rooms;
– Independence between the main and the secondary control room;
– Provision of device(s) for transferring control from the main control room to the supplementary control room;
– No single event could disable the main control room and the secondary control room at the same time.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from Accident analysis, regulatory guidance)</td><td>The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the technical area of the supplementary control room:
– Section 6.6 Facility layout;
– Section 7.9 Instrumentation and control;
– Section 7.20 Escape routes and means of communication;
– Section 7.21 Human factors;
– Section 7.22 Robustness against malevolent acts;
– Section 8.10.1 Secondary control room;
– Section 8.10.3 Emergency support facilities;
– Section 8.10.4 Equipment requirements for accident conditions.</td></tr>
</table>

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Human factor engineering.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering.
Level of effort in each review area.	150 person-hours for construction licence application review.

Supplementary Control Room	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification ; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – System test plan, test specifications; – System test results; – HMI validation plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of selected design information documents.
What type of confirmatory analysis (if any) is performed?	– Safety assessment by licence holder; – Safety assessment by designer.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 62138 cat B); – For quality management ISO 9001, IAEA GS-R-3, KTA 1401; – NUREG-0711. Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements.
Specialised training, experience and/or education needed for the review of this topic.	– Senior: security inspector and I&C engineer, computer engineer, nuclear engineer, quality engineer.
Level of effort in each review area.	– Regulator review: 10 working days.

Supplementary Control Room	**France** **ASN** Note: "Supplementary control room" is considered as being the "Remote shutdown station" (RSS). This system is considered as an extension of the "Principal Information Control System" (PICS) with geographical separation. Hence only a very limited specific assessment is performed regarding I&C issues.
Design information provided by applicant.	– High level development documentation for the platform; – Documentation necessary to substantiate the commercial dedication (including a detailed a posteriori conformance to IEC 62138); – Documentation on the architecture of the system.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Review essentially consists in the review of the commercial dedication of the platform.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	IEC 61328.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	I&C engineer.
Specialised training, experience and/or education needed for the review of this topic.	General knowledge in digital I&C.
Level of effort in each review area.	About 10 working days.

<table>
<tr><th>Supplementary Control Room</th><th>India
AERB</th></tr>
<tr><td>Design information provided by applicant.</td><td>The design description of safety analysis report (SAR) part should bring out the design provisions adopted according to AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants with respect to backup control room. Also it should demonstrate that the provisions of AERB document “Safety Systems For Pressurised Heavy Water Reactors” AERB/NPP-PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20 are met.

The Code mentioned above in its section 6.6.5.1 provides the requirement with respect to backup control room which covers:
– Sufficient instrumentation and control equipment be located, preferably at a single location, that is physically and electrically separated from the control room;
– The backup control room will meet the design requirements of the control room with respect to safety classification, seismic category, single failure criterion and radiation shielding.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The review and analysis if backup control room/backup control points ensure that the requirements stated in AERB document “Safety Systems For Pressurised Heavy Water Reactors” AERB/NPP-PHWR/SG/D-10 are met.

Further the backup control room/backup control points shall be provided as per guidelines given in safety guide, “Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants”, AERB/NPPPHWR/SG/D-20.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from Accident analysis, regulatory guidance)</td><td>AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants with respect to control room forms the basis of review.

Further safety analysis and review is conducted based on Chapter 4 of the guide on of “Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants”, AERB/NPP-PHWR/SG/D-20.</td></tr>
<tr><td>Skill sets (education) required by:
• Senior (regulator)
• Junior (regulator)
• TSO.</td><td>– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience;
– Reactor systems engineer, engineers with reactor operation and maintenance background;
– Experts capable of failure modelling and probabilistic assessments, etc.</td></tr>
</table>

Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Supplementary Control Room	Japan NISA/JNES
Design information provided by applicant.	If operators could not stay in the main control room because of a certain cause, a reactor would be rapidly shut-down at elevated temperature and led to lower temperature from a suitable location outside the main control room. Design consideration against this event is provided in the application in the establishment permit application stage. Design information of main equipment of reactor shutdown system outside the main control room is provided in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Identical with technical basis provided in Subsection of “Reactor trip system”.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Supplementary Control Room	Korea KINS
Design information provided by applicant.	– Safety analysis report for "human factors engineering"; – The implementation plan and result document for human factors program element according to NUREG-0711; – Technical or Topical Reports for any specific design issues; – Design specification for MMIS BOP; – Documents of "system design criteria" for each MMI; – Documents of "system functional descriptions" for each MMI.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Safety reviews and inspections based on technical basis (standards, codes, acceptance criteria); – Field audits of quality assurances for design and installation.
What type of confirmatory analysis (if any) is performed?	– Human Factors validations during the license application process such as integrated system validations and operating ensemble tests.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Government decree on nuclear safety; – KINS Regulatory Standards (RS) for Light Water Reactor (KINS/RS-N15.00); – KINS Regulatory Guidelines (RG) for Light Water Reactor (KINS/RG-N15.01~05); – KINS Safety Review Guidelines (SRG) for Light Water Reactor (KINS/GE-N001); – (as a reference only) NUREG-0711, ANSI/ANS-58.6.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: human factors engineering, nuclear engineering, I&C engineering, plant operations, computer engineering. – Junior: human factors engineering, nuclear engineering, I&C engineering, plant operations, computer engineering.
Specialised training, experience and/or education needed for the review of this topic.	– Training and experiences related to the human factors aspects for human-system interfaces, based on the knowledge of human performance, capabilities and limitations, human factors tests and evaluation and human factors principles; – Training and experiences related to the design of hardware and software aspects of control systems, based on the knowledge of the human-system interfaces including control and displays; – Training and experiences related to the plant operations based on the knowledge of operational activities including task characteristics.
Level of effort in each review area.	– Safety review: 30 working days.

Supplementary Control Room	Russia SEC NRS
Design information provided by applicant.	A safety analysis report (SAR) is to be submitted. Among other issues, this report contains information on the supplementary control room that is within the scope of the requirements of Chapter 7 of the federal rules and regulations NP-006-98 "requirements to the content of the safety analysis report for NPPs". The SAR shall also contain a substantiation for fulfilment of the requirements of the regulations and rules related to supplementary control room. In particular, observance of the requirements of the following federal rules and regulations shall be confirmed: OPB-88/97 (Sections 4.4, 4.5), NP-082-07 (Section 2.4).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review is carried out with regard to the SAR section concerned. If necessary, the expert may request the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials.
What type of confirmatory analysis (if any) is performed?	No confirmatory analysis to be performed.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Requirements of the federal rules and regulations: – OPB-88/97 (Section 4.4); – NP-082-07 (Section 2.4); – NP-006-98 (Chapter 7); – NP-026-04. Provisions of the IAEA Standards: – IAEA Safety Standards Series, Safety guide No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, versions of 2002 and 2008; – IAEA Safety Standards for Protecting People and the Environment. Draft Safety Guide. Design of Instrumentation and Control Systems for Nuclear Power Plants. DS-431, IAEA, Vienna, August, 2011. Provision of the national standard: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements (IEC 61513:2001, International Standard. Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems). Provision of the guideline document of the operating organisation: – RD EO 0554-2005. Guideline Document. Nuclear Power Plants. Control Systems Important to Safety. Manufacturing, Upgrading and Operation. General Provisions. Provision of IEC standard: – IEC 60965:1989. Supplementary Control Points for Reactor Shutdown without Access to the Main Control Room.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the field of I&C systems for NPPs.
Specialised training, experience and/or education needed for the review of this topic.	Experience in analysis, research, development and operation of NPP I&C systems.
Level of effort in each review area.	2-3 man-months.

Supplementary Control Room	Slovakia UJD
Design information provided by applicant.	– Detailed description and design basis; – Control building layout and structures; – Effectiveness of shielding and structure surrounding the control room; – Applicant has to demonstrate that supplementary control room is physically and functionally separated from the control room.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance; – Confirm that the supplementary control room fulfils all requirements for functionality, performance, reliability and resistance to the environment and quality.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	–
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: mechanical engineer. – Junior: mechanical engineer. – TSO: mechanical engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Experience with evaluation and safety analysis; – Knowledge about nuclear facilities.

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository, or repeated authorisation for operation of a nuclear installation are concerned.

Supplementary Control Room	Slovenia SNSA
Design information provided by applicant.	– Detailed description and design basis; – Design of the supplementary control room ventilation system; – Control building layout and structures; – Effectiveness of shielding and structure surrounding the control room.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance; – Verify that plant operators are adequately protected against the effects of accidental releases of toxic and radioactive gases; – Independent analyses are performed to determine the radiation doses and toxic gas concentrations.
What type of confirmatory analysis (if any) is performed?	Confirmatory analysis of the predictions and calculations.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	General aspects of design standards including: – IAEA, “Safety of Nuclear Power Plants: Design”, Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, “Site Evaluation for Nuclear Installations”, Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, “Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide”, Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, “Safety Assessment and Verification for Nuclear Power Plants”, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, “Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage”, Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, “Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants – Safety Guide”, Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). Regulation JV5, Control room: In an event of inaccessibility of the main control room, a supplementary control room shall be provided, physically and electrically separated from the main control room. The supplementary control room shall be fitted with instruments and controls that allow safe shutdown of the reactor, maintenance of the safe shutdown condition and removal of residual heat. The supplementary control room shall also provide for monitoring of the nuclear power plant's essential parameters.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: mechanical engineer, health physicist. – Junior: mechanical engineer, health physicist. – TSO: mechanical engineer, health physicist.
Specialised training, experience and/or education needed for the review of this topic.	Experience in radiation analysis.
Level of effort in each review area.	– Regulator review: 120 hours. – TSO's review time: 200 hours.

Supplementary Control Room	Sweden SSM
Design information provided by applicant.	See high level summary.

Analysis, reviews and/or research performed by the reviewer and scope of review.	– Document review;
	– Inspections;
	– Oral presentations by the licensee;
	– Research reports review;
	  o Halden;
	  o SKI 2005:15 (Swedish adaption of NUREG 0711);
	  o SKI 2006:06.

What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17. SSM general advice: – U.S. nuclear regulatory commission: "human factors engineering program review model", NUREG 0711.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Human factors specialist; – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements.
Level of effort in each review area.	– Approximately 10 working days (HFE). – Approximately 5 working days (computer system platform).

Supplementary Control Room	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe or provide the following related to remote shutdown capability: – Design bases of remote shutdown stations; – Basic description of what controls are available; – Description on how control from main control room to remote shutdown station is performed; – Required equipment outside the main control room to achieve and maintain hot and cold shutdown conditions; – Provisions for access to remote shutdown stations; – Logic diagrams, piping and instrumentation diagrams, and location layout drawings of safe shutdown systems and supporting systems; – Analyses that demonstrate how the remote shutdown system meets IEEE 603-1991 as required by the regulations; – Considerations of instrumentation installed to permit a safe shutdown in the event of the following: o Loss of plant instrument air systems; o Loss of cooling water to vital equipment; o Plant load rejection; o Turbine trip.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.4, "Safe Shutdown Systems"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff do not commonly perform confirmatory analyses in this technical area.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis,**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General Design Criterion (GDC): o GDC 1, "Quality Standards and Records"; o GDC 2, "Design Basis for Protection Against Natural Phenomena"; o GDC 4, "Environmental and Missile Design Basis"; o GDC 13, "Instrumentation and Control"; o GDC 19, "Control Room"; o GDC 24, "Separation of Protection and Control Systems";

regulatory guidance)	o GDC 34, "Residual Heat Removal"; o GDC 35, "Emergency Core Cooling"; o GDC 38, "Containment Heat Removal"; – 10 CFR 50.34(f), "Additional TMI-Related Requirements"; – 10 CFR 50.55a(a)(1), "Quality Standards"; – 10 CFR 50.55a(h), "Protection and Safety Systems"; – 10 CFR 52.47 (b)(1), "Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)"; – 10 CFR 52.80(a), "Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)". The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"; – RG 1.189, "Fire Protection for Operating Nuclear Plants". Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. The Codes and Standards related to this category are as follows: – IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"; – IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer; – Human factors engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	500 hours (estimated based on the level of complexity of the design).

APPENDIX I
DIVERSE I&C SYSTEMS

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	300 hours.
Finland	Yes.	Yes.	I&C engineer, computer engineer, nuclear engineer, quality engineer.	155 working days (1 240 hours).
France	Yes.	No.	I&C engineer.	15 working days (120 hours).
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[1]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[1]
Korea	Yes.	Yes.	I&C engineer electrical and electronics engineering, computer engineer, reactor systems engineer.	60 working days (480 hours)
Russia	Yes.	Yes.	Industry-specific education in the part of I&C.	2-3 man-months (480 hours)
Slovakia	Yes.	No.	Electrical engineer.	–[2]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer.	280 hours.
Sweden	Yes.	Yes.	I&C engineer.	60 working days (480 hours).
United States	Yes.	Yes.	Electrical engineer, human factors engineer, reactor systems engineer.	4 000 hours.

Notes:

1. In Japan and India, resources (hours) are not set up for each individual review area.
2. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Diverse I&C Systems	Canada CNSC
Design information provided by applicant.	Section 6.7.1 of the CNSC Licence Application Guide RD/GD-369 "Licence to Construction a Nuclear Power Plant" specifies information to be provided by applicant for safety system instrumentation and control. Specific information to be provided for this technical area includes: – Design basis requirements for individual actuation parameters (physical measurements used to trigger safety system action), including a list of the postulated initiating events for which each parameter is credited; – Identification of the interfaces with other systems, including the provisions to ensure the proper isolation of electrical signals, the means used to ensure the physical separation of redundant actuation system channels, and the means used to generate coincidence signals from redundant independent channels; – A description of the hardware and software quality assurance programmes and the software development process (including software requirements, design, implementation, verification, computer system integration, computer system validation, commissioning and configuration control). The description for software is needed when digital computers are used for safety systems.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC guidance document GD-385 "Pre-licensing Review of a Vendor's Reactor Design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include: – Focus Area 2: Classification of structure, systems, and components (SSCs); – Focus Area 5: Control system and facilities; – Focus Area 7: Emergency core cooling and emergency heat removal systems; – Focus Area 8: Containment/confinement and safety-important civil structure. The scope and level of detail of the staff's safety review is based on the guidance of the CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.7 "How to Assess the Instrumentation and Control". The following sections are applicable to this technical area: – Part A – Overall Instrumentation and Control; – Part B – Safety System Instrumentation and Control.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmatory analyses to verify: – Separation of diverse I&C systems with process control system; – Separation of diverse I&C systems with other safety systems; – Strategies to address software common cause failure.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis,**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the technical area of diverse I&C systems: – Section 5.3 Quality assurance program; – Section 5.4 Proven engineering practices; – Section 5.7 Design documentation; – Section 6.1 Application of defence-in-depth;

regulatory guidance)	– Section 6.2 Safety functions; – Section 6.3 Accident prevention and plant safety characteristics; – Section 7.1 Classification of SSCs; – Section 7.3 Plant states; – Section 7.4 Postulated initiating events considered in the design; – Section 7.6 Design for reliability; – Section 7.6.1 Common cause failure; – Section 7.6.2 Single failure criterion; – Section 7.6.3 Fail-safe design; – Section 7.6.4 Allowance for equipment outage; – Section 7.6.5.1 Shared instrumentation for safety systems; – Section 7.8 Equipment environmental qualification; – Section 7.9 Instrumentation and Control; – Section 7.14 In-service testing, maintenance, repair, inspection, and monitoring; – Section 8.4.3 Monitoring and operator action; – Section 9.3 Hazard analysis. The followings are the main codes and standards referenced: – CSA N290.0 "General requirements for safety systems of nuclear power plants"; – 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 Computer in Safe Systems of Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Methodology for determination of trip setpoint; – Reactor reactivity control; – Thermal hydraulics.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering; – Preferably higher education in electrical and electronics engineering or computer science.
Level of effort in each review area.	300 person-hours for construction licence application review.

Diverse I&C Systems	Finland STUK
Design information provided by applicant.	– System quality plan; – System V&V plan; – System qualification plan; – System requirements (including functional requirements) specification; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System description; – FMEA; – Reliability analysis; – Diversity analysis between protection system and hardwired backup system; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of all design information documents; – Audits and inspection visits to evaluate design processes, staff competencies and interface between different design organisations.
What type of confirmatory analysis (if any) is performed?	– See design information provided by supplier; – Safety assessment by licence holder; – Safety assessment by designer.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 62138 cat B); – For quality management ISO 9001, IAEA GS-R-3, KTA 1401; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – Junior: I&C engineer, computer engineer, nuclear engineer, quality engineer. – TSO: computer engineer, quality engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – Training programme on nuclear safety (compliant with IAEA syllabus); – I&C platform specific trainings; – Quality management system training (ISO 9001); – SPICE (ISO/IEC 15504) training; – Plant specific training. Tools and methods: – Document management system; – ISO/IEC 15504 for auditing. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods; – Quality management.
Level of effort in each review area.	– Regulator review: 140 working days. – Consultants' time: 15 working days.

Diverse I&C Systems	**France** **ASN** Note: On the EPR FA3, diversity mostly relies on diversity between the two main I&C platforms. There is no system designated as being a "diverse I&C system", some functions implemented in one platform are diversified by being also implemented (with a different definition) in a system based on the other platform.
Design information provided by applicant.	Justification for diversity between digital I&C platforms. Justification of diversity between developments of systems.
Analysis, reviews and/or research performed by the reviewer and scope of review.	None. Diversity is seen as a complement, main assessment effort and research is focused on the assessment of the systems themselves rather than on the diversity between them.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	None.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	I&C engineer.
Specialised training, experience and/or education needed for the review of this topic.	General technical knowledge on digital I&C.
Level of effort in each review area.	About 15 working days.

<table>
<tr><th>Diverse I&C Systems</th><th>India
AERB</th></tr>
<tr><td>Design information provided by applicant.</td><td>The design description of safety analysis report (SAR) part should bring out the design provisions adopted according to AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants with respect to diversity in I&C systems. Also it should demonstrate that the provisions of AERB document “Safety Systems For pressurised heavy water reactors” AERB/NPP-PHWR/SG/D-10 are met.

The information on design of systems and components with respect to diversity is generally classified as functional and equipment diversity:

– In functional diversity, two different means are used to accomplish a particular task when two different variables are used to detect a particular anticipated operational occurrence or accident conditions. This is the primary method of reducing the possibility that the protection system will not detect a departure from acceptable plant conditions in the case when one variable does not behave as predicted by the safety analysis;
– In equipment diversity, either similar equipment from different manufacturers or equipment employing different principles of operation are used in the system.

It should be demonstrated that design meets the requirement of diversity in the two shutdown systems. Also the actuation systems should be of diverse design and should be physically, functionally and conceptually independent of each other.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>As stated in AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants; the safety review is performed to ensure that the reactor shutdown shall be performed by two diverse systems of different design principles. Each of the systems shall be, on its own, capable of quickly rendering the nuclear reactor sub-critical by an adequate margin from operating and accident conditions.

Further in case of review of Computer Based Systems in Protection it is stated that where the required system integrity cannot be demonstrated with a high level of confidence, a diverse means of ensuring the protection functions shall be provided.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from Accident analysis, regulatory guidance)</td><td>AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants with respect to diversity in system design forms the basis of review.

Further the AERB document “Safety Systems For Pressurised Heavy Water Reactors” AERB/NPP-PHWR/SG/D-10 provides the diversity requirement in shutdown system and computer based safety systems.</td></tr>
</table>

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Diverse I&C Systems	Japan NISA/JNES
Design information provided by applicant.	In the establishment permit application stage, design information, such as the number of systems and flow rates, is provided in the application, as one item of emergency cooling system contained in the reactor cooling system facility. Above design specifications are provided in the description regarding the safety design of nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Identical with technical basis provided in Subsection of "Reactor trip system".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Diverse I&C Systems	Korea KINS
Design information provided by applicant.	– Safety analysis report chapter 7.8 diverse instrumentation and control systems; – System requirements (including functional requirements) specification; – System description; – Qualitative evaluation of design basis events with Common Mode Failure (CMF) in digitalized safety systems; – Quantitative evaluation of design basis events with CMF in digitalized safety systems.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluation of all design information documents.
What type of confirmatory analysis (if any) is performed?	– Safety assessment by regulator.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Regulation on Technical Standards for Nuclear Reactor Facilities: o (Article 20) Instrumentation and Control System; o (Article 26) Protection System; o (Article 27) Diverse Protection System; – Notice of NSSC(Nuclear Safety and Security Commission): o (Reactor 21) Guidelines of Application of Korea Electric Power Industry Code (KEPIC) as Technical Standards of Nuclear Reactor Facilities; – KINS Standard Review Guides: o (7.8) Diverse I&C System; o (App. 7-16) Review Guide on DID&D; – KEPIC ENB 2000(IEEE 384); – (as a reference only) SECY-93-087, II.Q.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, reactor systems engineer. – Junior: I&C engineer, computer engineer, reactor systems engineer.

Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training. Experience: – I&C (hardware, software); – Process and safety design.
Level of effort in each review area.	– Regulator review: 60 working days (480 hours).

Diverse I&C Systems.	**Russia SEC NRS**
Design information provided by applicant.	Information is to be submitted within the scope of requirements of the federal rules and regulations NP-006-98 (Chapter 7). According to paragraph 7.1.2 NP-006-98, the requirements of the safety regulations and rules, which set the requirements to I&C, are to be considered at I&C design, and observance of the mentioned requirements shall be confirmed in the SAR. The requirement of the diversity principle for I&C is set in the safety regulations and rules NP-026-04 (Annex 1), as well as in paragraph 4.4.5.7 OPB-88/97.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review of the SAR shall be carried out to check for compliance with the requirements of NP-006-98 (Chapter 7) and NP-026-04, as well as for compliance with the "General Safety Provisions for NPPs", specified in paragraph 1.1.2 OPB-88/97 (the certain technical solutions proposed shall be substantiated and established in the design in accordance with the state of the art).
What type of confirmatory analysis (if any) is performed?	An expert shall check for compliance of information (data) set forth in the SAR with the requirements of the safety regulations and rules. If necessary, the expert requests the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials performed for I&C, and evaluates observance of the acceptance criteria (substantiated in the design materials) for the tests and trials in question.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Requirements of the federal rules and regulations: – NP-006-98. Requirements to the content of the safety analysis report for VVER-type NPPs; – NP-026-04. Requirements to control systems important to safety of NPPs; – OPB-88/97. General safety provisions for NPPs. Provisions of the national standards: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements; – GOST R IEC 60880-2010. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software of Computer Based Systems Performing Functions of Category A; – GOST R IEC 62138-2010. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software of Computer Based Systems Performing Functions of Categories B and C; – GOST R IEC 60987-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements to Development of Computerized System Hardware; – GOST R IEC 62340-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements. Provisions of the IAEA Standards: – IAEA Safety Standards Series. Instrumentation and Control Systems Important to Safety in NPPs. Safety Guide NS-G-1.3 Vienna, 2008; – IAEA Safety Standards Series. Software for Computer Based Systems Important to Safety in Nuclear Power Plants. Safety Guide. NS-G-1.1. IAEA, Vienna, 2000.

	IEC standards: – IEC 61513:2011. Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirements for Systems; – IEC 60880-2006. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software Aspects for Computer-Based Systems Performing Category A Functions; – IEC 62138-2004. Nuclear Power Plants. Instrumentation and Control Important for Safety. Software Aspects for Computer-Based Systems Performing Category B or C Functions; – IEC 61226:2009. Nuclear Power Plants. Instrumentation and Control Important to Safety. Classification of Instrumentation and Control Functions; – IEC 60987:2013. Nuclear Power Plants. Instrumentation and Control Important to Safety. Hardware Design Requirements for Computer-Based Systems; – IEC 62340:2007. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements for Coping with Common Cause Failure.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the part of I&C.
Specialised training, experience and/or education needed for the review of this topic.	Experience in development and operation of I&C.
Level of effort in each review area.	2-3 man-months.

Diverse I&C Systems	Slovakia UJD
Design information provided by applicant.	– Description of the diverse I&C systems; – Safety analysis; – Requirements on quality, which producer has to fulfil; – Technical report about fulfilment of quality requirements conform to regulations, codes and standards.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	–
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Diverse I&C Systems	Slovenia SNSA
Design information provided by applicant.	The following issues should be consider for diverse I&C systems: – Design basis (identification of conditions that require protective action by the diverse I&C systems, identification of the range of transient and steady-state conditions…); – Power supply availability; – The diverse I&C system should be environmentally qualified (EQ); – Information should be in the control room; – Independence from the protection systems; – Potential for inadvertent actuation; – Completion of protective action; – Diversity and defence in depth analysis; – Safety analysis. The I&C systems which may perform diverse functions are: ATWS, reactor trip protection, engineered safety features actuation system, control systems, etc.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection techniques conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety and; – That these commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction, and testing of I&C systems and equipment commensurate with the importance of the safety functions performed. Confirmatory analysis of the predictions and calculations.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	General aspects of design standards including: – IAEA, “Safety of Nuclear Power Plants: Design”, Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, “Site Evaluation for Nuclear Installations”, Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, “Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide”, Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, “Safety Assessment and Verification for Nuclear Power Plants”, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, “Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage”, Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, “Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide”, Safety Standards Series No.NS-G-1.9, IAEA, Vienna (2004).

	IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No.NS-G-1.1, IAEA, Vienna (2000). Regulation JV5, instrumentation and control: – Instrumentation shall allow measurement of all the main variables of the nuclear power plant that may affect the fission process, the reactor-core integrity, the reactor coolant system and the containment. Instrumentation shall also allow the acquisition of all the plant information necessary for safe and reliable operation. All safety-related parameters shall be automatically recorded and archived; – Instrumentation and controls shall be qualified for application under all environmental conditions for which they are intended and shall be mutually electromagnetically compatible; – Any unauthorised access or ingress to the instrumentation and control systems shall be prevented by appropriate physical, technical and administrative measures; – Instrumentation and control systems shall be designed and implemented in a way that prevents any impact of a failure of faulty data transfer on the correct operation of safety systems; – The design, installation and testing of software and hardware of computer-supported systems relevant to safety shall apply appropriate standards. Software for digital instrumentation and control shall be verified, validated and tested. Due to the integral nature of computer-supported systems, an additional degree of conservatism shall be taken into account in their analyses.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer, computer engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	– Regulator review: 80 hours. – TSO's review time: 200 hours.

Diverse I&C Systems	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Document review; – Inspections; – Oral presentations by the licensee.
What type of confirmatory analysis (if any) is performed?	– Assessments by licensee (incl. PSADR); – SSM Assessment of level of diversity and independence between RPS and DPS; – Consultant assessment.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3: The Management System for Facilities and Activities. International Atomic Energy Agency, Vienna, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	– Approximately 50 working days. – Consultant approximately 10 working days.

Diverse I&C Systems	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should describe or provide the following: – Description of diverse I&C systems that includes initiating circuits, logic, bypasses, interlocks, redundancy, diversity, defence-in-depth design features and actuated devices; – Description of supporting systems; – Mitigation functions for anticipated transient without scram (ATWS); – Logic diagrams, piping and instrumentation diagrams and location layout drawings of all diverse I&C systems; – Analysis to demonstrate conformance with the regulatory requirements; – Analysis to demonstrate that the operator has sufficient information to perform required manual safety functions; – Analysis to demonstrate that the operator has sufficient time to make reasoned judgment and take action where operator action is essential for maintaining plant safety; – The information readouts and indications provided to the operator for monitoring conditions in the reactor, the RCS, the containment and safety related process systems; – Testing to confirm diverse systems meet analytic requirements (e.g. Diverse Actuation System (DAS) response time testing).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.8, "Diverse Instrumentation and Control Systems"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"; – SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff commonly perform confirmatory analyses to verify the adequacy of the following submittal(s) related to this technical area: – Diversity and defence-in-depth analysis. Other confirmatory analyses may be performed, if necessary, to aid the staff in making their safety finding. This is typically on a case-by-case basis.

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General Design Criterion (GDC): o GDC 1, "Quality Standards and Records"; o GDC 13, "Instrumentation and Control"; o GDC 19, "Control Room"; o GDC 24, "Separation of Protection and Control Systems"; – 10 CFR 50.55a(a)(1), "Quality Standards"; – 10 CFR 50.55a(h), "Protection and Safety Systems"; – 10 CFR 50.62, "Requirements for Reduction of Risk from ATWS Events for light-water-cooled Nuclear Power Reactors"; – 10 CFR 52.47 (b)(1), "Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)"; – 10 CFR 52.80(a), "Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)". The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"; – Generic Letter 85-06. "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related", April 16, 1986; – Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs", July 15, 1993; – Standard Review Plan, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses". November 2009 Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. The codes and standards related to this category are as follows: – IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"; – IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer; – Human factors engineer; – Reactor systems engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.;

	– Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	4 000 hours (estimated based on the level of complexity of the design).

APPENDIX J
DATA COMMUNICATION SYSTEMS

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	200 hours.
Finland	Yes.	Yes.	I&C engineer, computer engineer.	420 working days (3 360 hours).
France	No[1].	–	–	–
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[2]
Japan	Yes.	Yes.	No specific skill set required. Generally, staff who have more than 10 year-experience are taken on the task.	–[2]
Korea	Yes.	Yes.	I&C engineer, electrical and electronics engineering, computer engineering.	180 working days (1 440 hours).
Russia	Yes.	Yes.	Industry-specific education in the part of I&C.	2-3 man-months (480 hours).
Slovakia	Yes.	No.	Electrical engineer.	–[3]
Slovenia	Yes.	Yes.	Electrical engineer, computer engineer.	280 hours.
Sweden	Yes.	Yes.	I&C engineer.	20 working days (160 hours).
United States	Yes.	Yes.	Electrical engineer.	4 000 hours.

Notes:

1. In French reactors there has never been a specific data communication system. Communication features are handled as part of the review of other survey topics.
2. In Japan and India, resources (hours) are not set up for each individual review area.
3. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Data Communication Systems	Canada CNSC
Design information provided by applicant.	The applicant should provide the following information: – A high level overview of the I&C architecture, including a description of data communication among functional systems I&C systems and between the I&C systems and external systems; – A description of safety communication, including both communication networks and individual data-link interfaces. The deterministic characteristics of real-time data transfer should be demonstrated; – A description of non-safety communication, including both communication networks and individual data-link interfaces. Adequate system capacity should be demonstrated; – A description of communication between safety and non-safety equipment; – A description of manual control of safety systems at system-level and component-level; – Provisions of onsite and offsite access controls for both safety and non-safety communications.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC GD-385 "Pre-licensing Review of a Vendor's Reactor Design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. Focus Area 5 "Control system and facilities" is applicable to this technical area. The scope and level of detail of the staff's safety review is based on the guidance of the CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.7 "How to Assess the Instrumentation and Control". The following sections are applicable to this technical area: – Part A – Overall Instrumentation and Control; – Part C – Information Systems Important to Safety; – Part E – Control Room Instrumentation and Control.
What type of confirmatory analysis (if any) is performed?	As a minimum, CNSC staff normally perform confirmatory analyses to verify: – The data communication network topology and media access control should be designed and implemented to avoid CCF of safety systems.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the technical area of Data communication systems: – Section 5.3 Quality assurance program; – Section 5.4 Proven engineering practices; – Section 5.7 Design documentation; – Section 6.1 Application of defence-in-depth; – Section 7.1 Classification of SSCs; – Section 7.6 Design for reliability; – Section 7.6.1.3 Independence; – Section 7.6.3 Fail-safe design; – Section 7.9 Instrumentation and control; – Section 7.14 In-service testing, maintenance, repair, inspection, and monitoring;

	– Section 7.22 Robustness against malevolent acts; – Section 9.3 Hazard analysis. The codes and standards relevant to this area include: – IEC 61513 "Nuclear power plants - Instrumentation and control important to safety - General requirements for systems"; – IEC 61500 "Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions"; – IEEE Std 7-4.3.2 "IEEE Standard Criteria for Digital Computer in Safe Systems of Nuclear Power Generating Stations". In addition, the MDEP Generic Common Position "DI&C-04: Principle on Data Communication Independence" is used.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. Specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Digital communication.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering preferably higher education in electrical and electronics engineering or computer science.
Level of effort in each review area.	200 person-hours for construction licence application review.

Data Communication Systems	Finland STUK
Design information provided by applicant.	– System V&V plan; – System requirements (including functional requirements) specification and its independent assessment; – Overall I&C architecture; – Topical reports on specific issues in overall I&C; – System descriptions; – Interface analysis; – Decoupling concept; – FMEA; – Reliability analysis; – System test plan, test specifications; – System test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of all design information documents.
What type of confirmatory analysis (if any) is performed?	– See Design information; provided by supplier; – Safety assessment by licence holder (as part of each systems' design information); – Safety assessment by designer (as part of each systems' design information).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Government decree on nuclear safety; – Regulatory guidance (YVL Guides, especially YVL 5.5); – IEC TC 45 standards (like IEC 61513, 60880) Eki täydentää; – Acceptance criteria: same safety level must be demonstrated as required by YVL Guides and main standards. Unidirectional communication required between selected systems.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior: I&C engineer, computer engineer. – Junior: I&C engineer, computer engineer.

Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. Training: – I&C platform specific trainings. Tools and methods: – Document management system. Experience: – I&C (hardware, software); – Computer networks; – Testing methods; – Quality management.
Level of effort in each review area.	Regulator review: 420 working days.

Data Communication Systems	India AERB
Design information provided by applicant.	The design description of safety analysis report (SAR) part should bring out design criteria/bases and functional requirements and how these are met in the detailed design of I&C systems. The utility should provide information to adequately demonstrate the provisions as elaborated in AERB guide on "Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants", AERB/NPP-PHWR/SG/D-20. As stated in AERB safety code No. AERB/NPP-PHWR/SC/D (rev. 1) on design of pressurised heavy water reactor based nuclear power plants, the description on data acquisition and communication system should effectively demonstrate that the instrumentation provided are adequate to monitor process variables and status of systems for all plant states. Information on instrumentation provided for measuring all main process variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment and for obtaining any plant information required for the reliable and safe operation of the plant shall be provided.
Analysis, reviews and/or research performed by the reviewer and scope of review.	AERB guide on "Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants", AERB/NPP-PHWR/SG/D-20 forms the basis for assessment. Instrumentation and recording equipment shall be provided to ensure that essential information is available to monitor the course of design basis accidents and the status of essential equipment and for predicting, as far as is necessary for safety, the locations and quantities of radioactive materials that could escape from their locations intended in the design. The instrumentation and recording equipment shall be adequate to provide information, as far as practicable, about the status of the plant during severe accidents and for decisions during accident management.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	AERB guide on "Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants", AERB/NPP-PHWR/SG/D-20.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Data Communication Systems	**Japan NISA/JNES**
Design information provided by applicant.	In the establishment permit application stage, design information on the main control room including data communication systems is provided in the attached documents to the application, as one of design information for the instrumentation and control system. Design information on intensive monitoring is provided in the description on the safety design of the nuclear reactor facility.
Analysis, reviews and/or research performed by the reviewer and scope of review.	These activities are to conform to the standards, criteria, and the like described below.
What type of confirmatory analysis (if any) is performed?	In the establishment permit application stage, adequacy of an applicant's analytic method and the analysis results are verified. Independent evaluation is performed to demonstrate the analysis results, if needed (cross check analysis).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Identical with technical basis provided in Subsection of "Reactor trip system".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: director for nuclear safety examination. – Junior: nuclear safety examiner. – TSO: Japan Nuclear Energy Safety Organization (JNES). Generally the staff who have more than 10 year-experience are taken on the task, although no specific skill set is required.
Specialised training, experience and/or education needed for the review of this topic.	– Basic training for the examiner for nuclear safety; – Practical application training for the examiner for nuclear safety.
Level of effort in each review area.	Resources (hours) is not set up for the individual review area. Regarding the standard processing duration, 2 years is set up for the basic design of an entire plant, and 3 months per one application is set up for detailed design. Divided application is granted for the detailed design.

Data Communication Systems	Korea KINS
Design information provided by applicant.	– Safety Analysis Report Chapter 7.9 Data communication system; – Network Performances (Bandwidth, Latency, Error Rate and); – Protocols and Electrical Interfaces in Network; – Topical Report on Specific Issues in I&C System; – System Descriptions including Data Flow (Network) Diagram; – Software Program Manual; – Reliability Analysis; – Network-related Hardware Specification; – EMI/RFI; – FMEA; – Environmental and Seismic Qualification.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Check if the design items conform to their standards and criteria.
What type of confirmatory analysis (if any) is performed?	– Independent verification and validation; – Safety assessment.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Regulation on technical standards for nuclear reactor facilities: o (Article 20) Instrumentation and control system; o (Article 25) Control room; o (Article 26) Protection system; – Notice of NSSC (Nuclear Safety and Security Commission): o (Reactor. 15) Regulation on safety classification and applicable codes and standards for nuclear reactor facilities; o (Reactor. 21) Guidelines of application of Korea Electric Power Industry Code (KEPIC) as technical standards of nuclear reactor facilities; – KINS standard review guides: o (7.9) Data communication systems; – KEPIC ENB 1100(IEEE 603), KEPIC ENB 6370(IEEE 7-4.3.2); – KEPIC ENB 3000(IEEE 379).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer. – Junior: I&C engineer, computer engineer, nuclear engineer.

Specialised training, experience and/or education needed for the review of this topic.	– Data communication-related OJT (On the Job Training) such as design evaluation and plant inspection for 2 years; – Software and hardware experience.
Level of effort in each review area.	– Regulator review: 180 working days.

Data Communication Systems	Russia SEC NRS
Design information provided by applicant.	Information is to be submitted within the scope of requirements of the federal rules and regulations NP-006-98 (Chapter 7). According to paragraph 7.1.1 NP-006-98, the SAR shall describe I&C important to safety, including data (signals) communication features. According to paragraph 7.1.2 NP-006-98, the requirements of the safety regulations and rules, which set the requirements to I&C, are to be considered at I&C design, and observance of the mentioned requirements shall be confirmed in the SAR. The requirements in the part of data (signals) communication features are set in the safety regulations and rules NP-026-04, as well as in para. 4.1.4 OPB-88/97.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The review of the SAR shall be carried out to check for compliance with the requirements of NP-006-98 (Chapter 7) and NP-026-04, as well as for compliance with the “General Safety Provisions for NPPs”, specified in para. 1.1.2 OPB-88/97 (the certain technical solutions proposed shall be substantiated and established in the design in accordance with the state of the art).
What type of confirmatory analysis (if any) is performed?	An expert shall check for compliance of information (data), set forth in the SAR, with the requirements of the safety regulations and rules. If necessary, the expert requests the input design materials (used for SAR), as well as the results of factory and adjustment tests and trials performed for I&C, and evaluates observance of the acceptance criteria (substantiated in the design materials) for the tests and trials in question.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Federal rules and regulations: – NP-006-98. Requirements to the Content of the Safety Analysis Report for VVER-Type NPPs; – NP-026-04. Requirements to Control Systems Important to Safety of NPPs; – OPB-88/97. General Safety Provisions for NPPs. GOSTs: – GOST R IEC 61513-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements; – GOST R IEC 60880-2010. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software of Computer Based Systems Performing Functions of Category A; – GOST R IEC 62138-2010. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software of Computer Based Systems Performing Functions of Categories B & C; – GOST R IEC 60987-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements to Development of Computerized System Hardware; – GOST R IEC 62340-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements Aimed to Prevent a Common-Cause Failure; – GOST R IEC 61500. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Data Communication in Systems Performing Functions of Category A.

<table>
<tr><td></td><td>The IAEA Standards:
– IAEA Safety Standards Series. Instrumentation and Control Systems Important to Safety in NPPs. Safety Guide NS-G-1.3 Vienna, 2008;
– IAEA Safety Standards Series. Software for Computer Based Systems Important to Safety in Nuclear Power Plants. Safety Guide. NS-G-1.1.
IEC standards:
– IEC 61513:2011. Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirements for Systems;
– IEC 60880-2006. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software Aspects for Computer-Based Systems Performing Category A Functions;
– IEC 62138-2004. Nuclear Power Plants. Instrumentation and Control Important for Safety. Software Aspects for Computer-Based Systems Performing Category B or C Functions;
– IEC 61226:2009. Nuclear Power Plants. Instrumentation and Control Important to Safety. Classification of Instrumentation and Control Functions;
– IEC 60987:2013. Nuclear Power Plants. Instrumentation and Control Important to Safety. Hardware Design Requirements for Computer-Based Systems;
– IEC 62340:2007. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements for Coping with Common Cause Failure;
– IEC 61500:2009. Nuclear Power Plants. Instrumentation and Control Important to Safety. Data Communication in Systems Performing Category A Functions.</td></tr>
<tr><td>Skill sets (education) required by:
• Senior (regulator)
• Junior (regulator)
• TSO.</td><td>Industry-specific education in the part of I&C.</td></tr>
<tr><td>Specialised training, experience and/or education needed for the review of this topic.</td><td>Experience in development and operation of I&C.</td></tr>
<tr><td>Level of effort in each review area.</td><td>2-3 man-months.</td></tr>
</table>

Data Communication Systems	Slovakia UJD
Design information provided by applicant.	– System description; – Requirements on quality; – Reliability of the system; – Requirements on qualification.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review submit documentation whether fulfils requirements resulting from atomic act, regulation and applicable codes and standards; – Review the results of testing and surveillance;
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	IEC standards, Slovak Technical Standards.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository, or repeated authorisation for operation of a nuclear installation are concerned.

Data Communication Systems	Slovenia SNSA
Design information provided by applicant.	– System description; – Design basis; – Safety analysis.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Evaluate that the applicant has provided complete information to demonstrate that the materials, fabrication methods, inspection technique used conform to all applicable regulations, industrial codes and standards; – Review the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety, and; – That commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction, and testing of I&C systems and equipment commensurate with the importance of the safety functions performed. Confirmatory analysis of the predictions and calculations.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	General aspects of design standards including: – IAEA, “Safety of Nuclear Power Plants: Design”, Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, “Site Evaluation for Nuclear Installations”, Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, “Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide”, Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, “Safety Assessment and Verification for Nuclear Power Plants”, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, “Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage”, Nuclear Security Series No. 4, IAEA, Vienna (2007). IAEA, “Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide”, Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer, computer engineer. – Junior: electrical engineer. – TSO: electrical engineer, computer engineer.

Specialised training, experience and/or education needed for the review of this topic.	Experience in: – I&C; – Digital I&C (hardware and software).
Level of effort in each review area.	– Regulator review: 80 hours. – TSO's review time: 200 hours.

Data Communication Systems	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Document review; – Inspections.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. revision 2010, SSM rapport 2010:01, Jan 2010; – IAEA safety standards/safety requirements No. GS-R-3: The management system for facilities and activities. International atomic energy agency, Vienna, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	Approximately 20 working days.

<table>
<tr><th>Data Communication Systems</th><th>United States
U.S. NRC</th></tr>
<tr><td>Design information provided by applicant.</td><td>As part of the safety analysis report (SAR), the applicant should describe or provide the following:
– Describe all data communication systems (DCSs) that are part of or support the following systems;
o Reactor trip system;
o Engineered safety features;
o Safe shutdown systems;
o Information and Interlock systems important to safety;
o Control systems;
o Diverse I&C systems.
– Design bases of the data communication systems;
– Description of system architecture;
– Description and justification of both safety to safety and safety to non-safety interfaces;
– Analyses to demonstrate that the data communication systems conform to the applicable regulations, codes and standards.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The Nuclear Regulatory Commission (NRC) staff (1) reviews the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows:
– SRP 7.9, "Data Communication Systems";
– SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603";
– SRP Appendix 7.1-D, "Guidance for Evaluation of Conformance to IEEE Std 7-4.3.2".
The staff also considers emerging technical and construction issues, operating experience and lessons learned related to this category.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>The staff commonly perform confirmatory analyses to verify the adequacy of the following submittal(s) related to this technical area:
– Failure Modes and Effects Analysis.
Other confirmatory analyses may be performed, if necessary, to aid the staff in making their safety finding. This is typically on a case-by-case basis.</td></tr>
</table>

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General Design Criterion (GDC): o GDC 1, “Quality Standards and Records”; o GDC 2, “Design Basis for Protection Against Natural Phenomena”; o GDC 4, “Environmental and Missile Design Basis”; o GDC 13, “Instrumentation and Control”; o GDC 19, “Control Room”; o GDC 21, “Protection System Reliability and Testability”; o GDC 22, “Protection System Independence”; o GDC 23, “Protection System Failure Modes”; o GDC 29, “Protection Against Anticipated Operational Occurrences”; – 10 CFR 50.34(f), “Additional TMI-Related Requirements”; – 10 CFR 50.55a(a)(1), “Quality Standards”; – 10 CFR 50.55a(h), “Protection and Safety Systems”; – 10 CFR 50.62, “Requirements for Reduction of Risk from ATWS Events for light-water-cooled Nuclear Power Reactors”; – 10 CFR 52.47 (b)(1), “Requirement for DC application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”; – 10 CFR 52.80(a), “Requirement for COL application to contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC)”. The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 1.22, “Periodic Testing of Protection System Actuation Functions”; – RG 1.47, “Bypassed and Inoperable Statue Indication for Nuclear Power Plant Safety Systems”; – RG 1.53, Revision 1, “Application of Single-Failure Criterion to Nuclear Power Plant Protection Systems”; – RG 1.75, Revision 3, “Criteria for Independence of Electrical Safety Systems”; – RG 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation”; – RG 1.118, “Periodic Testing of Electrical Power and Protection Systems”; – RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”; – RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, October 2003; – RG 1.204, “Guidelines for Lightening Protection of Nuclear Power Plants” – NUREG/CR-6082, “Data Communications”, August 1993. Staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs”, July 15, 1993. Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. The Codes and Standards related to this category are as follows: – IEEE Std. 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”.

	– IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"; – IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	4 000 hours (estimated based on the level of complexity of the design).

APPENDIX K
SOFTWARE RELIABILITY

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering.	300 hours.
Finland	Yes[1].	–	–	280 working days (2 240 hours).
France	No.	–	–	–
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	–[2]
Japan	No.	–	–	–[2]
Korea	Yes.	No.	I&C engineer, electrical and electronics engineering, computer engineering.	120 working days (960 hours).
Russia	Yes.	Yes.	Industry-specific education in the part of I&C.	4-6 man-months (960 hours).
Slovakia	Yes.	Yes.	Computer engineer.	–[3]
Slovenia	Yes.	Yes.	Computer engineer, software engineer.	280 Hours
Sweden	Yes.	Yes.	I&C engineer.	450 working days (3 600 hours).
United States	Yes.	No.	Electrical engineer.	600 hours.

Notes:

1. In Finland, software reliability is reviewed as part of a systems inspection.
2. In Japan and India, resources (hours) are not set up for each individual review area.
3. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

<table>
<tr><th>Software Reliability</th><th>Canada
CNSC</th></tr>
<tr><td>Design information provided by applicant.</td><td>Section 6.7.1 of the CNSC licence application guide RD/GD-369 “licence to construction a nuclear power plant” specifies information to be provided by applicant for safety system instrumentation and control. Specific information to be provided for the technical area of Software reliability includes:
– A description of the hardware and software quality assurance programmes and the software development process (including software requirements, design, implementation, verification, computer system integration, computer system validation, commissioning and configuration control).</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>Appendix A of the CNSC guidance document GD-385 “Pre-licensing Review of a Vendor’s Reactor Design” describes review focus areas used in the assessment of a vendor’s reactor design. The objectives and review scope are specified for each focus area. Focus areas that are applicable to this technical area include:
– Focus Area 2: Classification of structure, systems, and components (SSCs);
– Focus Area 5: Control system and facilities.
The scope and level of detail of the staff’s safety review is based on the guidance of the CNSC work instruction document WI-2.01-CON-11NNNN-006.7 “how to assess the instrumentation and control”. The following sections are applicable to this technical area:
– Part A – Overall instrumentation and control;
– Part B – Safety system instrumentation and control.</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>As a minimum, CNSC staff normally perform confirmatory analyses to verify:
– Statistical validation to demonstrate that the reliability target is met.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from Accident analysis, regulatory guidance)</td><td>The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements are applicable to the technical area of Software reliability:
– Section 5.3 Quality assurance program;
– Section 5.7 Design documentation;
– Section 7.6 Design for reliability;
– Section 7.6.3 Fail-safe design;
– Section 7.9 Instrumentation and Control;
– Section 7.9.2 Use of computer-based systems or equipment;
– Section 9.3 Hazard analysis.
The main codes and standards relevant to this area include:
– IEC 61513 “Nuclear power plants - Instrumentation and control important to safety - General requirements for systems”;
– IEEE Std 7-4.3.2 “IEEE Standard Criteria for Digital Computer in Safe Systems of Nuclear Power Generating Stations”;
– IEC 60880 “Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions”;
– IEEE Std 1028 “IEEE Standard for Software Reviews and Audits”;
– IEEE Std 730 “IEEE Standard for Software Quality Assurance Plans”;</td></tr>
</table>

	– IEEE Std 828 "IEEE Standard for Software Configuration Management Plans"; – IEEE Std 829 "IEEE Standard for Software Test Document"; – IEEE Std 1012 "IEEE Standard for Software Verification and Validation"; – IEEE Std 1074 "IEEE Standard for Developing a Software Life Cycle Process".
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in Electrical and electronics engineering, computer engineering, nuclear physics, thermal hydraulics and human factor engineering. specific skills and knowledge are required in the following areas: – Design and implementation of hardware and software for safety systems; – Software engineering; – Software verification and validation.
Specialised training, experience and/or education needed for the review of this topic.	Specialised training, experience and education that is needed to perform reviews in this technical area include: – Knowledge and experience with the CNSC regulations and processes; – Knowledge and experience in I&C circuits theory, design and analysis techniques; – Knowledge and experience in programmable digital devices; – Knowledge and experience of operational nuclear facilities; – A minimum of B.E. degree in electrical and electronics engineering preferably higher education in electrical and electronics engineering or computer science.
Level of effort in each review area.	300 person-hours for construction licence application review.

Software Reliability	Finland STUK
Design information provided by applicant.	Inspected as a part of systems' inspection.
Analysis, reviews and/or research performed by the reviewer and scope of review.	–
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Standards: IEC 60880 for safety systems, IEC 62138 for safety related systems.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	–
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements.
Level of effort in each review area.	Regulatory review 280 working days.

Software Reliability	France ASN
Design information provided by applicant.	None is required.
Analysis, reviews and/or research performed by the reviewer and scope of review.	None. Quantitative reliability is considered as being technically irrelevant for addressing confidence in software.
What type of confirmatory analysis (if any) is performed?	None.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	None.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	None.
Specialised training, experience and/or education needed for the review of this topic.	None.
Level of effort in each review area.	None.

Software Reliability	India AERB
Design information provided by applicant.	Information should be provided as per AERB document on “computer based systems of Pressurised heavy water reactors” AERB/NPP-PHWR/SG/D-25. The information provided including software life cycle documents should be adequate for Review of software based system and should provide adequate evidences to build confidence about the integrity and reliability of the software. Analysis should (i) Confirm that traceability and correct implementation of safety requirements of the system in all development phases; (ii) Confirm compliance to single failure criteria as per AERB/NPP- PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20; (iii) Confirm protection against CCF in class IA systems. The detail information on System Safety Analysis includes the following: – Confirmation of safety function implementation which is checked during V and V process; – Failure analysis to establish that class IA and IB systems meet single failure requirements as per AERB/NPP-PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20 respectively; – Analysis for common cause failures (CCF) including (a) Identification of all potential CCF sources due to components (software or others) used within the C & I architecture; (b) Analysis of the possible effects of these CCFs with respect to each PIE (c) Confirmation that adequate diversity is provided to eliminate possibilities of CCFs (Requirement w.r.to CCF is given in subsection 3.2.3 (e) of AERB/SG/D-25).
Analysis, reviews and/or research performed by the reviewer and scope of review.	Review and safety and reliability analysis requirements for IA and IB systems (IA and IB are safety class of instrumentations as defined in AERB/NPP-PHWR/SG/D-1) consist of the following. Review/audit of system development life cycle documents including V&V and QA documents: – Confirmation of safety function implementation; – Failure analysis; – Common cause failure (CCF) analysis for IA systems; – Hardware reliability analysis. The detailed recommendation on these analyses is contained in Appendix-8 of AERB document on “computer based systems of Pressurised heavy water reactors” AERB/NPP-PHWR/SG/D-25.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees by the technical service organisation or at the designated division of AERB.

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Requirements specified in AERB document on "computer based systems of Pressurised heavy water reactors" AERB/NPP-PHWR/SG/D-25 forms the primary technical basis. The software integrity requirements should be commensurate with the criticality of the functions performed by the system. The operating experience of Pre Developed Systems shall be reviewed to ascertain that the observed reliability is commensurate with overall reliability goals stated in SR.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Software Reliability	Korea KINS
Design information provided by applicant.	– Outputs during all software lifecycle; o Software development plan; o Software management plan; o Software quality assurance plan; o Software V&V plan; o Software requirements specification and its design description; o Software test plan, test procedure, test results.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review the software documents; – Witness the FAT (Factory acceptance test); – Interview with project related persons; – Scope of review: safety critical class and important to safety class software.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Regulation on technical standards for nuclear reactor facilities: o (Article 20) Instrumentation and control system; o (Article 26) Protection system; o (Article 25) Control room; – Notice of NSSC (nuclear safety and security commission): o (Reactor. 15) Regulation on safety classification and applicable codes and standards for nuclear reactor facilities; o (Reactor 21) Guidelines of application of Korea electric power industry code (KEPIC) as technical standards of nuclear reactor facilities; – KEPIC ENB 1100(similar to IEEE 603), KEPIC ENB 6370 (similar to IEEE 7-4.3.2); – (as a reference only) IEEE 1012, 1024: Software V&V; – (as a reference only) IEEE 828: Software Configuration; – (as a reference only) IEEE 829, 1008: Software Testing.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer. – Junior: I&C engineer, computer engineer, nuclear engineer.

Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training; – Software reliability. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	Regulatory review 120 working days.

<table>
<tr><th>Software Reliability</th><th>Russia
SEC NRS</th></tr>
<tr><td>Design information provided by applicant.</td><td>Information is to be submitted within the scope of requirements of the federal rules and regulations NP-006-98. The requirements of Chapter 7 shall cover I&C, which use computers, IT-systems and microprocessor technology. According to paragraph 7.1.2 NP-006-98, the requirements of the safety regulations and rules, which set the requirements to I&C, are to be considered at I&C design, and observance of the mentioned requirements shall be confirmed in the SAR.

The requirements in the part of I&C software important to safety, are set in the safety regulations and rules NP-026-04, as well as in paragraph 2.1.5 NP-082-07. According to these requirements the codes that are applied in safety important systems shall be verified and certified in compliance with the established procedures.</td></tr>
<tr><td>Analysis, reviews and/or research performed by the reviewer and scope of review.</td><td>The review of the SAR shall be carried out to check for compliance with the requirements of NP-006-98 (Chapter 7) and NP-026-04, as well as for compliance with the “General Safety Provisions for NPPs”, specified in paragraph 1.1.2 OPB-88/97 (the certain technical solutions proposed shall be substantiated and established in the design in accordance with the state of the art).</td></tr>
<tr><td>What type of confirmatory analysis (if any) is performed?</td><td>An expert shall check for compliance of information (data), set forth in the SAR, with the requirements of the safety regulations and rules. If necessary, the expert requests the input design materials (used for SAR), as well as the results of verification of the software, and evaluates the results.</td></tr>
<tr><td>Technical basis:
• Standards
• Codes
• Acceptance criteria
(e.g. can come from Accident analysis, regulatory guidance)</td><td>Requirements of the federal rules and regulations:
– NP-006-98. Requirements to the content of the Safety Analysis Report for VVER-type NPPs;
– NP-026-04. Requirements to Control Systems Important To Safety of NPPs;
– NP-082-07. Nuclear Safety Rules for Reactor Installations of NPPs.

Provisions of the national standards:
– GOST R IEC 60880-2010. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software of Computer Based Systems Performing Functions of Category A;
– GOST R IEC 62138-2010. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Software of Computer Based Systems Performing Functions of Categories B & C;
– GOST R IEC 62340-2011. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements Aimed to Prevent a Common-Cause Failure.

Provisions of the IAEA Standards:
– IAEA Safety Standards Series. Software for Computer Based Systems Important to Safety in Nuclear Power Plants. Safety Guide. NS-G-1.1. IAEA, Vienna, 2000.

Provisions of IEC standards:
– IEC 60880-2006. Nuclear Power Plants. Instrumentation and Control</td></tr>
</table>

	Systems Important to Safety. Software Aspects for Computer-Based Systems Performing Category A Functions; – IEC 62138-2004. Nuclear Power Plants. Instrumentation and Control Important for Safety. Software Aspects for Computer-Based Systems Performing Category B or C Functions; – IEC 62340:2007. Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. Requirements for Coping with Common Cause Failure.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the part of I&C.
Specialised training, experience and/or education needed for the review of this topic.	Experience in development and operation of I&C.
Level of effort in each review area.	4-6 man-months (estimated value, no experience in such a review).

Software Reliability	Slovakia UJD
Design information provided by applicant.	– Requirements for software; – Verification and validation from independent organisation; – Software life cycle process.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review of conformance with standards and guides; – Review of software development life cycle; – Review of the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the software design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions. – Those commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction and testing of I&C systems and equipment commensurate with the importance of the safety functions performed.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	–
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: computer engineer. – Junior: computer engineer. – TSO: computer engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Digital I&C (hardware and software); – IT specialist.

Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Software Reliability	Slovenia SNSA
Design information provided by applicant.	– System description; – Design basis; – Safety analysis; – Software life cycle process.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Review of the system description; – Review of conformance with standards and guide; – Review of software development life cycle; – Review of the results of testing, inspection and surveillance.
What type of confirmatory analysis (if any) is performed?	Confirm: – That the software design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; – That these functions, the implementing systems and equipment have been properly classified to identify their importance to safety; – Those commitments have been made to use appropriate quality standards for I&C systems for the design, fabrication, construction, and testing of I&C systems and equipment commensurate with the importance of the safety functions performed.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	General aspects of design standards including: – IAEA, "Safety of Nuclear Power Plants: Design", Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, "Site Evaluation for Nuclear Installations", Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, "Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide", Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, "Safety Assessment and Verification for Nuclear Power Plants", Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, "Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide", Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: computer engineer, software engineer. – Junior: computer engineer, software engineer. – TSO: computer engineer, software engineer.

Specialised training, experience and/or education needed for the review of this topic.	– Digital I&C (hardware and software); – IT specialist.
Level of effort in each review area.	– Regulator review: 80 hours. – TSO's review time: 200 hours.

Software Reliability	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Focused review on vendor compliance with IEC 60880; – Inspections (focused on design changes and design changes process); – Oral presentations by the licensee; – Process auditing.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:17; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan 2010; – IAEA Safety Standards/Safety Requirements No. GS-R-3: The Management System for Facilities and Activities. International Atomic Energy Agency, Vienna, 2006; Other: – IEC TC 45 (incl. IEC 61513, 60880); – IEEE 603.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	No formal requirements. – Senior I&C engineers.
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements. – Experience from international cooperation and from previous modernisation projects (e.g. implementation of digital I&C systems at Oskarshamn Unit 1).
Level of effort in each review area.	Approximately 450 working days.

Software Reliability	United States U.S. NRC
Design information provided by applicant.	As part of the safety analysis report (SAR), the applicant should justify that the degree of redundancy, diversity, testability and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. The applicant should also provide the following: – Analysis and determination of software reliability.
Analysis, reviews and/or research performed by the reviewer and scope of review.	The Nuclear Regulatory Commission (NRC) staff (1) review the information provided in the SAR for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 7.1, "Instrumentation and Controls –Introduction"; – SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603; – SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2". The staff also consider emerging technical and construction issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	The staff does not commonly perform confirmatory analyses in this technical area.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 50, Appendix A, General Design Criterion (GDC): o GDC 21, "Protection System Reliability and Testability"; o GDC 24, "Separation of Protection and Control Systems"; – 10 CFR 50.55a(h), "Protection and Safety Systems". The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory guide (RG) 1.152, "Criteria for Digital Computers in Safety Systems Of Nuclear Power Plants". Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. The Codes and Standards related to this category are as follows: – IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations". – IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".
Skill sets (education) required by:	– Electrical engineer.

Senior (regulator) **Junior (regulator)** **TSO.**	
Specialised training, experience and/or education needed for the review of this topic.	All technical reviewers are required to complete a formal training and qualification programme prior to performing safety reviews independently. Other specialised training, experience and education that is needed to successfully perform reviews in this technical area include: – Experience with traditional and digital I&C systems; – Basic knowledge of software structure and application; – Basic knowledge of hardware types such as sensors, transmitters, detectors, etc.; – Basic knowledge of data communications devices; – Knowledge of applicable IEEE codes and standards and NRC-endorsed guidance.
Level of effort in each review area.	600 hours (estimated based on the level of complexity of the design).

APPENDIX L
CYBERSECURITY

Summary table

Country	Is this area reviewed?	Are confirmatory analyses performed?	Expertise of reviewers	Level of effort
Canada	Yes.	Yes.	Cybersecurity, physical security, information security.	300 hours.
Finland	Yes.	No.	_	40 working days (320 hours).
France	No.	_	_	_
India	Yes.	Yes.	Instrumentation/electronics or electrical engineer, reactor system engineer.	_[1]
Japan	No.	_	_	_[1]
Korea	Yes.	No.	I&C engineer, computer engineer.	120 working days (960 hours).
Russia	No[2].	_	Industry-specific education in the part of I&C.	2-3 man-months (480 hours).
Slovakia	Yes.	No.	Electrical engineer.	_[3]
Slovenia	Yes.	Yes.	Computer engineer, software engineer.	240 hours.
Sweden	No.	_	_	_
United States	Yes.	No.	Electrical engineer, I&C engineer, IT/cybersecurity specialist.	80 hours.

Notes:

1. In Japan and India, resources (hours) are not set up for each individual review area.
2. In Russia, no review is conducted in this area. However, the Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS) is currently developing regulations and rules in order to review this technical topic in the future.
3. In Slovakia, the standard Level of effort for the review of submitted documentation is defined by regulation and dependent upon the activity to be approved.

Cybersecurity	Canada CNSC
Design information provided by applicant.	Section 5.11 of CNSC licence application guide RD/GD-369 "licence to construction a nuclear power plant" specifies information to be provided by applicant for cybersecurity. This includes: – Cyber/network robustness against internal and external malevolent acts. The applicant should describe the measures taken to ensure the cybersecurity of the plant, and to depend against cyber threats. The information should also meet Section 7.22.4 of RD-337. The applicant should provide the following information on cybersecurity: – Design approach and strategy; – Design codes, standards and guidance; – Cybersecurity programme; – Interfaces with other programmes (e.g. safety, security and emergency preparedness and response programmes).
Analysis, reviews and/or research performed by the reviewer and scope of review.	Appendix A of the CNSC GD-385 "Pre-licensing Review of a Vendor's Reactor Design" describes review focus areas used in the assessment of a vendor's reactor design. The objectives and review scope are specified for each focus area. The following focus areas are relevant to the technical area of cybersecurity: – Focus Area 5: Control system and facilities; – Focus Area 15: Robustness, safeguards and security. The scope and level of detail of the staff's security review is based on the guidance of: – CNSC Work Instruction Document WI-2.01-CON-11NNNN-006.5.11.1 "How to Access the Security", Part B - Site Security Program; – CNSC Pre-Licensing Review of a Vendor Reactor Design, SRP-2.15.00-VDR-011NND-015B - Security and Cyber Security, including: o Part A Security (including Cyber Security) – Phase 1; o Part B Security (Including Cyber Security) – Phase 2.
What type of confirmatory analysis (if any) is performed?	CNSC staff normally perform confirmation analysis to verify the following topics meet CNSC staff's expectations: – Overall cybersecurity strategy and approach with defence-in-depth; – Cybersecurity programmes for all phases of I&C lifecycle; – Cybersecurity defensive architecture; – Cybersecurity features in design; – Cybersecurity controls.

Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The CNSC regulatory document RD-337 sets out the requirements concerning the design of new water-cooled nuclear power plants. The following requirements should be met for cybersecurity: – Section 7.22.4 Cyber Security. Other associated requirements include: – Section 5.3 Quality assurance program; – Section 5.7 Design documentation; – Section 7.9 Instrumentation and control; – Section 7.22 Robustness against malevolent acts.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review requires a team with combined knowledge and experience in cybersecurity aspects in all phases of computer-based I&C systems life cycle, physical security, information security, design or operation of systems important to safety and cybersecurity programme.
Specialised training, experience and/or education needed for the review of this topic.	Education, experience, training, and that is needed to successfully perform reviews in this technical area include: – Knowledge in CNSC regulatory requirements, regulatory guides; – Knowledge in IAEA security series; – Knowledge in applicable codes and standards for cybersecurity; – Knowledge or experience in design and/or operation of computer-based I&C systems engineering, communication network and safety software; – Knowledge or experience with cybersecurity standards for industrial control systems; – A minimum of B.E. degree in electrical and electronic system or computer or process control engineering; preferably higher education in digital control system, cybersecurity engineering.
Level of effort in each review area.	300 person-hours for construction licence application review.

Cybersecurity	Finland STUK
Design information provided by applicant.	– Risk assessment plans and results; – IT security plans.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of design information; – Onsite inspections.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– Regulatory guidance (YVL Guides, YVL 6.11 (latter not public)); – ISO/IEC 2700x series; – For software based systems in safety class 2, IEC 60880.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	–
Specialised training, experience and/or education needed for the review of this topic.	No formal requirements.
Level of effort in each review area.	– Regulator review: 10 working days. – TSO's review time: 30 working days.

Cybersecurity	India AERB
Design information provided by applicant.	Information should be provided on the system development planning process, configuration management during development and O and M, and system security planning as per AERB document on “computer based systems of Pressurised heavy water reactors” AERB/NPP-PHWR/SG/D-25. Information should be provided to demonstrate the security requirements of computer based systems important to safety which includes protection from unauthorised access and modification, and disruption of its functions (denial of service). The information on features that ensure prevention of unauthorised access to the hardware and software especially for alteration of crucial parameters. A security plan that specifies the procedural and technical measures shall be prepared for each system important to safety to ensure that the system is designed, developed, delivered and operated with adequate security measures (refer Appendix-1 of AERB/NPP-PHWR/SG/D-25).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The adequacy of security requirements, in terms of access to computer system to persons at different levels with different requirements through secure means such as hardware key interlocks and/or passwords, or through network, is analysed. These should also address need, for annunciation, on-line logging of accesses or recording identity of the user etc. Pre-developed software used in the system should be analysed for security vulnerabilities and configured so as to minimise the vulnerabilities. Any remaining vulnerabilities shall be mitigated through additional means. Security testing is also within the scope that aimed at checking that the basic security mechanisms provided in the system are able to protect the integrity and availability of the system in all modes of operation.
What type of confirmatory analysis (if any) is performed?	Confirmatory analyses are performed, if necessary, on a case-by-case basis as warranted by the AERB safety review committees, by the technical service organisation, or at the designated division of AERB.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Requirements specified in AERB document on “computer based systems of pressurised heavy water reactors” AERB/NPP-PHWR/SG/D-25 forms the primary technical basis. The review is carried out based on general design principles relevant to assuring safety as enunciated in AERB safety guides AERB/NPP-PHWR/SG/D-1 and AERB/NPP-PHWR/SG/D-20. Standards are referred in the relevant code/guides of AERB. The system security plan shall be made to specify the procedural and technical measures to be taken to protect the computer based I and C systems important to safety. An analysis of the potential security threats regarding the system and software shall be performed by taking into account the relevant phases of the system and software life cycles. It shall identify the counter measures including recovery procedures in case of loss of system due to any security related incident. It shall

	include: – Procedures related to the interface between administrative and technical security, access to systems, security aspects of data handling and storage, security aspects of modification and maintenance, security auditing and reporting, and security training; – The security plan shall also address security procedures to be applied during operation such as for periodic audits, resolution of anomalies discovered during operation, assessment of safety system changes and their impact on safety system security so as to ensure that modifications do not introduce any security vulnerabilities.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Instrumentation/electronics or electrical engineers having experience in system development, analysis and modelling, system review, regulatory experience; – Reactor systems engineer, engineers with reactor operation and maintenance background; – Experts capable of failure modelling and probabilistic assessments, etc.
Specialised training, experience and/or education needed for the review of this topic.	Reviewers from the regulatory staff undergo formal training in reactor systems and subsequently in regulatory/safety review. Further the regulatory staff are trained in various review areas through participation in the safety review and regulatory inspection process. The other members of the review team are from the TSOs who are working in specialised areas.
Level of effort in each review area.	Resource estimation is done for various review areas but not on each specific technical category in a routine manner. The regulatory review is done following the overall guideline as provided in AERB safety guide No. AERB/SG/G-1 and G-7, where the time required for review during each stage of licensing is given. However, the Level of effort during the review varies in many cases depending on reactor type (standard design or FOAK), innovative or evolutionary design of systems, extent of use of computer based systems, etc.

Cybersecurity	Korea KINS
Design information provided by applicant.	– Structure of the I&C system and network interconnection; – I&C security policy and security plan.
Analysis, reviews and/or research performed by the reviewer and scope of review.	– Inspection of design information; – Onsite inspections.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	– KINS regulatory guidance 8.13; – KINS regulatory guidance 8.22, "cyber security of I&C system"; – (as a reference only) IEEE 1012, security analysis during software lifecycle.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: I&C engineer, computer engineer, nuclear engineer. – Junior: I&C engineer, computer engineer, nuclear engineer.
Specialised training, experience and/or education needed for the review of this topic.	Training: – Training programme on nuclear safety; – I&C platform specific trainings; – Software engineering (software quality, software life-cycle, software V&V) training; – Plant specific training; – Cybersecurity. Experience: – I&C (hardware, software); – Process and safety design; – Testing methods.
Level of effort in each review area.	– Regulator review: 120 working days.

Cybersecurity	Russia SEC NRS
Design information provided by applicant.	Issues related to information protection (cybersecurity) were and currently are beyond the competence of SEC NRS. However, it should be noted, that SEC NRS is developing regulations and rules, which will regulate the issues of information protection in the part of software for systems important to safety.
Analysis, reviews and/or research performed by the reviewer and scope of review.	At present, there is no review conducted for materials substantiating cybersecurity. It is planned that the review of materials substantiating information protection will be carried out to check for compliance with the requirements of the regulations and rules “Requirements to Software Applied in the Systems Important to Safety of NPPs”, which are being developed, and regulations and rules “Requirements to Control Systems Important to Safety of NPPs” (NP-006-98), which are being revised.
What type of confirmatory analysis (if any) is performed?	Currently, there is no review conducted for materials substantiating cybersecurity. It is planned, that an expert will carry out the review of materials substantiating cybersecurity to check them for compliance with the requirements of the regulations and rules “Requirements to Software Applied in the Systems Important to Safety of NPPs”, which are being developed, and regulations and rules “Requirements to Control Systems Important to Safety of NPPs” (NP-006-98), which are being revised.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	Federal regulations and rules: – “Requirements to Software Applied in the Systems Important to Safety of NPPs” (under development); – “Requirements to Control Systems Important to Safety of NPPs” (under revision). IEC standards: – IEC 62645 (draft). Nuclear Power Plants. Instrumentation and Control Systems. Requirements for Security Programmes for Computer-Based Systems.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	Industry-specific education in the part of I&C.
Specialised training, experience and/or education needed for the review of this topic.	Experience in development and operation of I&C.

Level of effort in each review area.	2-3 man-months (estimated value, no experience in such a review).

Cybersecurity	Slovakia UJD
Design information provided by applicant.	– Design basis; – Safety analysis; – Change control programme for all life cycle phases.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Review of the programme, its conformance with standards and guides.
What type of confirmatory analysis (if any) is performed?	–
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	–
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: electrical engineer. – Junior: electrical engineer. – TSO: electrical engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Digital I&C (hardware and software); – IT specialist.
Level of effort in each review area.	Review of the submitted design information is a part of approval process which is performed as an administrative procedure based on administrative proceeding code. Based on this act we have 60 days for approval of the submitted documentation. In case that we need more time (for example if we need review from TSO or the other support organisation) we can ask our chairperson about extending the period for approval. In some cases, which are strictly defined in the atomic act the time period for reviewing is longer. These cases are as follows: – Four months if siting of nuclear installation, except repository is concerned; – Six months if nuclear installation commissioning or decommissioning stage is concerned; – One year if building authorisation, siting and closure of repository or repeated authorisation for operation of a nuclear installation are concerned.

Cybersecurity	Slovenia SNSA
Design information provided by applicant.	– Cybersecurity programme; – Design basis; – Safety analysis.
Analysis, reviews and/or research performed by the reviewer and scope of review.	Review of the programme, its conformance with standards and guides.
What type of confirmatory analysis (if any) is performed?	Confirm that the licensee has deepened knowledge of its digital computer and communication systems and networks and those provisions are in place to protect the critical equipment and thus assure high reliability and dependability of computer and communication systems and networks.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	General aspects of design standards including: – IAEA, "Safety of Nuclear Power Plants: Design", Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012); – IAEA, "Site Evaluation for Nuclear Installations", Safety Standards Series No. NS-R-3, IAEA, Vienna (2003); – IAEA, "Format and Content of the Safety Analysis Report for Nuclear Power Plants - Safety Guide", Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004); – IAEA, "Safety Assessment and Verification for Nuclear Power Plants", Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001); – IAEA, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", Nuclear Security Series No. 4, IAEA, Vienna (2007); – IAEA, "Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants - Safety Guide", Safety Standards Series No. NS-G-1.9, IAEA, Vienna (2004). IAEA, "Software for Computer Based Systems Important to Safety", Safety Standards Series No.NS-G-1.1, IAEA, Vienna (2000).
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	– Senior: computer engineer, software engineer. – Junior: computer engineer, software engineer. – TSO: computer engineer, software engineer.
Specialised training, experience and/or education needed for the review of this topic.	– Digital I&C (hardware and software); – IT specialist; – Security and cybersecurity.
Level of effort in each review area.	– Regulator review: 80 hours. – TSO's review time: 160 hours.

Cybersecurity	Sweden SSM
Design information provided by applicant.	See High Level Summary.
Analysis, reviews and/or research performed by the reviewer and scope of review.	No review was carried out.
What type of confirmatory analysis (if any) is performed?	Assessments by licensee (incl. PSADR + FSAR).
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	SSM regulation: – SSMFS 2008:1; – SSMFS 2008:12; SSM general advice: – Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010, SSM Rapport 2010:01, Jan 2010.
Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	NAN.
Specialised training, experience and/or education needed for the review of this topic.	NAN.
Level of effort in each review area.	NAN.

Cybersecurity	United States U.S. NRC
Design information provided by applicant.	Along with the safety analysis report (SAR), the applicant should provide the following: – Cyber Security Plan (CSP).
Analysis, reviews and/or research performed by the reviewer and scope of review.	The nuclear regulatory commission (NRC) staff (1) review the information provided in the CSP for compliance with the regulations, (2) issues requests for additional information (RAIs) as necessary, (3) reviews RAI responses, (4) resolves technical issues with applicants or licensees, and (5) produces a safety evaluation report (SER) documenting its findings. The scope and level of detail of the staff's safety review is based on the guidance of NUREG-0800, Standard Review Plan (SRP). The sections of the SRP that are applicable to this area are as follows: – SRP 13.6.6, "Cyber Security Plan". The staff also considers emerging technical challenges (i.e. new cybersecurity threats), administrative (procurement) issues, operating experience and lessons learned related to this category.
What type of confirmatory analysis (if any) is performed?	There are no confirmatory analyses related to the staff's review of the Cyber Security Plan.
Technical basis: • **Standards** • **Codes** • **Acceptance criteria** **(e.g. can come from Accident analysis, regulatory guidance)**	The following NRC regulatory requirements are applicable to this category: – 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"; – 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabatoge"; – 10 CFR 73.58, "Safety/Security Interface Requirements for Nuclear Power Plants"; – 10 CFR 73, Appendix G, "Physical Protection of Plants and Materials". The NRC guidance documents that provide an acceptable basis for meeting the regulations and are applicable to this category are as follows: – Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities". Note: Guidance documents are not a substitute for regulations, and compliance with guidance documents is not required. In addition, NRC has determined that NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors" is also acceptable for use (as an alternate to RG 5.71). NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule", was also determined to be acceptable for use; however, the NRC provided caveats to the document's use in a letter dated July 27, 2012 (ML12198A198). The NRC has also published several Security Frequently Asked Question (SFAQ) documents to assist licensees and inspectors in implementing their programs.

Skill sets (education) required by: • **Senior (regulator)** • **Junior (regulator)** • **TSO.**	The review of any given CSP is performed by a team of staff. The organisation that reviews CSPs is comprised of a variety of skill sets – e.g. electrical engineers, instrumentation and controls engineers, and staff with information technology/cybersecurity accreditations and experience.
Specialised training, experience and/or education needed for the review of this topic.	All reviewers are required to have a thorough understanding of the NRC regulations and guidance for cybersecurity. Note: A licensee's cybersecurity programme (i.e. implementation of their CSP) is evaluated on a periodic basis via inspection by NRC staff. periodic inspection is considered a more effective method to evaluation adequate protection against cyber threats, as cyber threats will evolve over time. Inspectors who perform cybersecurity inspections are required to: – Be a qualified inspector; – Be knowledgeable of NRC regulations and guidance for cybersecurity; – Complete cybersecurity-specific training.
Level of effort in each review area.	80 hours (estimated – review time varies by the number of deviations an applicant takes from the standard cybersecurity plan template).