IAEA TECDOC SERIES

IAEA-TECDOC-1801

IAEA-TECDOC-1801

Management of the Interface between Nuclear Safety and Security for Research Reactors

IAEA
International Atomic Energy Agency

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 on the IAEA Internet site

http://www-ns.iaea.org/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.

MANAGEMENT OF THE INTERFACE BETWEEN NUCLEAR SAFETY AND SECURITY FOR RESEARCH REACTORS

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
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
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
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
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
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
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".

IAEA-TECDOC-1801

MANAGEMENT OF THE INTERFACE BETWEEN NUCLEAR SAFETY AND SECURITY FOR RESEARCH REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

For further information on this publication, please contact:

Research Reactor Safety Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
August 2016

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Management of the interface between nuclear safety and security for research reactors / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2016. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1801 | Includes bibliographical references.
Identifiers: IAEAL 16-01058 | ISBN 978–92–0–106316–8 (paperback : alk. paper)
Subjects: LCSH: Nuclear reactors — Safety measures. | Nuclear reactors — Security measures. | Nuclear facilities.

FOREWORD

Through its Nuclear Security Programme, the IAEA supports States to establish, maintain and sustain an effective nuclear security regime. The IAEA has adopted a comprehensive approach to nuclear security. This recognizes that an effective national nuclear security regime builds on: the implementation of relevant international legal instruments; information protection; physical protection; material accounting and control; detection of and response to trafficking in such material; and national response plans and contingency measures. With its Nuclear Security Series, the IAEA aims to assist States in implementing and sustaining such a regime in a coherent and integrated manner.

The IAEA Nuclear Security Series comprises Nuclear Security Fundamentals, which includes objectives and essential elements of a State's nuclear security regime; Recommendations; Implementing Guides; and Technical Guidance.

Nuclear safety and security share the same ultimate goal, which is to protect individuals, the public and the environment from harmful effects of ionizing radiation. However, the activities that address nuclear safety and security are different, and sometimes actions taken to strengthen nuclear safety affect nuclear security, either positively or negatively. It is therefore essential to establish a well coordinated approach to managing the interface between nuclear safety and security so that relevant measures are implemented in a manner that does not compromise either nuclear safety or security and aims to capitalize on opportunities for mutual enhancement.

The aim of this publication is to provide technical guidelines and practical information to assist Member States, operating organizations and regulatory bodies, on the basis of international good practices, and to manage the interface between nuclear safety and security at research reactor facilities in an integrated and coordinated manner.

This publication was developed based on input from two IAEA Technical Meetings and two IAEA consultants meetings held between 2013 and 2015. In these meetings, the experience of Member States was gathered, providing the basis for the guidelines, approaches and examples used in this publication. The IAEA wishes to thank the contributors to this publication for their efforts and valuable assistance. The IAEA also wishes to thank the participants of the IAEA workshop on Managing the Interface between Safety and Security of Research Reactors held in Vienna in June 2015 for their review of the draft of this publication.

The IAEA officers responsible for this publication were W.B. Kennedy, A. D'Arcy and A.M. Shokr of the Division of Nuclear Installation Safety, and K. Brooks and M. Clarke of the Division of Nuclear Security.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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 publication 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 and security of research reactors have the same ultimate goal – to protect individuals, the public, and the environment from harmful effects of ionizing radiation. To accomplish this, nuclear safety is focused on achieving proper operating conditions, preventing accidents, mitigating those that do occur and protection from exposure to ionizing radiation or radioactive material. Nuclear security is oriented to provide protection against malicious acts, including theft, sabotage and other criminal or intentional unauthorized acts that may lead to unacceptable radiological consequences or other adverse situations.

The safety and security provisions implemented at research reactor facilities help to ensure that such protection is achieved. Many design features and facility procedures contribute to both safety and security and offer opportunities for mutual enhancements. However, there are circumstances in which design features or facility procedures serve only one of the disciplines (safety or security) and in some cases can negatively affect the other. Moreover, modifications to the design or changes to facility procedures in support of reactor utilization or for the sake of safety or security improvements in some cases can have unintended adverse effects on the one or the other. A properly managed interface between safety and security, as an element of both disciplines, is therefore essential for ensuring the protection of people and the environment from security-related threats to, and radiological hazards associated with, research reactors.

Experience has shown that in many cases safety and security programmes developed separately, without adequate attention given to their interface. The primary focus of research reactor operating organizations and regulatory bodies has long been safety in design and operation of research reactors and for this reason safety practices have been established for decades. Initially, security focused on the prevention of unauthorized removal of nuclear material, and was typically executed by the reactor operating staff as a secondary duty or by security forces which were often organizationally isolated from the reactor management. As international focus on security has increased in recent years, the development of enhanced security arrangements has been accelerated. It is important that the interface between safety and security is well understood and effectively managed to ensure that the objectives of both are achieved as the disciplines continue to mature and when security measures are implemented at research reactors.

World events and changes in the global threat environment have made the security of research reactors a subject of increased international focus. While concern about malicious acts and protection against them is not new and the IAEA has long published recommendations related to physical protection, international recognition of the need to enhance efforts to protect against security-related threats, including sabotage, has prompted the IAEA to expand the scope and detail of existing publications to specifically address the security of nuclear installations. These publications include Security Fundamentals, Security Recommendations, Implementing Guides and Technical Guidance that are applicable to the security of research reactor facilities.

In general, security is concerned with malicious actions by humans that could cause or threaten harm to other humans, whereas safety is concerned with the broader issue of harm to humans or the environment, whatever the cause. In the context of this publication, the

following terms related to safety, security and their interface are used. Passages in quotation marks are direct quotations from the IAEA Safety Glossary [1]:

(a) **Safety:** "The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards". As used in this publication, the term safety includes radiation protection and all other aspects of safety related to a research reactor facility (e.g. nuclear safety, radiation safety and radioactive waste safety). This also includes conventional safety when deterioration or failure could lead to radiation exposure of workers, the public or the environment.

(b) **(Nuclear) Security:** "The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities". As used in this publication, the term security on its own means nuclear security.

(c) **Safety–security Interface:** Aspects of safety and security requirements and measures at a research reactor facility that could mutually complement or counteract one another.

(d) **Management of the safety–security interface:** The procedural approach by all affected parties (the State, operating organization, regulatory body and other stakeholders) to implement measures to:
   (i) Ensure that safety and security complement one another at the research reactor facility, that measures introduced to attain the objectives of one do not compromise the objectives of the other and to ensure that areas of conflict between them are adequately and satisfactorily resolved,
   (ii) Coordinate the activities, responses and other provisions of the two disciplines in a way that minimizes the overall radiological risk and derives the greatest chance of meeting the objectives of both safety and security.

(e) **Protection:**
   (i) In the context of safety, protection means radiation protection: "The protection of people against exposure to ionizing radiation or radioactive materials and the control of radiation sources, including the means for achieving this, and the means for preventing accidents and for mitigating the consequences of accidents should they occur".
   (ii) In the context of security, protection means physical protection: "Measures for the protection of nuclear material or authorized facilities, designed to prevent unauthorized access to or removal of nuclear material or other radioactive material or sabotage".

(f) **Nuclear material:** "Any source material or special fissionable material as defined in Article XX of the statute of the IAEA" or otherwise subject to safeguards due to its usefulness in the production of nuclear weapons or other nuclear explosive devices. This includes "certain non-nuclear materials that are essential for the use or production of nuclear material", or explosive devices.

(g) **Radioactive materials or substances:** "Material designated in national law or by a regulatory body as being subject to regulatory control because of its radioactivity".

1.2. OBJECTIVE

The objective of this publication is to provide technical guidelines and practical information on managing the interface between safety and security of research reactors. It provides for a better understanding of the elements of that interface, and discusses means to manage it in an integrated manner so as not to compromise safety or security when planning and implementing different programmes and activities.

1.3. SCOPE

This publication presents background information on the existing IAEA requirements and guidance for safety and on the recommendations and implementing guidance for security, examines complementary and conflicting aspects at their interface and suggests general solutions that can help States, regulatory bodies, operating organizations and other stakeholders to effectively manage the interface in an integrated and coordinated manner so that acceptable levels of both safety and security are achieved.

This publication is applicable to research reactors that are covered by the scope of IAEA Safety Standards No. SSR-3, "Safety of Research Reactors" [2]. A research reactor *facility* usually consists of the reactor itself and associated facilities (such as a neutron beam experiment hall, hot cells used for handling of irradiated material, experiment assembly rooms, fresh and irradiated fuel storage, radioactive material laboratories, etc.) that form an integral part of the facility under the control and direct responsibility of the reactor manager.

The information provided in this publication is applicable to the site evaluation, design, construction, operation, utilization, modification, extended shut down and decommissioning phases in the lifetime of a research reactor facility. This publication complements the existing IAEA publications on safety and security of research reactors and does not replace or supersede any of them. It does not address offsite activities that are not under the control of the research reactor operating organization such as the transport of nuclear or other radioactive materials.

Some IAEA publications on nuclear security management for research reactors use the terminology "research reactor and associated facilities (RRAF)", which includes fuel research or fabrication facilities, radioisotope production facilities and waste disposal facilities that are co-located with a research reactor. While not explicitly within its scope, this publication may nevertheless be generally useful for managing the interface between safety and security at these types of facilities.

This publication is intended for use by the State, regulatory bodies, operating organizations, and other stakeholders involved in the safety and security of research reactors.

1.4. STRUCTURE

This publication is divided into five sections, three appendices and two annexes. In addition to this introductory section, Section 2 covers safety and security objectives, fundamentals and concepts, including discussion of the defence-in-depth concept, use of a graded approach, safety analysis, threat assessment and security plan, and safety and security measures. Section 3 discusses issues and challenges in the interface between safety and security, and provides information on features of research reactors affecting the interface and similarities and differences between safety and security. Section 4 provides general considerations in the

interface, including responsibilities for safety and security (State, regulatory body, and operating organization), leadership and management of safety and security, optimization of protection, preparedness and response, training and assessment of the interface. Section 5 discusses specific concerns for management of the interface during siting, design, construction, operation, utilization and modification, extended shutdown and decommissioning.

Appendices I, II and III discuss and provide information on good practices for a coordinated approach to safety and security, areas of potential conflict between safety and security and change management, respectively. The Annexes provide case studies and practical examples of managing the interface between safety and security.

2. SAFETY AND SECURITY OBJECTIVES, FUNDAMENTALS AND CONCEPTS

2.1. SAFETY AND SECURITY OBJECTIVES

The overall safety and security objectives are stated in Section 1, above. The objectives of safety and security at a research reactor facility share many common elements related to protecting people, society and the environment. In both cases the risks need to be minimized and the consequences that are considered acceptable cannot differ if the initiating event of a radiological release is due to human or equipment failures, internal or external events or an event of malicious origin.

2.2. SAFETY AND SECURITY FUNDAMENTALS

The IAEA Safety Standards No. SF-1, "Fundamental Safety Principles" [3], establishes the fundamental safety objective, safety principles and concepts that form the foundation of the IAEA's safety standards and its safety programme for nuclear facilities. The publication sets this foundation by means of ten fundamental "safety principles". The IAEA Nuclear Security Series No. 20, "Objective and Essential Elements of a State's Nuclear Security Regime" [4], establishes the fundamentals and objectives for nuclear security in the form of twelve "essential elements" of a State's nuclear security regime. Table 1 summarizes the "safety principles" and "essential elements" in the order they appear in the source documents.

TABLE 1. FUNDAMENTAL SAFETY PRINCIPLES AND ESSENTIAL ELEMENTS OF SECURITY

Fundamental Safety Principles [3]	**Essential Elements of Security [4]**
1 Responsibility for safety *(operator responsible for safety and defining the design basis accident)* 2 Role of government *(State provides legal framework to regulate safety)* 3 Leadership and management for safety *(management and quality systems, safety culture)* 4 Justification of facilities and activities *(overall benefit versus its radiation risk)* 5 Optimization of protection *(highest level of safety that can reasonably be achieved)* 6 Limitation of risks to individuals *(no person shall bear an unacceptable exposure risk)* 7 Protection of present and future generations *(protect people and the environment against radiation)* 8 Prevention of accidents *(based on graded approach and defence-in-depth)* 9 Emergency preparedness and response *(involves the operator, regulator, local authorities and cross-border cooperation if necessary)* 10 Protective actions to reduce existing or unregulated radiation risks *(natural and/or legacy sources, remediation measures, etc.)*	1 State responsibility *(for establishing a nuclear security regime)* 2 Identification and definition of nuclear security responsibilities *(determined by the State)* 3 Legislative and regulatory framework *(State provides legal and administrative framework to govern security)* 4 International transport of nuclear material and other radioactive material *(State responsible until handed over to another State)* 5 Offences and penalties including criminalization *(appropriate procedures and penalties for violations)* 6 International cooperation and assistance *(information exchange and assistance between States)* 7 Identification and assessment of nuclear security threats *(used in implementing the State's nuclear security regime)* 8 Identification and assessment of targets and potential consequences *(reviewed periodically)* 9 Use of risk informed approaches *(based on the threat, consequences and vulnerabilities)* 10 Detection of nuclear security events *(security systems and measures are in place)* 11 Planning, preparedness and response to a nuclear security event *(develop, exercise and evaluate response plans, including coordination with emergency plans)* 12 Sustaining a nuclear security regime *(integrated management systems, security culture, resources and training)*

The separate development and different viewpoints of safety and security already mentioned that resulted in these two sets of fundamentals (principles and elements) are immediately apparent. However, there are numerous parallels and interactions between them in the context of the safety–security interface at research reactors that yield opportunities for integrating the management of that interface:

- Legal and regulatory frameworks, including bodies effectively independent of the operating organization for inspection and verification of compliance, are established and maintained by the State for both safety and security. In the case of security, the State also determines the threat in a risk-based approach, and the associated nuclear security regime that needs to be implemented to deal with such a threat and its potential consequences;
- The prime responsibilities for implementing measures addressing safety and security measures to counter the threat at a research reactor facility rest with the licence holder (i.e. the operating organization). Effective leadership and management to carry out these responsibilities needs to be established and maintained at all facilities and activities that involve nuclear material or give rise to radiation risks (see Subsection 4.2);
- Facilities and activities that involve nuclear material or give rise to radiation risks have to be justified on the basis of an overall benefit. The safety and security risks cannot be so great that the measures needed to address them outweigh the benefits of the facility;
- Measures for controlling radiation risks (whether they arise from safety or security events) have to ensure that no individual bears an unacceptable risk of exposure and that people and the environment, both present and future, are protected against unnecessary radiation risks;
- Safety and security assessments and their associated radiation protection measures have to be conducted to a degree that is commensurate with the level of risk posed by the facility, by applying the graded approach to their formulation (see Subsection 2.4);
- All practical efforts have to be made to prevent and mitigate nuclear, security or radiation incidents/accidents by applying the principle of defence-in-depth, providing several layers and methods of radiation and physical protection;
- Emergency plans (called contingency plans for security events) for emergency preparedness and response for nuclear, security or radiation incidents/accidents have to be in place in case defences against such events fail or are breached or compromised;
- The integrated management system at the facility needs to address the policies, requirements, quality assurance, review and implementation of procedures, responsibilities and measures dealing with both safety and security at the facility (see Subsection 4.2.1);
- A strong safety culture and a strong security culture at the research reactor facility are indispensable to the maintenance of safety and security respectively. While the two cultures need to practice different philosophies, there are common approaches to building and maintaining such cultures that can be applied to both (see Subsection 4.2.2).

2.3. PREVENTION OF SAFETY OR SECURITY EVENTS – DEFENCE-IN-DEPTH

The concept of defence-in-depth applies to both safety and security. It entails the definition and implementation of physical and organizational measures to prevent or mitigate the risk of accidents and their consequences or the risk of breaches of security with potential malicious intent with their consequences. Requirements and recommendations for defence-in-depth to be incorporated into the design phase and each subsequent phase in the lifetime of a research reactor facility are established by the IAEA for safety in Ref. [2] and for security in Refs [4]

and [5]. Safety and security both base defence-in-depth on providing successive layers of protection; however, they differ in their strategy and implementation.

For safety, there are five levels of defence-in-depth that are aimed at:

- Preventing deviations from normal operation;
- Controlling deviations from operational states;
- Controlling accidents within the design basis;
- Mitigating accidents and ensuring confinement of radioactive materials;
- Mitigating the radiological consequences of radioactive releases.

In security, defence-in-depth is identified in Refs. [5] and [6] as several layers and methods of protection that have to be overcome or circumvented by an adversary in order to achieve his objectives and are applied in:

- Detecting a potential malicious act;
- Delaying the adversary for a sufficient period to allow for appropriate response, if necessary through external support;
- Responding to and neutralising an attack.

Therefore, it is important that the operating organization understands the means of application of the defence-in-depth concept that are actually in place at their facility for both safety and security when addressing interface issues.

2.4. GRADED APPROACH

Use of a graded approach means that the safety requirements and security recommendations have to be applied in a way that is commensurate with the potential hazards of the facility (see Refs [2, 4 and 7]). In particular, such an approach needs to be used when defining prevention and mitigation measures. The graded approach is applied to safety and security provisions covering all phases of the lifetime of a research reactor facility – siting, design, construction, commissioning, operation, utilization, modification, extended shut down, decommissioning, – and for all the disciplines and activities associated with each phase – training, qualification, response planning, emergency and contingency preparedness, and regulatory supervision.

The factors used for applying the graded approach include the research reactor power and source term, fuel design and handling, amount, enrichment and form of fissile materials, presence of high-pressure or high-energy piping, quality of confinement, inventory of radioactive material of the facility, and proximity to population. In the case of security, the State will categorize nuclear and other radioactive material into protection levels depending on their attractiveness and establish a graded approach to sabotage through defining unacceptable radiological consequences. Other examples of areas where a graded approach can be applied to security are information/computer security [8] and criteria for determining trustworthiness of personnel.

Use of the graded approach for safety and security does not result in waiving of any of the established requirements for research reactors, but rather serves to harmonize the scope of compliance to the requirements according to the magnitude of the hazards presented by the research reactor facility. Grading the application of safety requirements and security recommendations needs to be supported by established bases agreed by the regulatory body or

determined by the State, respectively. It is important that the operating organization considers these bases when addressing the interface issues between safety and security.

2.5. SAFETY ANALYSIS

The safety analysis provides the technical basis demonstrating that a research reactor facility can be operated safely in accordance with regulatory requirements and within the legal framework of the Member State (Refs [9 and 10]). The safety analysis is based on the analysis of a set of postulated initiating events that were considered in the reactor design. The results of the safety analysis identify the structures, systems and components important to safety and the requirements for their design, fabrication, installation, operation, and quality. The safety analysis is also forms part of the basis for the facility's operational limits and conditions and emergency preparedness and response.

It is important that the operating organization understand the potential hazards associated with the conduct of all activities at the research reactor. The research reactor management needs to fully understand the information presented in the facility's safety analysis report when addressing the safety and security interface issues.

2.6. THREAT ASSESSMENT AND SECURITY PLAN

The threat assessment is an evaluation of the threats based on available intelligence, law enforcement and open source information that describes the motivation, intention and capabilities of potential adversaries [11]. This may be supplemented by the regulatory body issuing a design basis threat for which the security requirements are specified in more detail. A facility's security system is an integrated set of measures, intended to prevent a threat (as described in the threat assessment or design basis threat) from completing malicious acts involving or directed at nuclear material, other radioactive material and/or the nuclear facility (see Refs [5 and 6]).

The design, evaluation, implementation and maintenance of the facility security system are described in the facility security plan and approved by the regulatory body. This plan also describes the contingency plan including the external response forces that may be involved. The research reactor management needs to fully understand the information presented in the threat assessment and the facility's security plan when addressing safety and security interface issues.

2.7. SAFETY AND SECURITY MEASURES

Safety measures and security measures have the common objective of protecting people, society and the environment. Therefore, safety measures and security measures have to be designed and implemented such that security measures do not unduly compromise safety and safety measures do not unduly compromise security. This can be accomplished by giving attention, in the context of both safety and security, to the following [3]:

- Appropriate provisions in the design and construction of nuclear installations and other facilities;
- Controls on access to nuclear installations and other facilities both for safety reasons as well as to prevent the loss of, or the unauthorized removal, possession, transfer and use of, nuclear and radioactive material or sabotage of the nuclear facility;

- 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 management of the security of nuclear and radioactive material.

One area where there is a need for close interaction between safety and security specialists within a nuclear facility is sabotage target identification and subsequent protection of these targets, using a graded approach, in a manner which does not compromise safety requirements and arrangements. Each facility needs to perform an analysis to determine:

- Whether the radioactive inventory at each location within the facility has the potential to result in unacceptable radiological consequences, as determined by the State using a graded approach;
- Similarly, identifying equipment, systems or devices, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences; and
- Identifying computer-based instrumentation and control systems important to safety.

Following such target identification, the security system needs to be designed (or redesigned) to be effective in meeting regulatory objectives or requirements against credible sabotage scenarios derived from the threat assessment. This process needs to be carried out every time there is a change in the threat assessment, a change in the State's determination of unacceptable radiological consequences or a change in radioactive inventory in the nuclear facility. It needs to take into account engineered safety systems which already exist. Recommendations in this respect are contained in Section 5 of [6]. Guidance on the identification of vital areas (which contain radioactive material, equipment, systems and devices, the sabotage of which could lead to high radiological consequences) is provided in [12]. Guidance on the protection of computer systems is given in [8].

Appendix I provides good practices when setting up a coordinated approach to managing the safety–security interface.

3. ISSUES AND CHALLENGES IN THE INTERFACE BETWEEN SAFETY AND SECURITY OF RESEARCH REACTORS

3.1. FEATURES OF RESEARCH REACTORS AFFECTING THE SAFETY AND SECURITY INTERFACE

Research reactors have a wide variety of designs, operational characteristics, and utilization programmes, and differ from nuclear power reactors and other nuclear installations in many aspects. This can have an impact (either positive or negative) on the effective management of the interface between safety and security. Some aspects relevant to most research reactors that could present challenges for managing the interface between safety and security include:

- Relatively short operating, refuelling, and maintenance cycles, with associated high frequency, short duration changes in the facility security configuration;
- Numerous operating modes for different purposes, each with its own safety and security challenges;
- Access to the reactor hall, reactor core, irradiation and experimental facilities, and reactor areas by operations personnel, researchers and contractors, including during power operation;
- Means to perform manual activities affecting the core reactivity and geometry, possibly with the reactor operating at power;
- Hands-on operation of equipment requiring unobstructed mobility of operations personnel around the whole facility during operation;
- Many parties with diverse vested interests in optimizing the operational, production and experimental programmes of the facility for their particular needs (e.g. numerous customers of irradiation products or services, universities and other organizations with experimental programmes at the reactor, etc., all with varying requirements and varying degrees of influence over how the facility is operated and managed).

Appendix II evaluates some of these aspects in detail and discusses strategies for addressing potential conflicting requirements.

On the other hand, there are numerous features of research reactor facilities that lend themselves to mutual enhancement of safety and security, such as:

- Design of the reactor safety systems for high reliability and availability by the use of redundancy, diversity and separation of safety functions, making it difficult for an adversary to cause a significant safety or radiological event with a single external or internal malicious act;
- Use of passive safety features which can provide additional resistance to malicious acts such as sabotage;
- The reactor building is often a reinforced concrete structure designed to remain intact during a design basis earthquake and serves to contain significant radioactive releases within the facility in case of an accident, and when it does not include windows can provide a robust structure complicating the execution of an external assault;
- Large shielding structures installed around radioactive materials for radiation protection purposes may also provide a barrier beneficial for security;

- Engineered safety features of the reactor, such as the emergency core cooling system, the emergency clean-up system and other measures that protect against the effects of energy releases inside the building;
- Access control measures (including key-code and biometric identification) implemented for security that benefit:
  - Protection against accidental exposure of operating personnel, researchers and visitors;
  - Prevention of unauthorized persons from accessing nuclear and radioactive materials and systems important to safety;
  - Limiting the number of persons authorized to access or remove nuclear or other radioactive material;
- Area surveillance and video monitoring implemented in the facility for security purposes also enhance safety where the relevant monitors are available to the operations personnel;
- Emergency responses related to offsite radiation protection measures are the same for safety and security events (considering that there may be an additional need to protect emergency personnel and equipment from a security-related threat).

By capitalizing on those features that promote mutual enhancements and focussing on minimizing areas of potential conflict, a well-coordinated approach to managing the safety–security interface can be developed.

3.2. SIMILARITIES AND DIFFERENCES BETWEEN SAFETY AND SECURITY OF RESEARCH REACTORS

Safety is concerned with the radiological risk to humans and the environment, whatever the cause of this risk. At a research reactor facility, the cause could be human error, equipment failure, an internal event (fire, pipe break, etc.) or an external event (earthquake, flooding, etc.). It could also be a security event – an act or acts with malicious intent leading to a release of radioactivity into the facility or into the environment.

Security is concerned with reducing the vulnerability of the facility to the theft of nuclear material (in the form of fresh and irradiated reactor fuel or isotope targets) or other radioactive material, and to sabotage resulting in the release of the large inventories of fission and activation products and other high activity radioactive materials contained in the research reactor facility.

Safety is necessary, but not adequate to protect nuclear or other radioactive material from theft, sabotage, or other intentional unauthorized acts. Similarly, security is necessary, but not sufficient on its own to protect people or the environment from a radioactive release caused by a malicious act. While some safety issues have no security implications and some security issues have no safety implications, in most cases they are not mutually exclusive and have to be managed in an integrated manner.

The acceptable risk to workers, the public and the environment cannot be different when the initiating event of a radiological release is due to human or equipment failures, internal or external events or an event of malicious origin. This is a major area of convergence between safety and security and is the basis for measures to be implemented for enhancing cooperation between safety and security, especially when responding to an accident or sabotage event. As an example of such cooperation, an on-site operation to recover radioactive material that proceeds in consultation with the radiological experts from the facility helps to ensure

adequate measures to limit exposure of the security response personnel when they recover the material. At the same time, information on the progress of the recovery operation provides essential guidance to the radiological response personnel on where to monitor for potential radioactive contamination.

3.3. CHALLENGES TO THE SAFETY–SECURITY INTERFACE

There are a number of challenges that have to be overcome in order to adequately manage the safety–security interface. Some challenges of an operational or procedural nature have already been mentioned in Subsection 3.1 and further discussed in Appendix II. In addition, there are basic cultural differences in the two areas, large differences in the background and experience of experts in the respective fields and in the engineering and technological aspects of their implementation that may make it difficult for safety and security personnel to communicate and interact effectively. The safety and security responsibilities could be in separate organizations, potentially resulting in a lack of effective cooperation and, in extreme cases, competition between the two functions.

Security considerations were not generally addressed early in the design of many existing facilities, so that conflicts with safety measures or operational requirements were not addressed until much later in the design process, or only after the facility had been built. This can result in more expensive and less than optimal security solutions, and a higher impact by the post-fitted security measures on operations and safety, than would be the case if the safety–security interface had been more carefully managed from the beginning.

Changes in facility operations, equipment, layout, etc., are not unusual for research reactors and can compromise both safety and security measures if not adequately managed. Without appropriate methods to track and evaluate proposed changes or modifications to the facility in terms of their potential impacts on both safety and security, the existing safety or security systems could be rendered largely ineffective. Appendix III presents useful information for consideration when managing changes and modifications.

The control of sensitive information and documentation presents another area of potential difficulty in managing the interface between safety and security, especially in electronic media. A single email exchange between two members of staff can proliferate, together with all its attachments, to dozens of unintended recipients in a very short time if there are no control measures in place to prevent it. The same applies to other forms of copying and disseminating sensitive information and documentation, and also to the disposition of such information and documentation when it is not being disseminated (e.g. sensitive documentation carelessly left unattended on a desk or on a computer screen). Gaining control over these forms of information dissemination, whether they are inadvertent or intentional, is one of the biggest challenges in information management, being as much a problem of culture as one of implementing policies and procedures, and needs to form an integral part of the management of the interface between safety and security. Some safety information may be of value to an adversary planning to sabotage the facility and also needs to be protected as sensitive information.

4. GENERAL CONSIDERATIONS IN THE SAFETY–SECURITY INTERFACE FOR RESEARCH REACTORS

4.1. RESPONSIBILITIES FOR SAFETY AND SECURITY

Responsibilities for nuclear safety and security and their interface are established for the State and various other organizations within a Member State by IAEA Safety Standards Series No GSR Part 1, "Governmental, Legal and Regulatory Framework for Safety" [13] and SSR-3, "Safety of Research Reactors" [2], and IAEA Nuclear Security Series No 13 (INFCIRC/225 Revision 5) "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities" [6]. The following subsections summarize the roles of the State, the regulatory body and the operating organization in in the context of these publications.

4.1.1. Role of the State

As already noted in Subsection 2.2, the State has the responsibility for setting up the national legal and regulatory frameworks for both safety and security, including the body or bodies, independent of nuclear facility operating organizations, for providing appropriate regulation, inspection and verification of compliance. The legal and regulatory frameworks have to establish adequate infrastructural arrangements for interfaces of safety with arrangements for security and with the State system of accounting for, and control of, nuclear material. These legal and regulatory frameworks have to clearly identify responsibilities for addressing all the elements of safety, security and their interface, and integrating emergency and contingency response arrangements for safety-related and security-related incidents.

In the case of security, the State also provides an assessment of the threat, as well as criteria for applying a graded approach based on radiological consequences against which the security system is designed and evaluated. The State also ensures that the strategies it determines are periodically reviewed and kept in pace with the evolution of the threat level and its determination of unacceptable consequences.

The management of a crisis associated with a security event at a research reactor generally requires involvement of more State bodies as compared with a safety-related event (e.g. the police and other response forces, see Subsection 4.5). The State needs to ensure that these bodies are adequately funded and staffed to be able to respond to such an event and that their training prepares them to coordinate their response activities with the safety and security experts at the facility. Additionally, there needs to be formal agreements between these bodies detailing their respective responsibilities for coordinating the on- and off-site response.

4.1.2. Role of the regulatory body

Consistent with the authority provided under the State's legal framework, the regulatory body is responsible for establishing and maintaining appropriate regulations that require the operating organizations to effectively manage safety and security at research reactors on their sites. It is essential that the regulatory body provide clear regulations (or requirements to meet those regulations) governing safety and security at research reactor facilities and the conditions or criteria for which facility operators need to obtain the approval of the regulatory body. The regulatory body also holds the responsibility for the periodic verification of compliance with those regulations through inspection or other review activities.

Different regulations apply to safety and security, and in the event that the security regulatory body is separate from the safety regulatory body, it is essential to have a consultation, interfacing and coordination mechanism between the two bodies to ensure that regulatory requirements are compatible and advance both safety and security. A similar coordination mechanism is necessary if there is one regulatory body with separate internal groups responsible for safety and security. The need for coordination applies to all regulatory functions including establishment of regulations, licensing, inspection, and enforcement.

4.1.3. Role of the operating organization

The operating organization has the primary responsibility for implementing safety and security regulations and requirements at the research reactor facility. This includes addressing both safety and security in coordinated manner while ensuring that all regulatory requirements are met. This responsibility is constant throughout the lifetime of the facility.

Safety is typically the focus of regular safety committee meetings at a research reactor facility. To facilitate effective management of the safety and security interface, the operating organization needs to ensure the appropriate participation of knowledgeable safety and security personnel in these meetings to contribute the benefit of their combined expertise related to the following:

- Safety analysis, layout, operation, and operational radiation protection programme of the facility;
- Operating licence, operational limits and conditions and requirements for regulatory compliance;
- Security programme of the facility and related regulatory requirements (e.g. security plans, measures and trustworthiness programme);
- Expected performance of the security systems, including the obligations of facility management in this regard;
- Awareness of the threat (and the design basis threat if applicable) and other adversary intentions and capabilities against which the security system is designed;
- Requirements for security implementation in the organization;
- Emergency plan (safety);
- Contingency plan (security);
- Facility training and qualification programme;
- Activities delegated to third party service providers (e.g. contractors) or State agencies.

An effectively managed safety–security interface requires that facility management establish and maintain strong safety and security cultures in all activities and among all levels of personnel and management in the organization (see Subsection 4.2.2).

4.2. LEADERSHIP AND MANAGEMENT OF SAFETY AND SECURITY

4.2.1. Integrated management system

The establishment of an integrated management system that includes the research reactor facility is a basic (high level) requirement for all the phases of the research reactor lifetime [2, 3 and 14]. This system integrates all quality, health, economic and environmental aspects as well as safety and security into a single coherent framework for management to adequately direct the interactions and interfaces between diverse activities, disciplines and requirements, and could be established at the level of the facility itself or be included within the

management system of the operating organization. The management system is the basis for facility operations and maintaining safety and security cultures.

The functional categories of the management system for safety and security are similar (management responsibility, resource management, quality management, process implementation, performance assessment and improvement). However, there are differences in the management system processes for safety and security. Typical processes for safety include the procedural management of safety analysis, fuel handling and core management, reactor operation, experiments, maintenance of systems and components important to safety and emergency preparedness. Typical security processes include personnel security, information security, computer security, access control, security training and exercises, system sustainability, security event reporting and management of the security organization and equipment.

Therefore, the management system needs to clearly identify not only safety and security as distinct processes to be managed, but also the interface between them, so that the areas of common ground and, in particular, the areas of potential conflict between the two disciplines can be properly managed.

4.2.2. Safety culture and security culture

An important aspect needed to achieve the highest degree of both safety and security, and to effectively manage the interface between them, is to maintain a cultural environment within the organization that places both safety and security at the highest awareness among all levels of personnel and management in the organization.

A safety culture is defined in Ref. [1] as: “The assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance”.

A (nuclear) security culture is defined in Ref. [4] as: “The assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support, enhance and sustain nuclear security”. Ref [15] provides a detailed discussion of a nuclear security culture.

An important shared objective of safety culture and security culture is to instil among all personnel a general awareness of the risks resulting from radioactive material and associated facilities and the sense of responsibility to minimize those risks. This objective is largely based on common principles, e.g. a questioning attitude, rigorous and prudent approaches and effective, open, two-way communication. A security culture also has the broader objective of instilling an awareness of the threat and the need for all employees and contractors to adopt a strict and prudent approach to security, be vigilant with a questioning attitude and react quickly and correctly when the need to do so arises.

As security deals with deliberate acts, security culture requires different attitudes and behaviour from those associated with safety culture. The main differences between these cultures that need to be factored into the culture-building process are:

(a) A safety culture pursues transparency. It is important to share feedback on experience, thereby preventing repetitive occurrences of incidents or accidents at the facility, and to disseminate information to prevent such occurrences at one research reactor facility from

being repeated at others. In some cases, however, it may be necessary to withhold safety information for security reasons, such as information that might reveal a vulnerability which could be exploited by a person or persons with malicious intent.

(b) A security culture, on the other hand, demands that the sharing of information typically be restricted only to authorized trusted personnel on a valid "need-to-know" basis, in order to prevent sensitive information related to security measures or safety/security weaknesses at the facility from falling into the hands of adversaries.

Due to their nature, safety and security cultures take time and effort to develop to the degree that all personnel are unified in their perceptions and duties in relation to each culture. Both safety and security are the responsibility of everyone at the facility, although more emphasis on the one or the other may apply to specific actors. Safety and security cultures have to be actively promoted and coordinated by management in order to successfully interface safety and security at the facility and to enable affected personnel to know instinctively when to disseminate information to enhance safety and how to control sensitive information to maintain security. All personnel need to have at least a basic understanding of the following aspects where they may be outside their particular area of expertise:

- The facility safety basis and how safety is ensured and maintained;
- Any safety issues at the facility;
- How information is managed;
- The security threat to the facility;
- How the security plan, arrangements and measures address the threat.

4.3. OPTIMIZATION OF PROTECTION

Optimization of protection is one of the basic radiation protection principles and it is of special importance to apply it, in addition to the authorized dose limits, to achieve an optimized level of protection [16 and 17]. Dose limits represent the lower boundary of a region of unacceptable doses and risks. Doses just below the limits can therefore only be tolerated if nothing reasonable can be done to further reduce them.

In most situations, however, additional measures can be implemented to provide for optimized protection, where dose constraints are used. Dose constraints are applied in planning and executing tasks and in designing facilities or equipment [17]. Dose constraints are established on a case-by-case basis that takes into account general trends, but that remains consistent with the specific characteristics of the radiation exposure situation within the facility. These are normally established by the operating organization and agreed upon by the regulatory body.

This principle is equally applicable whether the exposure to radiation is assessed from a safety or a security viewpoint and the dose constraints are to be established at a level as far below the prescribed dose limits as reasonably practicable. Furthermore, there has to be a harmonized approach to determining dose constraints for safety and security – i.e. the doses to persons and the environment considered acceptable cannot depend on whether the exposure is safety- or security-related.

The fundamental role of optimization is to bring about a state of thinking, or a culture, in everyone responsible for the safety and the security of the facility that constantly questions whether all reasonably practicable measures have been taken to minimize the risk of

exposure. In essence, it is an extension of the safety–security cultures discussed in the previous section.

All radiation risks, including those resulting from malicious acts, have to be identified and assessed, and periodically reassessed during the lifetime of the reactor. Factors to consider during the reassessment of the risks include the evolution of technologies, changes in threats and any modifications associated with changes in safety and security requirements.

4.4. OPERATING PROCEDURES

Operating procedures are developed to ensure that activities important to safety are performed in accordance with the approved operational limits and conditions of the facility [18]. These procedures cover aspects such as operation in all operational states; maintenance of major components or systems that could affect reactor safety; periodic inspections, calibrations and tests of structures, systems and components essential to safety; the operator's response to anticipated operational occurrences and design basis accidents; radiation protection activities and more [2]. Operating procedures, by their nature, affect the configuration of the facility in terms of safety; however, the security configuration can also be affected.

For the mutual benefit of safety and security, operating procedures can be developed in consultation with security specialists to ensure that interface issues are appropriately considered, including:

- The usefulness of operating procedures and the information included in them for planning and executing malicious acts by adversaries, such as procedures related to equipment needed to prevent or mitigate a beyond design basis event; procedures related to fuel handling and storage (fresh and irradiated fuel); the location of and means for accessing fuel handling tools;
- The potential impact of performing operating procedures on the security configuration of the facility, such as refuelling the reactor, performing maintenance on access points, bringing external contractors into the facility to perform work, bypassing safety systems for testing, testing the emergency power systems by disconnecting the external power supply;
- The possibility for operating procedures to unintentionally compromise security measures, such as obstruction of security cameras or sensors by poor placement of materials and equipment needed for periodic testing or inspection, disabling security barriers or access controls by propping open doors or leaving gates open for the convenience of performing operating procedures, damage to security features in the case that the operating procedures are performed incorrectly;
- Areas where operating procedures can address security aspects and improve overall efficiency, such as including functional checks of both safety and security equipment in periodic facility walk-downs.

As stated in Ref. [6], "the operator should develop and implement means and procedures for evaluations, including performance testing, and maintenance of the physical protection system." Similar to the discussion above, these means and procedures can be developed in consultation with safety experts to identify and appropriately address interface issues, including:

- Operational radiation protection considerations for security patrols or personnel performing in-service inspections and maintenance of security equipment;

- Harmonizing or combining maintenance procedures for equipment or structures that have both security and safety functions;
- The potential for security procedures to affect safety systems located in the vicinity of security equipment or areas with particular security sensitivity;
- Access controls included in security procedures.

4.5. PREPAREDNESS AND RESPONSE

Research reactor facilities generally have emergency plans to respond to and mitigate the consequences of a radiological accident [2 and 19]. The emergency plan is usually formulated in the context of a radiological release to the environment outside the reactor facility and/or off-site irrespective of the initiating event, i.e. resulting from an accident at the facility caused by equipment, procedural or human failure, by a natural event or a security event. An important part of the emergency plan is to hold regular exercises involving reactor operations staff, on-site emergency response teams, radiation protection groups and, at greater intervals, the regulator, off-site response teams, the police and civil support groups. In these exercises the focus is usually on evacuating people (site personnel and off-site members of the public) away from the danger areas identified in a simulation of a radiological release scenario. The simulated initiating events and on-site and off-site responses seldom include security events addressing criminal or malicious acts at the research reactor site, or the on and off-site neutralization and apprehension of adversaries.

The preparedness and response plan for security events is called a contingency plan [6, 20]. It generally requires more input from the State in establishing it at a research reactor facility and the involvement of a greater number of entities within the country in its execution, from special task forces of the police to local government to the military forces, if necessary. The contingency plan has to cover not only site security measures to respond to malicious acts but also effective measures to regain control over the site during and after the event, to neutralize the adversary(ies) and to recover stolen materials. It also has to allow for the parallel and complementary execution of the radiological emergency plan to recover from an associated radiological release. However, its priorities are usually the converse of the radiological emergency plan. The first action is to reverse the situation and neutralize the adversaries and then to consider potential safety problems arising from the security event. If possible, due to the severity of consequences and delays in neutralization of the adversary, these two activities (neutralization and mitigation) will occur concurrently, with response forces providing protection to emergency equipment and personnel. Consequently, the radiological emergency plan and contingency plan have to be coordinated to address security support for the members of the radiological emergency team.

The emergency and contingency plans therefore need to be developed in an integrated and coherent manner and, while they mostly remain separate plans, their similarities, differences and especially their interface, need to be clearly understood by the affected response personnel of the research reactor facility, the radiation protection groups, security personnel and external organizations involved in the response. Some common aspects of emergency and contingency planning that need to be interfaced include:

- Role and responsibilities of the support agencies;
- Number and type of responders and response time;
- Communication means, procedures and compatibility;
- On- and off-site response operations, chain of command and first response (safety or security);

- Familiarity with facility layout, targets and hazards;
- Joint training exercises and incorporating lesson learned in the plans.

In developing emergency and contingency plans, consideration has to be given to possible interactions between each plan and the other type of event. For example, an emergency event, such as a fire alarm or health crisis, could be used by an adversary as a ruse to initiate or distract from a security event. As such, the emergency plan has to be developed in consultation with a security specialist to ensure that security measures are maintained while addressing the emergency situation.

4.6. TRAINING OF PERSONNEL

To effectively manage the interface between safety and security, research reactor management needs to ensure that sufficient human resources are available and fully trained and qualified to perform their responsibilities for safety and security. The training and awareness programmes for safety personnel and security personnel need to be repeated at regular intervals and in response to emergent issues, to provide updates on revisions to the security plan, safety assessment and facility changes, and a review of lessons learned. Appropriate education and training is also needed across the wider spectrum of research reactor personnel on safety and security interface issues and to promote and coordinate safety culture and security culture as discussed in Subsection 4.2.2.

Complementary training of safety and security personnel and their mutual participation in exercises of both types can also help to effectively manage the interface between safety and security. In particular, personnel with responsibilities and expertise in safety analysis and safety assessment need to be provided with a working knowledge of the security requirements of the facility and security experts need to be provided with a working knowledge of the safety considerations of the facility, so that contradictory requirements between safety and security can be resolved most effectively.

4.7. ASSESSMENT OF THE INTERFACE BETWEEN SAFETY AND SECURITY

4.7.1. Periodic safety and security reviews

Periodic safety or security reviews and assessment of the results by the regulatory body or other competent authorities are required and/or recommended by the IAEA publications [2, 3 and 5]. As required by the IAEA safety standards, the operating organization has to perform a systematic periodic review to confirm that the safety analysis report and other selected documents (such as the documentation for operational limits and conditions, maintenance and training) for the installation remain valid or, if necessary, are improved [2]. Similarly, INFCIRC/225/Revision 5 states, “the operator should review the security plan regularly to ensure it remains up to date with the current operating conditions and the physical protection system” [6]. However, such reviews are likely to focus on either the one or the other discipline at a time without addressing the interface between safety and security.

The operating organization has to establish an internal process within the integrated management system (see Subsection 4.2.1) to specifically review the effectiveness of the management of the interface between the two disciplines and to determine that they do not adversely affect each other and that, to the degree possible, they are mutually supportive. The results of both periodic safety reviews and periodic security reviews have to be considered in this process, including any identified safety enhancements and security improvements. These

are of particular importance because they typically involve modifications to the physical facility and to its administrative controls and procedures. Subsection 5.5 of this document covers interface issues to consider when performing modifications.

4.7.2. Self-Assessment, continuous improvement and feedback from operating experience

An explicit requirement in the implementation of an integrated management system at a research reactor is a process of periodic self-assessment, in which every aspect of the management system is reviewed by the reactor management in order to assess its performance against predetermined goals and objectives, and to implement actions to make corrections to underperformance in any area revealed by the self-assessment [2]. Other reviews by independent experts to determine the extent to which the requirements for the integrated management system are fulfilled, to evaluate the effectiveness of the system and to identify opportunities for improvement are also recommended in the IAEA publications. The management of the interface between safety and security, as an important area of responsibility within the integrated management system, would fall into the scope of such periodic self-assessments and be subject to the process of continuous improvement along with the rest of the management system.

Weaknesses in the management of the interface need to be identified and corrected using, as the main inputs, feedback from operational experience gained in the field, relevant information from incident reports and audit/review reports, lessons learned from joint exercises which simultaneously test emergency and contingency plans and actions, and the combined expertise from safety and security experts.

5. MANAGEMENT OF THE INTERFACE BETWEEN SAFETY AND SECURITY DURING ALL PHASES OF RESEARCH REACTOR LIFETIME

5.1. SITING

Selection of a research reactor site needs to be based on both safety and security criteria. Requirements on the safety and security aspects of site selection and evaluation for nuclear installations, including research reactors, are established by Refs [21] and [6] respectively. For a new research reactor facility, the site selection takes both the safety and the security of the facility into account, ensuring that the site location, topography, geology, meteorology, demography, land use considerations/planning, infrastructure, etc., do not present any obstacles to either of these disciplines or to the management of their interface with each other.

The foreseeable evolution of factors in the region that may have a bearing on safety and/or security need to be evaluated for a time period that encompasses the projected lifetime of the research reactor facility. Safety considerations include changing population distribution, industrialization and commercialization of surrounding areas [22]. Considerations for security include the location and layout of the facility within the site in a way that on-site features (distance from the site boundaries, topographic obstructions, etc.) can be used to advantage in securing the site against potential adversaries. Site characteristics that may benefit adversaries also need to be carefully considered, such as its proximity to public transport infrastructure (roads, railways and airports) or to industry and populated areas. Other factors might include consideration of whether some areas within a country are more prone to malicious activities (of either domestic or international origin) or unrest than others or whether a given site is near the border with an unfriendly country.

5.2. DESIGN

While the design phase of a research reactor is usually taken as that phase in which the facility is conceptualized and designed prior to being built, the design process continues to play a dominant role in all subsequent phases of its lifetime due to the changing research mission and utilization activities of the facility (see, for example, Subsection 5.5 on utilization and modification). Safety measures, security measures and arrangements for the State system of accounting and control of nuclear material for a research reactor need to be designed and implemented in a coordinated manner so that they do not compromise one another. In addition, the operating organization has the responsibility to:

- Design, implement and maintain adequate organizational, technical and administrative measures to achieve the regulatory requirements related to safety and security and to facilitate the management of the interface between them;
- Maintain coordination throughout the lifetime of the facility with State organizations that are involved in safety and security to ensure that the design (including subsequent modifications) adequately addresses these disciplines and their interface;
- Ensure availability of a sufficient number of adequately trained personnel in the design team with knowledge and skills to manage the interfaces between safety and security;
- Ensure that management of the interface between safety and security is included in the integrated management system;
- Be aware that safety design can provide security advantages and security design can provide safety advantages;
- Take into account lessons learned from safety and security events, both at the research reactor itself and at other similar facilities.

Furthermore, a change management process needs to be established early in the design phase, which will be propagated throughout all phases in the lifetime of the facility, to ensure that any proposed changes in the design of the facility, including the introduction of new experimental facilities/devices or changes to procedures, are evaluated to verify that they take account of the requirements of both safety and security and properly manage the interface between them. Subsection 5.5 and Appendix III provide further information and direction on managing this interface during design.

5.3. CONSTRUCTION

Both safety and security considerations are crucially important during the construction phase of a research reactor: safety because it is during construction that structures, systems and components important to safety are assembled with or without latent defects; and security because it is during construction that the as-built robustness of physical structures is determined, the physical layout and location of what will become sensitive areas within the facility are clearly visible and measures need to be instituted to ensure defects are not introduced maliciously to structures, systems and components important to safety and security. It is therefore important to ensure that contractors engaged in the construction work are properly assessed for their integrity and competency in adhering strictly to design and quality requirements to ensure the future safety of the facility as well as for their trustworthiness to ensure its future security. Obtaining assurances in one respect does not necessarily imply assurance in the other, hence there is a need to carefully examine and manage the safety and security aspects in an integrated manner in the process of determining the trustworthiness of contractors.

Careful oversight has to be exercised during all aspects of the construction of the facility to ensure that it is constructed as designed, thereby serving both safety and security. This scrutiny needs to focus on preventing the inadvertent or intentional introduction of weaknesses that could result in a radiological release during operation or security vulnerabilities. Such oversight can present a major challenge because of the large number and diversity of workers entering the site during the construction period. Therefore, it has to form part of the framework of the integrated management system implemented by the operating organization on the construction site and give special attention to the interface between safety and security measures and requirements important to the future operation of the reactor.

During construction work associated with major modifications at an existing, operating facility, both safety and security measures need to be implemented that focus on the number and diversity of workers and personnel other than facility staff that may be working in the vicinity of the research reactor, in order to:

- Protect the construction workers from exposure to radiation or radioactive contamination originating from:
  - Normal operation of the facility or from storage of radioactive materials;
  - Abnormal operation, incidents or accidents at the operating facility;
  - Modification work being undertaken (e.g. the removal of radioactive components).
- Prevent inadvertent or intentional introduction of weaknesses, devices, access pathways and other opportunities for sabotage or theft.

The measures implemented have to be evaluated by experts in safety, radiation protection and security to ensure that all aspects of safety and security are addressed consistently with

regulatory and integrated management system requirements. Construction workers have to receive adequate training/instruction on the safety and security aspects of the facility. Where required, the workers have to participate in emergency/contingency exercises, in particular where the construction work is likely to be extended.

5.4. OPERATION

The operating phase in the lifetime of a research reactor is usually the longest phase of all, and therefore the longest period in which the safety–security interface needs to be managed to meet a particular arrangement of requirements. This phase would have been the focus of attention in the design of the facility and in the development of the operating and utilization programmes. It is also the phase during which the safety and security risks are the greatest, due to the presence in the facility of:

- Fresh and irradiated reactor fuel, that need to be adequately handled from the safety and security points of view to prevent inadvertent criticality or unauthorized access;
- Inventories of many diverse radioactive materials, structures and components;
- Numerous operational experiments each posing its own set of radiological hazards and security challenges;
- Maintenance activities that could purposely or accidentally disable the item being repaired, or other associated safety or security equipment;
- Operating and supporting personnel (e.g. researchers, security personnel, students and contractors) in areas that have structures, systems and components important to safety or are sensitive from a security standpoint.

The operating organization has to ensure control of, and be able to account for, all nuclear material and radioactive sources at the facility at all times. The operating organization has to report any nuclear material accounting discrepancy or radioactive material missing or unaccounted for in a timely manner as stipulated by the competent authority.

The operating organization has to periodically review the safety analysis and security plan for the facility as part of the maintenance of its operating licence consistent with the established integrated management system, and demonstrate to the regulatory body (or bodies) that implementation of safety and security at the facility is done in an coordinated manner to minimize the risk of both radiological releases and material theft. The safety analysis has to be based on the design basis accident. The security plan has to be based on the security requirements to address the design basis threat or threat assessment.

5.5. UTILIZATION AND MODIFICATION

Changes and modifications are normal activities of the operating phase of a research reactor. Typical changes or modifications to the facility can be driven by the need to meet changing operational requirements, innovations in the experimental or utilization programmes, evolving regulatory requirements and standards, addressing lessons learned from operating experience, upgrading the facility or addressing the effects of ageing. Effective management of change requires coordination and communication between management and staff responsible for facility safety and security, and has to be addressed by the integrated management system.

A change at a research reactor can be planned or emergent and may be permanent or temporary, but regardless of the nature of the change, a thorough assessment of the change is necessary. These changes can include but are not limited to a modification to, addition to or

removal from the facility or a procedure that affects a design function, a method of performing or controlling a function, or a test that is meant to demonstrate that the intended function will be accomplished. A change or modification has to neither compromise the design operational limits and conditions of the reactor nor the effectiveness of the security plan. Appendix III provides further information and direction on managing this interface during the design and implementation of changes to the facility.

5.6. DECOMMISSIONING

When a research reactor is permanently shut down and enters a decommissioning phase, the safety considerations change quite extensively, as the core is inevitably de-fuelled. However, there remain many significant safety considerations associated with decommissioning, such as:

- Intermediate to long-term storage of spent fuel in the reactor facility or its vicinity, with the associated ongoing maintenance of sub-criticality and maintenance of water quality and cooling, as appropriate;
- Maintenance of building ventilation systems and other services (e.g. overhead cranes) during dismantling activities;
- Maintenance of radiation protection at an adequate level, including maintenance of radiation protection equipment;
- Implementation of a comprehensive decontamination plan;
- Dismantling activities involving the handling of radioactive components and materials;
- Conventional safety considerations that can affect nuclear or radiation safety that are very different from those during the operational phase of the facility (e.g. deconstruction and disassembly activities, non-routine use of heavy machinery and lifting devices, fire hazards, use of solvents, etc.).

As long as the fuel inventory (fresh and spent) is still present in the facility, the security measures related to protecting nuclear material and the facility against theft and sabotage need to be maintained. Security measures related to radioactive material may need to be adapted (applying the graded approach) as the dismantling activities lead to an increased risk of inadvertent or intentional uncontrolled removal of radioactive materials from the site.

Hence the interface between safety and security has to continue to be adequately addressed and managed by the operating organization. Furthermore, both the emergency and the contingency plans need to be revised and updated to address the safety and security requirements of the decommissioning phase. The training, sensitising and exercising of the personnel involved in interfacing and executing these plans needs to continue.

5.7. EXTENDED SHUTDOWN

Many research reactors are shut down for extended periods for various reasons, such as for a major safety reassessment, refurbishment or upgrading, for preparing for decommissioning, or simply due to lack of a utilization programme or because there are no adequate funds to either operate or decommission them. While an extended shutdown may be planned, more often it will not have been anticipated and the research reactor is usually seen as still being in the operating phase of its lifetime, despite it being in a shutdown state. Whatever the reason, the conditions that characterize the extended shutdown state need to be examined for any features that affect safety, security or their interface, and that may require measures that differ from those applicable to the operational or the decommissioning phases.

During an extended shutdown, the number of personnel inside the facility may have been reduced to those needed only for maintaining the conditions of the nuclear fuel, the coolant or the moderator, for the inspection, periodic testing and maintenance of the relevant structures, systems and components of the facility, and for providing security. Furthermore, a part or all of the fuel elements may have been unloaded from the core and stored in the reactor pool or in the spent fuel storage pool to minimize the risk of inadvertent criticality in the reactor core. However, this may require implementation of additional security measures depending on the accessibility of the storage facility designs and locations and whether or not these locations were already appropriately protected.

These safety and austerity provisions might increase the vulnerability of the facility from the security point of view, both because there is reduced staff in attendance and because the fuel may be more accessible out of the core and could, over a long period of time, become more attractive to theft due to its decreased radioactivity. The fuel has to therefore be re-examined from time to time to determine whether its categorisation has changed because it is no longer deemed to be sufficiently radioactive for security purposes.

Such a situation needs to be addressed by the operating organization as a priority, in coordination with safety and security specialists, to ensure that adequate attention is given to both safety and security, and that the interface between safety and security is properly managed. This coordination has to also ensure that the emergency and contingency plans, and their associated response procedures and actions, are updated and made consistent with the conditions of the extended shutdown.

APPENDIX I: GOOD PRACTICES FOR A COORDINATED APPROACH TO SAFETY AND SECURITY OF RESEARCH REACTORS

In setting up the framework for managing the interface between safety and security at a research reactor, the following examples of good practices have been found to be useful:

- Promotion of a strong safety culture and a strong security culture is essential at all levels of the organization. Safety culture and security culture are not merged into one culture, but each is established and maintained in a complementary manner with the other so that potential contradictions are minimized.
- Promotion, by the facility management, of both a safety and a security culture in a balanced manner, ensuring that both safety and security objectives receive appropriate attention and mutually enhance each other.
- Implementation of regular reviews and, as necessary, updating of the security plan and safety documentation.
- Implementation of an integrated management system with clear provisions to manage the interface between safety and security.
- Assignment of a safety specialist and a security specialist with well-defined roles and responsibilities, including the participation of the security specialist in the reactor safety committee meetings. The safety specialist has to be trained in the philosophy of the security design and measures and the security specialist has to be trained in the philosophy of the safety design.
- Regular review of the safety and the security arrangements at the facility to identify any degradation in either area to address issues related to their interface, and to implement the appropriate corrective actions.
- Organization of regular induction training sessions for the operating personnel on safety and security as well as on their interface.
- Organization of introductory training and familiarization for the off-site response team (e.g. fire brigade, police, military etc.).
- Organization of internal inspections/audits in the facility that specifically address the interface between safety and security.
- Organization and conduct of regular (suggested annual) exercises that specifically test the interface between safety and security, and the effective implementation of the lessons learned from them.
- Cooperation between safety and security specialists in the evaluation of the consequences of malicious acts that could be initiated by an adversary with capabilities as described in the State's threat assessment, and to identify the minimum set of structures, systems and components that need to be protected and the corresponding vital areas within which this minimum set is located, or other enhanced protection arrangements.
- Access and operations by emergency/contingency teams (e.g. firefighting, law enforcement) have to not be impeded unnecessarily for safety reasons, but access to certain areas of the facility has to be limited or continuously monitored (e.g. intense radiation sources storage room).
- Security measures have to take into account the safety requirements such as accessibility to equipment for the purpose of normal operation, in-service monitoring and maintenance.
- Measures have to be in place to assure that a safety event is not fabricated as a ruse or diversion for a pending security incident.

- Physical barriers (or other delay systems) need to be able to accommodate, when necessary, a rapid evacuation of or access to site areas in the event of a security event or radiological accident.
- Some emergency access and egress measures need to be planned so that they do not introduce delays to incoming or evacuating personnel. This could include escorting emergency personnel and corralling evacuating persons into a safe, contained area.
- When managing the facility in degraded conditions (such as following an accident or external event), safety and security measures and their interface need to be reassessed in an integrated manner with account taken of the degraded conditions.
- Systematic consideration of which systems and components have to fail safe and which have to fail secure.
- Conduct of joint emergency exercises, which simultaneously test the implementation of emergency and contingency plans, have to be carried out at intervals compatible with the level of threat in order to assess and validate the adequacy of response coordination between emergency and security organizations involved in responding to various scenarios, and has to have a method for incorporating lessons learned to improve both plans.

APPENDIX II: AREAS SUBJECT TO POTENTIAL CONFLICTS BETWEEN SAFETY AND SECURITY AND STRATEGIES FOR SOLUTIONS

Potential conflicts between safety and security, consequences of such conflicts and strategies for addressing them in various areas of the interface between safety and security are presented in Table II.1.

Table II.1 AREAS SUBJECT TO POTENTIAL CONFLICTS BETWEEN SAFETY AND SECURITY AND STRATEGIES FOR ADDRESSING THESE CONFLICTS

Area	Potential conflicts	Consequences of conflicts	Strategy for addressing conflicts
Access Control	The necessity for rapid access and egress of personnel during emergencies can create vulnerability from the security point of view while the necessity for limited points of access and egress can increase the risk to personnel from a safety point of view.	A lack of balance between security provisions and safety can lead to delays in timely responses in emergency situations or can create vulnerability which could be exploited by adversaries.	Close cooperation between safety and security specialists for establishing access control procedures ensuring both safety and security objectives are met in accordance with regulatory requirements.
Information Management/ Management System	Obligation of transparency of information related to safety matters to facilitate improvements in safety and to reassure the public, while information on site vulnerabilities, safety analysis and sabotage targets as well as security matters needs to be controlled.	Sharing safety or security information that identifies a vulnerability (e.g. locates a sensitive target within the facility or highlights a weakness in the safety features) could potentially be exploited for malicious purposes. Insufficient information may decrease public confidence in the safety of the facility.	Effective and coordinated involvement of safety and security specialists in the establishment of the integrated management system which takes into account the specific aspects related to the management of information in each discipline. This includes a systematic process for determining whether certain safety-related information, including that contained in research publications, needs to be controlled as sensitive information in accordance with the State's classification policy [23]. Strong safety and security cultures are promoted through training of reactor staff on both types of information.

Area	Potential conflicts	Consequences of conflicts	Strategy for addressing conflicts
Siting	Research reactor site selection includes assessment of safety risks related to external natural and human induced events, assessment of security vulnerability from the local threat environment and natural features of the site and surroundings and considering the needs of the research mission and utilization activities. Conflicts may arise if both safety and security aspects are not considered systematically in the site evaluation and site selection process. For example, an area which might be beneficial to safety may be more vulnerable to malicious activities or unrest.	Proximity of the facility site to populated areas may increase the potential radiological consequences of accidents or security events at the facility.	Site evaluation and selection need to be facilitated by experts from both safety and security disciplines. Siting considerations solely having to do with convenience of the utilization programme need to be balanced with the risks posed by both safety and security issues. Areas which are vulnerable to civil unrest need to be excluded from consideration in the research reactor siting process.
Maintenance	The condition and configuration of the facility equipment could be modified when performing maintenance activities (e.g. cut of electrical power supply on some safety systems, opening of barriers and doors).	Configuration changes during maintenance activities could introduce vulnerability from the security point of view, which might be increased if the maintenance activities are performed by outside contractors. Conversely, maintenance on the security system may render some pathways inaccessible and obstruct operator mobility around the facility, with potential safety implications.	Coordination between the safety and security specialists concerning the temporary changes planned during maintenance activities as well as the associated compensatory measures.

Area	Potential conflicts	Consequences of conflicts	Strategy for addressing conflicts
Modifications	Modifications performed on SSCs may negatively affect security equipment and vice versa. For example, malfunction of safety equipment may damage nearby security equipment. In the same manner the installation of security equipment at the top of the reactor pool presents the risk of it falling into the pool and damaging the reactor core or fuel elements.	Degradation or loss of safety systems or security equipment may result in radiological exposure of operating personnel, releases of radioactive material to the environment or increased vulnerability to a malicious act.	Changes to the facility or its documentation need to be assessed and endorsed from the safety and security perspective before approval and implementation. For example, where these changes are examined by safety experts normally represented in the reactor safety committee, it is important that this committee also includes a security specialist in order to ensure that security concerns are taken into account.
Emergency Preparedness	Security personnel at the facility may not be available to perform certain tasks during an emergency response to a safety event (e.g. unlocking doors, escorting emergency responders, etc.) if they are simultaneously responding to it as a security event.	The emergency response could be delayed or made ineffective if it relies on actions by security personnel that are not available to perform these functions.	Emergency plans and contingency plans need to be developed in a coordinated manner, considering all of the responsibilities of the reactor personnel and security forces, to ensure that in the event of a simultaneous response of both groups to an event, all critical functions can be performed in a timely manner.
	Security forces may also respond to emergencies of unknown origin (e.g. malicious act or equipment failure) that have some characteristics of a potential security event (such as a fire or explosion) and their response may conflict with the emergency response.	If security forces and emergency responders are simultaneously responding to an event of unknown origin, an uncoordinated approach could delay the proper response of emergency personnel or put emergency responders in danger of attack from adversaries.	Emergency response plans need to consider the possible security initiators and their implications on emergency situations and be coordinated with the security response. Strategies for rapidly determining the origin of events and deploying appropriate first responders (safety personnel, security forces or a combination of both) need to be developed including the roles and actions of security forces and emergency personnel. These situations need to be jointly exercised and lessons learned used to improve the response.

Area	Potential conflicts	Consequences of conflicts	Strategy for addressing conflicts
Contingency Preparedness	Reactor personnel may become involved in the response to a security event. The training programmes and scenarios for responding to an event, including detailed information about security measures and vulnerabilities, is sensitive and needs to be controlled.	Lack of complete awareness and training of reactor staff involved in security response may lead to interferences in the scenarios during exercises, or for an actual event.	A number of persons from the management of the operating organization (e.g. reactor manager and reactor personnel who have been verified as trustworthy) need to be adequately informed and trained in regard to contingency preparedness and security response.
	Security forces may not receive adequate training on the safety aspects of the research reactor facility.	Lack of complete training and awareness of the security forces on the safety aspects of the facility may lead to security forces being unnecessarily exposed to radiation hazards or security forces unintentionally causing a nuclear or radiological emergency by damaging safety-related SSCs during the security response.	Security forces need to receive periodic training, including facility walkthroughs, on the safety aspects of the research reactor facility.
Long Shutdown Periods	Safety requires partial or full unload of fuel from the core. This may increase the vulnerability of the facility from the security point of view.	Vulnerability increases due to change of access control rules and the number of operating personnel present in comparison with the operation periods of the reactor.	Involvement of security specialists in planning for ensuring adequate surveillance and periodic testing and maintenance of the security equipment.

APPENDIX III: CONSIDERATIONS IN THE MANAGEMENT OF CHANGES AND MODIFICATIONS

The major portion of a research reactor's lifetime is spent in the operational phase, which is often punctuated by a continual process of redesign, modification, upgrading, refurbishment, new experimental facilities and changes in the operational focus of the facility. Management controls and processes are necessary to establish and maintain effective coordination between safety and security during this phase. The management of the interface between safety and security during this phase can be challenging, especially when a change needs to be accomplished effectively "on-the-run" (i.e. with minimal interruption of operations). Therefore, this Appendix provides information specifically focused on the control of changes during the operational phase, to supplement that already given in Subsections 5.2, 5.4 and 5.5.

One of the objectives of management controls and processes for change is to ensure that proposed changes, and the activities to implement them, will not adversely affect compliance with safety or security requirements, or reduce the relevance of safety analyses, operational limits and conditions or the facility's approved security plan credited for protection against theft and sabotage. Personnel holding the responsibility for facility safety and security have to be aware of all planned changes, including the potential for unforeseen consequences of the changes, to the facility and the site characteristics. Additionally, those personnel need to review each proposed change or activity in advance for potential adverse impacts on facility safety and security.

It is essential that personnel conducting these reviews collectively possess a complete understanding, as appropriate to the review being conducted, of:

- The physical layout of the facility;
- The layout of security layers in the facility surrounding security targets, including access controlled points;
- The configuration and purpose of structures, systems, and components important to safety and systems and equipment important to security at the facility;
- Integrated management system requirements and quality procedures;
- Facility operating procedures;
- Security plan and procedures;
- The operating programme of the facility;
- The safety analyses and the operational limits and conditions;
- Facility licence conditions and licensing process;
- Emergency and contingency plans and preparedness;
- Programmes for radiation protection and waste management;
- Engineering;
- Maintenance;
- Work management (control and planning);
- Training and qualification of personnel;
- Fire protection;
- Environmental protection;
- Conventional health and safety (includes chemical safety).

The following list gives examples of modifications that could potentially result in an adverse impact on either facility safety or security if not adequately reviewed or properly managed.

The listing is not all-inclusive, but provides some pointers to the types of activities that can result in interface issues:

- Modifications that could cause a loss of power to systems relied upon for safety or security;
- Modifications resulting in the installation or removal of a barrier that could adversely impact safety, security, or emergency/contingency response;
- Modifications involving the placement of heavy equipment, industrial materials or temporary structures that could:
  - Obstruct detection, assessment or response functions;
  - Aid or otherwise provide advantage to an adversary in the completion of a malicious act;
  - Increase the response times of security personnel or other emergency responders;
  - Prevent operator access to equipment important to facility safety or prevent timely completion of manual operator actions credited in safety analyses;
  - Prevent access of mobile emergency equipment (e.g. fire truck or ambulance).
- Modifications involving the installation of a chemical or hazardous material plant or storage facilities adjacent to or intersecting with:
  - A security central alarm station or other security post;
  - A protected security response position;
  - A security or emergency response pathway;
  - Facility equipment important to safety;
  - Facility equipment important to security.
- Construction activities associated with a modification that remove or degrade physical barriers, thus allowing established access controls to be bypassed;
- Modifications involving addition to, removal from or relocation of theft or sabotage targets (nuclear/ radioactive materials or equipment relied on for safety).

To facilitate an efficient and adequately detailed safety–security change control process, the management of a research reactor facility needs to establish a change management process to evaluate and approve all significant changes. Methodologies establishing such processes typically use predetermined questions that are specifically designed to identify potential conflicts. The following are examples of safety and security questions that may be used in such a programme for the screening of planned and emergent changes.

Security-focused questions

- Could the proposed change or activity decrease the reliability or availability of a security system to perform its intended functions?
- Could the proposed change or activity increase the likelihood of malfunctions or failure of security equipment or systems?
- Could the proposed change or activity decrease the effectiveness of security plans or invalidate the site protective strategy (e.g. communications, response timelines and pathways, equipment and systems, or protected response positions)?
- Could the proposed change or activity interfere with detection (i.e. interior and exterior sensors, zone of detection and field of view, alarm communications, or access control systems) and assessment functions?
- Could the proposed change or activity increase the response times of security personnel? (e.g. manmade or natural vehicle barriers, vehicle access control and channelling barriers).

- Could the proposed change or activity decrease delay times for adversaries (e.g. manmade or natural vehicle barriers, vehicle access control and channelling barriers, access delay systems, exterior or interior delay barriers?
- Could the proposed change or activity increase the numbers of, change the configurations of, or create a new theft or sabotage target from those previously evaluated?
- Could the proposed change or activity result in/lead to noncompliance with regulatory authority security requirements?

If the answer to any of the security screening questions is "yes" for a planned change, the research reactor management needs to devise appropriate changes to existing security measures, draft an amendment to its security plan and obtain the approval of the regulatory body to the amendment prior to the change taking place In the event of any unexpected (or emergent) change which results in the security system being incapable of providing the required level of protection (as contained in the approved security plan), the facility manager will have to immediately implement compensatory measures to provide adequate protection. The facility manager then needs to plan and implement, within an agreed period, corrective actions to be reviewed and approved by the regulatory body.

Under change management procedures, one designated manager in the facility approves each change and the change needs to be endorsed by those individuals whose area of responsibility is most affected. Hence, even if the answer to any of the security screening questions is "no" for a planned change, this decision by the designated manager still needs to be formally endorsed by the designated safety or security manager and the evidence and decision documented as part of the change control procedures

Safety-focused questions

- Could the proposed change result in an increase in the frequency of occurrence of an accident previously evaluated in the facility safety analysis?
- Could the proposed change result in an increase in the likelihood of occurrence of a malfunction or failure of a structure, system, or component important to safety previously evaluated in the facility safety analysis?
- Could the proposed change result in an increase in the consequences of an accident previously evaluated in the facility safety analysis?
- Could the proposed change result in an increase in the consequences of a malfunction of a structure, system or component important to safety previously evaluated in the facility safety analysis?
- Could the proposed change create a possibility for an accident of a different type than from any previously evaluated in the facility safety analysis?
- Could the proposed change create a possibility for a malfunction of a structure, system or component important to safety with a different result than from any previously evaluated in the facility safety analysis?
- Could the proposed change result in a design basis limit for a fission product barrier being exceeded or altered (e.g. changes to security measures aimed at preventing sabotage to the fuel cladding, reactor tank, pressure vessel, or confinement or containment structures)?
- Could the proposed change result in a departure from the method of evaluation used in establishing the design bases or in the facility safety analyses?
- Could the proposed change increase the risk of exposure to staff?
- Could the proposed change or activity obstruct the mobility of operations or emergency response personnel to carry out actions for which credit is given in the safety assessment?

If the answer to any of the safety screening questions is “yes” for a planned change, the research reactor management has to communicate with the regulatory authority concerning the need for regulatory review and approval prior to making the change. Emergent conditions may require an immediate change to the research reactor facility in the form of compensatory or mitigating actions or both in order to restore an adequate level safety or security. If such actions are required, facility management has to communicate the needed action to appropriate personnel including the regulatory authority.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, IAEA, Vienna (2007).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. SSR-3, IAEA, Vienna (in preparation).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13 (INFCIRC/225 Revision 5), IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna, (2012).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, 2011.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Research Reactors and Preparation of the Safety Analysis Report, IAEA Safety Standards Series No. SSG-20, IAEA, Vienna (2012).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Analysis for Research Reactors, IAEA Safety Reports Series No. 55, IAEA, Vienna (2008).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Governmental, Legal and Regulatory Framework for Safety, IAEA Safety Standards Series No. GSR Part 1 (Rev 1), IAEA, Vienna (2010).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2015).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2009).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors, IAEA Safety Standards Series No. NS-G-4.6, IAEA, Vienna (2008).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Research Reactors, IAEA Safety Standards Series No. NS-G-4.4, IAEA, Vienna (2008).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, The Interface between Safety and Security at Nuclear Power Plants, INSAG-24, IAEA, Vienna (2010).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (2015).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Survey and Site Selection for Nuclear Installations, IAEA Safety Standards Series No. SSG-35, IAEA, Vienna (2015).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

ANNEX I: CASE STUDIES IN MANAGEMENT OF THE SAFETY–SECURITY INTERFACE DURING CHANGES TO SECURITY AND SAFETY

This Annex presents two case studies, one on a security change affecting safety and the other on a safety change affecting security, at a typical research reactor facility. The case studies demonstrate the application of the safety and security questions listed in Appendix III to evaluate any unacceptable impact that the change in one of the disciplines may have on the functions of the other.

I-1. CASE STUDY 1 – A CHANGE TO SECURITY

I-1.1. Initial conditions

The security manager at a small university research reactor has proposed a modification to add a security fence around a portion of the exterior of a multi-purpose building housing the reactor, several classrooms, a utility room and faculty offices. In addition to the fence, several interior security doors will be required to segregate the reactor and the utility room from the classrooms and offices. The need to enhance the security barriers is in response to plans to increase the maximum licensed reactor power from 500 kW to 3 MW. Specific performance criteria have to be met in order for the exterior fence to meet the requirements of a security barrier. One requirement is that the fence posts have to be at least 2.3 meters underground and set in concrete. Furthermore, the increased safety requirements that become necessary to licence the reactor for operation at 3 MW will increase the importance of the electrical power and water supplies. The building services (electrical power, water and heating steam) enter the building underground through the utility room. Therefore, the utility room needs also to be provided with additional physical protection.

I-1.2. Change review

Given the information related to the proposed change to the facility security barriers, it would be necessary to review the security questions presented in Appendix III of this publication. However, since the information provided in this publication is specifically focused on the safety–security interface, further discussion will be limited to the review of the proposed activity against the safety questions in Appendix III.

The first question asks, “Could the proposed change result in an increase in the frequency of occurrence of an accident previously evaluated in the facility safety analysis?” The review of proposed change will require a level of understanding associated with the accidents evaluated in the facility safety analysis and their assumed frequency. This expertise is typically held by operations and engineering personnel. Communication with personnel in one or more of these areas is essential to adequately complete the necessary review.

The second question asks, “Could the proposed change result in an increase in the likelihood of occurrence of a malfunction or failure of a structure, system, or component important to safety previously evaluated in the facility safety analysis?” Once again, the review of proposed change will require a level of understanding of the safety functions associated with facility’s structures systems and components that have been identified as important to safety. This expertise is also typically held by operations and engineering personnel. Evaluation by personnel in these areas is essential to adequately complete the necessary review.

The third question asks, “Could the proposed change result in an increase in the consequences of an accident previously evaluated in the facility safety analysis?” This question is very similar to the first question, except that it focusses on the consequences of an accident rather than its frequency. Communication with personnel in one or more of these areas would be necessary to adequately complete the review.

Each of the subsequent questions is approached in a similar manner. The technical attributes addressed by each of the safety questions need to be identified and evaluated to demonstrate that the minimum regulatory requirements for safety have been maintained, given the scope of the proposed change to security. The technical attribute also identifies the appropriate expertise necessary for the review of the change. If the evaluation of the technical attributes presented in any safety question is “yes” then it can no longer be assumed that the minimum level of safety would be maintained. In that case, a revision to the proposed security change needs to be considered or additional or modified safety features may be necessary. If the conclusion of all the question evaluations is “no,” then the proposed security change would likely not result in the reduction safety below the minimum regulatory requirements.

An effective interface between safety and security would also include a broad review of the safety question evaluation results by research reactor staff with expertise in the all of the programme areas in an attempt to identify any adverse consequences early. The details of the proposed modification and the results of the evaluation would be reviewed and approved in accordance with facility’s change management procedures, e.g. through a reactor safety committee which includes sufficient members (or advisors) knowledgeable in both safety and security to advise the reactor manager on all implications of the modification.

I-2. CASE STUDY 2 – A CHANGE TO SAFETY

I-2.1. Initial conditions

A modification to a 20 MW research reactor has been proposed by the operations manager which would include a chemical storage tank and a chemical injection system for adding corrosion inhibiting chemicals to a cooling tower. The cooling tower’s safety function is to provide a heat sink for decay heat removal following operational transients and under accident conditions. The cooling tower is experiencing accelerated corrosion that could soon render the cooling tower inoperable if not corrected. The placement of the chemical storage tank is within the protected area, in an area with easy access for the chemical delivery vehicle. The placement of the tank will obstruct the view of the research reactor security personnel and may interfere with the detection of unauthorized personnel in the protected area. Additionally, the delivery vehicle will further obstruct observation of the outermost security physical barrier when making routine deliveries, which occur once a week and require about one hour.

I-2.2. Change review

Given the information related to the proposed change to enhance the reliability and availability of equipment important to safety it would be necessary to review both the safety and security questions presented in Appendix III of this publication. However, since the information presented in this publication is specifically focused on the interface between safety and security, further discussion will be limited to the review of the proposed activity against the security questions in Appendix III.

The first question asks, “Could the proposed change or activity decrease the reliability or availability of a security system to perform its intended functions?” Therefore, personnel with security expertise need to evaluate the impact of the proposed safety change on the reliability and the availability of security systems. If the evaluation of the technical attributes presented in the security question is “yes,” then it can no longer be assumed that acceptable security would be maintained. In that case, a revision to the proposed safety change needs to be considered, or modifications of the security measures made, to re-establish effective security. If the evaluation of all the questions results in the answer “no,” then the proposed safety change would likely be accommodated within the existing approved security plan.

ANNEX II: EXAMPLES OF EXPERIENCE IN THE MANAGEMENT OF SAFETY–SECURITY INTERFACE ISSUES AT RESEARCH REACTORS

This Annex provides a number of brief examples from research reactor facilities in Member States that have experienced contradictory requirements in the interface between safety and security which, in most cases, has been effectively resolved. The examples mostly represent actual experience and the solutions devised to deal with these contradictions. In some of the examples, the discussion of the issue and the solution does not reflect the specific experience of a particular facility, but a representative case derived from similar issues at a number of operating organizations and/or regulators, with their collective input applied to formulating an appropriate solution for managing the interface and resolving the contradiction. Due to the sensitive nature of the security aspects involved in these examples, they are presented in a generic manner to avoid identifying a specific security issue and solution with a specific facility.

Each example opens with background information on the situation encountered, describes the specific interface issue(s), discusses management of the interface and ends with comments and further elaboration (if any).

II-1. EXAMPLE 1: SAFETY DOORS VERSUS SECURITY DOORS

II-1.1. Background

During an internal assessment, a facility identified doors that were installed as original equipment to function as combined security and fire barriers that were now inconsistent with fire protection standards. Both their fire rating and their opening direction were not in accordance with present day fire protection standards. The installed doors still met specifications as security barriers.

II-1.2. Specific interface issue

At the time the security doors were installed, the present day fire safety standards did not exist. The doors could be upgraded to meet the new fire rating specifications, but if their opening direction was changed in accordance with the new fire protection standards, they would not meet the security requirements.

II-1.3. Management of the interface

Safety and security personnel identified the problem and met to resolve the issue. The proposed solution was to install a second set of doors to function as fire doors.

II-1.4. Comments

Changes in safety or security requirements or standards may lead to conflicts. Adequate interaction and consideration between safety and security staff can identify and resolve issues. A similar situation concerning the opening direction of confinement zone access doors has arisen at an older research reactor when strengthening the security of the confinement building.

II-2. IMPEDED ACCESS BY SECURITY RESPONSE PERSONNEL DURING A FIRE

II-2.1. Background

The operations personnel maintain access control to the battery backup room which contains safety-related equipment such as the vital electric bus and uninterruptible power supply (UPS) system. During a weekend, a fire started in the battery room. The operations personnel were unavailable, and the security personnel were needed to respond.

II-2.2. Specific interface issue

The on-site security personnel responding to the fire did not have access to the keys for the battery backup room and were not able to breach the fire protection door.

II-2.3. Management of the interface

A method to ensure access control (e.g. key securely located on campus) by an on-duty person during off-hours was determined.

II-2.4. Comment

Prior to requiring rooms to be locked, assessment of all the safety as well as the security risks needs to be conducted jointly by safety and security personnel.

II-3. IMPEDED FACILTIY ACCESS BY EMERGENCY RESPONSE PERSONNEL

II-3.1. Background

For security reasons, the entrance to the campus where a research reactor is located has installed a pop-up vehicle barrier (e.g. bollards). The key to operate the vehicle barrier is maintained by the security head of the campus.

II-3.2. Specific interface issue

During a weekend, when the security head of the campus was off duty, a fire started at the reactor and the emergency responders (and fire truck) could not access the reactor as the barrier was locked in the up position.

II-3.3. Management of the interface

A method to ensure access control (e.g. key securely located on campus) by an on-duty response person during off-hours was determined.

II-3.4. Comment

Prior to utilizing physical barriers impeding entrance to a reactor site, assessment of all the safety as well as the security risks needs to be conducted jointly by safety and security personnel.

II-4. FAIL-SAFE VERSUS FAIL-SECURE ACCESS CONTROL SYSTEMS

II-4.1. Background

The question of whether a security access control point needs to fail open or closed on loss of electrical power has arisen at numerous research reactor facilities while implementing security upgrades. In addition, the meaning of a security barrier failing open or closed is different for different situations. Some examples are:

- The barrier locks immovably in the closed position, blocking any passage through it;
- It locks closed in one direction only, allowing unhindered passage in the other direction (escape route);
- It locks, but allows mechanical key override in one or both directions under the supervision of security personnel. (The key could also be provided within a "break-glass" panel on the secure side of the barrier and out of sight from the exterior);
- It unlocks but stays closed using a mechanical closer, allowing manual opening;
- It unlocks and moves to the open position automatically (mechanical opener), allowing uncontrolled passage in both directions.

II-4.2. Specific interface issue

Given that the loss of electrical power might result simply from equipment failure, or more seriously from a significant accident scenario (safety event) or from a malicious act (security event), the solutions applied need to consider not only the security of the facility, but a variety of risks to the personnel inside the facility as well:

- Preventing people from being trapped in areas where there could be radioactive releases or other hazards due to an emergency or security event;
- Allowing rapid access for emergency response teams to assist with attending to and evacuation of injured personnel;
- Preventing unauthorized access by adversaries who, apart from any damage and theft they intend to perpetrate within the facility, could take hostages.

II-4.3. Management of the interface

In practice, the decision whether access control measures need to fail safe or fail secure is made on a case-by-case basis. Each access control point needs to be assessed from both the safety and the security viewpoints by experts in both disciplines. Generally, the apparently opposing requirements of the second and third bullet points in the previous paragraph are resolved by implementing successive barriers that allow a staged evacuation of personnel and/or access of emergency response teams in a way that ensures that there is always at least one access barrier in place. Consideration needs to be given to ensuring access by security forces to neutralize adversaries and regain control of the facility and preventing unauthorized access *control* by adversaries (i.e. manipulating fail-closed and fail-open designs for their own advantage) who could assume a defensive position in the facility.

II-4.4. Comment

The appropriate solution for each research reactor facility is unique to the circumstances of that facility and is determined by a large number of factors, and clearly no generic approach can be followed by all. The retention of all the required functionality during a loss of

electrical power has been accomplished at some facilities by the permanent presence of security personnel within the facility and applying the security-supervised mechanical key override option mentioned above. It is important that the approach followed and the measures implemented at any particular research reactor facility are made commensurate with both the safety and the security risks posed by the facility, (which includes applying the graded approach) and in consultation with persons knowledgeable about both the emergency plan and the contingency plan.

II-5. INFORMATION MANAGEMENT FOR LICENSING SUBMISSIONS

II-5.1. Background

Safety assessments and documents are generally treated as open information and shared with other research reactor facilities with similar safety considerations. Some States also require this transparency to extend to the public domain. Information which could compromise security needs to be designated as sensitive and its distribution limited (where appropriate, to people verified as trustworthy) on a need-to-know basis. Sometimes a licensing submission relates to a change or modification to the facility that has both safety and security implications.

II-5.2. Specific interface issue

Research reactor operators and regulators encounter difficulties with licence submissions that focus only on the safety aspects of a change or modification at the facility that leaves gaps in the information related to the impact on the associated security measures because it is sensitive. Furthermore, even those with a need-to-know sometimes have difficulty obtaining a "full picture" of the changes because the information is in separate documentation, generated by different groups who have not necessarily collaborated very well with one another on interfacing the presentation of their assessments.

The regulatory body cannot approve a safety submission if the full impact of the security measures on the safety functions is not analysed and justified in the licensing submission (or a supplement to it containing sensitive information).

II-5.3. Management of the interface

Firstly, it is important that designated individuals at the regulatory body are verified as trustworthy and cleared to work with sensitive information related to the facility's security system. This is especially important when the designated competent authorities for safety and security are different.

Secondly, the documentation that reveals the full safety and security impact of the change or modification on the associated risks needs to be reviewed by competent safety and security experts in the operating organization prior to submission to the regulator, to ensure that there are no gaps in the information. In particular, the documentation needs to pertinently address the interface between safety and security related to the change or modification. Given the likelihood that most safety experts responsible for generating the safety justification in the documentation at the operating organization, and those responsible for the safety review of the submission at the regulator, may not have a need to know the security details and considerations, there are a number of options regarding the disposition of the documentation:

- Separate documentation dealing with just the safety and security aspects of the change respectively, with a third document specifically addressing the interface issues, generated by safety and security experts;
- Separate safety and security documentation, but with the interface issues addressed in the security documentation;
- Combined documentation dealing with all the safety, security and interface aspects in a single, coherent presentation, into which material from a separate safety assessment is incorporated.

II-5.4. Comment

The latter option has the advantage that everything related to the change or modification is collected in a single reference for future use. In any event, it needs to be noted that certain safety documentation that might assist an adversary to sabotage a nuclear facility needs to be treated as sensitive information in its own right. A major challenge in addressing an issue that emerges in a reactor facility that has operated for many decades is reconstructing a coherent safety or security justification from fragmented or disjointed historical information on the facility design and operation, including safety and security considerations. In performing such reconstructions that involve security elements, whether or not they are part of a licensing submission, care needs to be given to assigning the task to personnel with a need to know and appropriately controlling sensitive information.

II-6. TWO PERSON RULE VERSUS OPTIMIZATION OF RADIATION PROTECTION

II-6.1. Background

As a means of defence against sabotage and insider threats (i.e. malicious acts being carried out by employees or other persons with authorised access to the facility), there is a tendency to adopt the two person rule when conducting operational tasks in particularly sensitive parts of a research reactor facility. This entails the procedural deployment of at least two authorized and knowledgeable persons to conduct the task, with the express intention of verifying that only authorized tasks are undertaken, in order to detect access or actions that are unauthorized, including theft or sabotage, that could result in radiation exposure or a radiological release to personnel, the public or the environment.

II-6.2. Specific interface issue

Given that many of the sensitive areas in a research reactor facility where the consequences of such an act could be serious are also designated as radiation or contamination zones, deployment of more personnel than is necessary to do the task could be in conflict with the principle of optimization of protection.

II-6.3. Management of the interface

There are various approaches applied to managing this contradiction, depending on the circumstances and application of the graded approach:

- Where a task can be conducted faster by two individuals than by one, the time limit for conducting the task is shorted accordingly, thereby decreasing the exposure of both individuals;

- Where the task cannot be done faster by two individuals, one individual could perform the work while the second individual observes from the lowest-risk vantage point available in the area;
- An assessment of the radiological risk to both individuals is balanced against the security risk of an act of theft or sabotage. Where the consequence of an act of theft or sabotage is sufficiently low, the four-eye principle is not applied (graded approach).

II-6.4. Comment

In most instances at a research reactor facility, tasks carried out by operations, maintenance or experimental personnel inside a radiological zone are required to be conducted under the supervision of a radiation protection officer equipped with the necessary monitoring instruments. With the appropriate briefing, his presence constitutes application of the four-eye principle, which presents a ready solution to this issue.

II-7. INSUFFICIENT MEASURES FOR INSIDER THREAT ON MODIFIED EQUIPMENT

II-7.1. Background

This example happened at a nuclear power plant, but its lesson can be relevant to modifications carried out at research reactor facilities as well. During a fire insurance inspection plant walk-through a header tank containing a large quantity of turbine lubricating oil was deemed to be a fire risk. In order to comply with the fire protection standards, the operating organization fitted a pipe and manual valve to drain the tank to a sump in the basement in case of fire. The valve was locked closed using a chain and padlock. During full power operation some time afterwards, there was an annunciation in the control room that the oil level in the tank was low and decreasing rapidly. The plant shut down automatically, but the turbine running gear sustained extensive damage.

On investigation, it was revealed that the lock and chain on the manual valve had been forcibly removed and the valve had been manually opened. This was clearly a deliberate act by an insider who had both the knowledge of the impact of his act as well as the opportunity to carry it out unseen.

II-7.2. Specific interface issue

At the time of the modification, not much attention was given to the full spectrum of security considerations. That the valve was chained and locked in the closed position indicates awareness of the operational vulnerability introduced by the modification, but more to the inadvertent and untimely opening of the valve during operational or maintenance activities. The chain and lock were intended to place the valve under the control of the operations supervisor and were inadequate to prevent a malicious act.

II-7.3. Management of the interface

Subsequently, each modification to the plant is reviewed considering both safety and security aspects in a systematic manner by experts in both fields, including defence against an insider threat.

II-7.4. Comment

In this example, the malicious act was apparently not intended to result in a radiological event or the theft of nuclear material, but to cause a great deal of physical damage to the plant and commercial damage to the operating organization. However, both the intention and the consequence might have been different and the example presents a lesson to be learned.

II-8. SAFETY TRAINING FOR SECURITY PERSONNEL

II-8.1. Background

The security personnel on the site are required to respond pre-emptively to any event at the research reactor facility on the assumption that the underlying initiator of the event is security-related. This approach ensures that no time is lost in their response to a real security event.

II-8.2. Specific interface issue

The security personnel were not trained in radiation protection and other safety aspects of the facility. Problems in this regard were highlighted during an emergency exercise.

II-8.3. Management of the interface

Safety training for the security personnel was organized on a regular basis by the safety department of the facility. The training programme was devised with the collaboration of both safety and security experts. Also, the training programme had to be repeated at regular intervals, in step with the rotation of security personnel between duties on and off-site, to ensure that new postings to the reactor facility are familiar with the safety aspects at all times.

II-9. SAFETY AND SECURITY BRIEFING FOR VISITORS AND EXTERNAL WORKERS

II-9.1. Background

Before entering a facility, visitors and external workers receive a safety briefing, followed by a quiz. This aims to facilitate the protection of outsiders during an emergency, informs the outsiders on the nature of the safety hazards at the facility and what measures are taken to protect them, and conforms to regulatory requirements.

II-9.2. Specific interface issue

The topics of the safety briefing focused only on safety issues (radiation protection, conventional safety, fire hazards, etc.). It included minimal information on security-related measures. This led to outsiders' frustration over the delays at access control points, retention of cell phones, cameras, laptops, etc. by security officials at these points, and unexpected difficulties in carrying out their work in the facility.

II-9.3. Management of the interface

The briefing provided to visitors and external workers was revised to include a security module. Both safety and security staff of the facility cooperated to set up the revised briefing to ensure that it presented the basic required information and did not reveal any details that could be used by adversaries to defeat safety features or security measures.

II-9.4. Comment

It is also important that the operating organization provides advance information on the security requirements at the facility to prospective external workers so that they arrive at the facility with an adequately prepared strategy for accomplishing their work in conformance with these requirements.

II-10. SAFETY MODIFICATION IMPAIRS SECURITY SURVEILLANCE

II-10.1. Background

A new safety component was installed.

II-10.2. Specific interface issue

The safety component was installed in a location that caused it to degrade the ability of security personnel to conduct surveillance of a sensitive area.

II-10.3. Management of the interface

The safety and security experts at the facility jointly assessed the issue. It was decided that the optimal solution in this case was to place the new safety component in a different position, thereby removing the obstruction to the security surveillance measures in the area. The relocation of the safety component had no effect on its safety function.

II-10.4. Comment

This interface issue could have been avoided by better coordination between safety and security personnel during the pre-implementation phase of the modification (i.e. proactive management of the interface between safety and security as opposed to reactive management). If the location of the safety component had been crucial to the performance of its safety function, the optimal solution may have needed the security surveillance measures to be adapted or redesigned. Each case needs to be carefully evaluated by experts from both fields in order to obtain the most suitable and cost effective solution.

II-11. INFORMATION AVAILABLE TO EMERGENCY RESPONDERS

II-11.1. Background

In order to effectively perform their interventions and responses during an emergency at a research reactor facility, the emergency services needed access to sensitive information such as:

- Access control security barriers and related security processes at the facility;
- Descriptions and locations of nuclear and radioactive material;
- Detailed building layouts and site maps that may show vulnerable areas and access points;
- Location of fire hoses, fire extinguishers, main power isolators, etc.

II-11.2. Specific interface issue

In this situation, the emergency response personnel's need to know sensitive information to adequately perform their duties still requires measures to prevent inappropriate further disclosure of such information.

II-11.3. Management of the interface

A folder, called the “target folder”, containing sensitive information concerning the facility is kept at the site emergency response centre in a secure storage container which meets the competent authority’s requirements. The emergency services can consult it during the intervention. The contents of the folder were agreed in collaboration between the safety and security experts at the facility.

II-11.4. Comment

The leader of the emergency response (or leaders of separate response teams) could be designated as having a “need-to-know” this sensitive information in order to have prior familiarity with aspects related to different response scenarios and thus facilitate a more efficient response to events.

CONTRIBUTORS TO DRAFTING AND REVIEW

Abou Yehia, H.	L'Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France
Adams, J.	United States Nuclear Regulatory Commission, United States of America
Brooks, K.	International Atomic Energy Agency
Carle, B.	Belgium Nuclear Research Center, Belgium
Clarke, M.	International Atomic Energy Agency
D'Arcy, A.J.	International Atomic Energy Agency
Ek, D.	Sandia National Laboratory, United States of America
Kennedy, W.B.	International Atomic Energy Agency
Lolich, J.	International Atomic Energy Agency
Lourens, D.	South African Nuclear Energy Corporation, South Africa
Price, C.	Nuclear Security Consultant, United Kingdom
Ryan, E.	Nuclear Security Consultant, Australia
Shokr, A.M.	International Atomic Energy Agency

Consultants Meetings

Vienna, Austria: 26-30 May 2014, 18-22 August 2014

Workshop

Vienna, Austria: 1-5 June 2015

IAEA
International Atomic Energy Agency

No. 24

ORDERING LOCALLY

In the following countries, 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.

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, s.r.o.
SESTUPNÁ 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA
Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY
Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN
Maruzen-Yushodo Co., Ltd.
10-10, Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: http://maruzen.co.jp

RUSSIAN FEDERATION
Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: http://www.secnrs.ru

UNITED STATES OF AMERICA
Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

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

IAEA Publishing Section, 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 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

16-28611

International Atomic Energy Agency
Vienna
ISBN 978–92–0–106316–8
ISSN 1011–4289