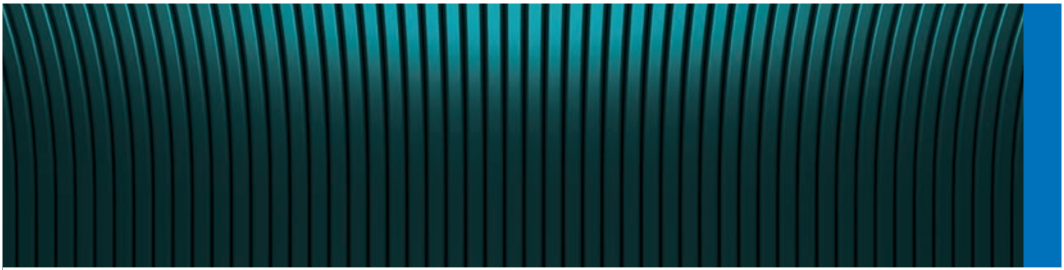
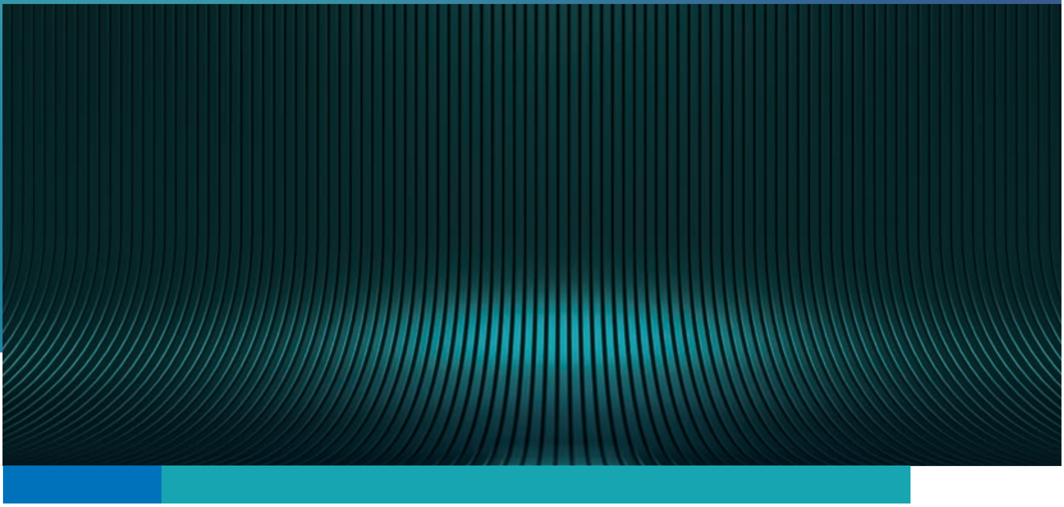
IAEA
International Atomic Energy Agency



TECHNICAL REPORTS SERIES No. 1003

Regulatory Oversight of the Interfaces between Nuclear Safety and Nuclear Security in Nuclear Power Plants



IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

www.iaea.org/resources/safety-standards

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

REGULATORY OVERSIGHT OF THE INTERFACES BETWEEN NUCLEAR SAFETY AND NUCLEAR SECURITY IN NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CABO VERDE
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GAMBIA
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUINEA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT KITTS AND NEVIS
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TONGA
TRINIDAD AND TOBAGO
TUNISIA
TÜRKİYE
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

TECHNICAL REPORTS SERIES No. 1003

REGULATORY OVERSIGHT OF THE INTERFACES BETWEEN NUCLEAR SAFETY AND NUCLEAR SECURITY IN NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2024

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
March 2024
STI/DOC/010/1003
https://doi.org/10.61092/iaea.1lzf-cguq

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Regulatory oversight of the interfaces between nuclear safety and nuclear security in nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2024. | Series: Technical reports series, ISSN 0074–1914 ; no. 1003 | Includes bibliographical references.
Identifiers: IAEAL 24-01656 | ISBN 978-92-0-136423-4 (paperback : alk. paper) | ISBN 978-92-0-136523-1 (pdf) | ISBN 978-92-0-136623-8 (epub)
Subjects: LCSH: Nuclear power plants — Safety measures. | Nuclear power plants — Security measures. | Nuclear facilities — Management.
Classification: UDC 621.039.58 | STI/DOC/010/1003

FOREWORD

Nuclear safety and nuclear security share the same goal: to protect individuals, the public and the environment from harmful effects of ionizing radiation. However, the activities that address nuclear safety and nuclear security are different, and actions taken to strengthen nuclear safety can affect nuclear security positively or negatively and vice versa. It is therefore essential to establish a well coordinated approach for managing the interface between nuclear safety and nuclear security so that relevant measures are implemented in a manner that capitalizes on opportunities that may be available for mutual enhancement without compromising either nuclear safety or nuclear security.

The responsibility for nuclear safety and nuclear security within a State rests entirely with that State. In this context, the importance of international cooperation and the central role of the IAEA is widely recognized. The IAEA assists Member States in establishing or strengthening their nuclear safety infrastructure as well as their nuclear security infrastructure. In addition, it provides support to establish synergy between both infrastructures to ensure that actions taken in the two fields complement rather than compromise each other. The interface between nuclear safety and nuclear security is highlighted in IAEA safety standards and nuclear security guidance.

Lessons from various IAEA peer review and advisory missions, training courses, exercises and workshops have highlighted that the understanding of many regulatory bodies and other competent authorities of the mechanism for oversight of the interfaces between safety and security during the various stages in the lifetime of a nuclear power plant is different, and practical information is needed that is consistent with the safety requirements established in the IAEA Safety Standards Series, the guidance in the IAEA Nuclear Security Series, and country specific practices.

This publication is the product of experts from regulatory bodies and other competent authorities from various Member States. It provides a broad view of regulatory oversight perspectives on the interfaces between nuclear safety and security during the stages in the lifetime of a nuclear power plant. The IAEA acknowledges the efforts of the participating experts and the IAEA staff involved in the development process. The IAEA officers responsible for this publication were S. Moazzam and Z.H. Shah of the Division of Nuclear Installation Safety and K. Horvath of the Division of Nuclear Security.

EDITORIAL NOTE

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Nuclear safety is the achievement of proper operating conditions, prevention of accidents and mitigation of their consequences, resulting in the protection of workers, the public and the environment from harmful effects of ionizing radiation. Nuclear security is the prevention of, detection of and response to theft, sabotage, unauthorized access, illicit transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. The following quotes highlight the connection to or the interface between nuclear safety and security.

Paragraph 1.10 of IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [1], states:

> "Safety measures and security measures have in common the aim of protecting human life and health and the environment. The safety principles concern the security of facilities and activities to the extent that they apply to measures that contribute to both safety and security, such as:
>
> — Appropriate provisions in the design and construction of nuclear installations and other facilities;
> — Controls on access to nuclear installations and other facilities to prevent the loss of, and the unauthorized removal, possession, transfer and use of, radioactive material;
> — Arrangements for mitigating the consequences of accidents and failures, which also facilitate measures for dealing with breaches in security that give rise to radiation risks;
> — Measures for the security of the management of radioactive sources and radioactive material.
>
> Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security".

Requirement 12 of IAEA Safety Standards Series No. GSR Part 1 (Rev. 1), Governmental, Legal and Regulatory Framework for Safety [2], states:

> "**The government shall ensure that, within the governmental and legal framework, adequate infrastructural arrangements are established for**

> **interfaces of safety with arrangements for nuclear security and with the State system of accounting for, and control of, nuclear material.**”

Furthermore, para. 2.39 of GSR Part 1 (Rev. 1) [2] states:

> “Specific responsibilities within the governmental and legal framework shall include (…) (d) Integration of emergency arrangements for safety related and nuclear security related incidents.”

The requirements for interfaces between safety and security for nuclear power plants (NPPs) are explicitly included in Section 4 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power: Design [3], and Section 5 of IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [4]. IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety [5], requires the management system to integrate safety and security.

Similarly, para 1.2 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State’s Nuclear Security Regime [6], stipulates:

“Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment”. Emphasis is placed on the consideration of nuclear safety and security interface on planning, preparedness for and response to nuclear security events.

Paragraph 3.17 of IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities [7], stipulates:

> “The recommended *physical protection measures* (…) should be additional to, and not a substitute for other measures established for nuclear safety, (…).”

In addition, para. 3.28 of Ref. [7] recommends:

> “For a new *nuclear facility,* the site selection and design should take physical protection into account as early as possible and also address the interface between physical protection, safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other.”

Sabotage targets include safety related equipment and devices based on safety analysis. Nuclear security systems and measures take advantage of safety provisions and procedures.

The objective of a regulatory body is to ensure that the operating organization of a nuclear power plant (NPP) fulfils its responsibilities to protect human health and the environment from possible adverse effects arising from the NPP. To achieve these objectives, the regulatory body performs its regulatory functions and activities.

1.2. OBJECTIVE

The objective of this publication is to compile relevant IAEA requirements, recommendations and guidance on identifying and addressing potential and actual interactions between nuclear safety and nuclear security systems and measures in NPPs. This publication also presents regulatory practices that are important to consider for nuclear safety and nuclear security, as they could reinforce or reduce the capacity of the regulatory bodies, competent authorities and operating organizations to meet nuclear safety and nuclear security requirements, including requirements relating to the interfaces between safety and security, during the application of different regulatory functions in the various stages of the lifetime of an NPP.

This publication will assist regulatory bodies in their oversight of the procedural approach developed by the operating organization to:

(1) Identify interactions between nuclear safety and nuclear security systems and measures;
(2) Analyze these interactions to determine potential impacts on safety and security (i.e. the extent to which they conflict with or reinforce each other);
(3) Make decisions to ensure that synergies between safety and security are appropriately identified and utilized to develop and implement coordinated solutions that meet both safety requirements and security requirements.

Guidance and recommendations provided here in relation to identified good practices represent expert opinion but are not made on the basis of a consensus of all Member States.

1.3. SCOPE

The publication will primarily be applicable for the interfaces of nuclear safety and nuclear security at NPPs. The publication also addresses activities of regulatory bodies and competent authorities in implementing regulatory oversight processes in nuclear safety, nuclear security and related interfaces.

Additionally, many of the processes and activities described could also be useful for regulatory oversight and associated activities performed in connection with other nuclear installations, nuclear or other radioactive material, and associated facilities and activities.

1.4. STRUCTURE

This publication is divided into three sections and two annexes.

Following this introductory section, Section 2 summarizes the IAEA requirements, recommendations and guidance about identifying and managing interfaces between safety and security related to regulatory functions and activities. Section 3 provides information on the regulatory practices that can be used to manage interfaces between safety and security.

Annex I presents an extract from the good practices identified during previously conducted Integrated Regulatory Review Service (IRRS) and International Physical Protection Advisory Service (IPPAS) missions regarding the interfaces between safety and security. Annex II offers specific case studies from Member States.

2. IAEA REQUIREMENTS, RECOMMENDATIONS AND GUIDANCE

This section compiles the requirements, recommendations and guidance established in IAEA safety standards and nuclear security guidance relevant to identifying, assessing and managing the interfaces between safety and security related to regulatory functions and activities.

2.1. REGULATORY FRAMEWORK FOR THE OVERSIGHT OF SAFETY AND SECURITY

One or more regulatory bodies and/or competent authorities are responsible for the oversight of NPPs, including the oversight of safety, security and their interfaces. Requirement 32 of GSR Part 1 (Rev. 1) [2] states:

> “**The regulatory body shall establish or adopt regulations and guides to specify the principles, requirements and associated criteria for safety upon which its regulatory judgements, decisions and actions are based.**”

In addition, para. 4.50 of GSR Part 1 (Rev. 1) [2] states:

> “The regulatory body shall develop and implement a programme of inspection of facilities and activities, to confirm compliance with regulatory requirements and with any conditions specified in the authorization”.

The following are requirements, recommendations and guidance relating to interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Principle 2 of SF-1 [1];
(b) Requirements 2 and 12 of GSR Part 1 (Rev. 1) [2];
(c) Requirements 1 and 2 of IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [8];
(d) Action 194 of IAEA Safety Standards Series No. SSG-16 (Rev. 1), Establishing the Safety Infrastructure for a Nuclear Power Programme [9];
(e) Paragraph 3.10 of IAEA Safety Standards Series No. GSG-12, Organization, Management and Staffing of the Regulatory Body for Safety [10];
(f) Paragraph 3.95 of IAEA Safety Standards Series No. GSG-13, Functions and Processes of the Regulatory Body for Safety [11];
(g) Section 4.6. of EPR–IEComm (2019), Operations Manual for Incident and Emergency Communication [12].

Security recommendations and guidance

(a) Fundamental Principle C and paras 3.53–3.55 of IAEA Nuclear Security Series No. 13 [7];
(b) Action 3-15 of IAEA Nuclear Security Series No. 19, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme [13];
(c) Essential Element 3 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [6];
(d) Paragraph 3.2 of IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [14];
(e) Action 1-2 of IAEA Nuclear Security Series No. 35-G, Security during the Lifetime of a Nuclear Facility [15].

The regulatory oversight of safety and security interfaces can be enhanced by establishing frameworks for the following areas that will be addressed in more detail in subsections 2.1.1−2.1.8:

(a) Protection and sharing of information;
(b) Design considerations;
(c) Drafting regulations and guidance;
(d) Licensing and authorization;
(e) Inspection and enforcement;
(f) Review and assessment, including analysis of operating experience;
(g) Consistency of regulatory control;
(h) International cooperation.

2.1.1. Protection and sharing of information

The nuclear industry, as many other industries, has to consider two different objectives that might occasionally be contradictory:

(a) Release of information (often called 'transparency') whose sharing may be beneficial for innovation, review and assessment, continuous improvement, awareness raising, capacity building, safety and security culture, public debate, public confidence building and robust physical protection measures;
(b) Protection of information (often called 'confidentiality'), as required by law, to protect privacy, commercial and industrial secrecy, medical privacy and national security (including nuclear security).

Both safety and security areas are affected by these two objectives, but release of information is more commonly done for safety related information, with the protection of information being limited to specific areas of concern. However, protection of information is instrumental for nuclear security. Information is mainly shared on a need-to-know basis and with a limited number of people to reduce the risk that security sensitive information could be used by adversaries.

The Convention on Early Notification of a Nuclear Accident (hereinafter referred to as 'Early Notification Convention') [16] and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency (hereinafter referred to as 'Assistance Convention') [17] are the primary legal instruments that establish an international framework to facilitate the exchange of information and the prompt provision of assistance in the event of a nuclear or radiological incident or emergency, regardless of its origin, with the aim of minimizing the consequences. The IAEA has specific functions assigned to it under these conventions. The arrangements provided between the IAEA Secretariat, IAEA Member States and/or Parties to one or both Conventions, relevant international intergovernmental organizations (hereinafter referred to as international organizations) and other States for facilitating the implementation of these Conventions — specifically concerning those articles that are operational in nature — are documented in Operations Manual for Incident and Emergency Communication, EPR IEComm (2019) [12]. EPR IEComm details the communication arrangements for points of contact identified under the Early Notification Convention and the Assistance Convention as well as the designated National Officers of the International Nuclear and Radiological Event Scale (INES) [18]. Points of contact, central authorities or competent authorities identified under other relevant conventions under the auspices of the IAEA can also be guided by the communications arrangements for nuclear or radiological incidents and emergency communication covered in EPR IEComm (2019) [12].

The Emergency Convention Standard Report Form includes an encryption feature for the exchange of sensitive information, including information related to nuclear security. If this feature is used, the content of the section titled "Other Relevant Information" is encrypted and is made available to authorized staff of the Member States' competent authorities on the IAEA Unified System for Information Exchange in Incidents and Emergencies (USIE). USIE is a secure IAEA web site for Contact Points of States Parties to the Early Notification and Assistance Conventions and of IAEA Member States to exchange urgent notifications and follow-up information during nuclear or radiological incidents and emergencies irrespective of their cause (i.e. safety or security related), and for officially nominated INES National Officers to post information on events rated using the INES. USIE offers encryption of information in transfer and storage and is monitored all the time.

2.1.2. Design considerations

The design of a NPP has to take nuclear security as well as the interfaces between security and safety into account as early as possible, to avoid later conflicts. This approach will ensure that safety measures and nuclear security measures reinforce each other. Potential malicious acts that involve physical access to the facility are not the only kinds of threats that need to be considered, but also those that use cyber-attacks. Such attacks could be aimed at computer-based systems used for nuclear safety (including instrumentation and control systems), nuclear material accounting and control and nuclear security or emergency response (including communication and alarm systems).

Good nuclear security system design can take advantage of the 'multiple layers' of the defence in depth concept for nuclear safety to reduce the need for specific security systems, including:

(a) Supplementary targets that malicious actors could destroy in order to reach their objective, making the attack scenario too difficult.
(b) Systems that render attack scenarios against other targets meaningless if they allow for the avoidance of unacceptable radiological consequences in case they are considered to be adequately protected. In this case, the protection of the other targets can be considered unnecessary, depending on national rules.
(c) Safety measures that can contribute to the detection of, or response to, malicious acts.

The following are requirements, recommendations and guidance relating to design considerations when dealing with the interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirements 2, 7, 8, 36 and 38 of SSR-2/1 (Rev. 1) [3];
(b) Action 176 of SSG-16 (Rev. 1) [9];
(c) Paragraph 4.4 of IAEA Safety Standards Series No. SSG-35, Site Survey and Site Selection for Nuclear Installations [19].

Security recommendations and guidance

(a) Paragraphs 3.28, 3.38, 3.44 and 3.45 of IAEA Nuclear Security Series No. 13 [7];
(b) Paragraph 5.11 of IAEA Nuclear Security Series No. 19 [13];
(c) Paragraphs 4.9, 4.10, 4.34 and 4.39 of IAEA Nuclear Security Series No. 27-G [14];
(d) Paragraph 2.19 of IAEA Nuclear Security Series No. 10-G (Rev. 1), National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements [20].

2.1.3. Drafting regulations and guidance

The regulatory body is responsible for the drafting and review of guidance and regulations.

The following are requirements, recommendations and guidance relating to drafting regulations and guidance regarding the interface between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirements 32, 33 and 34 of GSR Part 1 (Rev. 1) [2];
(b) Action 195 of SSG-16 (Rev. 1) [9].

Security recommendations and guidance

(a) Paragraphs 3.9, 3.10 and 3.11 of IAEA Nuclear Security Series No. 13 [7];
(b) Paragraph 3.10 of IAEA Nuclear Security Series No. 19 [13].

2.1.4. Licensing and authorization

The regulatory body defines the requirements to be satisfied by the operating organization for both safety and security. The regulatory body also establishes and implements a licensing process for NPPs [2].

The following are requirements, recommendations and guidance relating to licensing and authorization when considering interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 23 of GSR Part 1 (Rev. 1) [2];

(b) Paragraphs 3.98 and 3.102 of GSG-13 [11];
(c) Paragraphs 2.7, 2.19 and 3.98 of IAEA Safety Standards Series No. SSG-12, Licensing Process for Nuclear Installations [21].

Security recommendations and guidance

(a) Paragraph 3.12 of IAEA Nuclear Security Series No. 13 [7];
(b) Actions 3-16 and 5-6 of IAEA Nuclear Security Series No. 19 [13];
(c) Paragraphs 3.35 and 3.36 of IAEA Nuclear Security Series No. 27-G [14];
(d) Paragraph 2.3 and Actions 3-4, 5-6 and 6-6 of IAEA Nuclear Security Series No. 35-G [15].

2.1.5. Inspection and enforcement

The regulatory body ensures compliance with established requirements through inspection, verification and enforcement activities.

The following are requirements, recommendations and guidance relating to inspection and enforcement when considering the interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 27 of GSR Part 1 (Rev. 1) [2];
(b) Paragraph 4.18 of GSG-12 [10].

Security recommendations and guidance

(a) Paragraphs 3.20 and 3.21 of IAEA Nuclear Security Series No. 13 [7];
(b) Action 3-23 of IAEA Nuclear Security Series No. 19 [13];
(c) Paragraph 3.42 of IAEA Nuclear Security Series No. 27-G [14].

2.1.6. Review and assessment, including analysis of operating experience

One of the main functions of a regulatory body is to review and assess licensee submissions. Review and assessment are performed to ensure that the facility will be designed and operated in accordance with regulatory requirements and in line with safety standards and security requirements. Based on a review of the submissions related to safety and security, the regulatory body decides on whether to issue the license.

The following are requirements, recommendations and guidance relating to review and assessment of interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirements 12 and 25 of GSR Part 1 (Rev. 1) [2].

Security recommendations and guidance

(a) Paragraphs 3.48, 4.30 and 4.148 of IAEA Nuclear Security Series No. 27-G [14].

2.1.7. Consistency of regulatory control

A consistent approach in implementing procedures for the oversight of safety and security will ensure that regulatory actions regarding regulatory control of safety do not compromise security and vice versa.

The following are requirements, recommendations and guidance relating to regulatory control when considering interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 22 of GSR Part 1 (Rev. 1) [2];
(b) Requirement 17 of SSR-2/2 (Rev. 1) [4];
(c) Paragraph 2.22 of SSG-12 [21].

Security recommendations and guidance

(a) Paragraphs 3.17 and 5.13 of IAEA Nuclear Security Series No. 13 [7];
(b) Paragraph 5.7 of IAEA Nuclear Security Series No. 19 [13].

2.1.8. International cooperation

International cooperation under different conventions, treaties, global nuclear safety and security frameworks, expert missions and other IAEA activities provides insights into safety security interfaces through which States can benefit from the practices and experiences of other States on the subject matter.

The following are requirements, recommendations and guidance relating to international cooperation when considering interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 14 of GSR Part 1 (Rev. 1) [2];
(b) EPR-RANET, IAEA Response and Assistance Network [22];
(c) Paragraph 4.25 of IAEA Safety Standards Series No. GSG-6, Communication and Consultation with Interested Parties by the Regulatory Body [23].

Parties to the Assistance Convention have undertaken to cooperate between themselves and with the IAEA to facilitate the timely provision of assistance in the case of a nuclear accident or radiological emergency to mitigate its consequences. As part of the IAEA's strategy of supporting the practical implementation of the Assistance Convention, in 2000, the IAEA Secretariat established the Response and Assistance Network (RANET).

RANET is a network of States established to provide international assistance in a nuclear or radiological emergency upon request from a State. States' Parties to the Assistance Convention are obliged, within the limits of their capabilities and resources, to identify national assistance capabilities that could be made available to assist another State.

Security recommendations and guidance

(a) Essential Element 6 of IAEA Nuclear Security Series No. 20 [6];
(b) Action 5-9 and para. 8.2 of IAEA Nuclear Security Series No. 19 [13];
(c) Paragraph 5.4 of IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [24].

2.2. LEADERSHIP AND MANAGEMENT FOR SAFETY AND SECURITY

Leadership and management are important aspects for both safety and security and are the responsibility of senior management of the regulatory bodies or competent authorities.

The following are the main aspects of leadership and management common to both safety and security that will be addressed in subsequent subsections:

(a) Leadership for safety and security;
(b) Integrated management system;
(c) Promotion of safety culture and security culture;
(d) Organizational structure and allocation of resources;
(e) Staffing and competence of the regulatory body or competent authority;
(f) Human factors.

2.2.1. Leadership for safety and security

Leadership for both nuclear safety and security has a key role in ensuring that staff members are appropriately motivated and that their roles in enhancing safety and security are recognized and valued within the regulatory body or competent authority.

The following are requirements, recommendations and guidance relating to leadership and interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 2 of GSR Part 2 [5].

Security recommendations and guidance

(a) Essential Element 12 of IAEA Nuclear Security Series No. 20 [6];
(b) Action 4-56 of IAEA Nuclear Security Series No. 19 [13].

2.2.2. Integrated management system

An integrated management system integrates all of a regulatory body’s systems and processes into one complete framework, enabling the regulatory body to work as a single unit with unified objectives. An integrated system provides a clear, holistic picture of all aspects of the regulatory body as well as the way in which they affect each other and their associated risks.

The following are requirements, recommendations and guidance relating to interfaces between nuclear safety and nuclear security and integrated management systems:

Safety requirements and guidance

(a) Requirement 19 of GSR Part 1 (Rev. 1) [2];
(b) Requirements 2 and 6 of GSR Part 2 [5];
(c) Paragraph 5.4 of GSG-12 [10].

Security recommendations and guidance

(a) Essential Element 12 of IAEA Nuclear Security Series No. 20 [6];
(b) Action 4-19 of IAEA Nuclear Security Series No. 19 [13];
(c) Action 4-3 of IAEA Nuclear Security Series No. 35-G [15].

2.2.3. Promotion of safety culture and security culture

For the interfaces between safety and security to be effectively managed, the regulatory body establishes and maintains strong safety and security cultures in all its activities and among all levels of personnel and management.

The following are requirements, recommendations and guidance relating to the promotion of safety and security culture:

Safety requirements and guidance

(a) Requirements 12 and 14 of GSR Part 2 [5];
(b) Action 197 of SSG-16 (Rev. 1) [9].

Security recommendations and guidance

(a) Fundamental Principle F and paras 3.48–3.51 of IAEA Nuclear Security Series No. 13 [7];
(b) Paragraphs 4.13 and 4.30–4.33, and Actions 2-3, 4-23, and 4-53–4-58 of IAEA Nuclear Security Series No. 19 [13];
(c) Paragraph 3.106 of IAEA Nuclear Security Series No. 27-G [14];
(d) Section 2.4 of IAEA Nuclear Security Series No. 7, Nuclear Security Culture [25];
(e) Paragraph 3.9 of IAEA Nuclear Security Series No. 28-T, Self-assessment of Nuclear Security Culture in Facilities and Activities [26].

2.2.4. Organizational structure and allocation of resources

The regulatory body establishes its organizational structure in a way to perform its responsibilities for both safety and security efficiently and effectively. The State is responsible for ensuring the allocation of adequate resources to support the regulatory body in fulfilling its intended functions.

The following are requirements, recommendations and guidance relating to organizational structures, resource allocation and interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirements 3, 6 and 16 of GSR Part 1 (Rev. 1) [2];
(b) Requirement 9 of GSR Part 2 [5].

Security recommendations and guidance

(a) Paragraph 3.56 of IAEA Nuclear Security Series No. 13 [7];
(b) Paragraph 3.39 of IAEA Nuclear Security Series No. 27-G [14].

2.2.5. Staffing and competence of the regulatory body or competent authority

To effectively manage the interfaces between safety and security, the regulatory body ensures that sufficient and fully trained and qualified human resources are available to perform their responsibilities.

The following are requirements, recommendations and guidance relating to human resources and interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 18 of GSR Part 1 (Rev. 1) [2];
(b) Requirement 9 of GSR Part 2 [5];
(c) Section 6 of GSG-12 [10].

Security recommendations and guidance

(a) Paragraphs 3.39, 3.43 and 4.78 of IAEA Nuclear Security Series No. 27-G [14];
(b) Paragraph 2.29 of Nuclear Security Series No. 30-G, Sustaining a Nuclear Security Regime [27].

2.2.6. Human factors

Human factors (e.g. complacency, insiders, human, technological and organizational factors and their respective interactions) are important to ensure that safety measures and security measures are properly implemented.

The following are requirements, recommendations and guidance relating to interfaces between nuclear safety and nuclear security and human factors:

Safety requirements and guidance

(a) Paragraph 3.14 of SF-1 [1];
(b) Requirement 12 of GSR Part 2 [5];
(c) Paragraph 2.20 of GSG-12 [10].

Security recommendations and guidance

(a) Section 2.3 of IAEA Nuclear Security Series No. 7 [25];
(b) Paragraphs 1.1 and 7.4 of IAEA Nuclear Security Series No. 28-T [26].

2.3. COOPERATION AND JOINT ACTIONS AMONG COMPETENT AUTHORITIES

The effective implementation of both safety and security objectives and requirements involves cooperation and joint actions among the regulatory body and other competent authorities, in which organizations responsible for safety and nuclear security establish effective mechanisms for communication with each other.

The following are requirements, recommendations and guidance relating to interfaces between nuclear safety and nuclear security and cooperation and joint actions among the regulatory body and other competent authorities:

Safety requirements and guidance

(a) Requirements 7 and 12 of GSR Part 1 (Rev. 1) [2];
(b) Requirement 8 of SSR-2/1 (Rev. 1) [3];
(c) Action 194 of SSG-16 (Rev. 1) [9];
(d) Paragraph 4.45 of GSG-12 [10].

Security recommendations and guidance

(a) Paragraph 3.25 of IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [28];
(b) Actions 5-17 and 7-28 of IAEA Nuclear Security Series No. 19 [13];
(c) Paragraphs 3.9 and 3.10 of IAEA Nuclear Security Series No. 27-G [14];
(d) Section 3.1.5 of IAEA Nuclear Security Series No. 7 [25];
(e) Paragraphs 5.1 and 5.3 of IAEA Nuclear Security Series No. 23-G [24].

2.4. ADVISORY BODIES AND TECHNICAL SUPPORT ORGANIZATIONS

To accomplish the responsibilities assigned to the regulatory body, technical support in all the core processes (i.e. licensing, inspection and enforcement) can be sought from independent external organizations. Staff of the regulatory body need to be competent enough to evaluate the input of such technical support organizations (TSOs) for further decision making. Such support from any external organization does not relieve the regulatory body from its statutory role. Technical and other expert professional advice or services could be provided in several ways by experts external to the regulatory body. The regulatory body could also consider establishing a dedicated TSO.

The following are requirements, recommendations and guidance relating to advisory bodies and TSOs when considering interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 20 of GSR Part 1 (Rev. 1) [2];
(b) Paragraphs 4.35, 4.36 and 4.38–4.43 of GSG-12 [10];
(c) Paragraph 3.59 of GSG-13 [11].

Security recommendations and guidance

Taking account of requirements established for the protection of security related information, advisory bodies and TSOs in the field of nuclear security can support the regulatory body — including the development of regulatory requirements and verification of their implementation by the operating organization — and the evaluation of security performance; however, specific reference to advisory bodies does not exist in the published recommendations and guidance of the IAEA Nuclear Security Series.

2.5. COMMUNICATION AND CONSULTATION WITH THE OPERATING ORGANIZATION

Communication and consultation with the operating organization are sometimes handled differently for safety and security. Formal and informal processes for constructive communication will be needed, ensuring confidentiality when appropriate.

The following are requirements, recommendations and guidance relating to communicating and consulting with the operating organization and interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Requirement 21 of GSR Part 1 (Rev. 1) [2];
(b) Paragraph 2.17 of IAEA Safety Standards Series No. GSG-6 [23];
(c) Paragraphs 2.18, 6.48 and 6.56 of GSG-12 [10].

Security recommendations and guidance

(a) Essential Element 3 of IAEA Nuclear Security Series No. 20 [6].

2.6. PUBLIC CONSULTATION AND COMMUNICATION

The regulatory body communicates and consults with interested parties, including the public when appropriate, in a transparent manner, about the possible radiation risks associated with facilities and activities, as well as the regulatory decision-making processes and regulatory decisions made. The regulatory body will also need to communicate with the public during a nuclear or radiological emergency.

The following are requirements, recommendations and guidance relating to communicating and consulting with the public and interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Paragraphs 2.18 and 4.23 of GSG-12 [10];

(b) Paragraphs 3.93 and 3.292 of GSG-13 [11];
(c) Paragraph 3.5 of GSG-6 [23].

Security recommendations and guidance

(a) Section 3.5 of IAEA Nuclear Security Series No. 7 [25].

2.7. EMERGENCY AND CONTINGENCY PLANNING AND RESPONSE

Both nuclear safety and nuclear security events might initiate a nuclear or radiological emergency, in which case the response will address the safety aspects and the nuclear security aspects of the emergency. Contingency plans are predefined sets of actions for response to unauthorized removal of nuclear material or sabotage of nuclear material.

The following are requirements, recommendations and guidance relating to emergency planning and responses and interfaces between nuclear safety and nuclear security:

Safety requirements and guidance

(a) Paragraph 3.322 of GSG-13 [11];
(b) Paragraphs 1.2, 1.5, 1.6, 1.9, 1.16, 5.16 and 5.69, and Requirements 2, 4, 6, 7, 13, 19, 22 and 23 of IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [29];
(c) Action 196 of IAEA Safety Standards Series No. SSG-16 (Rev. 1) [9];
(d) Paragraphs 3.57, 3.132 and 5.10–5.14 of IAEA Safety Standards Series No. GSG-14, Arrangements for Public Communication in Preparedness and Response for a Nuclear or Radiological Emergency [30];
(e) Paragraphs III.16 and III.23 of IAEA Safety Standards Series No. GSG-2, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency [31];
(f) Paragraphs 4.2 and 5.2 of IAEA Safety Standards Series No. GS-G-2.1, Arrangements for Preparedness for a Nuclear or Radiological Emergency [32].

Security recommendations and guidance

(a) Fundamental Principle K and paras 3.58, 4.19, 4.20, 4.52 and 5.53 of IAEA Nuclear Security Series No. 13 [7];

(b) Actions 3-25, 5-17 and 7-28 of IAEA Nuclear Security Series No. 19 [13];

(c) Paragraphs 4.79 and 4.82 of IAEA Nuclear Security Series No. 27-G [14].

3. REGULATORY PRACTICES TO MANAGE INTERFACES BETWEEN SAFETY AND SECURITY

This section addresses interfaces between safety and security that exist during the application of various regulatory functions and activities. In this section, commonalities and potential conflicts of nuclear safety and nuclear security are recognized, and their synergetic applications are described as opportunities for the management of their interfaces. The intention is that the presented practices and provided examples can be of use when regulatory bodies are in the process of developing their own approaches to address safety and security interfaces, recognizing that they may need some adaptation to align with the specific configuration of a State's regulatory framework.

3.1. REGULATORY FRAMEWORKS FOR THE OVERSIGHT OF SAFETY AND SECURITY

A cornerstone for the establishment and implementation of a regulatory framework is to recognize, and to deal with, the mutual implications of the interface between safety and security.

The regulation of nuclear safety and of nuclear security are of equal importance in achieving the common objective of protecting people and the environment from harmful effects of ionizing radiation.

3.1.1. Protection and sharing of information

Concerns about sharing and protecting information are similar for safety and security. Nevertheless, practices in the two areas are very different, because of the specificities of each area. For example, in theory, the transparency principle can apply to security, but its implementation is very limited in practice; transparency of security is limited by the rule of protection of information, and most of the information related to security is classified. This is the reason is why transparency is generally not associated with nuclear security. Instead, sharing of information regarding nuclear security is more often presented as information to promote public confidence and to deter malicious acts.

Habits, behaviours and culture developed in the area of safety regarding the act of regulating can also differ from those in the area of security. For example, security experts dealing mainly with sensitive information can believe 'need to know' is more important than 'need to share'. This is the converse of the approach of safety experts, who consider that 'need to share' is more important than 'need to know'.

It needs to be emphasized that sensitive information is not limited to nuclear security information. For example, detailed information regarding operation and safety assessment insights (e.g. deterministic or probabilistic safety assessment), such as the precise description of operations, locations of equipment, or accident analysis, can be very useful for the planning and execution of malicious actions and are to be considered sensitive.

Operating organizations and regulatory bodies need to have an integrated organization to manage both the objectives of 'need to know' and 'need to share', while ensuring that one does not compromise the other. For example, 'need to know' can be implemented with caution, while considering the benefits of sharing information with safety experts. Similarly, protection of information cannot be misused to retain information that is not sensitive and that is of public interest. However, transparency needs to take into consideration that release of information has no potentially harmful consequences.

Finding a balance between these different objectives is often difficult and needs to be based on a collective and joint decision process.

This concern is also very important with regard to the information that is released to staff. For raising awareness and acceptance of security measures, some information related to security has to be provided. For example, all staff members need to have some basic information about the threat facing them and their activity or facility, in order to convince them, individually, of the importance of their respective roles (e.g. helping detect suspicious situations or behaviours, measures to apply in case of a security event). However, releasing too much information can decrease the effectiveness of security measures (e.g. the case of an insider threat). Again, a collective process can help, for example, in understanding what kind of information is necessary to motivate the staff that is not acquainted with nuclear security.

'Need to know' can also be applied with consideration of a graded approach. More sensitive information can be protected more strictly than less sensitive information. Information whose broad release is very beneficial can be released more widely. For example, specific inspection findings related to nuclear security that are relevant to a certain site will only be shared with the operator and the inspection team. However, it can be beneficial to involve observers from other operating organizations and safety experts for national level exercises. Most general findings will be relevant to any situation and any site, and exercises are very effective in raising awareness.

3.1.2. Determination of the design basis

Defence in depth means the use of multiple, independent and redundant safety-security measures. This concept is used in terms of both safety and security to protect workers, the public and the environment from harm in accident conditions (caused unintentionally or intentionally) in the event that individual protective barriers alone are not fully effective.

A physical protection system (PPS) needs to be designed based on a graded approach; the graded approach for both nuclear safety and nuclear security is based on the radiological consequences, and specifically on the consequences that the relevant State decides it is willing to accept. This can be achieved by identifying the level and effectiveness of nuclear security measures that provide protection against unauthorized removal of nuclear or other radioactive material and sabotage of the nuclear material or nuclear facility.

The design of the PPS can incorporate defence in depth to provide reliability that the failure of a single security component does not result in the failure of the security function.

Security and safety by design are important concepts. Safety and security measures of nuclear facilities need to be designed from their initial lifetime stages by providing the same priority to nuclear and security objectives. The design of a nuclear facility needs to address the interfaces between physical protection and safety to avoid any conflicts and to ensure that they support each other. Experts from safety and security have to be involved to optimize the benefits from the intrinsic features of the processes, materials and structures. In some areas, measures included in the design to improve nuclear safety will also assist security and vice versa. In others, a design solution needs to be sought that will minimize conflicting requirements. It could also be useful to periodically reassess the design of a facility and the processes and procedures relevant for safety and security. This reassessment needs to take into account any changes in accident scenarios resulting from research and development (R&D) or actual accidents, operating experience, advanced knowledge and findings from actual events such as the accident at the Fukushima Daiichi NPP.

While it is not always feasible to adjust all the design modifications and/or upgrades for older NPPs, they need to be considered to the extent possible to ensure safety.

Unacceptable radiological consequences and high radiological consequences need to be defined and considered together with the design basis threat (DBT) [15]. In reaching those definitions, it could be useful to consider harmonizing the acceptable levels for different types of initiating events defined in the safety case with those malicious initiators. The IAEA Nuclear Security Series allows for the harmonization of those definitions. In case it does not suit the State's infrastructure, the reasons for not harmonizing could be fully explored and understood.

The design basis is the collection of conditions and events which are considered in the design of structures, systems and components and equipment of an NPP, according to set criteria, such that the NPP can withstand them without exceeding authorized limits.

Both design basis accidents (DBAs), with accident conditions and operating states, and DBTs describe the conditions against which protection of workers, the public and the environment are ensured. Therefore, determination of the design basis involves both safety and security considerations.

Site specific design basis inputs are considered during the early stages when the design of the PPS is initiated. DBAs that can impact the functionality of the PPS need to be identified and addressed in the assessment and incorporated in the design. From the safety perspective, plant protection against potential accident conditions is designed considering two situations, namely DBAs and design extension conditions.

The first is a postulated accident that leads towards conditions for which an NPP is designed in agreement with established design criteria and conservative methodology, and for which discharges of radioactive material are retained within acceptable limits.

The second includes conditions that are not considered in the DBAs but are accounted for in the design process of the facility, the operational management, emergency planning and preparedness and other considerations by which releases of radioactive material are kept within acceptable limits.

From the security perspective, the protection of a facility is based on the consideration of DBTs. It represents the physical and cyber attributes and characteristics of external adversaries and/or potential insider threats that might attempt unauthorized removal or sabotage against which a PPS is designed and evaluated.

In the case of NPPs, malicious acts can target either areas where nuclear fuel (fresh or spent) or radioactive material is kept or stored (theft or direct attack for sabotage of nuclear materials), or systems whose failure would cause damage to nuclear fuel, leading to radiological consequences (indirect attack for sabotage).

Operators of NPPs and safety experts need to cooperate with security experts, those agencies responsible for emergency preparedness and other governmental agencies at different levels to provide protection against events initiated by sabotage and unauthorized removal (theft).

The understanding that has developed as a result of facing the challenges of the present-day threat environment is that cooperation across all national agencies or authorities is needed. This includes governmental agencies such as the police, the armed forces and the intelligence community.

Complementing/conflicting areas and development of synergies

The capabilities determined in the DBT are considered during the development of credible attack scenarios for nuclear security. Safety experts support security experts to determine credible sabotage attack scenarios that could lead to unacceptable radiological consequences or high radiological consequences.

Supplementary attack scenarios that are not covered by design and the safety case are possible and can occur. Safety experts can also assist security experts in identifying these scenarios, for example, by considering situations in which potential accidents envisioned in the safety case were excluded for reasons that are not valid for security (e.g. extremely improbable situations, practically excluded situations).

Protection from DBAs and the DBT share the same objective, which is to protect people and the environment from harmful effects of ionizing radiation. Synergies among these objectives can naturally occur, such as the design of measures to prevent human mistakes contributing to the prevention of insider attacks, and vice versa.

A special approach can be useful for NPPs that were designed before the international guidance on design basis was refined (e.g. DBAs, design extension conditions or the relevant parts of DBTs).

A DBA is a potential event that is considered in the design of the plant. A DBA is defined as a “postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.” [3]. DBAs lead to the identification of postulated initiating events.

A DBT is a credible threat that informs the design of the security programme, defined as “attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated” [20]. In effect, the DBT is the threat that forms the basis of the design of the physical protection programme.

Typically, regarding sabotage, the capabilities defined by the DBT aim to develop attack scenarios having initiating events of malicious origin (i.e. malicious acts that upset the operation in such a way that, if mitigation were unsuccessful, would lead to unacceptable radiological consequences [33]). Nuclear security aims as much as possible to prevent the occurrence of initiating events of malicious origin. When security measures are not considered to be effective, these events could need to be considered as postulated initiating events and treated as such in the safety case.

The malicious capabilities described in the DBT can change over time. Operating organizations and regulatory bodies need to be aware of the potential need for changes to physical protection measures based on a change in the DBT.

The use of emergency operating procedures, as well as severe accident management guidelines, need to be well known to plant operators to ensure that they can be effectively implemented for the mitigation of the consequences of accidents triggered by nuclear safety or security events.

3.1.3. Regulations and guidance

Regulatory bodies can establish and implement appropriate regulations which require the operating organizations to effectively manage safety and security and their interfaces at NPPs during each stage in the lifetime of a facility, from planning through to decommissioning. The competent authorities ensure that security regulations do not compromise safety, and safety regulations do not compromise security. It is essential that the competent authorities provide clear regulations and guidance governing safety and security at NPPs and clearly stipulate the conditions which operating organizations need to fulfil in order to obtain the approval from their respective regulatory body.

Different regulations and guidance can be applied to safety and security. If the security competent authorities are not the same as the safety competent authorities, it is vital to have a consultation, interfacing and harmonization mechanism in place to ensure that regulatory requirements and guidance agree and promote both safety and security. A coordination mechanism is necessary if there is only one regulatory body with separate internal groups responsible for safety and security.

Alignment of regulations and guidance can have a beneficial effect in making them more readily understood, furthering the understanding of security considerations by safety experts and of safety concerns by security staff. Good practice could involve safety experts being involved in the drafting of security regulations and guidance (and vice versa) so that alignment and coordination are built in from the outset rather than implemented at a later stage. Similarly, the involvement of safety experts in drafting such guidance can improve their ownership of security concepts, driving an improved culture of joint terminology and coordination. This, in turn, could reduce the regulatory burden and facilitate the cooperation of regulatory bodies (e.g. joint inspections).

Some countries, including Romania and the United States of America, have issued specific regulations and/or regulatory guidance, which include the interfaces between safety and security. The benefit to Romania of a separate regulation was to have one place capturing all components of the interfaces and of regulatory guidance, which has resulted in a greater level of detail for implementation.

In drafting safety regulations and guidance, it can be useful to include a section on nuclear security and vice versa, to the extent possible. Depending on the national infrastructure, it may or may not be beneficial to establish common regulations and guidance. The important aspect is for the competent authorities to discuss and decide this matter for the mutual advantage of both nuclear safety and security.

Complementing/conflicting areas and development of synergies

Regulations and guidance for nuclear safety and security need a process of drafting and revision. Techniques and competencies for establishing and maintaining regulations and guidance are not specific to safety or security.

Similar practices and techniques are used for regulating safety and security, such as the enforcement process, reporting of events, requirements for an integrated management system, graded approach, emergency planning and preparedness. Expertise acquired, lessons learned, and good practices identified in both areas can be used to enhance one another.

Due to the aforementioned similarities, it may be possible and even beneficial to follow the same process for safety and security regulations and guidance, particularly when the same authority is in charge of both areas in the country.

However, some techniques and concepts used for regulating one area might not be directly applicable to the other, such as the concept of transparency for regulations related to nuclear security.

The same terms could be used or interpreted in the regulations and guidance for safety and for security, but in different ways. For example, defence in depth is used in both safety and security related IAEA guidance. While the general definition of defence in depth is very similar for both safety and security, the implementation is quite different. It can result in experts of one area being misled in understanding the methods and decisions from the other area, sometimes creating conflicts ('dialogue of the deaf') or, on the contrary, a 'false sense of security'.

It is beneficial to include safety and security specialists when drafting regulations and guidance to benefit from 'cross-pollination' and, when appropriate, coordination. There are instances in which safety and security may benefit from specialists in each area cooperating on common regulatory guidance and even regulations. This could apply, for example, to those covering the safety-security interface, culture, competence, leadership and management. Similarly, those covering human factors in a central alarm station can be the same as, or similar to, those covering human factors in the reactor control room. Identifying synergies between these areas and capturing them in regulations and guidance, rather than repetition and the risk of introducing inconsistencies, can be highly beneficial to both areas.

Moreover, when the two disciplines are the responsibility of the same authority, the common organization and joint procedures could reduce duplication of effort and facilitate coordination and integrated management. A useful principle to adopt between disciplines is 'the same wherever possible, different wherever necessary'. Such an approach assists in the identification of synergies and allows regulatory bodies to adopt similar processes to achieve common aims or expectations, reducing a duplication of effort. It also assists the general understanding through the use of common terminology and concepts. On the other hand, it has to be ensured that the development of harmonized regulations and guidance does not lead to diluted specificities and an overgeneralization in the requirements or guidance of the expertise needed for each area. A fine balance needs to be found between harmonization and specialization, and past experience has shown a tendency to go forward and backward in both directions in order to find the right balance.

In the process of developing regulatory requirements and guidance, it is important to identify possible interfaces between safety and security. To facilitate the proper arrangements for the implementation of the different requirements, cross referencing between the relevant regulatory guidance could be used in areas where interfaces are identified. In addition, regulatory guidance documents could be developed to explain these issues in greater detail. Common legal and technical principles underlying the safety and security requirements can be identified where interface issues might arise. When different authorities address interfaces, including those of safety and security, it is good practice to have jointly signed commitments and guidance to demonstrate and explain how interfaces need to be managed.

With respect to maintenance, inspection and testing, there might be differences in the expectations set in regulations and guidance, such as a requirement for the predetermination of trustworthiness of external contractors.

Similarly, disabling certain systems, such as electrical power supply, can inadvertently impact other systems. However, by aligning regulations and guidance in this area, it is possible to make use of arrangements to cover both safety and security infrastructure and to reduce duplication.

Performance based approaches can be more flexible than prescriptive approaches in drafting regulations and guidance that take account of safety, security and the interfaces between them. On the other hand, performance-based approaches could include a greater degree of sharing potentially sensitive information in drafting the regulations.

In some countries (e.g. Sweden), regulatory bodies have made concerted efforts to provide joint regulation for the purpose of increased efficiency and simplicity in the regulatory oversight of safety and security.

3.1.4. Licensing and authorization, including management of changes

The terms ‘licensing’ and ‘authorization’ might be considered as regulatory activities to grant a licence, authorization, permission or approval after review and assessment and/or inspection. This also covers all stages in the lifetime of the NPP, from planning, siting and construction to decommissioning.

Considering these stages, there is a benefit in including explicit assessment of the safety-security interfaces at every stage and by starting from an early planning stage. For example, during the design phase, evaluation of the interfaces helps to ensure that, to the extent possible, conflicts between safety and security are designed out.

Different authorizations could be required during different stages in the lifetime of the NPP, so it is helpful if a common language and terminology is used to describe these stages. Both safety and security, and the interface, are evaluated at all those stages.

When the same authority is in charge of the two areas, a coordinated stepwise licensing process for safety and security can be one way of ensuring that the expectations of both areas are satisfied in due time. A comprehensive licensing review and assessment process, where safety and security aspects, including their interfaces, are fully integrated into the licensing process facilitates the assessment of changes, considering both safety and security considerations.

For NPPs, along with the preliminary safety analysis report, the licensee submits an initial physical security plan that also addresses the management of interface issues. At the time of first fuel loading, the regulatory body and/or the competent authority will request the licensee to conduct a dedicated drill to demonstrate the functionality and integration of physical security systems followed by an integrated emergency drill, which can include scenarios based on security events.

Even when authorities and licensing processes are different, coordination between authorities is needed to ensure that safety and security approaches are consistent whenever there are interfaces between the two disciplines.

Security analysis requires an extensive understanding of the facility design and safety case in all operating conditions, particularly to identify potential targets, to determine the vital areas. The process of analysing security vulnerabilities also requires relevant subject matter expert opinion, which can envision the various routes by which vulnerabilities can be explored (e.g. adversary sequence modelling) once targets have been identified. A span of security measures or controls can then be identified, with potential benefits and drawbacks for both safety and security. Interdisciplinary expertise to select the most appropriate experience of safety and security events (including at other facilities), together with the measures to be adopted to prevent their recurrence, could assist in the assessment of the licence application.

To support the above expectation, the regulatory bodies can establish joint multidisciplinary specialist teams staffed, for example, by safety specialists who are trained and experienced in radiation protection and external hazards alongside security specialists with expertise in such matters as blast effects and other damages caused by military devices. Alternatively, they could train specialists to acquire expertise on both safety and security. Regulatory bodies can also ask their TSO to establish such teams.

The intent is for the team to be familiar with relevant aspects of both the safety case and the security plan.

Nuclear safety experts have expertise in the accident conditions resulting from a radiological release, but they could have experience in dealing with accidents and faults to a greater extent than the malicious acts of attackers. Similarly, security experts understand the DBT and methods of attacking but, without extensive study and training, are not as familiar with the consequences of an attack on particular structures, systems and components, including those at different plant states and in different stages of the lifetime of the plant.

This combined knowledge assists in the verification of vital area identification studies submitted by licensees that determine any ‘nuclear material/other radioactive material’ and associated facilities, structures, systems or devices the sabotage or failure of which, alone or in combination, through malicious acts as defined in the DBT, could directly or indirectly result in unacceptable radiological consequences. Section 3.6 of IAEA Nuclear Security Series No. 4, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage [34], provides useful practical guidance on the identification of vital areas and the composition of multidisciplinary teams for sabotage margin assessment.

Changes that are significant for safety and security can also be overseen by the regulatory bodies, for example by implementing a dedicated regulatory process or through inspections.

The safety change management process is very important for interface management because it can create important vulnerabilities when managed by staff that are not fully acquainted with nuclear security. Any change to a structure, system, component or equipment that is important to nuclear safety or security needs to be considered in terms of the potential mutual impact of that change. For instance, engineering changes could inadvertently compromise security by making a radiological release easier to achieve. Similarly, modifications to security measures can affect nuclear operations, for example in relation to access control. A formal process needs to be implemented. For example, a checklist mentioning very clearly that security matters have to be considered can help avoid an oversight.

The same process of licensing or authorization can be adopted for NPPs, which takes inputs from the assessment of all relevant areas important to safety and security.

The nature of vulnerabilities created by poor interface management can be permanent, as the two examples mentioned above, or temporary. The creation of a new electric conduit, for example, can create a breach in a physical barrier, as can construction machines that could be used for a malicious act. Temporary vulnerabilities cannot be overlooked, in particular regarding nuclear security, because malicious actors can be waiting to seize such opportunities. This is the reason is why nuclear security also needs to be assessed during working activities.

Change management, at the operator's level, needs to ensure that safety and security are equally considered, in an integrated approach. Impacts of any change need to be assessed to make sure that safety and security are not compromised. The regulatory bodies need to ensure that this process is effective and that, in particular, safety related changes are assessed from the security point of view and vice versa.

Complementing/conflicting areas and development of synergies

Experience and lessons learned in the licensing or authorization process in one area can be useful for the other area (such as verification of vital areas helped by the safety case).

The report of the safety assessment is often made available to the public, with only a small proportion of it being withheld from general access (because of industrial and commercial secrecy, confidentiality concerns, etc.). Nevertheless, detailed information regarding the operating and safety assessment (such as the precise description of operations, locations of equipment or accident analysis) can be very useful for planning and executing malicious actions and has to be considered as sensitive. The public safety assessment therefore intends to contain only information needed for the public, since such information, in general, would not be sensitive.

On the other hand, nuclear security related information is mostly confidential, and the report of the security assessment is limited to a restricted readership within both the licensee and regulatory bodies. The details of the security assessment could be made available on a well defined 'need to know' basis, both by the licensee and the regulatory bodies. Certain details of the security assessment that are not security sensitive can be shared with the public to increase confidence in the independent oversight by the regulatory bodies. A strict process needs to be implemented to assess the sensitivity of both safety and security related information, in particular regarding the public safety assessment and management of the release of such information.

3.1.5. Inspection and enforcement

The regulatory body performs inspections for verification of compliance of the operator or licensee with the regulatory requirements and with the conditions specified in the authorization. Using a graded approach, regulatory inspections cover all areas of safety, security and interfaces for which the facility operator is responsible.

The regulatory body needs to be empowered by provisions within the legal framework to take enforcement actions in case of non-compliance by the operator with regulatory requirements or with any conditions specified in the authorization.

The regulatory body needs to warrant that its inspectors have the essential qualifications, training experience and related tools to perform their roles. The regulatory body can specify qualification and training requirements for inspectors.

The regulatory body has an inspection plan dedicated to interface management. This inspection plan can be drafted together with other bodies within the State that have some responsibility for security and/or safety and may include joint inspections.

Complementing/conflicting areas and development of synergies

Inspection plans from regulatory bodies for nuclear safety and security, if different, could be both joint and aligned. Aligned plans contribute to deconfliction — that is, coordinated and concurrent joint visits by inspectors to a site, asking only once for information from the same person(s) can help to avoid unnecessary burden on the operating organizations. Joint plans can cover safety and security inspectors with similar purposes (e.g. culture, competence, reliability, leadership and management, technical security of computer based systems important to safety). When thoroughly planned and coordinated, with objectives shared and agreed upon in advance, joint inspections can result in real synergy and added value.

The methods of inspection of nuclear security activities can vary in scope and depth during the various stages of the lifetime of a facility. For example, during the inspection of the commissioning phase of an NPP, the system installation for physical protection will be tested and commissioned in an integrated manner. Later configuration control will be applied both on safety and security systems.

Interface arrangements managed or applied during the construction phase need to be verified during the commissioning of an NPP, whereas, at the construction phase, field observation and review of documentation and records will be enough to verify the management of the safety and security interfaces.

There are specific interface areas where inspections could be conducted by the presence of both safety and security inspectors. Such areas are, for instance, computer security (information technology and operational technology) and emergency response.

If performed independently, such inspections can be very ineffective, because each inspector will only deal with his or her own concerns.

The enforcement process is minimally affected by the field to which it is applied. Expertise acquired, lessons learned and good practices identified in both areas (or other areas) can be used for one another. In particular, expertise and experience in legal aspects of regulatory enforcement could be limited to a small number of people within a regulatory body and a State. Pooling such resources that have common regulation and guidance for different regulatory fields such as safety and security could be very useful.

Processes and procedures, including guidance documents for inspectors, for conducting and reporting on nuclear safety and security inspections can be aligned in a helpful manner, particularly when the same authority is in charge of both areas. Shared aspects can be beneficial by emphasizing the common goal of safety and security.

Some principles are shared across both safety and security inspections: the inspection programme, plan, techniques and coordination mechanism for both safety and security; the enforcement process of the regulatory body in case of non-compliances, including the graded approach principle; access to the facility, including admittance for unannounced inspections; the questioning methodology and professional and courteous conduct. Moreover, the consistent use of terminology by the regulatory bodies assists the licensee in understanding what is required.

Inspection findings and enforcement actions can be shared between safety and security inspectors on a need-to-know basis. This is particularly helpful where the issue potentially covers both safety and security, such as culture, modifications, leadership and management and supply chain. It is helpful in finding common root causes for failures across both safety and security and also in highlighting synergies — for example, a finding in nuclear safety competence management could be equally applicable to security competence. However, it is important to maintain the confidentiality of security information, which can be shared only after a careful consideration of its risk benefit.

The development of a joint process needs to ensure a fine balance between harmonization and specialization to prevent diluting specificities and expertise needed from each area.

Specificities of each area need to be also considered in the enforcement process. For example, if not properly planned, corrective actions for addressing a safety finding could create a security vulnerability and vice versa. Similarly, conflicting regulatory expectations, both from a tactical and strategic perspective, could be disclosed. Furthermore, details of security inspection findings could involve a more limited disclosure than details of safety inspections. That is why the enforcement process needs to be adapted to avoid such situations.

One way to address this risk is to also use a performance based regulatory approach for enforcement actions. For example, instead of requiring an operator to implement a specific provision (e.g. a specific barrier, detector, procedure), the regulatory body could issue a reminder to this operator regarding the requirements that have not been met and require the operator to find a solution, within a limited timeframe, that will meet the requirements. It will then be the responsibility of the operator to solve the safety or security requirement, without mutual compromise.

A coordinated process for enforcement can consider both safety and security. When the same regulatory body oversees both safety and security areas, all competent sections of the regulatory body need to be involved in decisions of enforcement actions. This practice enables the regulatory body to consider interface issues in its final decision and combine both approaches.

Effective management provides training for safety inspectors in essential security matters and vice versa. One of the benefits of this is to minimize the possibility of inadvertently introducing a vulnerability through the actions undertaken during an inspection or because of corrective actions. Such training can also assist safety inspectors to identify security issues during inspections and vice versa. Management needs to ensure that discussion of inspection findings between safety and security inspectors takes place to prevent such vulnerabilities.

National requirements and framework will dictate the extent to which information can be disclosed.

3.1.6. Review and assessment, including analysis of operating experience

Learning from experience is an essential element of review and assessment activities. This includes an analysis of relevant good practices by both the operator and the regulatory bodies. It is essential to ensure that the review and assessment addresses the interfaces between safety and security. However, when reviewing security, it is necessary to restrict certain information to those personnel with a need to know. This might complicate a joint review when it could otherwise have been possible.

While cyber security has been an issue for a long time, the new focus on the nuclear industry is now a reality. Regulatory bodies will need to increase their knowledge and awareness of cyber security threats and develop expertise and organizations to address computer based systems and security that could impact operations. Experts for computer and cyber security will identify computer security issues that need to be remediated during the design review. The experts could also provide industry guidance and best practices within a facility to increase the computer security regime.

At an early stage of design, the regulatory body needs to encourage the licensee to take input from probabilistic safety assessment into account to complement the list of vital area components [34].

Review and assessment, including analysis of the operating experience, can be considered equally applicable to the competent authority reviewing its own experiences as well as to reviewing the licensees' reports.

Some States conducted licensing reviews and assessments in an integrated manner, in which the team finalizing licensing issues dealt with both areas. Hence, an issue which impacted safety or security was resolved through a synergetic approach. During review, special care is taken to highlight and evaluate the dependencies between safety and security systems. For example, dependency of the PPS on safety systems (e.g. power supply) is reviewed and ensured to avoid any problematic situation at a later stage of the NPP.

Complementing/conflicting areas and development of synergies

Having conducted a review and assessment, it is considered good practice to learn from its results by implementing improvements to processes, procedures, training, etc.

The principles and rationale for review and assessment are common for safety and security. In this respect, expertise acquired, lessons learned and good practices identified in one area can be used for the other.

There is a potential benefit in conducting reviews and assessments that consider both the nuclear safety and security perspectives. The interface areas themselves — including regulations, technical aspects and processes to coordinate the interface — merit review and assessment. As an example, the Romanian regulation contains some specific requirements concerning review and assessment. A joint review of the safety and security performance that includes specialists from both disciplines and the licensees can be useful in ensuring a shared understanding of concerns and agreeing on strategies and tactics to resolve them.

Input for review could include feedback from the analysis of operating experience, field experience of safety and security experts, relevant information from incident and inspection reports and lessons learned from exercises.

Review and assessment need to also cover the effectiveness of the management of the interfaces between the two areas, in particular to verify that they do not adversely affect each other and that, to the degree possible, they are mutually supportive. The regulatory body could also consider periodic safety and security reviews to assess the effectiveness of the management of the interfaces between them at an NPP. Drills and exercises, involving experts from both fields, could also be a very effective way to assess the effectiveness of crisis management for events combining safety and security aspects.

If some changes are identified during review and assessment, personnel need to be aware of the need to manage interfaces, as described in Section 3.1.3. Solutions could consider the balance between safety and security in a holistic way to find a solution that is the best for the protection of people and the environment.

It is useful for competent authorities to conduct review and assessment and analyze operating experience using a common methodology.

The regulatory bodies of some States insist that all licensees of NPPs revise and report their assessments on nuclear security events using the same process as nuclear safety events. The decision is supported both by the 'traditional provisions' on nuclear security but also by the more 'general provisions' on safety assessment. If there is a common process for reporting events and gathering operating experience, it needs to cover the full range of potential security and safety aspects.

When reviewing and assessing areas that may cover the safety-security interface, the competent authorities need to involve experts of both fields in the review. Similarly, the authorities need to verify that the licensee has a process in place to identify potential interface issues with a view to finding solutions that satisfy safety and security.

The national requirements and framework will dictate the extent to which information can be disclosed. Regulatory bodies can have a useful role in sharing operating experience and its analysis between different licensees. Where this may contain sensitive information, the regulatory body will have to form a balanced judgement of the benefits of sharing, the need to know, etc.

In Brazil, important items are listed in terms of their relevance, both for safety and security. This list can be used for assessment, inspection and enforcement. For example, an emergency door that can play a role in containment can also have an impact in security.

3.1.7. Consistency of regulatory control

Consistency and stability of regulatory control are equally important for safety and security and are based on the same principles; for example, a graded approach; decisions and sanctions proportionate to the importance of issues; limitation of subjectivity in decision making; ability to justify decisions if challenged; and transparency regarding criteria taken into consideration for a decision. The process needs to be well documented, comprehensive, cover all regulated activities and facilities and ensure a clear allocation of responsibilities.

Complementing/conflicting areas and development of synergies

Expertise acquired, lessons learned, and good practices identified in either area (or other areas) regarding consistency of regulatory control can be used for the other, and each area can benefit from cross-pollination.

Consistency in terminology is also helpful. Consistency in terminology may be, for example, a common way to describe the level of non-compliance and the regulatory tools that can be used to address it. This consistency helps strengthen leadership and culture by showing that the same principles are recognized and applied by experts of very different areas, while differences could lead to consider or disregard them.

Moreover, consistent terminology helps ensure a common understanding of each area, with their commonalities and their specificities. Better mutual understanding is a first step towards a better mutual acknowledgment of importance and relevancy of the other area.

Such synergetic effects can be further enhanced by recalling that the goal of both safety and security regulation is to prevent and minimize radiological consequences resulting from a nuclear incident, regardless of the cause.

Because of the aforementioned similarities, it is possible and even beneficial to follow the same process for safety and security control, particularly when the same authority is in charge of both areas.

It can be beneficial for competent authorities to evaluate safety and security risks through a common risk metric, in particular where there is a potential conflict between them, to choose the best solutions for both safety and security in a given situation (see Ref. [35]).

In Sweden, for example, a risk informed, systematic oversight is in place to ensure that all parts of the regulatory code are covered consistently for most of the oversight activities (see Annex II).

Consistency of regulatory control could be increased by using similar internal regulatory procedures for licensing, authorization, inspection and enforcement as well as for emergency preparedness and response activities.

Consistency in the licensing process of NPPs can be achieved by issuing a single operational licence that includes safety and security provisions. All competent sections of the regulatory body need to be involved and the licence issued with the consent of all parties. For the proper assessment concerning interface issues, it is a good practice to set up dedicated working groups from the staff of the competent sections involved in the licensing procedure.

Inspections are conducted in both areas based on a similar process, including common elements of preparatory, on-site and post-inspection evaluation activities.

In dealing with safety and security interfaces, consistency is not necessarily a goal. It is a strategy to avoid problems, but sometimes specific tailored approaches can be more effective or are necessary. For example, the sensitive nature of some security information could lead to certain specificities regarding approaches for safety and security. There are other organizations within the State with security responsibilities, which could impact on the way nuclear security regulation is undertaken, further impacting the consistency of approach with nuclear safety.

Looking for consistency does not negate the relevance of past approaches. On the contrary, diversity of approaches can be seen as an opportunity for mutual learning among experts and improvement of awareness that both safety and security disciplines have their own specificities and that complete consistency is not always necessary, desirable or possible.

3.1.8. International cooperation

International cooperation is recognized as beneficial for both safety and security. Nevertheless, specificities of the two areas often lead to different practices and organization. For example, points of contact for the Convention on Nuclear Safety [36] and the Convention on the Physical Protection of Nuclear Material and Its Amendment [37, 38] are often different at the State level.

Roles and responsibilities for international cooperation need to be described and assigned. Depending on the State, the assigned staff member can be a member of the competent authority or of the office of foreign affairs. Within one State, the staff holding these roles could coordinate effectively with each other.

International cooperation is especially important in the case of the preparation for nuclear emergencies with transboundary radiological consequences. Sharing of information during a nuclear emergency, particularly if it was caused by a malicious act, can be challenging. Therefore, it is important for neighbouring States to have established preparations for an effective dialogue. In this context, para. 3.57 of GSG-14 [30] recommends:

> "To the extent possible, bilateral and multilateral agreements should be established at the preparedness stage on the coordination necessary for disseminating accurate information on an emergency to the public in neighbouring States in a timely manner. A coordination mechanism (e.g. using national disaster response tasks forces or regional emergency response networks) prepared and exercised in advance should be established by the organization in the State with the main responsibility for the public communication response in an emergency."

For example, it can be useful to distinguish information that is related to the protection of people and the environment and that needs to be shared with neighbouring States, from strictly security related information (e.g. number and means of attackers, detail of the response) that can be protected in order to provide an effective response. Sometimes, the need to protect information can be temporary (e.g. until the attack has been terminated). Such information needs to be released in a very controlled manner. The release of information regarding the environment can be, at least in part, the responsibility of the safety authority, including an authority at the international level; however, security information is generally managed at the State's level. For incidents related to nuclear security, all competent authorities have to coordinate their communication to avoid inconsistencies and release of information that can hinder safety or security.

There could be benefit in conducting international drills and exercises involving two or more States that cover the possibility of nuclear emergencies, including those with malicious initiators. One area that can be particularly useful to consider, given it often involves crossing borders, is the transport of nuclear material. The organization of such exercises is complex, but it merits the effort.

International cooperation is also very beneficial for benchmarking and peer review and advisory missions. In particular, the IAEA provides such services for both safety and security. These services increasingly take into account the management of interfaces between safety and security.

It can be beneficial to include a safety expert in an IPPAS mission [39] or a security expert in an IRRS mission [40] held by the IAEA. The participation of such experts will not only help to better understand the concept of safety-security interfaces but also assist States to incorporate and manage the interface issues in an acceptable manner.

Nuclear security needs to consider confidentiality constraints. Confidentiality can hinder international cooperation, but a well documented process for determining whether nuclear information is actually sensitive or whether it can be shared is helpful in lowering this barrier. It is necessary and helpful to share some sensitive, confidential information with trusted international partners. Many States have signed agreements with other States to provide a process for sharing such confidential information and this is a good practice. During a nuclear emergency with a malicious initiator that has the potential to cross international borders, the barriers to sharing confidential information could be reduced.

It is normally easier to share security information among a smaller number of States. Therefore, two or more States can have useful bilateral or regional exchanges for the safety-security interface.

Safety and security culture using the methodologies for assessment by employing the methods suggested either by the IAEA or others can be conducted even at the international level to evaluate the effectiveness of the interface.

Complementing/conflicting areas and development of synergies

It is recognized that during expert missions and IAEA peer review missions (such as IRRS including the scope of the safety-security interface), less detailed information is disclosed about security arrangements.

Nuclear security is a cross cutting area that can be handled with collaborative effort. Joint safety and security missions will help to identify gaps in regulations, processes and practices in an integrated manner. Corrective action plans to fill these gaps will help to consider the synergy in addressing safety and security together. Interface modules can act as a bridge between safety and security missions.

There could be a benefit of combined missions, but care needs to be exercised in the kind of information being shared, especially about the security arrangements.

3.2. LEADERSHIP AND MANAGEMENT FOR SAFETY AND SECURITY

Leadership and management are important aspects for both safety and security and need to be addressed at the highest levels of an organization.

In case of a single regulatory body for matters related to safety and security, an integrated management system (IMS) supports the leadership in systematically responding to interface issues. Leadership needs to be aware that, to some extent, differences can exist, but these differences might be documented and widely known and acceptable within the organization. Similarly, management of safety and security has different constraints, but execution of processes as described in the IMS can be applied to both regimes.

Safety and security principles stipulate that safety and security measures have in common the aim of protecting human life and health and the environment. Commonalities and differences in safety and security practices can be both recognized and used with the intention of utilizing their synergies.

3.2.1. Leadership for safety and security

Effective leadership and management of nuclear safety and security within the regulator's organization is essential, and due regard needs to be paid to the synergies in these areas. The organization needs to reflect the fact that safety and security are considered equally important, with clear values and associated behaviours that support safety and security within the system. This starts with senior management (both at the regulatory body and operator's level) viewing both fields as equally important, and this could be stated unambiguously in the organization's policies.

Some States allow frequent rotation of staff between the two domains (i.e. safety and security).

For example, positions, opportunities for advancement, and salaries of people in charge of safety and security will be similar. Also, people need to be encouraged to switch from security to safety and vice versa.

3.2.2. Integrated management system

An IMS is imperative to support the processes and measures necessary for the timely identification and adequate resolution of any potential conflicts between the requirements of nuclear safety and security. Concerns about safety and security could be embedded in any relevant processes and procedures.

An IMS with clear processes and procedures facilitates the management of the interfaces between safety and security, and as an integral part of the IMS, the organizational structure and allocation of resources of the regulatory body reflect the regard given to safety, security and their interface activities. A clear organizational structure with well-defined roles, responsibilities and reporting mechanisms is essential to avoid conflicts between safety and security and influences how effectively the safety and security interfaces are managed. An effective organizational structure, including the chain of command, allows for the alignment of regulatory processes and procedures. The IMS would also promote safety and security cultures as an essential ingredient for leadership and management. The regulatory body needs to promote strong safety and security cultures internally, at the operator and at both organizational and individual levels in all activities to achieve the highest degree of safety and security and their interfaces. Safety culture and security culture need not be merged into one culture, but each can be established and maintained in a complementary manner with the other so that potential contradictions are minimized.

The organization could try to build a common ground to ensure that staff feel an element of personal responsibility in achieving safety and security culture. It could establish key values and elements of the organizational culture to integrate safety and security culture in a coherent manner and to allow the regulatory goals and objectives to be met by safety and security staff in an efficient and effective way. Safety and security culture aspects also need to be considered while defining the lines for internal communication.

Due to the increased usage of digital technology even within the regulatory domain (i.e. online display of plant critical parameters for emergency assessment), cyber security has to be addressed in the IMS to complement both safety and security.

Complementing/conflicting areas and development of synergies

An IMS defines the responsibilities for safety and security. The organizational structure and allocation of resources have an impact on the effectiveness of managing the safety-security interface. The regulatory body can address in its management system its commitment to allocating adequate resources to perform safety, security, and their interface responsibilities effectively. An effective and efficient organizational structure with well-defined roles, responsibilities and reporting mechanisms can manage regulatory functions and tasks to enable inclusion of interface considerations and avoid conflicts. Some States have two separate working units dealing with safety and security, and in such cases, the management system might describe the processes through which interface issues and communication between the two units will be addressed. If practically possible, the management of interfaces can also be performed through assignment of tasks — for example, the coordination of oversight tasks for NPPs in operation — to identify synergies and foster cooperation between safety and security experts from different parts of the organizational structure.

It needs to be widely known within the organization and documented in the IMS that everybody has safety and security responsibilities. Therefore, accountability, a questioning attitude, trustworthiness and avoidance of complacency support strong cultures regardless of the role of the staff. An effective management system promotes a culture that recognizes both safety and security. The sensitive nature of some security information does not always allow a consistent approach between safety and security cultures. Nevertheless, cultures for both safety and security require common grounds. This may include information sharing, a questioning attitude, trustworthiness and openness. On the other hand, as security deals with deliberate acts, the security culture requires different attitudes and behaviours from those associated with the safety culture. Encouraging a culture of open reporting, free of blame, is another important aspect of an effective safety-security interface. It is important that leadership which includes both safety and security professionals needs to understand that there are differences in outlook and culture and these differences need to be respected.

Culture within an organization is an important area. Clear interfaces and good regulatory practice can act in a way that promotes a culture that recognizes the importance of both safety and security. Furthermore, regulatory bodies, like other organizations, are not immune to the risks posed by insiders and poor culture. Certain policies and practices can assist both safety and security and aim to support staff across a range of personal circumstances — such as stress, relationship breakdown, addiction, and financial difficulties — that could lead to risky behaviour (in both a safety and security context) if left ignored and unsupported.

3.2.3. Promotion of safety and security culture

Both safety culture and security culture need to be promoted as part of the organizational culture and management system as stated in Section 3.2.2. The regulatory body needs to promote strong safety and security cultures internally and emphasize its overarching impact on operating organizations and among all interested parties, at both organizational and individual levels in all activities to achieve the highest degree of safety and security and their interfaces. Culture for safety and security cannot be merged into one culture but each can be established and maintained in a complementary manner with the other so that potential contradictions are minimized.

The organization will try to build a common ground to ensure that all people feel the need to be concerned with safety and security. There is a need to establish key values and elements of the organizational culture that integrate safety and security culture in a coherent manner and allow the regulatory goals and objectives to be met by safety and security staff in an efficient and effective way. Safety and security cultural aspects also need to be considered while defining the lines for internal communication.

Complementing/conflicting areas and development of synergies

A common goal is to recognize the risk of undesirable radiological consequences, whether the cause is a safety event or a security event.

Every member of the organization is responsible for the implementation of the safety and security cultures. Accountability, a questioning attitude, trustworthiness and avoidance of complacency need to be addressed regardless of a staff member's role within the organization. An effective management system promotes an organizational culture which recognizes both safety and security.

The sensitive nature of some security information may not always allow a consistent approach by safety and security cultures.

As security deals with deliberate acts, security culture requires attitudes and behaviours different from those associated with safety culture.

Both safety and security professionals need to recognize that there are differences in the two cultures, and that it is very important to respect these differences.

Training programmes for all staff, at both the regulatory body and the operator, impart awareness for the promotion of safety and security cultures. Exercises including both safety and security concerns and involving all personnel (e.g. with sheltering applied to all workers during a security event) could also help raising their awareness on interfaces between safety and security.

The culture within an organization is an area of clear interface, and regulatory practice can act in a way that promotes a culture that recognizes the importance of both safety and security. Furthermore, regulatory bodies, like other organizations, are not immune to the risks posed by insiders and poor culture. Certain policies and practices can assist both safety and security and aim to support staff across a range of personal circumstances such as stress, relationship breakdowns, addiction and financial difficulties. These could lead to risky behaviour (in both a safety and security context) if left ignored and unsupported.

Encouraging a culture of reporting that is open and free of blame is another important aspect of an effective safety-security interface.

3.2.4. Organizational structure and allocation of resources

The organizational structure and allocation of resources of the regulatory body reflects the emphasis given to safety, security and their interface activities and is an integral part of an IMS as discussed in Section 3.2.2. Consequently, the effectiveness of the management of the interfaces between safety and security is influenced by the organizational structure. An effective organizational structure, including the chain of command, allows for the alignment of regulatory processes and procedures, which has been described as having benefits to both the regulatory body and the operator.

Complementing/conflicting areas and development of synergies

The IMS defines the safety and security responsibilities.

The existence of separate organizations responsible for safety and security could make it difficult to handle potential conflicts. Nevertheless, conflict has the advantage of exposing root problems or different perspectives and, if well managed, can help global improvement. On the other hand, a structure that is primarily led by one of the disciplines could be inclined to favour that discipline in allocating resources and decision making — a situation that ought to be handled with great care.

The organizational structure and allocation of resources may have an impact on the effectiveness of managing the safety-security interface. The regulatory body needs to address in its management system the fact that it is committed to allocating adequate resources to perform safety, security and their interface responsibilities effectively.

An effective and efficient organizational structure can manage regulatory functions and tasks to enable the inclusion of interface considerations. A clear organizational structure with well defined roles, responsibilities and reporting mechanisms is essential to avoid safety and security conflicts. The differences in the technical areas for safety and security require close cooperation of departments. The management of interfaces can also be achieved through an assignment of responsibilities, for example the coordination of oversight tasks for NPPs in operation to make sure that synergies and cooperation are found between safety and security experts from different parts of the organizational structure.

3.2.5. Staffing and competence of the regulatory body

Having adequate and competent staff enables the regulatory body to effectively fulfil its role. The regulatory body determines the necessary qualification and competence of staff with safety and security responsibilities. It also determines the number of staff within both safety and security functions that is necessary to fulfil its responsibilities.

The regulatory body establishes nuclear safety and security education and training programmes that develop the competence needed for both areas.

To the extent that the regulatory body has a function during nuclear or radiological emergencies, both safety and security need to be considered during training of regulatory staff.

Complementing/conflicting areas and development of synergies

Because safety and security are both important to consider for anyone in the nuclear context, all staff at the operator and the regulatory body have some basic training in both areas. This training supports the promotion of safety and security cultures.

Cross training, as well as specialized training, may be delivered using by the same infrastructure, which has benefits in relation to cross-fertilization of ideas, using a common language, etc.

The regulatory body may devise an approach in which some common training areas are identified, and staff will be trained in these areas irrespective of their domains (i.e. safety or security). This common approach will not only increase the capacity and competency of the staff to highlight the interface issues but also help the regulatory body to rotate a staff member from one domain to another.

Providing the same basic induction training programme for safety and security staff on the regulatory functions and practices highlight the safety and security aspects as well as their interface. Regular refreshment training programmes ensure the collaboration of both safety and security experts.

Management oversight may be employed to verify that one particular regulatory viewpoint is not emphasized to the detriment of the interface.

The regulatory body may choose to utilize the four-quadrant model for regulatory competence outlined in IAEA-TECDOC-1757 [41] in developing regulatory competencies necessary for addressing the safety-security interfaces. The regulatory body provides training for core regulatory functions and specialized areas of safety and security as well as their interfaces.

Basic competence for security ought to be necessary for safety personnel and vice versa for the proper management of interfaces at the organizational level. The training and awareness programmes for safety personnel and security personnel will be repeated as appropriate and in response to emergent issues. Some training modules, for example those regarding crisis management, can also contain aspects of both safety and security and be used for all personnel. Such trainings, when they contain team drills, can help people from different backgrounds to get to know each other and to break silo effects.

Training regarding the interfaces between safety and security will not be limited to technical concerns but also include organizational and management aspects. For example, training of managers to address the personal difficulties of their subordinates can cover, in addition to the well-being of the personnel, both safety concerns (their ability to accomplish the tasks related to safety) and security concerns (an unusual behavior can be an indication of an insider threat).

A common staffing policy can also be of mutual benefit to safety and security. For example, staff rotation within each discipline may be a valuable tool to avoid complacency and lack of objectivity, while career paths involving experience in both areas can significantly help to break silo effects.

Regulatory bodies can use external technical support for both safety and security to cover gaps in capacity and/or capability.

3.2.6. Human factors

The development of programmes and resources concerning human performance needs to treat elements of human factors in considering the interfaces between safety and security.

Complementing/conflicting areas and development of synergies

Human factors apply to both safety and security. For example, cognitive biases can affect both safety and security. The organization of security and safety takes into consideration human factors to guarantee that the performance of important human tasks can be effective in any situation, including acknowledgement that security events lead to situations that may be different from safety events. It is important to find relevant expertise and not to assume that experts on human factors trained for safety or security, respectively, are competent to deal with any situation. Safety and security measures need to both be explained and proportionate to the goal in order to be understood and accepted.

It is nevertheless important to take into account that nuclear safety and nuclear security may have very different perspectives regarding human behaviour. In nuclear safety, the emphasis is often placed on the right to make mistakes, to encourage employees to detect and report any problem, including those caused by one’s own mistake. In nuclear security, any problem caused by an individual is analysed to identify a potential insider threat.

In reality, these differences are superficial, because for both areas, a balance has to be found between complacency and understanding. For both, people are resources that cannot be replaced by machines, even if they can sometimes be a risk or a threat. But these different perspectives can be taken into consideration when analyzing human factors to ensure that organizations address both concerns equally.

3.3. COOPERATION AND JOINT ACTIONS AMONG COMPETENT AUTHORITIES AND TECHNICAL SUPPORT ORGANIZATIONS

Based on a State’s legal system, different authorities can be assigned separately the responsibility for safety and security. Care needs to be taken while developing rules and regulations for carrying out different authorizations by different State entities. Identification of areas where cooperation is needed has to be known to each entity, and joint actions among competent authorities can optimize resources for carrying out their activities. Cooperation and joint actions involving nuclear security and safety authorities can enhance the mutual understanding of issues related to:

(a) Information protection;
(b) Training and awareness;
(c) Technical exchanges;
(d) Regulatory work on safety-security interfaces, including submission of safety case addressing consequences of security attacks;
(e) Radioactive sources;
(f) Coordinated inspections;
(g) Exercises and drills;
(h) Information in case of a nuclear event.

To present nuclear related information in international settings, as well as at the State level, States can consider joint work among the different interested parties. In this regard, regular meetings at both the top management level and the working level could be a regular feature. An agreement reached during such meetings may be considered in the revision of regulatory processes to manage the interface issues. At some point, this agreement can also be incorporated in the revision of the regulatory framework to inform the licensee in time and to minimize the effort of the licensee. The sharing of information regarding the implementation of regulatory processes is based upon different principles for safety and security. For safety, experiences gained from the implementation of regulatory processes are shared widely. Whereas, for security, information is shared based on a ‘need to know’ approach. The interfaces between safety and security during communication and consultation may consider the guidance provided in IAEA Nuclear Security Series No. 23-G [27].

Similarly, care needs to be taken when the regulatory body entrusted with both mandates of safety and security sets up advisory bodies to provide advice in matters related to safety, security and their interface. In accordance with IAEA-TECDOC-1835 [42], advisory bodies and TSOs can contribute to the management of interfaces, providing expertise on safety and security matters.

Involvement of advisory bodies and TSOs in security related activities may require access to nuclear security information. In such cases, this information could be handled in accordance with the relevant national requirements to protect the misuse of restricted information, especially related to the security regime.

Complimenting/conflicting areas and development of synergies

A TSO can be entrusted with a wide range of missions concerning both safety and security, from providing advisory services to operational tasks (e.g. radiation measurements in case of radiological emergencies, independent safety assessments, supervision of the transport of nuclear material, communication regarding radiological situations). Depending on the missions, they can be directly concerned with safety and security interfaces. The division of tasks and procedures needs to be carefully organized. For example, the intervention of radiation protection experts to assess the radiological consequences during a security event needs to be carefully performed, with due consideration given to avoid exposing these experts to security situations. Sometimes, TSOs or other competent authorities can be entrusted with providing technical information to the public, both in normal conditions and in emergency situations. Technical information is often more sensitive than general information. Therefore, TSOs or other competent authorities may be at risk of compromising, by mistake, sensitive information. They need to have a robust process in place to assess the sensitivity of any information that can be released.

3.4. COMMUNICATION AND CONSULTATION WITH THE OPERATING ORGANIZATION AND THE PUBLIC

Communication and consultation with the licensees and the public is the responsibility of the regulatory body. The purpose of this interaction is to keep licensees informed about the safety and security of their facilities, regulatory decisions, regulatory processes and practices, and operating experiences. Communication and consultation with the public and other interested parties are important means to share information and to maintain a dialogue throughout the lifetime of a nuclear facility. Communication is not a goal but a strategy to foster open discussions, provide information that is needed by national legislation, and facilitate the sharing of knowledge and experience.

Complementing/conflicting areas and development of synergies

Communication and consultation of safety and security matters need to be managed with full awareness of commonalities and potential ambiguities. While both safety and security need the confidence of the public, the level of information sharing and transparency can be quite different for both aspects. Communication and consultation policy can require governmental approval for security related matters. Therefore, the regulatory body needs to develop and implement a communication and consultation strategy that addresses the safety concerns of the public, ensuring transparency while protecting sensitive security information that is in accordance with national requirements. The confidentiality of security related information will normally restrict communication and consultation and will require an approach based on the need to know.

The regulatory body can allow and facilitate members of the public to report safety and security concerns and to be considered in the regulatory decision making. Regulatory bodies can support joint attendance at meetings with interested parties, including meetings attended by non-governmental organizations. This unified approach to public engagement gives confidence that the regulatory body works in a collaborative manner to address the concerns of the public and ensures that the relevant experts are at the table to comprehensively answer a wide range of questions that may be asked.

It is essential to note that the confidentiality of security information is not only due to its origination from a security source — the important consideration is whether the information is useful to somebody with malicious intent.

3.5. EMERGENCY AND CONTINGENCY PLANNING AND RESPONSE

Planning for and response to nuclear accidents or sabotage events is a major area of interfaces between safety and security, requiring coordinated efforts of both. The regulatory body sets the requirements for emergency and contingency plans and verifies the implementation of these plans through an observation of drills and exercises.

Emergency plans for safety events and contingency plans for security events need to be available, understood by the staff with responsibilities for implementing them, and be mutually supportive and complementary.

The regulatory body ensures the proper liaison for coordinated execution of facility plans and national emergency and contingency plans.

Complimenting/conflicting areas and development of synergies

The response to both safety and security events involves mobilizing the internal emergency response function and potentially also off-site responders and agencies. As external response forces supporting a contingency response at an NPP will likely be the same forces that would respond to nuclear security events involving material out of regulatory control elsewhere, it is important to recognize that these forces might not be familiar with the relevant contingency plans and procedures inside an NPP, so they might be involved in regular exercises, including the testing of command and control arrangements.

Both safety and security use drills and exercise to refine and validate the effectiveness of the response plans and procedures. In addition, joint emergency exercises may be conducted to periodically test the implementation of emergency and contingency plans, to assess and validate the adequacy of the coordination between organizations involved in responding to various scenarios.

There is need for relevant staff and responders to be trained and ready to respond at short notice to either a safety or security event.

When an event initiates, the operator might not immediately know the cause (malicious or accident) but must respond anyway.

Security responses and barriers may impede the safety response, including the response of external agencies.

Aspects of the contingency plan may be confidential.

The actions to mitigate the consequences of a radiological release may contradict the principles of preserving a crime scene.

Emergency planning and response is an area in which close working and cooperation is essential. During the development of both contingency and emergency plans, due regard might be given to ensuring that they are mutually supportive and complementary. This is particularly the case for aspects such as access control. The regulatory body needs to review contingency plans for security events, mindful that they are developed to allow for emergency responders to access, when necessary, to deal with the event.

While giving top priority to safety, attention might also be paid to preserving the event scene for future investigations and lessons learned.

Emergency and contingency response planning needs to be coordinated to ensure that, regardless of the initiator, a command structure is in place.

Regulatory practice may include ensuring joint representation at safety and security exercises and encouraging licensees to design scenarios with elements of both disciplines. However, consideration needs to be given to the fact that a scenario based on a security initiated event resulting in radiological consequences is likely to be reliant on the security response having failed and, therefore, might not achieve regulatory expectations for that part of the exercise.

REFERENCES

[1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006),
https://doi.org/10.61092/iaea.hmxn-vw0a

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Governmental, Legal and Regulatory Framework for Safety, IAEA Safety Standards Series No. GSR Part 1 (Rev. 1), IAEA, Vienna (2016).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016),
https://doi.org/10.61092/iaea.cq1k-j5z3

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013),
https://doi.org/10.61092/iaea.ajrj-ymul

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011),
https://doi.org/10.61092/iaea.ko2c-dc4q

[8] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014),
https://doi.org/10.61092/iaea.u2pu-60vm

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Safety Infrastructure for a Nuclear Power Programme, IAEA Safety Standards Series No. SSG-16 (Rev. 1), IAEA, Vienna (2020).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Organization, Management and Staffing of the Regulatory Body for Safety, IAEA Safety Standards Series No. GSG-12, IAEA, Vienna (2018).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Functions and Processes of the Regulatory Body for Safety, IAEA Safety Standards Series No. GSG-13, IAEA, Vienna (2018).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Operations Manual for Incident and Emergency Communication, Emergency Preparedness and Response, EPR-IEComm (2019), IAEA,Vienna (2020).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

[16] Convention on Early Notification of a Nuclear Accident, INFCIRC/335, IAEA, Vienna (1986).

[17] Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, INFCIRC/336, IAEA, Vienna (1986).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, INES: The International Nuclear and Radiological Event Scale User’s Manual, 2008 Edition, IAEA, Vienna (2013).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Survey and Site Selection for Nuclear Installations, IAEA Safety Standards Series No. SSG-35, IAEA, Vienna (2015).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Licensing Process for Nuclear Installations, IAEA Safety Standards Series No. SSG-12, IAEA, Vienna (2010).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Response and Assistance Network, EPR-RANET (2018), IAEA, Vienna (2018).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication and Consultation with Interested Parties by the Regulatory Body, IAEA Safety Standards Series No.GSG-6, IAEA, Vienna (2017).

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28-T, IAEA, Vienna (2017).

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[29] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015), https://doi.org/10.61092/iaea.3dbe-055p

[30] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERPOL, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS OFFICE FOR OUTER SPACE AFFAIRS, Arrangements for Public Communication in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-14, IAEA, Vienna (2020).

[31] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).

[32] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2013).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA-TECDOC-1868, IAEA, Vienna (2019).

[36] Convention on Nuclear Safety, INFCIRC/449, IAEA, Vienna (1994).

[37] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[38] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1/Mod. 1 (Corrected), IAEA, Vienna (2021).

[39] INTERNATIONAL ATOMIC ENERGY AGENCY, International Physical Protection Advisory Service (IPPAS) Guidelines, Services Series No. 29, IAEA, Vienna (2014).

[40] INTERNATIONAL ATOMIC ENERGY AGENCY, Integrated Regulatory Review Service Guidelines, IAEA Services Series No. 37, IAEA, Vienna (2018).

[41] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodology for the Systematic Assessment of the Regulatory Competence Needs (SARCoN) for Regulatory Bodies of Nuclear Installations, IAEA-TECDOC-1757, IAEA, Vienna (2015).

[42] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical and Scientific Support Organizations Providing Support to Regulatory Functions, IAEA-TECDOC-1835, IAEA, Vienna (2018).

Annex I

GOOD PRACTICES IDENTIFIED IN IRRS AND IPPAS MISSIONS REGARDING THE INTERFACES BETWEEN SAFETY AND SECURITY

This annex compiles good practices relating to the safety-security interface identified during two different types of IAEA peer review mission hosted by many IAEA Member States: Integrated Regulatory Review Service (IRRS) and International Physical Protection Advisory Service (IPPAS). These good practices are part of the final reports issued at the conclusion of the review mission. Good practices are identified in recognition of an outstanding organization, arrangement, programme or performance superior to those generally observed elsewhere. They will be worthy of the attention of other regulatory bodies or competent authorities as a model in the general drive for excellence [I–1, I–2].

(a) Determination of design basis conditions:
  - In assigning systems, structures and components that need to be protected against malicious acts in order to prevent a radiological threat, the regulatory body, together with the supervisory authority for nuclear safety, has issued a guideline. For all existing nuclear facilities, this guideline defines which systems and/or material have to be located in which of the defined security zones.
  - The classification of the vital areas into two categories supports a graded approach to physical protection against sabotage and the relative allocation of protection resources in risk management.

(b) Drafting regulations and guidance:
  - The regulations and guides issued by the regulatory body to avoid the potential for adverse effects on safety from security and vice versa are comprehensive and provide an appropriate framework to ensure that the licensees put in place an adequate management of the safety-security interfaces.

(c) Licensing and authorization:
  - In addition to nuclear safety, emergency preparedness and radiation protection, the licensing process also places a heavy emphasis on physical protection. Facility operating licences are issued for a described period of time. Before a licence can be reissued, the licensee must demonstrate that current physical protection regulations have been met. This demonstration includes demonstrated cooperation with other supporting agencies, such as the national police and local

authorities. Licences are reissued based on subsequent safety analysis reports.

(d) Inspection and enforcement:
  - The regulatory body has integrated its security inspection and oversight programme into its integrated system for plant oversight.
  - The regulatory body has 'resident inspectors' at nuclear power plants and other high risk facilities. The primary role of resident inspectors is to provide a continuous presence at the site to ensure compliance with safety, security and emergency preparedness requirements. These inspectors are trained to detect significant nuclear security problems and will communicate any anomalies with either the regulator's headquarters or the relevant regional regulator's office. This provides potential for the early detection of any degradation of nuclear security at sensitive facilities.

(e) Review and assessment, including analysis of operating experience:
  - The integrated approach adopted by the regulatory body in the review and assessment as well as supervision of plant modifications, which always involve in a systematic manner safety and security experts, promote a very effective management of the existing interfaces so as to optimize mutual benefits on nuclear safety and security measures and to avoid possible mutual detrimental effects.
  - The systematic analysis of significant non-nuclear events not only in the safety-security interfaces but in the entire operating experience programme, the coordination and communication of the operating experience analysis to make them suitable for different uses and applications inside the regulatory bodies is considered a good practice.

(f) Staffing, competence and training of staff:
  - The regulatory body and competent authorities have established a comprehensive system for addressing the interfaces between safety and security, including identification of specific technical areas sensitive to conflicts between safety and security, joint safety security inspections, organization specific workshops and training.
  - To enable the guards to act properly in a case of a malicious act endangering the safety of the NPP, group exercises are conducted using teams that work together in normal operation with their dogs. One of the supervisory authorities for nuclear safety's regulation defines annual emergency exercises involving safety and security staff to improve the cooperation.

(g) Cooperation and joint actions among the competent authorities:
  - The regulatory body has been very proactive in working with multiple national organizations that are competent authorities in areas

interrelated with the physical security of nuclear facilities, nuclear materials and radioactive sources. This has brought about excellent collaboration and cooperation, resulting in considerable progress being made on some very sensitive and complex security related issues.

- To exchange technical experience, the interaction of the regulatory body with authorities competent for security matters in other sectors is quite positive.
- The organization of all activities related to nuclear safety, radiation safety, physical protection and emergency preparedness within the same department simplifies coordination and cooperation between specialists of cross-related safety and security areas.
- The assignment of responsibility for physical protection to the division of safety, which reports directly to the CEO, ensures an effective mangement of interfaces between safety and security and helps to ensure that physical protection receives sufficient authority for action.
- The radiation safety authority — without formal obligation — has taken the initiative to establish an informal working group comprising representatives of all major organizations involved in physical protection to address and coordinate important issues related to nuclear security.
- Safety, security and safeguards are in the same organization, thereby offering greater opportunities to promote increased synergies between the three regulatory disciplines.
- The organization of all activities related to nuclear safety, radiation safety, physical protection and emergency preparedness within the same department simplifies coordination and cooperation between specialists of cross-related safety and security areas.

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Integrated Regulatory Review Service Guidelines, IAEA Services Series No. 37, IAEA, Vienna (2018).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, International Physical Protection Advisory Service (IPPAS) Guidelines, Services Series No. 29, IAEA, Vienna (2014).

Annex II

CASE STUDIES FROM EXPERIENCE IN MEMBER STATES

II–1. SAFETY AND SECURITY OVERSIGHT PROCESS OF NPPs IN CANADA

II–1.1. Legal and regulatory framework

Safety, security and safeguards/non-proliferation are addressed in a single national law in Canada: the Nuclear Safety and Control Act (NSC Act). The NSC Act addresses the ‘3S’ aspects (safety, security, safeguards) for all activities and facilities across the full life cycle. The act also establishes the Canadian Nuclear Safety Commission (CNSC) as the regulatory authority in Canada for safety, security and safeguards.

Scope of the Canadian Nuclear Safety Commission oversight

- Establishing requirements, licensing and authorization, compliance verification and regulatory action;
- Complete nuclear fuel cycle — from uranium mining to waste management;
- Complete life cycle — design, siting, construction, commissioning, operation, decommissioning and waste management.

The CNSC’s regulatory framework is broken down into 14 safety and control areas (SCAs), addressing all areas of safety, including security and safeguards. The CNSC establishes regulations through the Parliament for all aspects of the 3S, whether general, facility specific or activity specific, safety or security. Regulatory documents with expectations and guidance are approved by the Commission and are structured in accordance with the 14 SCAs.

Safety and control areas

(1) Management system;
(2) Human performance management;
(3) Operating performance;
(4) Safety analysis;
(5) Physical design;
(6) Fitness for service;
(7) Radiation protection;
(8) Conventional health and safety;

(9) Environmental protection;
(10) Emergency management and fire protection;
(11) Waste management;
(12) Security;
(13) Safeguards and non-proliferation;
(14) Packaging and transport.

Drafting regulations and regulatory documents on requirements and guidance

The CNSC utilizes a cross-disciplinary team approach to developing regulations and regulatory documents, whereby security and safety specialists can be involved in a cross-functional manner as required.

The CNSC requirements for safety culture and security culture are formally documented in REGDOC-2.1.2 and "safety culture and security culture coexist through the shared common objective of limiting risk, and they share common goals and techniques for promotion and monitoring activities. In this document, 'safety culture' denotes safety culture and security culture collectively, except where a distinction is made. It is therefore key for all licensees to engage in fostering a healthy safety culture in their organizations" [II–1].

II–1.2. Regulatory oversight and activities

Resources

- The CNSC has an internal TSO. The nuclear security division is part of its TSO.
- Nuclear security specialists have expertise across across all areas: intelligence, cyber, intrusion and response.
- Many traditional nuclear safety specialists in the TSO have expertise in security aspects (e.g. civil structures and I&C).
- They cover all applicable areas from categorized sources to NPP.

Licensing

- Licensing and renewal: CNSC staff assess safety and security programmes, plans and performance (the 14 SCAs).
- No facility can be authorized to operate if not both safe and secure.
- Staff recommendations and commission deliberation of security topics are carried out on camera.

Compliance assessment

- The CNSC compliance plan is based on all SCAs, including security.
- Activities include resident inspector rounds, one-day field inspections with or without technical specialists and multiday field inspections with technical specialists.
- Reporting to the commission is annual, detailed and public (all SCAs, including security).
- The CNSC inspector training includes basics of security.
- Licensing and compliance staff are generally included among those with a need to know.

II–1.3. Structure of the licensee

The licensee has the prime responsibility for both safety and security.

All NPP operators have a security organization which is embedded within the organization's integrated management system. The responsibilities for safety and security are placed at the same level. Typically, a senior level position, such as the chief nuclear officer or vice-president, would be responsible for operations. It is common for licensees to have emergency and security combined into one portfolio, managed by one senior staff (normally at the vice-president level, reporting to the chief nuclear officer), whereas the plant/reactor senior staff (normally a station vice-president, station director, etc.) is responsible for the use of security staff at the station. Operation, maintenance and the proper use of security policy and equipment are the responsibility of the station vice-president (which would be the same for radiation protection, nuclear safety and industrial safety).

II–1.4. Summary

A single authority performs the regulatory oversight of nuclear safety and nuclear security — the CNSC. Having both functions combined within the same organization enhances communications across all functional topics. Security requirements and expectations are built into the regulatory framework and are appropriately considered during licensing and inspection activities. Many opportunities for managing the interface are built into the CNSC's management system, thus ensuring a coherent and effective implementation of both safety and security within the CNSC's regulatory framework.

Similarly, Canadian NPP licensees have included their security services in their organization and them in their management system.

II–2. EXPERIENCE IN ADDRESSING INTERFACES BETWEEN SAFETY AND SECURITY OVERSIGHT OF NPPs IN HUNGARY

II–2.1. Legislative and regulatory framework

Integrated nuclear regulatory body

The Government of Hungary, at the end of 2015, promulgated several decrees to establish a new regulatory system intended to harmonize the safety and security regulatory oversight. Consequently, the following regulatory tasks are currently delegated to the Hungarian Atomic Energy Authority (HAEA) by the Act CXVI of 1996 on Atomic Energy (hereinafter referred to as the Atomic Act).

The regulatory oversight applies to nuclear facilities; radioactive waste storage repositories; the application of nuclear and other radioactive materials, including transport in the areas of nuclear safety; security; safeguards; radiation protection; and emergency preparedness and response. In this way, the regulatory oversight tasks of safety and security are integrated under the responsibility of the same regulatory body.

The HAEA is an independent governmental body responsible for the safe, secure and peaceful use of atomic energy in Hungary. It works under the direction of the Government of Hungary with independent budget. It is supervised by a Minister appointed by the Prime Minister, independent of his/her portfolio. The HAEA issued resolutions and decisions cannot be appealed in the frame of a public administration process and cannot be changed or eliminated in supervisory role. It has the right to provide proposals that relate to the Atomic Act and related regulations. The HAEA submits annual reports to the Government and the Parliament on the safe, secure and peaceful application of atomic energy. According to the mission of the HAEA, the general objective of the regulatory control is to protect people and environment from the harmful effects of ionizing radiation (generated by the various applications of atomic energy), without unduly limiting the operation of facilities or the conduct of activities. Harmful effects may occur as a consequence of:

- Incidents, accidents and severe accidents (safety);
- Sabotage against nuclear and other radioactive materials or their associated facilities as well as theft of such materials (security);
- Use of nuclear and other radioactive materials or their associated facilities by the licensee for non-peaceful purposes (safeguards).

As far as nuclear facilities are concerned, the general objective of the regulatory control can be accomplished by ensuring their safe, secure and peaceful operation.

Allocation of regulatory resources

To have the integrated regulatory approach effectively implemented by a single regulatory body, sufficient human and other resources need to be available. The two regulatory control areas that were delegated to the HAEA in recent years are related to the regulatory oversight of radiation protection and the general oversight of buildings serving the application of nuclear energy. In order to ensure adequate resources, the Government authorized the increase of the staff of the HAEA by 76 persons from 2 January 2015 and by 10 additional persons from 1 July 2015. The modifications of the responsibilities, tasks and staffing of the HAEA made changes in its organizational structure necessary.

Regulatory requirements

Requirements on and conditions of the application of nuclear energy in Hungary are regulated on the level of acts. The Atomic Act formulates the basic requirements ensuring the protection of the population and the environment from harmful effects of ionizing radiation. According to the act, nuclear energy may only be applied in strict compliance with the relevant legislation and under continual regulatory supervision, while safety has priority over any other consideration. The act has created a multilevel legislative and regulatory system. Implementation of the requirements of the act is assisted by governmental decrees and ministerial orders. Non-binding guidelines are also issued by the Director General of the HAEA in the area of its competence. The guidelines aim to support the licensees in complying with the requirements by showing the way that is most advised to be followed by the HAEA. This legislative and regulatory system is in full accordance with international requirements and expectations regarding the safe, secure and peaceful use of nuclear energy.

In the process of developing regulatory requirements, it was important to identify possible interfaces between safety and security. To facilitate the proper arrangements for the implementation of the different requirements, cross-referencing between the relevant governmental decrees was used in areas where interfaces were identified. Regulatory guidance documents have been developed to explain these issues in more detail. The current legislative pyramid for safety and security is shown in Fig. II–1.

Common legal and technical principles underlying the safety and security requirements can be identified. Typical examples are shown in the following lists.

Common legal principles for safety and security requirements:

- Based on international conventions and cooperations;
- Prime responsibility;
- Justification and optimization;
- Independent and continuous regulatory oversight;
- Sustainability and quality management;
- Culture;
- Transparency and confidentiality.

Common technical and engineering principles for safety and security requirements:

- Use of proven technical solutions;
- Deterministic approach;
- Graded approach;
- Defence in depth;
- Establishment of the design basis.

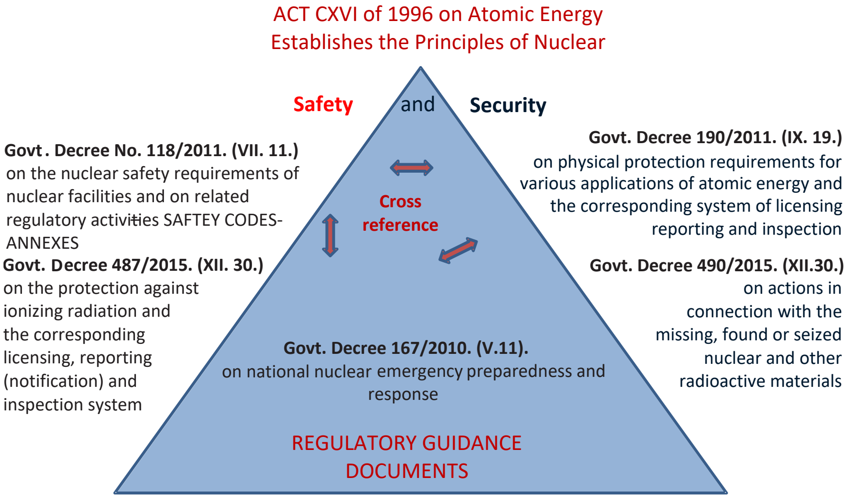

ACT CXVI of 1996 on Atomic Energy
Establishes the Principles of Nuclear
Safety
and
Security
Govt . Decree No. 118/2011. (VII. 11.)
on the nuclear safety requirements of nuclear facilities and on related regulatory activities SAFTEY CODES-ANNEXES
Govt. Decree 487/2015. (XII. 30.)
on the protection against ionizing radiation and the corresponding licensing, reporting (notification) and inspection system
Cross reference
Govt. Decree 190/2011. (IX. 19.)
on physical protection requirements for various applications of atomic energy and the corresponding system of licensing reporting and inspection
Govt. Decree 490/2015. (XII.30.)
on actions in connection with the missing, found or seized nuclear and other radioactive materials
Govt. Decree 167/2010. (V.11).
on national nuclear emergency preparedness and response
REGULATORY GUIDANCE DOCUMENTS

FIG. II–1. Legislative pyramid for safety and security.

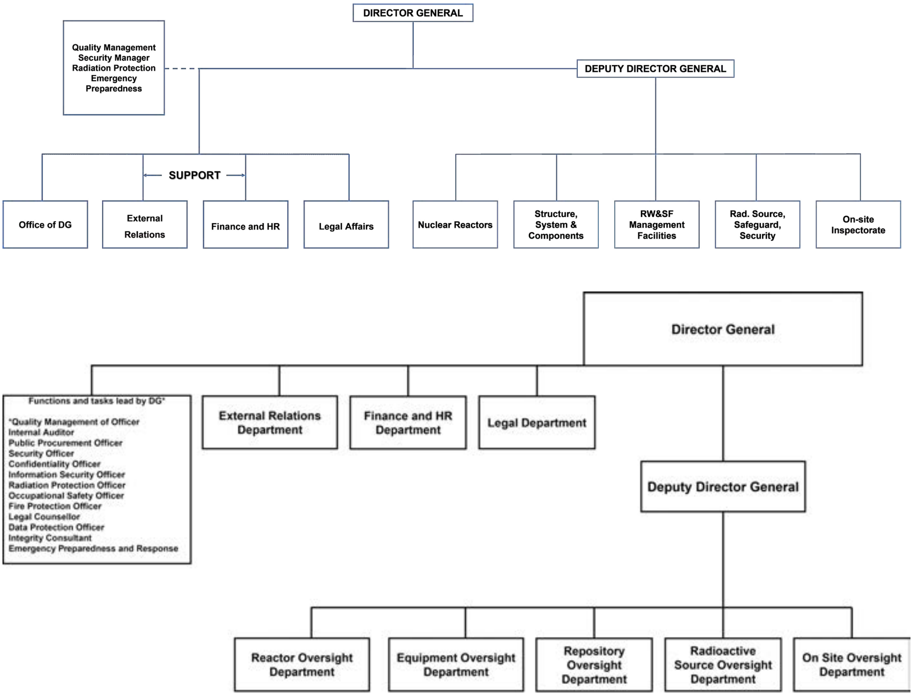

DIRECTOR GENERAL
Quality Management
Security Manager
Radiation Protection
Emergency
Preparedness
DEPUTY DIRECTOR GENERAL
SUPPORT
Office of DG
External Relations
Finance and HR
Legal Affairs
Nuclear Reactors
Structure, System & Components
RW&SF Management Facilities
Rad. Source, Safeguard, Security
On-site Inspectorate
Director General
Functions and tasks lead by DG*
*Quality Management of Officer
Internal Auditor
Public Procurement Officer
Security Officer
Confidentiality Officer
Information Security Officer
Radiation Protection Officer
Occupational Safety Officer
Fire Protection Officer
Legal Counsellor
Data Protection Officer
Integrity Consultant
Emergency Preparedness and Response
External Relations Department
Finance and HR Department
Legal Department
Deputy Director General
Reactor Oversight Department
Equipment Oversight Department
Repository Oversight Department
Radioactive Source Oversight Department
On Site Oversight Department

FIG. II–2. Organizational structure of the HAEA (DG: Director General; HR: human resources; RW&SF: radioactive waste and spent fuel).

II–2.2. Regulatory functions

Organizational structure

To be adequately prepared for the completion of the new obligations and tasks, the HAEA has revised these tasks and the resources necessary for their completion. For this purpose, a project entitled ‘Increase of operational efficiency of HAEA’ has been completed that includes the preparations to take over the new regulatory tasks. Recently, the staffing has been stabilized and seems to be sufficient for the completion of future tasks. The organizational structure of the HAEA is shown in Fig. II–2.

The functionally separated departments have the following technical tasks:

- Reactor Oversight Department: supervision of the NPP and the research reactors;
- Equipment Oversight Department: regulatory supervision of structures, systems and components and of buildings;

- Repository Oversight Department: regulatory supervision of the radioactive waste management facilities and of the spent fuel interim storage facility;
- Radioactive Source Oversight Department: regulatory supervision of activities related to physical protection, safeguards and safety of radiation sources;
- On-site Oversight Department: inspection activities by resident inspectors on-site of the NPP.

Licensing and authorization of NPPs

For the operation of an NPP, an operating licence and a separate physical protection licence issued by the HAEA are required. The licensing applications are evaluated with reference to the act, the relevant government decrees, nuclear safety codes and guidelines during the licensing process. In the administrative procedures for issuing the licence for the physical protection plan of the NPP, the National Police Headquarters is also involved as a co-authority competent to assess the adequacy of the response forces.

Within the frame of the new regulatory structure, all (e.g. safety, security and safeguards) facility level applications of nuclear reactors are processed by the Department of Reactor Oversight, as shown in Fig. II–3. In each case, all competent sections of the other departments are involved, and the licence is issued with the consent of all parties. For the discussion on interface issues between safety and security, common working groups are established with the staff of the competent sections involved in the licensing procedure as shown in Fig. II–3.

For the licensing of a new NPP, the security related licence requirements are integrated in the overall nuclear safety licensing process as shown in Fig. II–4.

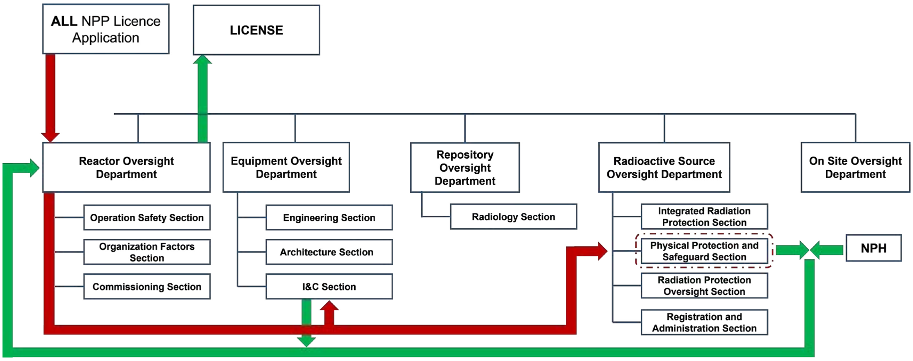

ALL NPP Licence Application
LICENSE
Reactor Oversight Department
Equipment Oversight Department
Repository Oversight Department
Radioactive Source Oversight Department
On Site Oversight Department
Operation Safety Section
Organization Factors Section
Commissioning Section
Engineering Section
Architecture Section
I&C Section
Radiology Section
Integrated Radiation Protection Section
Physical Protection and Safeguard Section
Radiation Protection Oversight Section
Registration and Administration Section
NPH

FIG. II–3. Competent sections involved in the licensing procedure (NPH: National Police Headquarters).

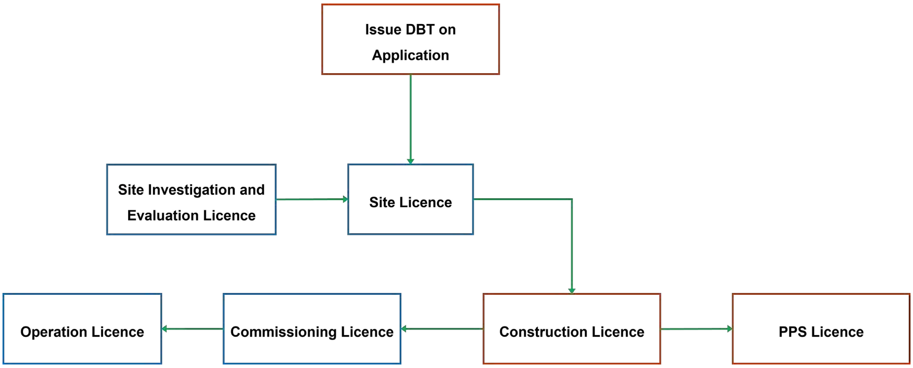


FIG. II–4. Licensing process of NPPs.

In the case of a planned nuclear facility, the licensee is obligated to request the HAEA to determine the DBT. It is recommended to submit this application in parallel with the site licence application for safety. In the DBT application, the licensee is required to assess the adequacy of the site from a nuclear security point of view. The minimal content of such an application includes the basic design of the reactor, safety critical systems and components, type and amount of nuclear material to be used and stored, the topography of the site, meteorological conditions of the site, extreme water levels in the environment of the site, geological and seismological conditions of the site, land use, population and economic activities in the environment of the site, accessibility of the site, physical protection related the suitability of the site relating to adversary pathways, as well as the area of the land available for the site. With its many common elements of the safety assessment of the site, this application documentation is a typical interface document requiring the licensee to develop efficient cooperation and coordination between its safety and security staff. From the experience gained during the licensing procedure of the new units to be built under the framework of the capacity maintenance of the Paks NPP project, it is clear that the introduction the DBT application requirement proved to be a very useful regulatory tool in facilitating the interface management capabilities of the operator at the early stage of the design phase of the project.

II–2.3. Inspection and enforcement

The HAEA implements an annual inspection plan for the nuclear facilities, which involves all regulatory control areas and which is also published on the website of the HAEA as required by the legislation. At the nuclear facilities, the HAEA inspectors are specialized, only performing either nuclear safety or nuclear security inspections. Although in the general training modules for inspectors, all the regulatory areas are covered, expert level training is only provided according to the regulatory area of the inspectors (either safety or security).

According to HAEA experience, an ‘integrated inspection (2S or 3S)’ can only be performed by a single inspector in the case of low risk facilities and small users of nuclear or other radioactive materials. High risk facilities are too complex for integrated inspections to be conducted by one individual inspector. The HAEA usually does not use external technical support for its inspectors on site.

There are specific areas where inspections are conducted by the presence of both safety and security inspectors together. These are the inspection of the protection of programmable systems (information technology and operational technology) as well as of emergency response.

In both safety and security, the HAEA uses a risk informed planning, taking the risk significant to the inspected area and the assessment of past operational experience into account. Inspections are conducted in both areas according to a similar integrated process (preparation, on-site activity, post-inspection evaluation).

The same types of regulatory procedure and instruments that are used by the HAEA for enforcement purposes have been established for safety and security. The principle of a graded approach is applied in both areas when an enforcement action is to be taken. Like the case of the facility licensing procedure, all competent sections of the HAEA are involved if decision about an enforcement action is to be made. This practice enables the HAEA to take any interface issues into account in the final decision.

II–2.4. Interfaces in safety and security response

As an important segment of the defence in depth concept, response activities are vital both in safety and security to ensure the protection of the public and the environment from the harmful effect of ionizing radiation connected to the application of atomic energy. As such, they are inherently of an interface nature.

For the identification of the interfaces between safety and security response actions, plans and procedures, and between contingency and emergency responses at the facility level, the severity of security incidents and safety events can be grouped in three levels based on their consequences and the capabilities required for responding to them as shown in Table II–I.

Level I is the operative level response to most frequently occurring events that are the least serious. It requires efforts mainly from the operator by strictly following the routine procedures developed in advance; however, their repetition may attract the attention of the regulatory body and initiate enforcement actions. Examples of such events are the anticipated operational occurrences, expected

TABLE II–1. RESPONSE LEVELS TO SAFETY OR SECURITY EVENTS AND THE BASE OF THEIR MANAGEMENT

Response level	Event type		Documents used for acting/responding	
	Security	Safety	Security	Safety
Level I	Anticipated security incidents	Anticipated operational occurrences	Regular security procedures	Operational safety procedures
Level II	Security incidents postulated in the threat assessment or Security incidents within the DBT	Design basis events Beyond design basis events Severe accidents without environmental consequences	Contingency response plan	Emergency operating procedures Severe accident management guidelines
Level III	Successful sabotage with environmental consequences	Severe accidents with environmental consequences	Emergency response plan	Emergency response plan

failures of equipment, false and nuisance alarms and certain less serious unintentional or intentional human errors. The response actions to Level I security incidents typically include warning, re-checking and taking prompt complementary actions.

Level II includes those security incidents that are postulated in the threat assessment, and thus provides the basis for the measures described in the security plan. Level II security incidents do not entail the release of radioactive materials. Such events could be, for example, unauthorized access to the site through the fence, a suspicious object left unattended, an attempt to steal nuclear or other radioactive material or the attempt to sabotage the facility. The response actions to Level II security incidents typically include the implementation of security measures described in the contingency plan as part of the physical protection plan. It is a requirement in Hungary that the contingency plan and the emergency plan are harmonized by the licensee.

Level III includes those security incidents that involve radioactive releases and cause adverse environmental consequences, such as the successful sabotage of vital equipment or the successful sabotage to spent nuclear fuel. The response actions to Level III security incidents typically include the implementation of measures to handle the situation from a security point of view and the implementation of the necessary protective actions described in the emergency response plan to protect the workers and the public. These two sets of measures are currently harmonized in Hungary and will be included in a common national emergency preparedness and response plan.

As can be concluded from the above grouping of security incidents, the response to Level I and Level II incidents requires actions mainly from the security organization. In the case of such events, the interface with safety is rather limited. However, in certain cases, information should be provided to the safety organization, to allow for the preparation of safety measures, especially if the security incident may evolve further to a Level II or Level III safety event.

II–3. MAINTAINING SAFETY AND SECURITY INTERFACES DURING THE REGULATORY OVERSIGHT FOR NPPs IN PAKISTAN

II–3.1. Regulatory frameworks for the oversight of safety and security

Pakistan has in place an effective national legal and regulatory framework for oversight of nuclear safety, radiation protection and nuclear security. The Pakistan Nuclear Regulatory Authority (PNRA) was established in 2001 as an independent regulatory body to control, regulate and supervise all matters related to nuclear safety and radiation protection in Pakistan. To effectively meet its regulatory obligations, the PNRA devises, adopts, makes and enforces rules, regulations, orders and codes of practice for nuclear safety and radiation protection. It plans, develops and executes comprehensive policies and programmes for the protection of life, health and property from the harmful effects of ionizing radiation.

Under the PNRA Ordinance 2001, the PNRA is entrusted with the responsibility of licensing and authorization of safe and secure management of nuclear materials and nuclear installations in the country. The PNRA, being the sole regulatory body for nuclear safety and security, has adopted a systematic approach and methodology to deal with the interfaces of nuclear safety and nuclear security to achieve the common objective of protecting the public, the society, and the environment from harmful radiological consequences. The systematic approach consists of the following arrangements to ensure that both nuclear safety and nuclear security are mutually supportive and complement each other in minimizing radiological risks.

(1) Cooperation and joint actions between the nuclear regulatory body and the relevant competent authority

The roles and responsibilities of various organizations have been defined under the national nuclear safety and security regime that includes: the National Command Authority (the national coordinating body); the PNRA (the regulatory body); the Pakistan Atomic Energy Commission (PAEC, the sole licensee of nuclear installations); and other national organizations.

(2) Staff competence and training of staff

The importance of a sustainable human resource development for nuclear safety and security is undeniable. The PNRA recognizes that both nuclear safety and security require their own expertise and methodologies with understanding of each other's disciplines and requirements. The PNRA sponsors a fellowship programme of the Pakistan Institute of Engineering and Applied Sciences, a degree awarding university, for its Master of Science degree in Nuclear Engineering. The fellows are offered courses on nuclear security and physical protection, in addition to other courses mandatory for nuclear engineering. After completion of their Master of Science degrees, these fellows are integrated into the PNRA and are posted at the regional offices of the PNRA, where they get on-the-job training. The PNRA has also established a National Institute of Safety and Security to provide training to newly recruited officers as well as to arrange refresher courses for the existing staff in the fields of nuclear safety, radiation protection and nuclear security. Training courses are also arranged for the staff working in nuclear safety, to familiarize themselves with nuclear security and vice versa. This enables security and safety experts to better understand the safety and security interface issues.

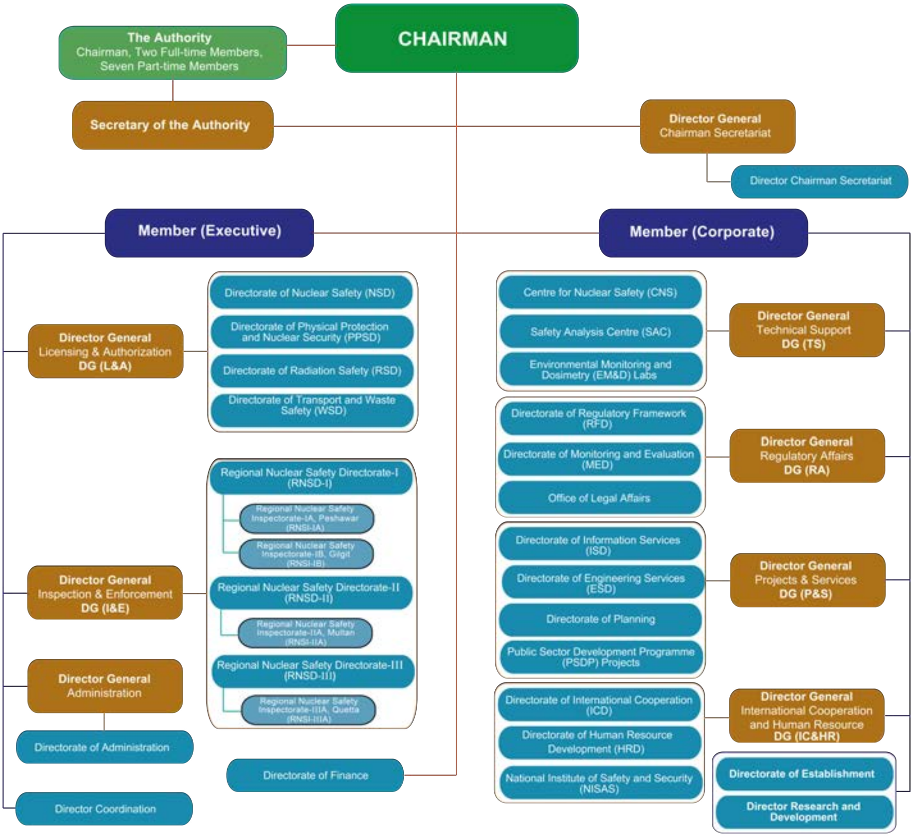
The PNRA has adopted a rotation policy for its technical experts to work at different sites with different responsibilities to avoid complacency in their work.

(3) Organizational structure and allocation of resources

The PNRA Ordinance 2001 defines the composition of the authority, which consists of a chairperson, two full-time members, seven part-time members and a secretary as a non-voting member. The Federal Government designates the chairperson and members of the authority. The part-time members of the authority include one distinguished professional each from the engineering, medical, and science sectors and one representative each from the Ministry of Health, the Pakistan Environmental Protection Agency, the PAEC, and the Strategic Plans Division.

The functions and responsibilities assigned to the PNRA are performed by the different departments of the executive and corporate wings. In addition to different safety departments, a separate department for nuclear security has been established to perform assigned tasks in an integrated manner. The organizational structure of the PNRA is given in Fig. II–5.

The resources needed to perform the functions of the PNRA and to meet the nuclear safety and security objectives include human resources, administrative resources, financial resources, technical resources and



CHAIRMAN
The Authority
Chairman, Two Full-time Members, Seven Part-time Members
Secretary of the Authority
Director General
Chairman Secretariat
Director Chairman Secretariat
Member (Executive)
Member (Corporate)
Director General
Licensing & Authorization
DG (L&A)
Directorate of Nuclear Safety (NSD)
Directorate of Physical Protection and Nuclear Security (PPSD)
Directorate of Radiation Safety (RSD)
Directorate of Transport and Waste Safety (WSD)
Director General
Inspection & Enforcement
DG (I&E)
Regional Nuclear Safety Directorate-I (RNSD-I)
Regional Nuclear Safety Inspectorate-IA, Peshawar (RNSI-IA)
Regional Nuclear Safety Inspectorate-IB, Gilgit (RNSI-IB)
Regional Nuclear Safety Directorate-II (RNSD-II)
Regional Nuclear Safety Inspectorate-IIA, Multan (RNSI-IIA)
Regional Nuclear Safety Directorate-III (RNSD-III)
Regional Nuclear Safety Inspectorate-IIIA, Quetta (RNSI-IIIA)
Director General
Administration
Directorate of Administration
Director Coordination
Directorate of Finance
Centre for Nuclear Safety (CNS)
Safety Analysis Centre (SAC)
Environmental Monitoring and Dosimetry (EM&D) Labs
Director General
Technical Support
DG (TS)
Directorate of Regulatory Framework (RFD)
Directorate of Monitoring and Evaluation (MED)
Office of Legal Affairs
Director General
Regulatory Affairs
DG (RA)
Directorate of Information Services (ISD)
Directorate of Engineering Services (ESD)
Directorate of Planning
Public Sector Development Programme (PSDP) Projects
Director General
Projects & Services
DG (P&S)
Directorate of International Cooperation (ICD)
Directorate of Human Resource Development (HRD)
National Institute of Safety and Security (NISAS)
Director General
International Cooperation and Human Resource
DG (IC&HR)
Directorate of Establishment
Director Research and Development

FIG. II–5. Organizational structure of the PNRA (Courtesy of the PNRA).

information and knowledge resources. All these resources are determined and provided to safety and security departments based on a graded approach to perform regulatory processes and activities.

(4) Drafting regulations and guides

The PNRA issues regulations based on the PNRA Ordinance 2001 and regulatory guides for appropriate guidance for implementing requirements of PNRA regulations.

The regulations are developed in a transparent manner by involving safety, security and legal experts and seeking the opinion of all national stakeholders, including the licensee, government and the public.

The existing regulations and regulatory guides are periodically reviewed based on national and international experience feedback and technological developments.

The security requirements are also addressed in the safety regulations applicable during the authorization and licensing of the nuclear installations.

The PNRA is in the process of issuing separate regulations for nuclear security. Specific requirements for the safety and security interface will be addressed in the security regulations. Regulatory requirements are set so that safety and security measures are implemented in an integrated manner. In these regulations, prime responsibility for both safety and security is set with the licensee.

The process of formulating PNRA regulations and regulatory guides is shown in Fig. II–6.

(5) Licensing and authorization

The PNRA is responsible for licensing and authorization of nuclear installations as well as that of equipment manufacturers of nuclear safety class equipment and service providers. These licences and authorizations are issued based on review and assessment of the licensee’s submissions and regulatory inspections.

The process of issuing authorizations and licences to nuclear installations during various stages in their lifetime is illustrated in Fig. II–7.

The PNRA issues a single licence or authorization for safety and security during the stages in the lifetime of nuclear installations, and the licence or authorization is issued only when the operator complies with both safety and security requirements.

The PNRA requires that the training syllabus for the operating personnel of nuclear installations has nuclear safety and nuclear security modules. The PNRA conducts operator licence examination to ensure that knowledge and expertise of candidates about safety and security are adequate for award of operating licence.

(6) Inspection and enforcement

The inspections at NPPs are managed through Regional Nuclear Safety Directorates of PNRA, and only authorized inspectors perform such regulatory inspections. The PNRA ensures that its inspectors have the necessary qualifications, training and experience to conduct an effective inspection. Joint inspections are also conducted with a team comprising both safety and security inspectors. This helps in identifying and managing interface issues.

The PNRA attaches equal importance to any non-compliance with regulatory requirements or licence conditions related to safety and security. Enforcement actions are taken through well established regulatory frameworks.

II–3.2. Review and assessment, including analysis of operating experience

The PNRA performs review and assessment of various documents submitted by the licensee to support application for licensing or authorization. Design modifications and changes are also evaluated to verify that they take account of the requirements of both safety and security and properly manage the interfaces between them. In addition, the PNRA also reviews documents required under various regulations, licence conditions and directives or policies issued from time to time.

The PNRA performs analyses of the feedback captured during inspections, meetings and other interactions with various stakeholders or licensees. A formal systematic process has been established to utilize the national and international operating experience feedback. The process is executed by the collecting, screening and evaluation of events and providing recommendations and actions to be taken by the licensee.

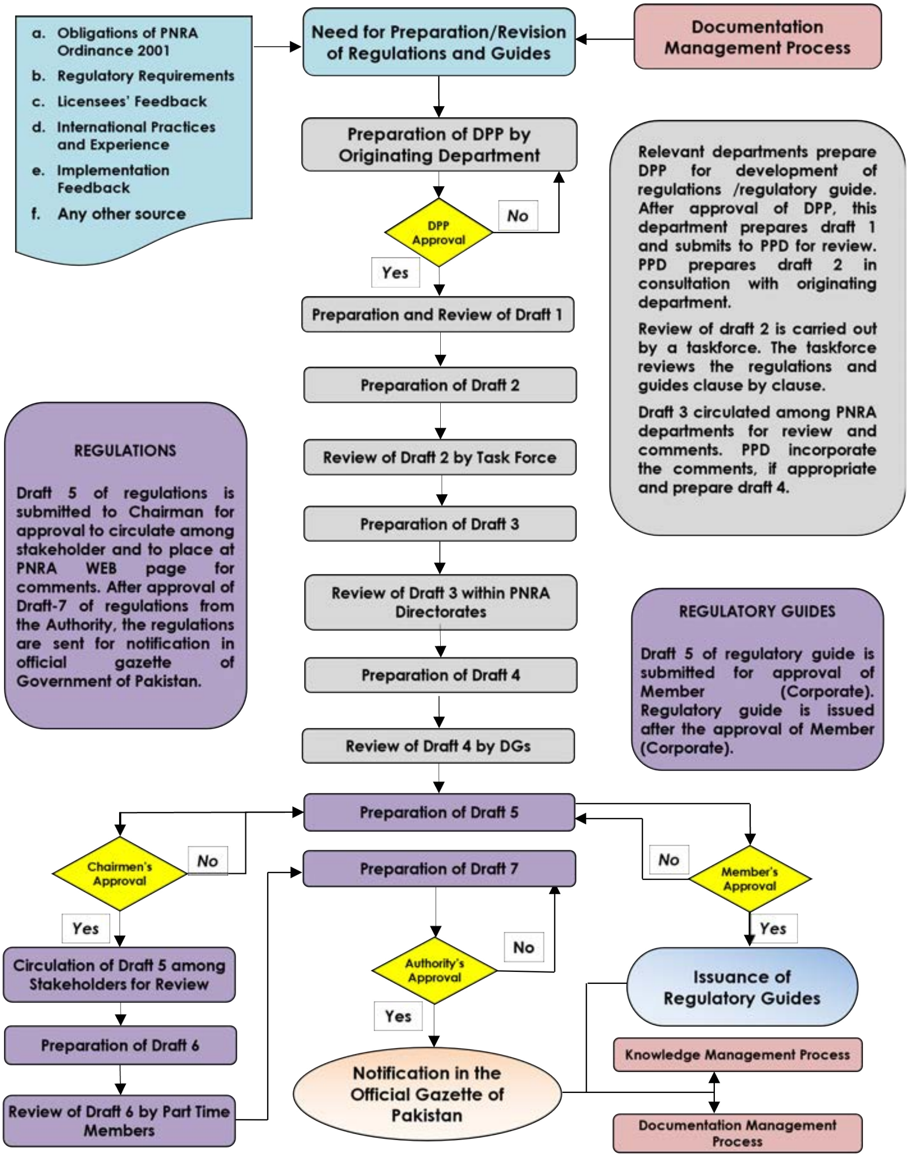

a. Obligations of PNRA Ordinance 2001
b. Regulatory Requirements
c. Licensees' Feedback
d. International Practices and Experience
e. Implementation Feedback
f. Any other source
Need for Preparation/Revision of Regulations and Guides
Documentation Management Process
Preparation of DPP by Originating Department
DPP Approval
No
Yes
Relevant departments prepare DPP for development of regulations /regulatory guide. After approval of DPP, this department prepares draft 1 and submits to PPD for review. PPD prepares draft 2 in consultation with originating department.
Review of draft 2 is carried out by a taskforce. The taskforce reviews the regulations and guides clause by clause.
Draft 3 circulated among PNRA departments for review and comments. PPD incorporate the comments, if appropriate and prepare draft 4.
Preparation and Review of Draft 1
Preparation of Draft 2
Review of Draft 2 by Task Force
Preparation of Draft 3
Review of Draft 3 within PNRA Directorates
Preparation of Draft 4
Review of Draft 4 by DGs
REGULATIONS
Draft 5 of regulations is submitted to Chairman for approval to circulate among stakeholder and to place at PNRA WEB page for comments. After approval of Draft-7 of regulations from the Authority, the regulations are sent for notification in official gazette of Government of Pakistan.
REGULATORY GUIDES
Draft 5 of regulatory guide is submitted for approval of Member (Corporate). Regulatory guide is issued after the approval of Member (Corporate).
Preparation of Draft 5
Chairmen's Approval
No
Yes
Preparation of Draft 7
No
Member's Approval
Yes
Circulation of Draft 5 among Stakeholders for Review
Authority's Approval
No
Yes
Issuance of Regulatory Guides
Preparation of Draft 6
Knowledge Management Process
Review of Draft 6 by Part Time Members
Notification in the Official Gazette of Pakistan
Documentation Management Process

FIG. II–6. Process for the development of PNRA regulations and guides.

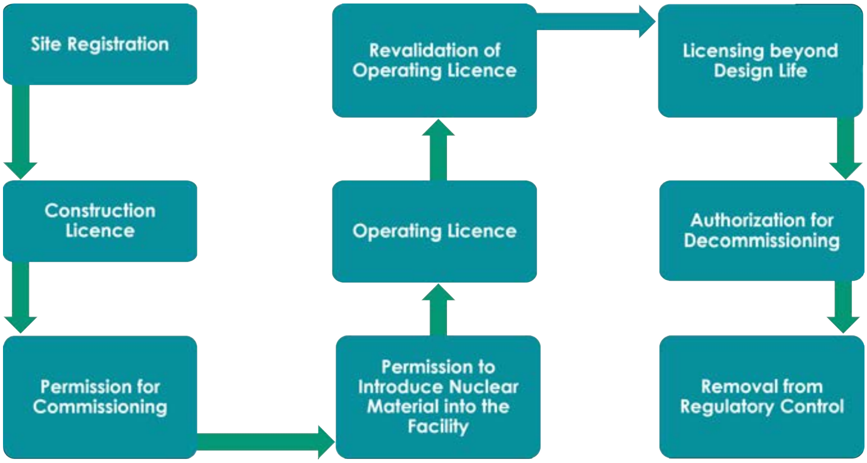

Site Registration
Construction Licence
Permission for Commissioning
Permission to Introduce Nuclear Material into the Facility
Operating Licence
Revalidation of Operating Licence
Licensing beyond Design Life
Authorization for Decommissioning
Removal from Regulatory Control

FIG. II–7. PNRA process for authorization and licensing during various stages in the lifetime of nuclear installations.

II–3.3. Consistency of regulatory control for both safety and security

The PNRA has established regulatory control for both safety and security by issuing common licences and authorizations, performing common inspections, as well as ensuring emergency preparedness and response arrangements for both nuclear safety and nuclear security events.

Dedicated teams conduct review and assessment of the licensee's submissions related to nuclear safety and nuclear security in accordance with regulatory requirements and agreed codes and standards.

Any violation of nuclear safety and nuclear security requirements is dealt with under common enforcement processes.

II–3.4. Advisory bodies and technical support organizations

The PNRA has established several advisory committees composed of experts with high professional competence to advise on regulatory matters. These committees are autonomous in their working and present their recommendations to the Chairperson of the PNRA.

The PNRA has also established a TSO to provide technical support in safety assessments of licensees' submissions.

II–3.5. Communication and consultation with licensed entities (integrated approach)

Focal points are designated to share and receive information from licensees. The PNRA arranges periodic meetings at different levels with licensees to resolve any conflicts or safety-security interface issues. The PNRA is also in the process of developing regulations on dispute resolution.

II–3.6. Considerations for safety and security culture

The PNRA regulations address requirements for both safety and security cultures. The PNRA has already developed an assessment programme for safety culture and is working on the methodology for the assessment of security culture. This methodology includes a checklist in the form of a questionnaire specifically aimed at different segments of the staff and officers in the PNRA. Subsequently, after assessment, the integration of both cultures will be worked out.

II–3.7. Public consultation and communication

The PNRA has developed a programme for enhancing public awareness about risks and benefits associated with radiation. It shares information about major regulatory decisions and its activities through various means. The PNRA strives to enhance of public involvement in different regulatory processes, including the development of regulatory documents, by placing draft regulations on its website for feedback and comments.

II–3.8. International cooperation

The PNRA attaches great importance to the fulfilment and implementation of its international obligations. It establishes effective linkages with international organizations through a range of bilateral and multilateral cooperation programmes and continuously strives to maintain these linkages. The PNRA, as a national nuclear regulatory authority, continuously seeks to establish and maintain close cooperation with other regulatory authorities and promotes the sharing of necessary information and experiences among the nuclear regulatory bodies to provide support in regulatory matters. The PNRA is also the point of contact for international conventions under the auspices of the IAEA to which Pakistan is party, namely the Convention on Nuclear Safety [II−2]; the Convention on the Physical Protection of Nuclear Material and Its Amendment [II−3, II−4]; the Convention on Early Notification of a Nuclear Accident [II−5]; and the

Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency [II−6].

II–3.9. Emergency and contingency planning and response

The PNRA has established a Nuclear and Radiological Emergency Coordination Centre (NRECC) to act as a centralized emergency coordination and event reporting centre for both nuclear safety and nuclear security events. A nuclear emergency management system has been established at State level which defines roles and responsibilities of various organizations in case of on-site and off-site radiological emergencies either due to a safety or security event. The NRECC interface and coordination mechanism with licensees and national response organizations is tested through joint exercises. NRECC is also responsible for the coordination with the IAEA Incident and Emergency Centre and the IAEA RANET.

The PNRA regulations address key requirements related to the licensing process with key conditions for a licensee's submission of a contingency plan as part of the physical protection programme and an emergency preparedness and response plan and demonstration of these plans through periodic drills and exercises to ensure that the licensee's response capabilities are in accordance with the regulatory requirements.

II–3.10. Leadership and management

Leadership and management are vital for nuclear safety and security. Leadership is essential at the individual level and the highest management level to ensure safety and security. The PNRA considers leadership an important aspect in dealing with safety and security interface issues. It has initiated a leadership development programme in collaboration with Lahore University of Management Sciences. Two batches of leaders have been trained and are functional at the PNRA. The third batch of future leaders was selected in 2015. The PNRA revised its management system and made it consistent with the requirements established in IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety [II−7]. Similarly, the principles of leadership and management for safety and security have been addressed in regulatory frameworks to achieve the common goal of safety and security.

II–3.11. Protection and confidentiality of information

Dealing with both safety and security activities involve interaction with information that is sensitive in nature and requires protection against unauthorized disclosure and dissemination. The PNRA has set up a process to deal with management of sensitive information, and only authorized individuals have access to such information. The PNRA staff is also part of periodic trustworthiness and reliability programmes at State level, which also helps individual to deal with sensitive information.

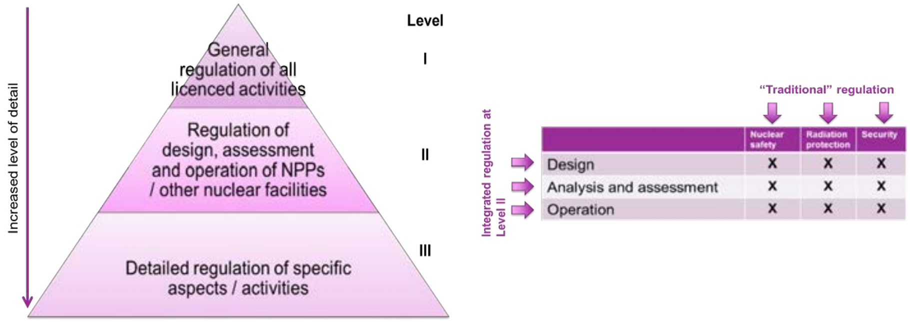
II–4. STRÅLSÄKERHET AND NUCLEAR SAFETY AND SECURITY IN SWEDEN

The Swedish Act on Nuclear Activities as well as existing regulations include provisions and definitions or more implicit descriptions in background texts etc., stating that the areas of radiation protection, nuclear safety and nuclear security should be considered in the design and operation of nuclear facilities. In practice, however, the areas have been managed more separately using traditional methods aimed at one of the aspects. In the revision of the regulatory code, it has been clarified that the fuzzy delimitations between these areas, as well as overlapping areas and measures in one area, can result in either synergies or contradictions with another area. Due to the common objective, mainly related to protection of workers, the public and the environment from undue radiological hazards, a decision in principle was taken by the Swedish Radiation Safety Authority (SSM) that to a greater extent regulate the different aspects in an integrated manner using the term 'strålsäkerhet'. The structure of the regulations has also been changed to enable this strategy, as shown in Fig. II–8.

The Swedish term 'strålsäkerhet'[1] was established when the two separate regulatory authorities the Nuclear Safety Inspectorate (SKI) and the Radiation Protection Institute (SSI) were merged into the Swedish Radiation Safety Authority (SSM) in 2008. The term 'strålsäkerhet' is now acknowledged as a formal definition in the regulations for licensable activities involving ionizing radiation (SSMFS 2018:1), which stipulates provisions at the first level of the new regulatory code. The next step is to decide upon new overall regulations for NPPs (level 2), as well as more specific regulations applicable for certain aspects or certain activities (level 3). An overview of the hierarchical structure of the new regulatory code is shown in Fig. II–8.

To enable the use of 'strålsäkerhet' in requirements of the design, assessment and operation of NPPs, a graded, function based approach is used. Also, the level of detail of requirements has been assessed. Thus, this type of

[1] A direct translation to English of this term has used 'radiation safety', even though this is not quite in line with the meaning of how radiation safety is described, for example, in the IAEA Safety Glossary (2018 Edition) [II−8].


Increased level of detail
General regulation of all licenced activities
Regulation of design, assessment and operation of NPPs / other nuclear facilities
Detailed regulation of specific aspects / activities
Level
I
II
III
"Traditional" regulation
Integrated regulation at Level II

	Nuclear safety	Radiation protection	Security
Design	X	X	X
Analysis and assessment	X	X	X
Operation	X	X	X

FIG. II–8. Levels of the new regulatory code and structure for an integrated regulation for nuclear facilities.

regulation is not based on a predefined plant equipment structure in combination with plant states. The approach rather defines requirements concerning structures, systems and components, as well as human tasks, that must be met to reach an acceptable level of 'strålsäkerhet', based on the importance of their required functions at identified events that could lead to an increase in probability or unwanted consequences. The identified events and conditions to be considered in design include DBTs, provided by the authorities, which define the intention and possible realization of unauthorized acts.

II–5. NUCLEAR SAFETY AND SECURITY INTERFACES IN THE UNITED KINGDOM

II–5.1. Cooperation between safety and security

In the United Kingdom, the Energy Act established the Office for Nuclear Regulation (ONR) as a statutory corporation with defined regulatory purposes of:

- Nuclear site health and safety;
- Nuclear safety;
- Nuclear security;
- Nuclear materials safeguards;
- Transport (of radioactive materials).

The ONR has pursued an agenda of 'One ONR', adopting aligned processes and cross-discipline working wherever possible. This includes, for example, joint attendance at governance board meetings to determine regulatory strategy and management of issues.

II–5.2. Drafting regulations and guidance

The ONR ensures cross-discipline inclusion as part of the development and consultation process for new regulatory policy and guidance to ensure alignment and deconfliction. Of particular note is the publication of the ONR's Security Assessment Principles in 2017 [II–9], which are closely aligned with the well established Safety Assessment Principles [II–10]. Its drafting was based on the premise of adopting security concepts that were the same wherever possible, different where necessary to safety equivalents. This resulted in the development of fundamental security principles that are highly coherent with fundamental safety principles to the extent that, in many cases, operators have been able to simply extend their existing arrangements that were in place to satisfy safety licence conditions to also apply to security to satisfy that regulatory expectation. The following areas where an effective interface is likely to bring benefit through synergy are stated in Security Assessment Principles for the Civil Nuclear Industry, 2017 Edition, Version 0 [II–9]:

Fundamental Security Principles (cont.)	**Leadership and Management for Security**	**FSyP 1**
"Dutyholders must implement and maintain organizational security capability underpinned by strong leadership, robust governance, an adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes."		
Fundamental Security Principles	**Organizational Culture**	**FSyP 2**
"Dutyholders must encourage and embed an organizational culture that recognises and promotes the importance of security."		
Fundamental Security Principles	**Competence Management**	**FSyP 3**
"Dutyholders must implement and maintain effective arrangements to manage the competence of those with assigned security roles and responsibilities."		

Fundamental Security Principles (cont.)	Nuclear Supply Chain Management	FSyP 4
“Dutyholders must implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security.”		
Fundamental Security Principles	**Reliability, Resilience and Sustainability**	**FSyP 5**
“Dutyholders must design and support their nuclear security regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle.”		

Another example of an area where a security concept has been designed to mirror that for safety is in the development of the defence in depth model as shown in Fig. II–9. These two comparable hierarchies of control are provided in Fig. II–9.

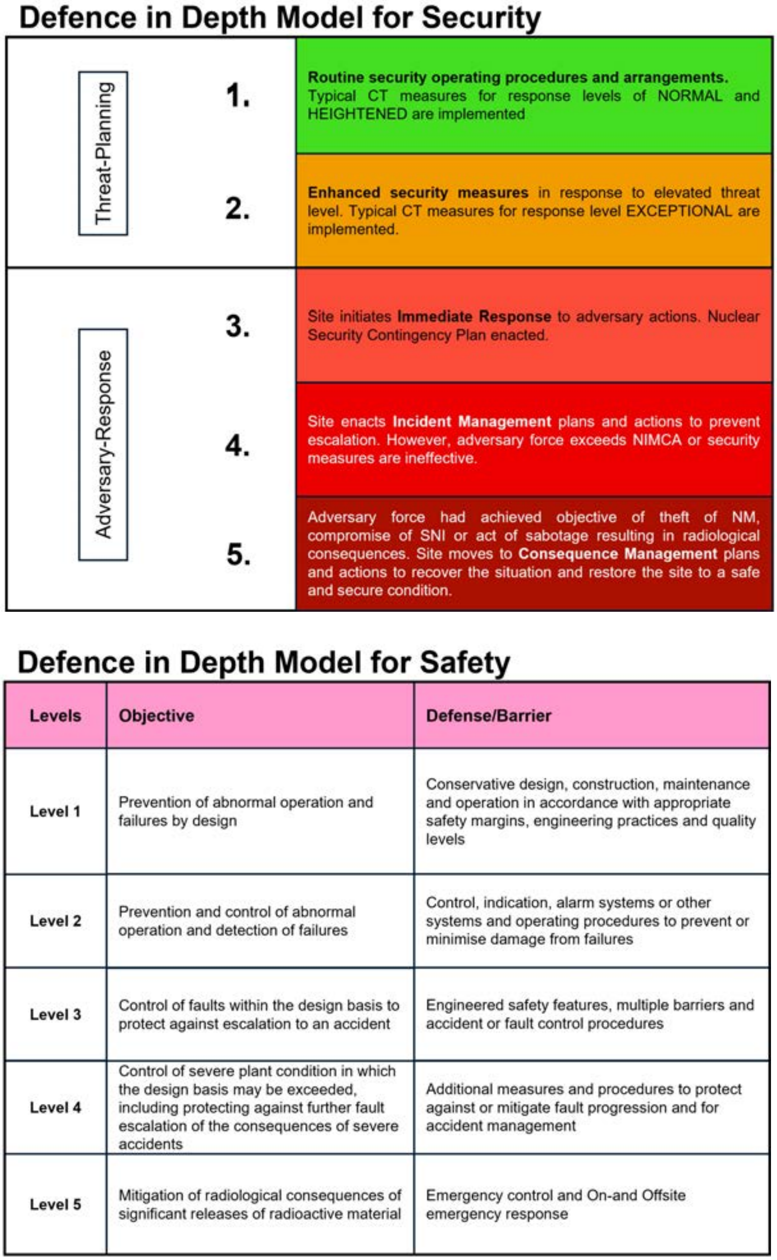
In both cases, designing security and safety measures across all levels of defence will help with the implementation of defence in depth through deploying multiple, independent barriers in a balanced way to assist in the mitigation of both safety and security events.

II–5.3. Emergency planning and response

Emergency planning and response is an area where close cooperation is essential to deliver an appropriate effect, as recognized by ONR’s Fundamental Security Principle 10 [II–9].

Fundamental Security Principles (cont.)	Emergency Preparedness and Response	FSyP 10
“Dutyholders must implement and maintain effective security emergency preparedness and response arrangements which are integrated with the wider safety arrangements.”		

To support this delivery, the ONR ensures safety and security representation at safety and security exercises and encourages duty holders to design scenarios with elements of both disciplines. However, consideration must be given to the fact that a scenario based on a security event resulting in radiological consequences is likely to be reliant on the security response having failed and, therefore, might not achieve regulatory expectations for that part of the exercise.



Defence in Depth Model for Security

Threat-Planning	1.	**Routine security operating procedures and arrangements.** Typical CT measures for response levels of NORMAL and HEIGHTENED are implemented
	2.	**Enhanced security measures** in response to elevated threat level. Typical CT measures for response level EXCEPTIONAL are implemented.
Adversary-Response	3.	Site initiates **Immediate Response** to adversary actions. Nuclear Security Contingency Plan enacted.
	4.	Site enacts **Incident Management** plans and actions to prevent escalation. However, adversary force exceeds NIMCA or security measures are ineffective.
	5.	Adversary force had achieved objective of theft of NM, compromise of SNI or act of sabotage resulting in radiological consequences. Site moves to **Consequence Management** plans and actions to recover the situation and restore the site to a safe and secure condition.

Defence in Depth Model for Safety

Levels	Objective	Defense/Barrier
Level 1	Prevention of abnormal operation and failures by design	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Prevention and control of abnormal operation and detection of failures	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures
Level 3	Control of faults within the design basis to protect against escalation to an accident	Engineered safety features, multiple barriers and accident or fault control procedures
Level 4	Control of severe plant condition in which the design basis may be exceeded, including protecting against further fault escalation of the consequences of severe accidents	Additional measures and procedures to protect against or mitigate fault progression and for accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Emergency control and On-and Offsite emergency response

FIG. II–9. Defence in depth for security and safety (adapted from [II–9]).

The ONR has also a regulatory requirement and associate guidance in the security assessment principles for sites to conduct cyber security exercises [II–9]:

FSyP 7 — Cyber Security and Information Assurance (cont.)	**Preparation for and Response to Cyber Security Incidents**	**SyDP 7.5**
“Dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges.”		

While tabletop exercises and simulated attacks have been relatively easy to incorporate, it has proved far more challenging to arrange for more intrusive ‘real play’ exercising of industrial control systems due to the inherent risks of undertaking such penetration testing on live systems and associated breach of licence conditions. Consequently, the ONR safety and security inspectors have been working closely with technical cyber specialists to develop a methodology that identifies what is possible and determines the scope and objectives of conducting the test.

II–5.4. Licensing and authorization

The ONR recognizes and articulates in its security assessment principles that the process of analysing security requires relevant subject matter expert insight,

> “…where people can envisage the variety of routes by which vulnerabilities can be exploited (e.g. adversary sequence [modelling]) once targets have been identified. A range of security measures or controls can then be identified, from which the most appropriate can be selected and implemented. Security analysis requires an extensive understanding of the facility and its safety case, both in the present and the foreseeable future, its profile in a variety of conditions (e.g. during movements of nuclear material and/or other radioactive material, outages and shutdown) and experience of security events (including at other facilities), together with the measures adopted to prevent their recurrence” [II–9].

To support the above expectation of involving subject matter experts in the analysis of security, the ONR has a well established team named ‘Security Informed Nuclear Safety’. This specialist team is trained and experienced in nuclear specialisms such as radiation protection and external hazards, in addition to nuclear security aspects such as blast effects. As such, the members of the team are familiar with relevant aspects of both safety cases and security plans. They provide verification of vital area identification studies submitted by licensees that determine all areas containing nuclear material and/or other radioactive material "…or equipment, systems, structures or devices, the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant DBT, could directly or indirectly result in unacceptable radiological consequences…" [II–9].

An aligned approach to licensing and authorization is especially important when considering designs for a new NPP. The ONR has specifically recognized this and produced a Technical Assessment Guide on the security assessment of generic new nuclear reactor designs [II–11]. According to Ref. [II–11], ONR security inspectors should ensure that their activities are integrated with those being undertaken by the ONR safety inspectors to help provide a consistent response to the potential operator and "It is important that the security assessment is integrated into the wider ONR and Environment Agency assessment process to [minimize] and, as necessary, manage any potentially conflicting requirements." Similarly, Ref. [II–11] states that ONR "…security inspectors should verify that any design changes arising for safety and/or environmental reasons have taken due account of potential impacts on security." To enable security inspectors to effectively undertake this responsibility, it is expected that ONR security inspectors will familiarize themselves with the proposed reactor technology.

II–5.5. Staff competence and training

The ONR ensures that security inspectors are given training in safety legislation and relevant aspects of safety regulation. Security training is also available for safety inspectors, and the intent is for this to be developed further. This allows inspectors to have a wider understanding of regulation, informing more balanced judgements and better decision making.

The ONR is also strongly encouraging the professionalization of security through providing incentives for security inspectors to achieve similar levels of qualification to that typically attained by safety inspectors. This upskilling has raised the profile of the discipline and has been beneficial in supporting security regulations implement an outcome focused approach aligned with that taken for safety.

II–5.6. Safety and security culture

Organizational culture is also an area of clear interface, and the ONR promotes a culture that recognizes the importance of both safety and security. The ONR, like any other organization, is not immune to the risks posed by insiders and poor culture. Certain policies it deploys assist both safety and security, such as its employee assistance scheme, which aims to provide support to staff across a range of personal circumstances such as stress, relationship breakdown, addiction and financial difficulties, any of which may lead to risky behaviour (in both a safety and security context) if left ignored and unsupported. The ONR also employs a staff rotation policy, which helps to avoid regulatory capture and to identify security anomalies.

II–5.7. Inspection and enforcement

The policy of the ONR for intervention planning states:

> "Safety, safeguard and security inspectors are to consult on preparation of the annual [IIS integrated intervention strategy]. This is to ensure that any synergies can be exploited. For example, an inspection of the site perimeter can cover protective security and site Licence Condition 2 … Some duty holders, particularly where they are smaller and staff have responsibilities covering multiple disciplines, may have limited resource to facilitate a concurrent inspection covering different aspects of safety and security. It is therefore also important that the [IIS] is managed to avoid possible resource burdens on duty holders. Furthermore, inspectors should liaise to ensure that the plan is de-conflicted to minimise the impact of other concurrent activities such as exercises or plant outages" [II–12].

In light of this policy, the ONR conducts several joint inspections as part of its intervention strategy and also deconflicts between inspections of different disciplines. Most recently, building on several years of experience of joint evaluation of emergency exercises, there has been a particular focus on inspections of operational technology involving specialist cyber security and instrumentation and control inspectors. The ONR operates under a single enforcement policy statement and enforcement management model.

This assists in the application of consistent regulatory decision making on enforcement across the disciplines.

REFERENCES TO ANNEX II

[II–1] CANADIAN NUCLEAR SAFETY COMMISSION, Safety Culture, Regulatory Document Series No. REGDOC-2.1.2, CNSC, Ottawa, Canada (2018).

[II–2] Convention on Nuclear Safety, INFCIRC/449, IAEA, Vienna (1994).

[II–3] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[II–4] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1/Mod. 1 (Corrected), IAEA, Vienna (2021).

[II–5] Convention on Early Notification of a Nuclear Accident, INFCIRC/335, IAEA, Vienna (1986).

[II–6] Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, INFCIRC/336, IAEA, Vienna (1986).

[II–7] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[II–8] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[II–9] OFFICE FOR NUCLEAR REGULATION, Security Assessment Principles for the Civil Nuclear Industry, 2017 Edition, Version 0, ONR, Bootle, Merseyside (2017).

[II–10] OFFICE FOR NUCLEAR REGULATION, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1 (January 2020), ONR, Bootle, Merseyside (2020).

[II–11] OFFICE FOR NUCLEAR REGULATION, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs, Nuclear Security Technical Assessment Guide No. CNSS-TAST-GD-11.1 Issue 1.2, ONR, Bootle, Merseyside (2021).

[II–12] OFFICE FOR NUCLEAR REGULATION, Guidance for Inspection Strategy Planning and Recording, ONR Compliance Inspection Guide No. ONR-INSP-GD-059 Revision 8, ONR, Bootle, Merseyside (2020).

ABBREVIATIONS

CNSC	Canadian Nuclear Safety Commission
DBA	design basis accident
DBT	design basis threat
HAEA	Hungarian Atomic Energy Authority
IEC	Incident and Emergency Centre (IAEA)
IMS	integrated management system
IPPAS	International Physical Protection Advisory Service (IAEA)
IRRS	Integrated Regulatory Review Service (IAEA)
NPP	nuclear power plant
NRECC	Nuclear and Radiological Emergency Coordination Centre (Pakistan)
NSC Act	Nuclear Safety and Control Act (Canada)
ONR	Office for Nuclear Radiation (United Kingdom)
PAEC	Pakistan Atomic Energy Commission
PNRA	Pakistan Nuclear Regulatory Authority
PPS	physical protection system
RANET	Response and Assistance Network (IAEA)
SCA	safety and control area
SKI	Nuclear Safety Inspectorate (Sweden)
SSI	Radiation Protection Institute (Sweden)
SSM	Swedish Radiation Safety Authority
TSO	technical support organization
USIE	Unified System for Information Exchange in Incidents and Emergencies (IAEA)

CONTRIBUTORS TO DRAFTING AND REVIEW

Baig, Z.A.	Pakistan Nuclear Regulatory Authority, Pakistan
De Azevedo Baeta, D.	National Nuclear Energy Commission, Brazil
Gomaa, R.	Egyptian Atomic Energy Authority, Egypt
Habib, U.	Pakistan Nuclear Regulatory Authority, Pakistan
Hagemann, A.	Consultant, Germany
Hasted, D.	Office for Nuclear Regulation, United Kingdom
Horvath, K.	International Atomic Energy Agency
Jianu, L.	National Commission for Nuclear Activities Control, Romania
Johnson, D.	United States Nuclear Regulatory Commission, United States of America
Khaliq, M.	International Atomic Energy Agency
Kirakosyan, K.	Armenian Nuclear Regulatory Authority, Armenia
Languin, T.	SG/SDSIE, Ministère de la Transition Ecologique et Solidaire, France
Lederman, L.	Consultant, Brazil
Lindahl, P.	Swedish Radiation Safety Authority, Sweden
Mahmood, R.	Pakistan Nuclear Regulatory Authority, Pakistan
Markosyan, G.R.	State Committee under the Government of Republic of Armenia for Nuclear Safety, Armenia
Mohammed Ahamed, A.	Sudanese Nuclear and Radiological Regulatory Authority, Sudan
Obenius Movitz, A.	Swedish Radiation Safety Authority, Sweden
Rosano, R.P.	Consultant, United States of America
Senior, M.D.	International Atomic Energy Agency

Shah, Z.A.	International Atomic Energy Agency
Shahzad, M.	International Atomic Energy Agency
Shull, D.	International Atomic Energy Agency
Sigouin, L.	Canadian Nuclear Safety Commission, Canada
Sims, M.	Office for Nuclear Regulation, United Kingdom
Thirumalai, S.	Indira Gandhi Centre for Atomic Research, India
Vincze, A.	Hungarian Atomic Energy Authority, Hungary

Consultants Meetings

Vienna, Austria: 26–30 November 2018; 1–5 July 2019; 25–29 May 2020

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray’s Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

There is a growing societal awareness of having a visible oversight mechanism of safety and security interfaces in the regulatory systems for nuclear facilities and activities. This publication compiles relevant IAEA requirements, recommendations and guidance on identifying and addressing potential and actual interactions between nuclear safety and nuclear security systems and measures in nuclear power plants. It also presents regulatory practices that are important to consider for nuclear safety and nuclear security, as they may reinforce or compromise the capacity of the regulatory bodies, competent authorities and operating organizations to meet nuclear safety and nuclear security requirements, including requirements relating to the interfaces between safety and security, during the application of regulatory functions in the various stages of the lifetime of a nuclear power plant.

International Atomic Energy Agency
Vienna, 2024
www.iaea.org