RRFM

EUROPEAN RESEARCH REACTOR CONFERENCE 2013

Transactions

St. Petersburg, Russia
21 -25 April 2013

EUROPEAN NUCLEAR SOCIETY

ENS CONFERENCE

supported by:

ROSATOM

organised in collaboration with:

IAEA

© 2013
European Nuclear Society
avenue des Arts 56
1000 Brussels, Belgium
Phone + 32 2 505 30 54
Fax +32 2 502 39 02
E-mail ens@euronuclear.org
Internet www.euronuclear.org

ISBN 978-92-95064-18-8

These transactions contain all contributions submitted by 19 April 2013.

The content of contributions published in this book reflects solely the opinions of the authors concerned. The European Nuclear Society is not responsible for details published and the accuracy of data presented.

Table of Contents:

RRFM2013-A0092	UNIQUE RESEARCH REACTOR FEATURES POTENTIALLY IMPACTING NUCLEAR SECURITY	Lolich, J. (1); Krychenkov, V. (1); Adelfang, P. (1) 1 - IAEA, Austria

International Programmes

European Research Reactor Conference
Saint Petersburg, Russia 2013

"Unique Research Reactor Features potentially impacting Nuclear Security"

J.Lolich, V. Kryuchenkov, P. Adelfang
IAEA Office of Nuclear Security/Research Reactor Section

Abstract

The title "Research Reactor" represents a diverse category of non-power reactors that can include a wide variety of co-located facilities. The design diversity, as well as other certain specific features of a research reactor facility can present many complex situations that can greatly influence the nuclear security system and therefore, must be addressed. These features include inherent design vulnerabilities, availability of tools and operational equipment, diversity of safety systems, attractiveness of target nuclear material for theft (e.g. portable HEU fuel elements), frequent on-site movement of nuclear and other radioactive materials, co-location with other facilities (e.g. radioisotope production, hot cells, nuclear fuel fabrication), openness of facility—free exchange and access control, research reactor site location (e.g. university campus), non- adequate funding, regulatory and operational issues (e.g. facility aging, extended shut down).
Keeping in mind a need to develop a comprehensive, systematic, and focused program to assist Member States to establish, enhance, and sustain nuclear security at research reactors, IAEA has developed a program on security of research reactors for 2013-2017. The objectives of this program are: a) Assist adherence to and implementation of nuclear security related international instruments; and b) Strengthen the international cooperation and coordination of assistance given through bilateral programs and other international initiatives in a manner which also would contribute to enabling the safe, secure and peaceful use of nuclear energy and of such applications with research reactors.

1. Introduction

Description of Nuclear Security

The IAEA defines nuclear security as the prevention of malicious acts by an adversary that could result in unacceptable radiological consequences. This definition is specific to nuclear and other radioactive materials and facilities and is inclusive of physical, personnel, information and computer security as well as material control and accountability or inventory control. Each of these individual nuclear security elements also has its own specific definition:

- Physical security is security of the physical, tangible assets (such as nuclear and other radioactive materials and facilities) and employs technical security measures such as sensors, cameras, access control equipment, equipment to communicate alarms, physical barriers such as doors, fences, and locks, security guards; and administrative security measures such as security procedures. Physical security is called physical protection in NSS ≠13.
- Personnel security is ensuring the honesty, reliability, and trustworthiness of staff and others with access to targets being protected to minimize the likelihood that they would be motivated to participate in a malicious act (insider threats as defined by NSS ≠8). This is achieved by assessing the character of those with access to nuclear and radioactive facilities through background checks and interviews. In addition, management should ensure that personnel are responsible and professional with respect to an effective security program, including security culture measures. Personnel security is also known as human reliability.
- Information security is the control and protection of electronic and printed data, text, maps, drawings and photographs the disclosure of which could facilitate an adversary in the execution of a malicious act against nuclear or other radioactive materials or facilities. Information security includes classification, information control, and information accountability to restrict assess to sensitive information and to assign responsibility to those who have access. Information security employs physical security techniques (technical and administrative) to limit access to sensitive information to those with authorized information, and to secure materials from those without authorized access.
- Computer security is the protection of computer-based systems, networks and digital systems that control processes and information (such as security or safety information) the compromise, damage, control or infiltration of which could aid an adversary in the execution of a malicious act against the nuclear or other radioactive materials of facilities (See NSS ≠17). In NSS ≠17, computers and computer systems refer to the computation, communication, instrumentation and control devices that make up functional elements of the nuclear facility. This includes desktop computers, mainframe systems, servers, network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers), and with all components that may be susceptible to

electronic compromise. Computer security consists of firewalls, protected passwords, network security and control, redundancy, and system reliability. Computer security is considered synonymous with cyber security and IT (Information Technology) security.

- Nuclear Material Accounting and Control (NMAC) and Radioactive Material Inventory Control (RMIC) are an integrated set of measures designed to provide information on, control of, and assurance of the presence of nuclear and other radioactive material. It includes those systems necessary to establish and track nuclear and other radioactive material inventories, control access to and detect loss or diversion of nuclear and other radioactive material, and ensure the integrity of those systems and measures.

1.2 Legal and Regulatory Basis for Nuclear Security

The Convention of Physical Protection of Nuclear Materials highlights the need for a legal and regulatory basis for nuclear security. Development of a legal basis and a regulatory structure, including licensing, regulations and inspection is a State responsibility. Specific nuclear security requirements should therefore exist and should be available through the regulatory authority. The IAEA has published recommendations for nuclear security, which are intended to be input for the national regulations. These IAEA nuclear security recommendations relevant to research reactors can be found in NSS ≠13 and ≠14.

2. Unique Research Reactor Challenges

Research Reactors, due to their diverse objectives, settings, funding, and staffing present a unique set of challenges to implementing an effective nuclear security program. These are summarized below and will be addressed in greater detail within this Technical Guidance. These issues are:

2.1 Security Vulnerabilities Inherent in Design

The majority of research reactors were not designed with security in mind and this complicates the task of providing security. The research reactors designs were rather optimized around their specific objective, be it education and training, research, material testing or radioisotope production. These objectives often necessitated ease of access to the core for introducing experiments (e.g. beam tubes and rabbit systems) and for frequent reconfiguration of the core (exposed core and hand tools to remove assemblies); or openness for ease of instruction and training, such as open, glass enclosed control rooms. Further, the lack of a security and safety emphasis in design resulted in open and exposed spent fuel pools. These security vulnerabilities could be exploited by an adversary to gain quick access to material and the operating core to commit theft or sabotage.

2.2 Availability of tools and operational equipment

In additional to security vulnerabilities introduced in the design, research reactors are often found to have the tools and equipment readily available to facilitate the research and training. These tools and equipment include handling poles for the fuel removal, cranes, forklifts, fuel casks, power tools, and man-portable shielding blocks. Again, these tools and equipment could be exploited by an adversary to accelerate his/her tasks.

2.3 Specific Safety Design

Research reactors, due to reduced thermal energy and fission product inventory, typically do not present the hazards or risks of power reactors and as such, are not subjected to the same stringent safety requirements. As a result, safety systems may be less diverse, redundant, and robust and therefore more easily defeated than those at a nuclear power plant. The importance of research reactor safety systems for each research reactor must be specifically considered in the facility physical security protection regime. Considerations include:

1. Lack of power supply redundancy
2. Type of reactivity control
3. Robustness of cooling and decay heat removal
4. Absence of containment/confinement
5. Less robust fire protection
6. Lack of diversity/redundancy of safety systems
7. Lack of compartmentalization

2.4 Attractiveness of Target Material for Theft

The research reactor typically uses a form of uranium that is more highly enriched than power plants and as such, is more attractive. Additionally, research reactor operating duration and frequency, especially at underutilized research reactor facilities may result in spent or irradiated fuel that is less likely to be immediately incapacitating to an adversary. As a result of these two factors, research reactors can possess more highly attractive theft targets than do power reactors. The following are factors that contribute to this attractiveness:

1. man-portability of the fuel
2. chemical and physical form, enrichment and quantity of fuel
3. activity of spent fuel

2.5 Co-location with Other Facilities

Research reactors often are part of a larger enterprise (e.g. medical radioisotope production), or are part of a larger research campus of unrelated activities. As such, they can be co-located with several other types of facilities, often under the same security umbrella. The co-location of research reactor facilities among other types of industrial or research facilities can present specific security

concerns, the impacts of which must be considered when developing a research reactor physical security protection regime. The following is a list of typical facilities co-located with research reactors:

1. radioisotope production facilities
2. fuel research and fabrication facilities
3. storage of fresh fuel, spent fuel, or radioactive sources
4. radioactive waste storage and disposal
5. laboratories, hot cells
6. irradiation facilities

2.6 Openness of Facility—the Free Exchange of Information and Access

The business of research reactors often requires an environment where access to the reactor facility is required to be successful. Teaching, training, medical procedures, and research involves a constant rotation of temporary partners, clients, and students. This situation creates complications for a security system.

The business of research reactors often requires an environment where access to the reactor facility is required to be successful. Teaching, training, medical procedures, and research involves a constant rotation of temporary partners, clients, and students. The number of temporary personnel without unescorted access creates complications for a security system. In addition, the transparency and sharing of information as part of research culture creates difficulties for a security system, including computer-based system security. Examples are listed below:

1. culture of sharing of information
2. competitive need for openness
3. high computer literacy of users of Information Technology infrastructure creating a potential insider cyber threat

2.7 Variety of Uses of Research Reactor Complicate Standardization of Security

Research Reactors represent a wide variety of reactors designs, typically for specific purposes. This variety complicates any effort to produce a standard approach to security. This variety includes:

1. training, research, education
2. irradiation
3. neutron scattering experiments
4. neutron radiography
5. source/radioisotope production
6. medical therapy and research
7. activation

2.7 Funding

Research reactors are owned and/or supported by a number of different types of organizations. This influences the strength of funding support, particularly with respect to security. Further, competing priorities within the organization particularly when funds are scarce, can put acute economic strains on the maintenance of reactor security. Funding limitations make it difficult to construct and maintain adequate security systems. The following are funding issues particular to research reactor security:

1. commercialization of the reactor
2. internal competition for limited resources between safety-security-operations functions
3. competition for government/corporation funding
4. competition between government funding of research reactor oversight and research assistance

2.8 Regulatory and Operator Issues

Research reactors operating organizations sometimes have a lack of a regulatory culture, at times believing that the reactor purpose or mission is more important than compliance with regulatory requirements. This can be exacerbated by the lack of nuclear security expertise and by the lack of organizational independence of the regulator in States where nuclear research operation/promotion and regulatory oversight responsibilities are co-located within the same government organization. Such conditions result in the lack of effective regulatory oversight. This combined with a lack of security culture of the researchers can significantly complicate security implementation. Likewise, this problem may be further exacerbated by the closed and insular nature of security organizations.

2.9 Research Reactor Site Location

Many research reactors are located in geographic locations that might be undesirable from a security perspective. In some cases, research reactors were sited without adequate consideration of safety and security criteria. These locations might include the following characteristics:

1. close proximity to population
2. dense traffic environment
3. unfavourable meteorology
4. areas of seismic activity
5. disadvantageous topography from a security perspective
6. considerations of hydrology
7. co-location with other facilities
8. are not under control of the State

2.10 Level of Security Expertise

The security function at all but the largest research reactors is typically a collateral duty. Often, staff responsible for security lack specialized experience and knowledge of security systems or measures. Examples of this may include the following:

1. non-dedicated personnel (multi role)
2. no background or training in security
3. lack of security expertise within the regulatory body
4. lack of specific security responsibilities (security culture of whole of organization including management)
5. complete reliance on local law enforcement agency, sometimes without any mutual aid agreements

2.11 Facility Aging Issues

More than 70% of research reactors are older than 30 years. As such, they were built with older technology and did not consider security in their initial design and construction. Although many are upgraded, these upgrades did not consider security. This results in less than an optimal implementation of security systems.

1. lack of robust barrier design
2. degradation of security and safety components
3. inability to support upgrades due to lack of infrastructure, structural robustness
4. security system obsolescence
5. facility configuration/geometry and compactness limits security options

2.12 Research Reactors in Extended Shut Down

Many research reactors are in an extended shut down state. These pose unique security concerns with maintaining the required commitment necessary for the effective protection of the material. These concerns are based on the following:

1. fuel remains onsite
2. degradation of security vigilance over time due to regulatory and operator complacency
3. lack of funding/personnel
4. Fuel is less likely to be self-protecting

2.13 On-Site Movement of Nuclear and Radioactive Material

Operations can require frequent on-site movements of material. These movements may not have defined formal security procedures. This informality results in potential security vulnerabilities of theft and diversion. These vulnerabilities are a function of the frequency, duration, and attractiveness of material being moved.

3. New IAEA Work-Plan on Research Reactors Security

In line with the objectives of the current Nuclear Security Plan, the objective of the IAEA Security Program for Research Reactors is to develop a comprehensive, systematic, and focused approach to assist Member States to establish, enhance, and sustain Security at Research Reactors.

3.1 New IAEA Document on Research Reactor "Security"

Technical guidance and other publications are an important mechanism for disseminating information to the Member States.

Since the beginning of 2012 the Office of Nuclear Security (NSNS) is working in two new documents on *"Research Reactors Nuclear Security"*:

1. Security Management for Research Reactor Operators
2. Nuclear Security Considerations in the Training and Qualification of Personnel for Research Reactors

Document Category: Nuclear Security Series – Technical Guidance

Nuclear Security is used by the IAEA to refer to physical, personnel, information and cyber security as well as material control and accountability (nuclear material) or inventory control (radioactive material) specifically for nuclear and other radioactive materials and facilities that could initiate unacceptable radiological consequences if subjected to intentional malicious acts by an adversary.

3.2 Objective of This Technical Guidance

These documents is intended to be a single source of guidance to assist research reactor facility management personnel responsible for implementation of nuclear security in the:

- Development and maintenance of an effective and comprehensive site-wide nuclear security program for nuclear and other radioactive materials and associated co-located facilities.
- Training and Qualification of Security Personnel.

These documents will also assist the management to demonstrate the effectiveness of the program to inspectors from the national competent authority/security regulator body(ies).

Note: the authors would like to thank the following IAEA Consultants on Nuclear Security for their valuable contribution to this paper: Mr. E. Ryan (Australia), Mr. B. Carle (Belgium), Mr. K. Lefreniere (Canada), Mr. D. Ek (USA), and Mr. J. Adams (USA).

European Nuclear Society
56, avenue des Arts
1000 Brussels, Belgium
Telephone: +32 2 505 30 50 - FAX: +32 2 502 39 02
rrfm2013@euronuclear.org
www.rrfm2013.org