Nuclear Energy Agency

NEA/CNRA/R(2021)2

Unclassified

English text only

3 November 2022

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants [CP-08]

This document is available in PDF format only.

JT03506540

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES (CNRA)

The Committee on Nuclear Regulatory Activities (CNRA) addresses NEA programmes and activities concerning the regulation, licensing and inspection of nuclear installations with regard to both technical and human aspects of nuclear safety. The committee constitutes a forum for the effective exchange of safety-relevant information and experience among regulatory organisations. To the extent appropriate, the committee reviews developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them and assist in the development of a common understanding among member countries. In particular, it reviews regulatory aspects of current safety management strategies and safety management practices and operating experiences at nuclear facilities including, as appropriate, consideration of the interface between safety and security with a view to disseminating lessons learnt. In accordance with *The Strategic Plan of the Nuclear Energy Agency: 2023-2028*, the committee promotes co-operation among member countries to use the feedback from experience to develop measures to ensure high standards of safety, to further enhance efficiency and effectiveness in the regulatory process, and to maintain adequate infrastructure and competence in the nuclear safety field.

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

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

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

Acknowledgements

The Nuclear Energy Agency (NEA) would like to thank the following member country participants of the Working Group on Digital Instrumentation and Controls (WGDIC) for their input in the development of this consensus position and endorsement of 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:	Autorité de sûreté nucléaire (ASN), Institut de radioprotection et de sûreté nucléaire (IRSN)
Germany:	Federal Office for the Safety of Nuclear Waste Management (BASE)
Hungary:	Hungarian Atomic Energy Authority (HAEA)
India:	Atomic Energy Regulatory Board (AERB)
Japan:	Nuclear Regulation Authority (NRA)
Netherlands:	Authority for Nuclear Safety and Radiation Protection (ANVS)
Poland:	Office of Technical Inspection (UDT)
Russian Federation:	Rostechnadzor, VO Safety
Spain:	Nuclear Safety Council (CSN)
Korea:	Korea Institute of Nuclear Safety (KINS)
Sweden:	Swedish Radiation Safety Authority (SSM)
United Kingdom:	Office for Nuclear Regulation (ONR)
United States:	United States Nuclear Regulatory Commission (US NRC)

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 partners, in the development of this consensus position.

IEC	International Electrotechnical Commission
IEEE NPEC	Institute of Electrical and Electronics Engineers Nuclear Power Engineering Committee

Table of contents

List of abbreviations and acronyms **6**

Executive summary **7**

1. Introduction **8**

2. Definitions **9**

3. Scope **10**

4. Consensus position on the impact of cyber security features on digital I&C systems important to safety **11**

5. Conclusions **14**

References **15**

List of abbreviations and acronyms

AERB	Atomic Energy Regulatory Board (India)
ANVS	Authority for Nuclear Safety and Radiation Protection (Netherlands)
ASN	Autorité de sûreté nucléaire (France)
BASE	Federal Office for the Safety of Nuclear Waste Management (Germany)
CNRA	Committee on Nuclear Regulatory Activities (NEA)
CNSC	Canadian Nuclear Safety Commission
CP	Consensus position
CPLD	Complex programmable logic devices
CSN	Nuclear Safety Council (Spain)
FPGA	Field programmable gate arrays
HAEA	Hungarian Atomic Energy Authority
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers (United States)
IP	Intellectual property
I&C	Instrumentation and control
IRSN	Institut de radioprotection et de sûreté nucléaire (France)
KINS	Korea Institute of Nuclear Safety
NEA	Nuclear Energy Agency
NNSA	National Nuclear Safety Administration (China)
NPEC	Nuclear Power Engineering Committee (IEEE)
NRA	Nuclear Regulation Authority (Japan)
ONR	Office for Nuclear Regulation (United Kingdom)
SSM	Swedish Radiation Safety Authority
STUK	Finnish Centre for Radiation and Nuclear Safety (Finland)
SÚJB	State Office for Nuclear Safety (Czech Republic)
UDT	Office of Technical Inspection (Poland)
US NRC	United States Nuclear Regulatory Commission
WGDIC	Working Group on Digital Instrumentation and Controls (NEA)

Executive summary

The Nuclear Energy Agency (NEA) Working Group on Digital Instrumentation and Controls (WGDIC) has agreed that a consensus position on the impact of cyber security features on digital instrumentation and control (I&C) systems important to safety is warranted given the increased use of I&C in new reactor designs and upgrades on operating plants, the safety implications of this use, and the need to develop a common understanding from the perspective of regulatory authorities. This action follows the WGDIC's examination of the regulatory requirements of its participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) publications. The WGDIC proposes a consensus position based on its recent experience with new reactor applications and operating plant experiences.

This consensus position provides evaluation guidance for ensuring that safety functions and cyber security features for digital I&C systems important to safety at nuclear power plants are designed and implemented so that they do not adversely affect one another. The guidance herein is not to be interpreted as a requirement or regulation; instead, it is intended to serve as a source of information to be used to develop clear and sufficient regulatory guidance to assess safety features and cyber security features for digital I&C systems important to safety.

1. Introduction

Cyber security features and safety functions are implemented in digital I&C systems at nuclear power plants to protect against cyberattacks and protect the plant from postulated initiating events, respectively, that could compromise safety. Specifically, cyber security features are implemented to protect digital I&C systems against unauthorised access. The safety functions and cyber security features should be designed and implemented to prevent them from compromising one another.

This consensus position provides guidance for achieving such an objective for digital I&C systems important to safety at nuclear power plants. Nonetheless, the implementation of such cyber security features and safety functions can vary based on site-specific requirements and each country's regulatory framework(s).

It should be noted that security can be compromised through supply chains, which are getting longer, more complex and more difficult to control. Therefore, consideration should be given to applying the consensus positions discussed herein to hardware and software used along the supply chain that can affect the ability of components to perform their safety functions. This includes items on which the supply chain products and services depend as well as items used by contractors, vendors, technical support organisations and any other service provider. Relevant supply chain activities include software upgrades, patching, analysis using external tools, testing, system modifications and transportation.

2. Definitions

Cyberattack: attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset. Cyberattacks include targeted and non-targeted (e.g. malware) attacks by digital means (IEC 62859, 2019).

Cyber security feature: provision, control, or function specifically designed for cyber security purposes (IEC 62859, 2019).

Cyber security: seeks to prevent unauthorised access to information, software and data in order to ensure that the following three attributes are met:

- the prevention of disclosure of, or access to, information that could be used to perform malicious or misguided acts that could lead to an accident, an unsafe situation or plant performance degradation (confidentiality);
- the prevention of unauthorised modifications that degrade a safety function (integrity);
- the prevention of unauthorised withholding of information, data or resources that could compromise the performance of a safety function (availability)[1].

Control of access: the administrative control of access to safety system equipment, supported by provisions within the safety systems (access controls), by provision in the plant design (physical security) or by a combination thereof ([IEC 62859, 2019] and [IEEE Std. 7-4.3.2, 2016]).

Security degree: gradation of the security protection, with associated sets of requirements, that is assigned to a system according to the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance (IEC 62645, 2016).

Threat: potential cause of an unwanted incident that may result in harm to a system or organisation (IEC 62645, 2016)[2].

Security zone: concept for grouping computer-based I&C systems for administration, communication and application of protective measures (IEC 62645, 2016).

---

1 Adapted from reference (IEC 62859, 2019) and from the regulators task force on safety critical software report

2. Threats can involve items on which the safety function depends (components, supply chain and supporting systems or components). These threats use a variety of techniques such as:
   a. unauthorised access through items on which the safety function depends;
   b. unauthorised influence (such as provision of false information);
   c. unauthorised access or modification through supporting activities;
   d. other techniques identified by the licensee and/or the regulatory authority.

3. Scope

This consensus position is intended to apply to all hardware and software digital I&C systems important to safety. In this context, hardware includes industrial digital devices of limited functionality, for example, while software includes firmware and logic in any form, including supporting data; this includes, but is not limited to application, operational and pre-existing software and software tools, intellectual property (IP) cores, field programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs), network equipment, and items intended for non-safety purposes with the potential to interfere with safety systems.

4. Consensus position on the impact of cyber security features on digital I&C systems important to safety

1. All items within the scope of this consensus position should be explicitly identified in order to fully apply this consensus position.
2. Cyber security features should not adversely impact the required performance, effectiveness, reliability or operation of safety functions.
3. Where cyber security features need to be implemented in displays and controls for digital I&C systems important to safety, they should not adversely impact the operating personnel's ability to maintain the safety of the plant.
4. Cyber security requirements and safety requirements should be developed in a co-ordinated manner for the system under development throughout its lifecycle. This co-ordination should include, but not be limited to, safety and cyber security demonstration, roles and responsibilities, policies, processes and procedures, plans, assurance, and the management and content of operational and maintenance procedures.
    a) Avoiding designs that will be difficult or impossible to adequately protect after their implementation.
    b) Avoiding new cyber security requirements later in the system development lifecycle, since they could introduce unintended consequences or vulnerabilities.
5. Requirements, including constraints, should be specified and controlled for cyber security features throughout the life cycle (including system recovery) to protect against credible threats with the potential to degrade a safety function, based on the consequences of a successful cyberattack. Since security is continuously evolving, the effect on safety of any changes in cyber security features, including new security requirements, should be continuously evaluated.
6. Cyber security requirements and safety requirements should be verified and validated throughout the lifecycle, thereby providing assurance that both are implemented and co-ordinated correctly.
7. Cyber security features for digital I&C systems important to safety should be carefully evaluated and technically justified. This evaluation should assess whether the gain in security from the features is worth any increase in complexity in the system, as well as accounting for any potential new failure modes that could be introduced due to the addition of cyber security features.
8. To the extent feasible, digital I&C systems important to safety should not include design features that create vulnerabilities to known cyber threats. When included, these design features must offer a clear safety benefit and take into account compensating measures to mitigate any resulting vulnerability.

9. A cyber security feature, when activated, should not inhibit, override or deactivate safety functions. For example, an antivirus software could unintentionally block or hinder the functionality of a digital I&C system important to safety.

10. Cyber security features protecting digital I&C systems important to safety should be developed and/or qualified to the same level of safety classification as the system these features secure. If not, evidence should be presented that the cyber security features cannot adversely affect the safety function. Any cyber security aspects not addressed during the digital I&C platform qualification need to be addressed during the system implementation (see CP-14 for definitions and the consensus position on the qualification of I&C platforms for use in systems important to safety).

11. The architecture of digital I&C systems important to safety should support both safety and cyber security objectives. Examples in the field of communications include:

    a) Data transmission between systems of different safety classes (see CP-04 for the consensus position on data communications independence) and security degrees should meet the constraints imposed by the respective standards in each field for different countries[3].

    b) Secure control of communication pathways between a digital I&C system important to safety and any system external to the I&C architecture (e.g. the enterprise network) should be established.

12. Potential cyber security vulnerabilities should be considered for all software and hardware and in all lifecycle stages, including system operation, maintenance and modification. Vulnerabilities can result from operational and resource requirements imposed by the safety systems/functions, but also, for example, from a poor development process, from inadequate application of pre-developed software or from infection with malware. All known vulnerabilities should be analysed using a graded approach and mitigated either through eliminating the vulnerability or by requiring adequate protection.

13. Security testing and analysis should be performed as part of qualification to identify if vulnerabilities are present in the system (e.g. fuzz testing of communication protocols, source code analysis). This should be done in the appropriate stage of design or qualification and as early as possible. Any security testing from installation onwards that could impact safety should be avoided.

14. Requirements, including constraints, should be formulated to protect against intrusion or unauthorised modification during supporting activities such as testing, calibration (including update of calibration data), configuration, modification, loading software, other maintenance activities, and documenting the associated management activities. Examples of requirements include:

    a) restricting modes and/or times of use;

3. It is recognised that there are different categories and requirements for safety and security and that they can be in conflict. Resolution of any conflict should be technically justified.

b) restricting or limiting access during the development, testing, use, and modifications of software development;

c) protecting communication content;

d) checking the software integrity (e.g. comparing software or data against its original source, stored independently);

e) limiting interfaces and interactions;

f) preventing unauthorised modifications;

g) protecting boundaries between different security zones, by both logical and physical means;

h) appropriately assessing procedures and equipment for transportation.

15. Physical, logical, and administrative control of access to digital I&C systems important to safety should be included in the design (e.g. password or key lock access), while ensuring that it does not adversely impact the required performance, effectiveness, reliability or operation of safety functions.

16. Maintenance and operational procedures should contain instructions for removing the cyber security controls, applying any alternate cyber security controls, re-establishing the cyber security controls following maintenance, and confirming that the cyber security controls are effectively back in service (e.g. through post maintenance activities such as testing), as necessary.

17. Any event tracking, monitoring and reporting process should also include events concerning adverse interactions between security and safety. Operating experience of cyber security features can provide valuable insight and should be taken into account when applying this consensus position.

18. Cyber security training should consider the appropriate level of knowledge, skills and experience to ensure that safety functions and cyber security features do not adversely affect one another.

5. Conclusions

While there are different approaches to ensuring that safety functions and cyber security features for a nuclear power plant are designed and implemented so that they do not compromise one another, the WGDIC concludes that the agreed CPs herein represent a set of regulatory consensus positions on the topic.

In support of the continual evolution of digital I&C technology and its associated challenges, the WGDIC will continue to assess whether there are gaps in contemporary regulations and guidance related to the impact of cyber security features on digital I&C systems important to safety. Future revisions to this CP will allow the bridging of those gaps while ensuring the relevance and technical adequacy of the CP.

Any enquiries associated with this CP should be directed to the NEA via the WGDIC website[4].

4. www.oecd-nea.org/jcms/pl_21460.

References

IAEA (2011), "Computer Security at Nuclear Facilities", Nuclear Security Series No. 17, International Atomic Energy Agency, Vienna.

IAEA (2016), "Design of Instrumentation and Control Systems for Nuclear Power Plants", Specific Safety Guide No. SSG-39, International Atomic Energy Agency, Vienna.

IAEA (2018), "Computer Security of Instrumentation and Control Systems at Nuclear Facilities", Nuclear Security Series No. 33-T, International Atomic Energy Agency, Vienna.

IEC (2006), "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions", IEC 60880, Second Edition, Switzerland.

IEC (2011), "Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", IEC 61513, Second Edition.

IEC (2014), "Nuclear Power Plants Instrumentation and Control Systems – Requirements for Security Programs for Computer-based Systems", IEC 62645, Second Edition.

IEC (2018a), "Nuclear Power Plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions", IEC 62138, Switzerland.

IEC (2018b), "Nuclear Power Plants - Instrumentation and control systems important to safety – Data communication in systems performing category A functions", 61500.

IEC (2019), "Amendment 1 - Nuclear Power Plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity", IEC 62859:2016/AMD1:2019.

IEEE (2016), IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Station, IEEE Std. 7-4.3.2.

IEEE (2018), IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std. 603.

ISO/IEC (2015), Information technology – Security techniques – Network security part 1: network security overview and concepts, ISO/IEC 27033-1.

NEA (2019a), "Consensus Position on Data Communication Independence for Nuclear Power Plants (CP-04) ", NEA/CNRA/R(2018)2, OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_19870.

NEA (2019b), "Consensus Position on the Qualification of I&C Platforms for Use in Systems Important to Safety [CP-14]", NEA/CNRA/R(2018)3, OECD Publishing, Paris, www.oecd-nea.org/jcms/pl_19884.

TF SCS (2018), "Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations".

US NRC (2010), "Cyber Security Programs for Nuclear Facilities", Regulatory Guide 5.71.

US NRC (2011), "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", Regulatory Guide 1.152.