IAEA
International Atomic Energy Agency
Atoms for Peace and Development

Technical Meeting on the Software Reliability of Digital Instrumentation and Control Systems for Nuclear Power Plant Safety

IAEA Headquarters, Vienna, Austria
and virtual participation via Microsoft Teams

13–16 December 2022

Ref. No.: EVT2102726

Information Sheet

Introduction

Instrumentation and control systems (I&C) are a key element for the safe design, operation and management of nuclear power plants during all plant states. The functions allocated to the I&C systems include those functions that provide information and control capabilities relevant to operation of the plant in the various modes of operational states and in accident conditions. The objectives of these functions, corresponding to the concept of defence in depth, are to prevent the failure of one level of defence causing the failure of other levels. Indeed, equipment and components of I&C play a crucial role in plant operations with regard to safety by making possible the processing, calculation, transmission and display of physical plant parameters as well as commanding and controlling the actuation of plant equipment either by allowing manual intervention or by automatic regulation.

The analogue I&C, initially installed on operating nuclear power plants have been gradually replaced by digital I&C systems to provide control and protection functions. In addition, digital I&C is commonly used in all new nuclear power plant designs. Dependent on their functions and designs, digital I&C may incorporate an embedded software code or algorithm or even a computer-based software.

In many NPPs, programmable digital I&C systems are interconnected and more complex to analyse (and, thus, safety assurance is more difficult to demonstrate than was the case for earlier generations of I&C systems). Analysis of defence in depth and diversity is one of the means of investigating the vulnerability of I&C safety systems to common cause failure. The programmable digital systems may

depend upon software that is common to every division of the safety actuation. Software errors may lead to common cause failure in redundant digital systems if the same software is used in multiple redundancies. Thus, to estimate digital system reliability, it is necessary to estimate the probability of system failure due to hardware failure and software errors.

The choice for installing digital I&C is based on the clear advantages that digital I&C systems have compared to the analogue I&C by making easier regular operating activities such as the control and monitoring of equipment and component status, as well as their testing and maintenance. However, the failures that might result from software errors are difficult to predict. A demonstration that the final product is fit for its purpose depends greatly on the use of a high-quality development process that provides for disciplined specification and implementation of design requirements. Verification and validation activities are necessary for ensuring that the final product is suitable for use.

Objectives

The purpose of the event is to provide Member States with an opportunity to share experiences, practices and approaches related to ensuring the software reliability of programmable digital instrumentation and control systems important to safety for nuclear power plants.

It is expected that the outcomes from the meeting will contribute to the draft of the safety report capturing the experience in Member States regarding the implementation of solutions aiming at ensuring the reliability of the software used in programmable digital instrumentation and control systems important to safety for nuclear power plants.

Target Audience

The event is targeted at professionals from NPP design organizations, operating organizations, nuclear regulatory authorities, technical support organizations and research institutions who are engaged in activities related to or in support to the development and assessment of software reliability of digital instrumentation and control systems for nuclear power plants. Particular areas are listed in the Topics section, here below.

The event is open to representatives of all Member States with an active nuclear power programme, including those from embarking countries in Phase 3 of their nuclear programme.

Working Language(s)

English.

Expected Outputs

Participants will gain sound knowledge and a better understanding related to the difficulties at the design phase aiming at ensuring the required reliability of digital I&C systems for nuclear power plants. In addition, the participants will have opportunity to discuss various practices and approaches related to reliability determination for digital I&C systems. The information exchanged as well as the summary of the discussions will be compiled for the development of an IAEA publication on software reliability of digital instrumentation and control systems for nuclear power plants.

Topics

The event will address recent experiences in Member States to overcome difficulties as well as to promote solutions affecting the reliability of the software embedded in digital I&C systems for nuclear power plants, such as:

- Experiences in performing reliability analysis for programmable digital I&C systems, with particular focus on safety I&C systems:
    - Challenges and solutions;
    - Use of quantitative methods for reliability assessment of digital systems;
    - Use a qualitative approach for determining software reliability (i.e. based on strong requirements on the deterministic behaviour of the software to allow full verification and validation);
    - Consistency between the reliability requirements of the I&C systems and the probabilistic safety assessment by maintaining an explicit numerical reliability target for each I&C system important to safety.
- Software verification and analysis, such as:
    - Fault identification leading to potential errors in software embedded in programmable digital I&C and analysis of its propagation using analytical methods or testing;
    - Verification techniques:
        - Manual examinations such as reviews, walk-throughs, inspections and audits;
        - Static analysis of the source code;
        - Dynamic analysis.
    - Third party assessment
- Consideration of common cause failures:
    - Assessment of common cause vulnerabilities in safety I&C systems;
    - Applying diversification strategies to cope with potential common cause failures;
- Using probabilistic safety assessment in support of the design of digital I&C.

Participation and Registration

All persons wishing to participate in the event have to be designated by an IAEA Member State or should be members of organizations that have been invited to attend.

In order to be designated by an IAEA Member State, participants are requested to send the **Participation Form (Form A)** to their competent national authority (e.g. Ministry of Foreign Affairs, Permanent Mission to the IAEA or National Atomic Energy Authority) for onward transmission to the IAEA by **30 September 2022**. Participants who are members of an organization invited to attend are requested to send the **Participation Form (Form A)** through their organization to the IAEA by the above deadline.

Selected participants will be informed in due course on the procedures to be followed with regard to administrative and financial matters.

Papers and Presentations

The IAEA encourages participants to give presentations on the work of their respective institutions that falls under the topics listed above.

Participants who wish to give presentations are requested to submit an abstract of their work. The abstract will be reviewed as part of the selection process for presentations. The abstract should be in A4 page format, should extend to no more than two pages (including figures and tables) and should not exceed 1500 words. It should be sent electronically to Mr Jorge Luis Hernández, the Scientific Secretary of the event (see contact details below), not later than **30 September 2022**. Authors will be notified of the acceptance of their proposed presentations by **31 October 2022**.

In addition, participants have to submit the abstract together with the **Participation Form (Form A)** to their competent national authority (e.g. Ministry of Foreign Affairs, Permanent Mission to the IAEA or National Atomic Energy Authority) or their organization for onward transmission to the IAEA not later than **30 September 2022.**

IAEA Contacts

Scientific Secretary:

Mr Jorge Luis Hernández
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 VIENNA
AUSTRIA

Tel.: +43 1 2600 24568
Fax: +43 1 26007
Email: J.Luis-Hernandez@iaea.org

Administrative Secretary:

Ms Leticia Sedlazek
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 VIENNA
AUSTRIA

Tel.: +43 1 2600 22687
Fax: +43 1 26007
Email: L.Sedlazek@iaea.org

Subsequent correspondence on scientific matters should be sent to the Scientific Secretary and correspondence on other matters related to the event to the Administrative Secretary.

Event Web Page

Please visit the following IAEA web page regularly for new information regarding this event:

www.iaea.org/events/EVT2102726