

Report

Interfaces between Nuclear Safety and Nuclear Security

10 April 2019

Table of Content

Interfaces between Nuclear Safety and Nuclear Security

01	Introduction	3
02	Objective and methodology	4
03	Interfaces between Nuclear Safety and Nuclear Security	6
04	Conclusion	15

01 Introduction

—

During their plenary meeting in April 2017, WENRA members decided to create a Task Force, to include nuclear safety and nuclear security experts, in order to identify challenging interface issues and areas of cooperation between nuclear safety and nuclear security. The interface between nuclear safety and nuclear security is an important aspect for nuclear regulators. A mandate for this Task Force was drafted by the Technical Secretariat of WENRA. According to the mandate, the Task Force should bring together nuclear safety and nuclear security experts and identify existing interfaces between nuclear safety and nuclear security for nuclear power plants (NPP) in operation as well as potential issues of a safety-security-interface.

ENSRA (European Nuclear Security Regulators Association) endorses this report as a positive step in cooperation between WENRA and ENSRA.

02

Objective and methodology

—

Nuclear safety and nuclear security measures have in common the aim of protecting human life and health and the environment from the harmful effects of ionizing radiation. Thus, both must be designed and implemented in an integrated manner to ensure security measures do not compromise nuclear safety and nuclear safety measures do not compromise security. If there are interactions between nuclear safety and nuclear security functions of technical systems, organizational and administrative measures including plant procedures in a NPP in operation and within or between regulatory authorities, it is called an “interface between nuclear safety and nuclear security” within the scope of this document.

To identify potentially relevant interactions of the interface between nuclear safety and nuclear security with a level of detail comparable to the level of detail given by WENRA Safety Reference Levels for Existing Reactors, the following tasks have been performed:

- (1) Identification of national and international nuclear safety regulations where an interface with nuclear security is present. On an international level, IAEA standards have been used as source of information.
- (2) Identification of national and international security regulations where an interface with nuclear safety is present. On an international level, IAEA standards have been used as source of information.
- (3) Evaluation of national and international experiences related to nuclear safety if an interface with nuclear security was identified. On an international level IRS and INES ≥ 2 events have been evaluated.
- (4) Evaluation of national experiences related to nuclear security if an interface with nuclear safety was identified.
- (5) Identification of further sources of information with relevant input for the Task Force, e.g. results of activities performed by technical support organizations or other relevant authorities dealing with the interface between nuclear safety and nuclear security.

This non-classified report documents the results of the WENRA Task Force on the interface between nuclear safety and nuclear security. The interfaces identified with the previously introduced approach are described below. This report includes guidance for work in the field of nuclear safety or nuclear security to be aware of and take into consideration the effects of potential interfaces. Interfaces between nuclear safety and nuclear security are also relevant to consider for the licensee, competent authorities and for other stakeholders (e.g. technical support organizations). In addition it is intended to highlight the common aim of nuclear

safety and nuclear security and to strengthen the arguments for nuclear safety and nuclear security experts to work together to achieve this aim.

03

Interfaces between Nuclear Safety and Nuclear Security

—

To identify interfaces between nuclear safety and nuclear security the methodology described above was used. In the following sections of this report, the identified interfaces between nuclear safety and nuclear security are described, sorted according to their related WENRA Safety Reference Level for Existing Reactors:

Interface	Related WENRA Safety Reference Level for Existing Reactors
01 Communication, Transparency and Confidentiality	Issue A "Safety Policy"
02 Independent Assurance and Oversight Functions	Issue B "Operating Organisation"
03 Integrated Management System	Issue C "Management System"
04 Organizational Culture	Issue C "Management System"
05 Staff Qualification and Training	Issue D "Training and Authorization of NPP Staff (Jobs with Safety Importance)"
06 Site Area	Issue E "Design Basis Envelope for Existing Reactors"
07 Requirements for Nuclear Safety and Nuclear Security Measures	Issue E "Design Basis Envelope for Existing Reactors"
08 Requirements for IT-Systems related to Nuclear Safety and Nuclear Security	Issue E "Design Basis Envelope for Existing Reactors"
09 Systems, Structures and Components	Issue G "Safety Classification of Structures, Systems and Components"
10 Feedback from Operating Experience and Plant Modification	Issue B "Operating Organisation" Issue Q "Plant Modification"
11 On-site Emergency Response	Issue R "On-Site Emergency Preparedness"
12 Zones, Access and Escape Routes	Issue S "Protection against Internal Fires"
13 Regulatory Framework	

Aim of Nuclear Safety and Nuclear Security Measures

Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment from the harmful effects of ionizing radiation. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and ensure that security measures do not compromise safety and vice versa.¹

Interface 01 – Communication, Transparency and Confidentiality

Transparency and confidentiality are issues when communicating where nuclear safety and nuclear security have differences. Nevertheless exchanging information is important to improve nuclear safety as well as nuclear security.

- (1) Transparency and information exchange promote nuclear safety. Operating experience assessment are based on detailed information about observed incidents, accidents, failure mechanisms etc.
Nuclear security primarily relies on the confidentiality of security measures (e.g. numbers of security personnel, response times of security forces and postulated scenarios). Therefore, information exchange about these topics is primarily restricted and limited to a select group of individuals to ensure that this knowledge cannot be exploited for malicious purposes. Nevertheless, also in nuclear security it is very important for the licensees as well as the regulators and other competent authorities to share information and to learn from experiences to prevent similar incidents.

Guidance:

When communicating about the interface between nuclear safety and nuclear security the topic transparency vs. confidentiality constitute an important issue.² Transparency may also promote e.g. public confidence, but release of information should be done in a measured way. A process to identify, control and protect sensitive information should be in place.³

¹ based on IAEA NSS No. 20, Nuclear Security Fundamentals "Objective and Essential Elements of a State's Nuclear Security Regime", 2013 similar to IAEA GSR Part 1 "Governmental, Legal and Regulatory Requirements for Safety"

² based on IAEA INSAG-23 "Improving the international System for Operating Experience Feedback" and IAEA INSAG-24 "The Interface between Safety and Security at Nuclear Power Plants"

³ WENRA Task Force – Meeting on March 6th 2018

Interface 02 – Independent Assurance and Oversight Functions

The objective for the licensee is to ensure that the plant is operated in a safe and secure manner and in accordance with all applicable legal and regulatory requirements.⁴ Regarding this interface, nuclear safety and nuclear security have the following in common:

- (1) Accountabilities, responsibilities, authorities, and lines of communication should be clearly defined and documented for all staff with duties important to nuclear safety and/or nuclear security.⁵
- (2) There should be independent assurance and oversight functions for nuclear safety and nuclear security within the licensee organization. There should be a clear mandate for these functions from the top management.⁶

Guidance:

A process for the independent assurance and oversight functions should be in place and it should include a means to identify and resolve any conflicts between nuclear safety and nuclear security.

Interface 03 – Integrated Management System

Nuclear safety and nuclear security have the following in common:

- (1) The management system should include all the elements of management to ensure processes and activities that may affect the way nuclear safety or nuclear security are addressed in an integrated manner.⁷

Interface 04 – Organizational Culture

There are differences between nuclear safety and nuclear security in regards of focus, approaches and language used. This is partly explained by the difference in technical training and professional experiences that exists amongst the experts in the two disciplines.

- (1) A good organizational culture should cover all relevant aspects of nuclear safety and nuclear security, fostering an approach that integrates safety and security in a mutually supporting manner. Leadership is key element to achieve an organizational culture promoting nuclear safety and nuclear security.⁸

⁴ based on WENRA RL B2.1

⁵ based on WENRA RL B1.3

⁶ WENRA Task Force – Meeting on March 6th 2018

⁷ based on IAEA SSR-2.2 "Safety of Nuclear Power Plants: Commissioning and Operation"

⁸ based on FI Guide YVL A.11 Security of a nuclear facility

- (2) The licensee should also give personnel the opportunity to comment and make suggestions for practical, effective alternatives in the case of measures that particularly affect the personnel and the organization of the plant.⁹
- (3) It is essential that any possible conflicts between the needs of nuclear safety and nuclear security are appropriately identified and addressed within the organization's culture in a prompt manner.¹⁰

Combined training or the use of joint assessment teams covering nuclear safety and nuclear security experts are useful to develop a common understanding.

Guidance:

In this context, the creation of a common understanding of the interfaces between nuclear safety and nuclear security is essential.¹¹

Interface 05 – Staff Qualification and Training

Nuclear safety and nuclear security have the following in common:

- (1) All personnel should be suitably qualified and experienced to comply with relevant aspects of both nuclear safety and nuclear security regimes.¹²

Guidance:

Roles, responsibilities and accountability for each level of the organization should be clearly defined and supported by effective training.¹³

Interface 06 – Site Area

Selection and design of the site area of a nuclear power plant has implications for nuclear safety as well as nuclear security.

- (1) Design of the site area layout should be appropriate considering the facility's nuclear and radiation safety, emergency preparedness and rescue arrangements as well as nuclear security.¹⁴

⁹ based on UK ONR Security Assessment Principles and German Guideline for the protection of nuclear power plants with light-water reactors against malicious acts, restricted, 1995

¹⁰ based on UK ONR Security Assessment Principles

¹¹ WENRA Task Force – Meeting on March 6th 2018

¹² based on German Guideline for the protection of nuclear power plants with light-water reactors against malicious acts, restricted, 1995

¹³ WENRA Task Force – Meeting on March 6th 2018

¹⁴ based on FI Guide YVL B.7 Provisions for internal and external hazards at a nuclear facility
WENRA Interfaces between Nuclear Safety and Nuclear Security

- (2) The impact of local conditions on nuclear safety and on the implementation of the nuclear security and emergency arrangements should be considered when selecting the site of a nuclear power plant. The site should be such that the impediments and threats posed by the plant to its vicinity remain extremely small and heat removal from the plant to the environment can be reliably implemented.¹⁵

Interface 07 – Requirements for Safety and Security Measures

Previously the design of nuclear power plants focused mainly on nuclear safety aspects. Nuclear security was generally addressed as a separate topic. However, nuclear safety provisions alone will not always be sufficient to ensure that possible consequences of malicious acts are mitigated. Below, some important examples of interface aspects are discussed.

a. Nuclear Safety and Nuclear Security Measures

- (1) Nuclear safety and nuclear security have in common that all equipment that is necessary for shutting the reactor down safely, for maintaining it in shutdown condition, for removing the residual heat or for preventing a release of radioactive materials should be designed and maintained in such a condition that their safety-related functions are also fulfilled in the case of internal and external hazards including malicious acts.¹⁶
- (2) Several well established concepts in nuclear safety like defense-in-depth, use of multiple barriers and redundancy or spatial separation promote nuclear safety as well as nuclear security. A well designed containment can serve as a barrier against both accidental (e.g. tornado missiles) and malicious (e.g. deliberate airplane crash) events. A safety system with a sufficient degree of redundancy and strict spatial separation accompanied by access controls serves both as a protection against safety related issues like fire or flooding as well as security related issues like an insider threat.¹⁷
- (3) Additional nuclear security measures should be implemented to address vulnerabilities that cannot be mitigated by safety-related design alone to ensure the requisite protection against malicious acts.¹⁸ Implications for nuclear safety, e.g. accessibility for operative personnel during a safety-related event, should be considered when implementing these measures.

b. Joint Assessments and Vital Area Identification

- (1) Nuclear safety and nuclear security specialists should together evaluate the consequences of malicious acts, given by the State's design basis threat, and identify the necessary equipment, systems or devices that should be protected. Measures

¹⁵ based on FI Radiation and Nuclear Authority Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2016) and Guide YVL A.11 Security of a nuclear facility

¹⁶ German Safety Requirements for Nuclear Power Plants, 2015

¹⁷ based on IAEA SSR-2.1 "Safety of Nuclear Power Plants: Design"

¹⁸ based on German Guideline for the protection of nuclear power plants with light-water reactors against malicious acts, restricted, 1995

that have been designed into the facility for nuclear safety purposes should be taken into account for this purpose.¹⁹

- (2) The information about the nuclear security measures for the protection of the facility and its operation against malicious acts should be presented in a security concept. The security concept should also indicate those safety-related measures that serve at the same time for the necessary protection against malicious acts.²⁰

Guidance:

A 'security by design' philosophy should be adopted to ensure security measures are considered and implemented at the earliest stages of design or plant modification to avoid post design security modifications and ensure there is no conflict with safety requirements.

Interface 08 – Requirements for IT-Systems related to Nuclear Safety and Nuclear Security

IT-systems are implemented in the design of existing nuclear power plants.

- (1) In the design of computer based systems important to nuclear safety and nuclear security, appropriate cyber security measures should be incorporated.
- (2) Cyber security should be integrated into existing concepts for the nuclear safety and nuclear security of the facility in such a way that the effectiveness of the nuclear safety systems and nuclear security systems is not impaired.²¹
- (3) The licensee should develop and test cyber event response, and disaster recovery arrangements to demonstrate the ability to maintain nuclear safety and nuclear security and facilitate a rapid and effective response to, and recovery from cyber security incidents.²²

Guidance:

I&C specialist should work together with cyber security specialists to create a common understanding and ensure the technology is resilient to cyber security incidents.

Interface 09 – Systems, Structures and Components

- (1) The classification of systems, structures and components (SSC) associated with nuclear safety or nuclear security should be based on the potential safety and security significance of these SSCs.²³

¹⁹ based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

²⁰ based on German Guideline for the protection of nuclear power plants with light-water reactors against malicious acts, restricted, 1995

²¹ WENRA Task Force – Meeting on March 6th 2018

²² based on UK ONR Security Assessment Principles

²³ based on FI Guide YVL A.11 Security of a nuclear facility

- (2) Due account should be taken of the need for nuclear security structures, systems and components to be designed to be inherently secure (e.g. mechanical backup in case of failure of electric door control), or to fail in a secure manner where it does not impact on nuclear safety.²⁴

Interface 10 – Feedback from Operating Experience and Plant Modification

a. Operating Experience

During the lifespan of a nuclear power plant, various experiences and developments relevant to nuclear safety and nuclear security may be identified. Nuclear safety and nuclear security have in common:

- (1) The licensee should ensure that relevant operating experience, international development of nuclear safety and nuclear security standards and new knowledge are analysed in a systematic way and continuously used to improve the plant.²⁵
- (2) All events concerning nuclear safety or nuclear security should be recorded and evaluated as an event related to nuclear safety may reveal a vulnerability related to nuclear security and vice versa.
- (3) The information gained from identified incidents in the nuclear power plant or in others of similar design or operation makes it possible to improve its nuclear safety or its nuclear security.²⁶

b. Plant Modification

During the lifespan of a nuclear power plant, various modifications to SSCs related to nuclear safety and SSCs related to nuclear security are performed. All modifications involve the risk, that other SSCs, not directly related to the modifications, could be impaired via unforeseen physical or administrative interaction. Therefore, nuclear safety and nuclear security have the following in common:

- (1) A comprehensive modification process should be in place, which includes design, review, implementation and control of modifications in order to take nuclear safety and nuclear security aspects into account.²⁷

Guidance:

Joint evaluation programs between nuclear safety and nuclear security personnel should be performed. The processes applicable for modifications should ensure that modifications of SSCs related to nuclear safety do not impair SSCs related to nuclear security and vice versa. This requires close engagement at all stages of the modification process of both nuclear safety and nuclear security personnel.

²⁴ based on UK ONR Security Assessment Principles

²⁵ based on WENRA RL B2.5

²⁶ based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

²⁷ based on German OPEX

Interface 11 – On-site Emergency Response

A nuclear security event may impact on nuclear safety (e.g. malicious damage of a SSC) and vice versa (e.g. a safety event may require evacuation and exits opening while prompt access for emergency personnel may be required). Additionally, the cause of a safety related event may not be immediately identifiable (malicious activity should be considered).

- (1) The licensee as well as the competent authorities should develop plans to limit the consequences of a radiological accident. Such plans should encompass events related to both nuclear safety and nuclear security.²⁸
- (2) For nuclear power plants arrangements should be made for the on-site emergency response to be promptly executed and managed without impairing the performance of the continuing operational nuclear safety and nuclear security functions both at the facility and at any other facilities on the same site.²⁹
- (3) The licensee should establish and maintain arrangements such that security personnel are fully integrated with the wider security, safety and event response (including clarity over command and control arrangements) and are driven by a shared understanding of threat and vulnerability assessments.³⁰ A key principle of this integration is considering nuclear events to be cause agnostic until the initiator is confirmed.³¹

Guidance:

Joint exercises should be organized and conducted to confirm the coordination among all organizations involved.³²

Interface 12 – Zones, Access and Escape Routes

Design of zones, access and escape routes of a nuclear power plant has implications for nuclear safety as well as nuclear security.

- (1) Nuclear security should be based on the utilization of several security zones placed within each other to ensure systems and components important to nuclear safety, and nuclear material and nuclear waste, are afforded particular protection and access control and the control of goods traffic can be arranged.³³
- (2) Nuclear security should be taken into account in the design of access and escape routes.³⁴

²⁸ based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

²⁹ based on IAEA GSR Part 7 "Preparedness and Response for a Nuclear or Radiological Emergency"

³⁰ based on UK ONR Security Assessment Principles

³¹ based on UK ONR Security Assessment Principles

³² based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

³³ based on FI Guide YVL A.11 Security of a nuclear facility

³⁴ based on FI Guide YVL B.8 Fire protection at a nuclear facility

Access openings, security zones and interlocking arrangements should fulfil nuclear security requirements and fire safety and accident preparedness requirements as well as the nuclear safety of facility operation should be taken into account.³⁵

For example, in case of fire, safety measures also aim at allowing rapid evacuations without constraint while physical protection measures aim at controlling accesses. Solutions should be found to achieve the two aims.

Interface 13 – Regulatory Framework

Both nuclear safety and nuclear security are built on a legal and regulatory framework which is monitored by competent authorities.

- (1) The legal and regulatory framework should define the responsibilities of several organizations: the State, the competent authorities, and the operating organizations.³⁶ The competent authorities should define the requirements to be satisfied by the licensee for both nuclear safety and nuclear security taking relevant interface issues into account.
- (2) The competent authorities should verify that the responsibilities in nuclear safety and nuclear security are well defined and are satisfied.³⁷
- (3) The competent authorities should set up and implement a licensing system and an inspection and enforcement system.
- (4) The competent authorities should ensure that an adequate emergency and contingency response system is in place, including various off-site elements that are not the responsibility of the licensee.
- (5) The competent authorities should observe international commitments in the fields of nuclear safety and nuclear security.³⁸

³⁵ based on FI Guide YVL A.11 Security of a nuclear facility

³⁶ based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

³⁷ based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

³⁸ based on INSAG 24 "The Interface Between Safety and Security at Nuclear Power Plants"

04 Conclusion

—

A number of areas with interfaces between nuclear safety and nuclear security were identified by the chosen methodology. Most of the interfaces were addressed by international or national regulations. The interfaces were described within this document and further guidance has been suggested based on the experience of the Task Force members. The identified interfaces consist of aspects that are in common or need to be managed in an integrated way in order to achieve the common aim of nuclear safety and nuclear security. Additional regulations concerning the described interfaces exist, but their description would exceed the aimed level of detail.