Nuclear Energy Agency

NEA/CNRA/R(2018)2

Unclassified

English text only

9 August 2019

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

Consensus Position on Data Communication Independence for Nuclear Power Plants [CP-04]

This document is available as PDF only.

JT03450246

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 36 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

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

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

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission and the International Atomic Energy Agency also take part in the work of the Agency.

The mission of the NEA is:

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

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

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

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES (CNRA)

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

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

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

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

Foreword

This consensus position (CP) provides agreed-upon principles on data communication independence for digital instrumentation and control (I&C) systems. Digital I&C architectures may employ data communications between safety systems, between redundant portions of a safety system, and between systems of different safety classes. One of the more significant regulatory implications is maintaining data communication independence, thereby ensuring that faults from data communications do not propagate and adversely affect safety functions. Therefore, a consolidated set of design principles is necessary to maintain communication independence between safety systems, between redundant divisions of a safety system, and between systems of different safety classes. Although the focus of this consensus position is on data communication independence, the agreed-upon principles discussed herein may also apply to other forms of communications.

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

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

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

Table of contents

Acknowledgements **6**

List of abbreviations and acronyms **7**

Consensus Position on Data Commnication Independence for Nuclear Power Plants **8**

Executive Summary 8
Introduction 8
Definitions 9
Scope 10

Consensus Position on Data Communication Independence for Nuclear Power Plants **11**

Conclusions **13**

References **14**

Acknowledgements

The Nuclear Energy Agency (NEA) would like to thank the following Working Group on Digital Instrumentation and Control (WGDIC) member countries which participated in the development of this consensus position and endorsed its publication.

Canada:	Canadian Nuclear Safety Commission (CNSC)
China:	National Nuclear Safety Administration (NNSA)
Czech Republic:	State Office for Nuclear Safety (SÚJB)
Finland:	Finnish Centre for Radiation and Nuclear Safety (STUK)
France:	Nuclear Safety Authority (ASN) Institute for Radiological Protection and Nuclear Safety (IRSN)
India:	Atomic Energy Regulatory Board (AERB)
Japan:	Nuclear Regulation Authority (NRA)
Republic of Korea:	Korea Institute of Nuclear Safety (KINS)
Russian Federation:	Rostechnadzor, VO Safety
Sweden:	Swedish Radiation Safety Authority (SSM)
Spain:	Spanish Nuclear Safety Council (CSN)
United Kingdom:	Office for Nuclear Regulation (ONR)
United States:	United States Nuclear Regulatory Commission (USNRC)

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

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

The Institute of Electrical and Electronics Engineers (IEEE)

The International Electrotechnical Commission (IEC)

List of abbreviations and acronyms

CCF	Common cause failure
CNRA	Committee on Nuclear Regulatory Activities (NEA)
CP	Consensus positions
DI&C	Digital instrumentation and control
I&C	Instrumentation and control
IAEA	International Atomic Energy Agency
NEA	Nuclear Energy Agency
OECD	Organisation for Economic Co-operation and Development
PDD	Programmable digital device
WGDIC	Working Group on Digital Instrumentation and Control (NEA)

Consensus Position on Data Communication Independence for Nuclear Power Plants

Executive Summary

The Nuclear Energy Agency (NEA) Working Group on Digital Instrumentation and Control (WGDIC) has agreed that a consensus position to address principles on data communication independence is warranted given the increased reliance on digital instrumentation and control (I&C) systems, its safety implications and the need to develop a common understanding from the perspective of regulatory authorities. This action follows the WGDIC examination of the regulatory requirements of the participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) documents. The WGDIC proposes a consensus position based on its recent experience with the new reactor licensing reviews.

This consensus position addresses agreed-upon principles on data communication independence for digital I&C systems between safety systems, between redundant divisions of a safety system, and between systems of different safety classes. Although the focus of this consensus position is on digital I&C data communications, the principles discussed herein may also apply to other forms of communication. The principles discussed herein are not to be construed as a requirement or regulation; instead, they are intended to serve as a source of information to be used for developing clear and sufficient regulatory guidance for maintaining data communication independence.

Introduction

Digital I&C architectures may employ data communications between safety systems, between redundant portions of a safety system, and between systems of different safety classes. One of the more significant regulatory implications is maintaining not only physical and electrical independence but also data communication independence, thereby ensuring that faults from data communications do not propagate and adversely affect safety functions. Otherwise, fault propagation can lead to undesired behaviour of I&C systems, which could create hazards that challenge plant safety. Hazards may result from lost independence as a result of interconnectivity or functional relationships among digital I&C systems through their data communications. These hazards may be more difficult to identify and control because of system complexity, when the potential for faults and their impacts are considered. To effectively control such hazards, a consolidated set of design principles is necessary to maintain communication independence between safety systems, between redundant divisions of a safety system, and between systems of different safety classes,[1] thereby ensuring that faults from data communications do not propagate and adversely affect safety functions This consensus position provides agreed-upon principles on data communication independence for digital I&C systems. This consensus position also addresses data communication interfaces and buffering function for digital I&C systems.

1. Safety systems or redundant portions (e.g. divisions) within safety systems should be independent of each other to the extent necessary so as to ensure that all safety functions can be accomplished when required.

Definitions

Architecture: Organisational structure of I&C systems of the plant (Adapted from IEC 61513).

Buffering function: An interface between the communications link and the safety function (IEEE 7- 4.3.2-2016).

Channel: An arrangement of components and modules required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined (IEEE 603-2009).

Common cause failure (CCF): Failure of two or more structures, systems or components due to a single event or cause (IEC 61513-2011).

Communications: (1) The transmission of information from one point to another by means of electromagnetic waves. (2) The flow of information from one point, known as the source, to another, the receiver (Adapted from IEEE 100-2000).

Data: Representation of information or instructions in a manner suitable for communication, interpretation, or processing by computers (IEC 61513).

Data communication: Exchange of digital data between communication nodes via communication channels (IEC 61500).

Defect: A problem which, if not corrected, could cause an I&C component or system to either fail or to produce incorrect results (adapted from ISO/IEC 20926:2003).

Deterministic: Deterministic is a behaviour that any given input sequence that is within the specification of the item will always produce the same outputs and response times, i.e. the time delay between stimulus and response has a guaranteed maximum and minimum (Adapted from IAEA SSG39).

Division: The collection of items, including their interconnections that form one redundancy of a redundant system or safety group. Divisions may include multiple channels (IAEA SSG39).

Dual port memory: A set of registers (or memory) that are asynchronously accessible from each of two ports (or buses, in the context of a Bridge) without the requirement for arbitration on one bus while accessing the memory from the other bus (IEEE 1014.1-1994).

Fault: Defect in a hardware, software or system component (IEC 61513-2011). An error may lead to a fault, a fault may lead to a failure, and failure may lead to a hazard, and a hazard may lead to harm.

Failure: Loss of the ability of a structure, system, or component to function within acceptance criteria (Adapted from IAEA Safety Glossary, 2016).

Gateway: A device connecting two computer systems that usually use different protocols, or to connect two independent networks (IEEE 1046-1991).

Handshaking: The exchange of predetermined signals or control measures between two systems or system components upon initial exchanges. Note: When the connection is established, the two components acknowledge each other (IEEE 100-2000).

Hardwired: (1) Wired interconnections of relays and other control devices. (2) Pertaining to a circuit or device whose characteristics are permanently determined by the interconnections between components (Adapted from IEEE 100-2000).

Hazard: Potential source of harm (ISO/IEC Guide 51:2014, Definition 3.5).

Plausible: Not eliminated by justified and documented technical means (Generic Common Position DICWG-13: Common Position on Spurious Actuation or CP-13).

Programmable digital device (PDD): Any device that relies on software instructions or programmable logic to accomplish a function. Examples include a computer, a programmable hardware device, or a device with firmware (IEEE 7-4.3.2-2016).

Safety function: A specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions (IAEA Safety Glossary 2016).

Spurious actuation: Unintended operation by an I&C component or system (CP-13).

Scope

Data communication encompasses a wide range of technical solutions varying from simple hardware-only multiplexing to complex self-correcting and multilayer communication protocols controlled by software. Although the focus of this consensus position is on data communication independence, other forms of communications (e.g. hardwired) also need to be considered to address independence. The agreed-upon principles on data communication independence discussed herein may also apply to these other forms of communications. It is recognised that data communications may affect the cyber security of digital I&C systems; however, cyber security is not in the scope of this consensus position. The reader should refer to the "Generic Common Position DICWG-08: Impact of Cyber Security Features on Digital I&C Safety Systems", or CP-08, for information on this topic.

Consensus Position on Data Communication Independence for Nuclear Power Plants

1) General principles

   i. Data communication between safety systems, between redundant divisions of a safety system, and between systems of different safety classes should be designed so that plausible failures do not propagate and adversely affect safety functions.

   ii. The topology of any data communications network should be designed and implemented to avoid common cause failure (CCF) of systems important to safety (see Generic Common Position DICWG-09: Safety Design Principles and Supporting Information for the Overall I&C Architecture or CP-09).

2) Communication between safety systems and between redundant divisions of a safety system

   i. There should be communication independence established between safety systems and between redundant divisions of a safety system to the extent necessary to ensure that all safety functions can be accomplished when required.

   ii. Unnecessary communications between safety systems and between redundant divisions of a safety system should be avoided.

   If communications between safety systems or between redundant divisions of a safety system are proposed, the following principles then apply:

   iii. A documented technical basis should be provided for all communications between safety systems or between redundant divisions within a safety system (e.g. data communications to support voting may be necessary to meet the single failure criterion or prevent spurious actuation).

   iv. Where communications between safety systems or between redundant divisions of a safety system are necessary, then there should be sufficient measures to ensure that:

      a. No plausible failures from the transmitting system should be propagated to the receiving system, thereby inhibiting a safety function.

      b. Consequences from unexpected behaviour (e.g. data storm/avalanche) from data communications should not adversely affect the safety function. For example, a means to avoid the unexpected behaviour is to have designs that have a fixed amount of data communicated regardless of the plant process conditions.

      c. Delays in communication should not impact the performance of the safety function. For example, asynchronous communication without acknowledgement is one acceptable approach to avoid delays.

3) Communication between systems of different safety classes

   i. Where communications between systems of different safety classes are necessary, then the communication flow should be from the higher to the lower safety class systems.

ii. Communications from lower- to higher-class systems should be avoided.

iii. If communications from lower- to higher-class systems are proposed, a documented technical basis should be provided [2] to demonstrate it does not adversely affect safety.

iv. Communications between higher and lower safety class systems should be designed so that no plausible failures in the systems of the lower safety class will prevent any connected higher-class system from accomplishing its safety functions. One method to avoid failure propagation is to restrict data flow between systems using hardwired connections or communication gateways. Additional methods could include unidirectional communication (e.g. data diode), error detection and transfer restrictions on data volume (quantity and data type).

4) Data communication interfaces and buffering function

i. PDDs that perform safety functions (e.g. safety function processors) should perform no communications handshaking or interruptions that could disrupt deterministic safety function processing.

ii. The buffering function (e.g. separate communications processor) that performs the communications should be of the same classification as the PDD that performs the safety function.

iii. The data communication interface should be designed so that the data in the buffering function is correct when the safety function uses it.

iv. The buffering function should ensure that faults and failures on communications originating externally do not propagate to the PDDs performing the safety function. Specifically, the safety processing should be independent from the communications processing. One implementation method could be the use of dual ported memory to facilitate the independence between the safety processing and the communication processing. Other implementation methods could include: 1) for a computer-based PDD, the safety function processor operating asynchronously from the communication processor (buffering function); and 2) for a non-computer-based PDD (e.g. Field Programmable Gate Array), allocating the communication function and the safety function in separate logic circuits within the same PDD.

2. It is recognised that different countries use different classification schemes; regardless, in all cases, data communications from lower-classified systems to higher-classified systems should be avoided.

Conclusions

While there may be different approaches for maintaining data communication independence, the WGDIC concludes that the agreed-upon principles herein represent an effective and technically viable approach. This conclusion is based on the collective scientific and technical knowledge and experience of the WGDIC members that was brought together to develop this consensus position (CP). As such, this CP represents the common understanding from the WGDIC members and harmonisation of regulatory practices related to data communication independence.

In support of the continual evolution of digital instrumentation and control technology and its associated challenges, the WGDIC will continue to assess any gaps not being addressed by contemporary regulations and guidance related to data communication independence. Future revisions to this CP will allow bridging those gaps while ensuring its relevance and technical adequacy.

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

References

1. IAEA (2016) - SSG-39, "Design of Instrumentation and Control Systems for Nuclear Power Plants"
2. IAEA (2016)- Safety Glossary, "Terminology used in nuclear safety and radiation protection"
3. IEC 60709 (2018), "Instrumentation and Control Systems Important to Safety – Separation"
4. IEC 61226, (2009) "Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions"
5. IEC 61500 (2018), "Instrumentation and Control Important to Safety – Data Communication in Systems Performing Category A Functions"
6. IEC 61513 (2011), "Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", Ed2
7. IEEE Std 100 (2000), "The Authoritative Dictionary of IEEE Standards Terms"
8. IEEE Std 603 (2009), "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
9. IEEE 1014.1 (1994), "IEEE Standard for Futurebus+/VME64 Bridge"
10. IEEE 1046 (1991), "IEEE Application Guide for Distributed Digital Control and Monitoring for Power Plants"
11. IEEE 7-4.3.2 (2016), "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations"
12. ISO/IEC 20926 (2003), "Software and system engineering – Software measurement – IFPUG functional size measurement method"
13. ISO/IEC Guide 51 (2014), "Safety aspects – Guidelines for their inclusion in standards"
14. MDEP (2012), Generic Common Position DICWG No. 8: Common Position on the impact of cyber security features on digital I&C safety systems actuation, 2012
15. MDEP (2015), Generic Common Position DICWG No. 9: Common Position on safety design principles and supporting information for the overall I&C architecture,
16. MDEP (2017), Generic Common Position DICWG No. 13: Common Position on spurious actuation,
17. TF-SCS (2018), Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations