Nuclear Engineering and Technology 53 (2021) 1479–1482

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Enhancing utilization and ensuring security: Insights to compromise contradicting conditions in new research reactors

Ibrahim Alrammah

Nuclear and Radiological Control Unit, King Abdulaziz City for Science and Technology (KACST), Riyadh, 11442, Saudi Arabia

ARTICLE INFO

Article history:
Received 31 July 2020
Accepted 5 November 2020
Available online 19 November 2020

Keywords:
Research reactor
Safety
Security

ABSTRACT

Research reactors are typically well-suited for outreach activities at different levels. However, unplanned seeking to increase the utilization of a research reactor may result in weakening the nuclear security of this facility. Research reactor staff might be in shortage of a functional nuclear security culture; specifically, there might be a conviction that the necessities of research can be given the priority over consistence with security procedural requirements.

Research reactors are usually parts of bigger institutes or research labs of different activities. Moreover, the employments of research reactors are usually with the purpose that easy entry to the reactor premises is fundamental. So, they could be co-situated in places with different sorts of activities, mostly under similar security arrangements. The co-area of research reactor offices among different kinds of research labs introduces explicit security issues, the effects of which should be viewed as when building up a nuclear security framework.

Notwithstanding potential security vulnerabilities presented in the design, research reactors frequently have devices kept promptly accessible to encourage research and education. The accessibility of these sorts of hardware could be used by an authorized person to commit an unapproved activity or cause harm.

This paper aims to present insights to compromise contradicting conditions in new research reactors in which both enhancing utilization and ensuring security are satisfied.

1. Introduction

Launch of a research reactor is a big project that demands detailed planning, preparation, implementation, time investment and manpower resources. The execution of such a project demands founding of reliable infrastructures, as well as legal and regulatory, safety, technical and economic aspects [1].

Research reactors include a wide range of facilities in terms of objectives, power levels, fuel enrichment and complexity. This wide range presents different security issues and considerations when compared with other facilities in nuclear industry. These issues and considerations comprise, but are not limited to:

- Diversity of designs: Research reactors are designed to meet various operational objectives. In some cases, these objectives lead to designs that complicate the security system.
- Fuel enrichment: Research reactors sometimes utilize a form of uranium that is more highly enriched than that used for power plants, which might be a more attractive target for theft.
- Ageing: More than two-thirds of research reactors worldwide are more than 30 years old. Many were constructed with older technology that did not take into account security in their preliminary design and construction, and many are nowadays in a phase of extended shutdown.
- Utilization: Research reactors are typically part of a larger facility of unrelated activities. Moreover, the uses of research reactors are typically such that ease of access to the reactor facility is crucial.
- Culture: Research reactor personnel may lack an efficient nuclear security culture; particularly, there might be a belief that the requirements of research can be given priority over compliance with security requirements [2].

Some of research reactors were not structured with security as a need, which can fall short in the duty of ensuring security. Research

E-mail address: irammah@kacst.edu.sa.

https://doi.org/10.1016/j.net.2020.11.010

reactor plans were commonly focused on their particular goal (for example: training and education, research, material testing or radioisotope production). The emphasis on these goals frequently prompted the consideration of highlights that are essential in nuclear security, for example:

- High hazard targets could be from theft of HEU fuel and harm of enormous inventories of fission products, storage of fresh fuel, spent fuel or radioactive materials;
- Beam tubes proposed to give easy access to the core so as to present tests;
- Exposed cores and hand tools for withdrawing assemblies afforded to enable regular reconfiguration of the center;
- Radioactive waste storage and disposal;
- Glass-walled control rooms (to enable guidance and education);
- Access to PC frameworks (information and system access);
- Open and uncovered spent fuel pools, to lessen cost (without focus on security).

These points would present security vulnerabilities that could be misused by a person on committing unapproved practice or harm.

Research reactors commonly utilize a type of uranium that is more highly enriched than that utilized in NPPs. The term and recurrence of activities in research reactors, particularly those that are underutilized, may likewise be with the end goal that the fuel burnup is low and the dose rates from spent or irradiated fuel might be less inclined to be promptly weakening to an adversary.

Research reactors may, along these lines, contain material that is a more appealing focus for unapproved removal than that held at NPPs because of the straightforward entry to sensitives materials [2].

2. The issue of underutilization in research reactors

Nowadays, the fleet of research reactors faces a bunch of important issues and critical challenges, which may include: ageing, non-existent or inappropriate strategic plans, underutilization [3]. A research reactor built without a detailed utilization plan could face an underutilization issue and funding cuts [4]. One of the essential reasons for underutilization in research reactors is the lack of purpose and strategy [5]. Many research reactor managers recognize that there is a necessity to develop a strategic utilization plan for long-standing sustainability, considering the 'marketing' of their services [6].

An effective utilization plan, established with input from a broad community of prospective users, will be appearing in high levels of utilization, the accessibility to necessary funding, long-standing safe and environmentally sustainable operation of the facility [7]. A utilization plan is a dynamic process, and hence this plan will need monitoring and frequent updating to be truly reflecting the reactor goals [8].

The strategic planning methodology for a research reactor could involve the following steps:

a) Identifying the potential users and their requirements in the utilization of the reactor;
b) Identifying the required capabilities of the new reactor based on these requirements;
c) Performing an iterative assessment that studies (a) and (b) in the framework of the atmosphere and restrictions under which the reactor will operate [9].

Nevertheless, trying to increase the level of utilization in a research reactor is usually associated with increasing the number of customers and users. Unplanned effort to increase utilization could result in security vulnerabilities due to higher level of exposure to different types of users. The following sections discuss challenges and issues of security vulnerabilities in research reactors and how to compromise utilization-security dilemma.

3. Challenges to the Utilization–Security contradiction

There are some challenges existing in most research reactors handling the interface between enhancing utilization and ensuring security, which include:

3.1. Siting

Research reactors lean towards to be sited within research institute or on college campuses, which may make easy access of possible intruders or attackers [10]. Selection the site of a research reactor requires to be based on both utilization and security factors which ensure that the site location, geology, topography, demography, meteorology, land use considerations/planning, infrastructure, etc., do not introduce any impediments to either of these disciplines or to the management of their interaction with each other.

The prospective evolution of factors in the area that may have an impact on utilization and/or security require to be assessed for a time period that includes the expected lifetime of the research reactor. Utilization considerations comprise changing in population distribution, commercialization or industrialization of surrounding areas. Considerations for security comprise the location and the facility layout within the site in a way that on-site characteristics (distance from the site boundaries, topographic obstructions, etc.) can be used to benefit in securing the site against possible adversaries [11].

3.2. Utilization

The necessity to utilize the reactor by external experimenters to the organization may introduce a risk of sabotage (e.g., exposure of sensitive materials into the reactor core or breaking beam tube isolation windows).

Damage to core components caused by security problems lead to significant radiological consequences to people and environment. At the same time, prohibiting utilize of the reactor by external experimenters to the organization reduces the usefulness and utilization of the reactor [12].

The operation phase is the phase during which the security risks are the highest, because of the existence in the facility of:

- Fresh and irradiated reactor fuel, that require to be adequately handled from the security perspective to prevent inadvertent criticality or unauthorized reach;
- Inventories of diverse radioactive sources, structures and components;
- Several operational experiments each introducing its own set of radiological hazards and security issues;
- Operating and supporting staff (e.g. researchers, security personnel, students and contractors) in areas that have SSCs (structures, systems and components) sensitive from a security perspective.
- Relatively short operating, refuelling, and maintenance periods, with related high frequency, short duration changes in the plant security configuration;
- Various operating modes for different objectives, each with its own safety and security concerns;

- Tools to execute manual activities impacting the core reactivity and geometry, probably with the reactor operating at power [11].

Modifications in the configuration of the research reactor may negatively affect security equipment. This could be due to degradation or loss of safety or security function [12].

Modifications and changes are typical activities of the operating phase of a research reactor. Typical modifications or changes to the facility can be due to the need to satisfy changing operational requirements, innovations in utilization programmes, updating regulatory standards and requirements, addressing lessons learned from operating experience, upgrading the facility or treating the effects of ageing. Effective management of change necessitates coordination and communication between management and staff responsible for facility utilization and security, and has to be treated by the integrated management system.

Maintenance activities could deliberately or inadvertently disable the item being repaired, or other related safety or security equipment [11]. Modification or change of reactor configurations during maintenance (e.g., cut of electrical power supply) impact operability of safety (e.g., doors opened) and security tools (surveillance cameras). Configuration changes during maintenance could present vulnerability from the security standpoint (could be increased if the activities are executed by contractors) [12].

3.3. Access control

Increasing the utilization of a research reactor requires authorizing an access to the reactor hall, reactor core, experimental and irradiation facilities, and reactor areas by operations personnel, researchers and contractors. Hands-on training on equipment requires unobstructed mobility of operations personnel around the whole facility [11].

Various parties with diverse interests in optimizing the operational, production and experimental programs of the reactor for their particular requirements (e.g. several customers of irradiation services, universities and other institutes with experimental programs at the reactor, etc.) [11].

The need for rapid access during emergency events can introduce vulnerability from the security point of view. Vulnerability increases as a result of change in access control rules and the number of operating staff present compared with the normal operation periods of the reactor. Non-existence of balance between utilization and security provisions can result in delays in responding to emergencies situations or can lead to security vulnerability [12].

3.4. Management of information

For safety culture, all entities are entitled to openly share information due to the requirement of transparency. In the same manner, security culture necessitates that entities respond instantly to potential threats and events, and restrict communication to authorized entities with a need to know [13]. A safety culture of 'openness of information' can introduce an easy mechanism by which an adversary can collect sensitive information. Information would be assessed from the view of how the information could be used by an adversary and then protected accordingly [2].

Information on security weakness could be used by potential adversary for malicious acts. Moreover, inadequate protection of the security information increases the risk of malicious acts. On the other hand, transparency is needed for utilization enhancement while information should be confidential in security standpoint [12]. The main differences between safety culture and security culture that need to be factored into the culture-building process are:

a) A safety culture requires transparency. It is vital to share comments on experience, in order to avert repetitive occurrences of incidents at the reactor, and to circulate information to avert such incidences at certain research reactor from being occurred at others.
b) A security culture, in contrast, requires that the distribution of information typically be restricted only to authorized and trusted individuals on a valid "need-to-know" rule, in order to prevent sensitive information involving security measures or safety/security weaknesses at the reactor from reaching to the hands of adversaries [11].

4. Recommendations to enhancing utilization and ensuring security

1. Utilization plan could encompass the security culture together with safety culture framework as its basic parts [14].
2. Presenting the framework of an optimum organizational culture and meet all the requirements of the ideal safety and security procedures within and to communicate the message effectively.
3. Introducing an effective collaboration between the different departments, rules and duties.
4. Performing the self-assessment effectively during the entire process with special consideration must be taken on both safety and security measures [15].
5. Access control procedures should ensure balanced considerations between utilization and security, and should be established jointly by utilization and security specialists.
6. Coordination with the security specialists concerning the provisional changes planned during maintenance activities along with the related compensatory measures.
7. Modifications need to be evaluated from the utilization and security perspective before execution.
8. Participation of security specialists in planning for ensuring adequate surveillance, periodic testing and maintenance of the security equipment [12].

There are some other means by which security awareness instructions can be brought to the attention of reactor users:

a) Regular security newsletters issued by the national regulatory authorities.
b) Posters to remind users of the security threats and of the main security controls required to counter them.
c) Stickers to remind individuals of their personal accountability for the security of when performing specific practises.
d) Security reminder notices in the startup background of a computer screen, which the individual has to acknowledge reading before the computer will finish logging in.
e) Security notices, bulletins and circulars issued by security department to remind users of certain security rules, to counter possible weaknesses.

f) Raising awareness by providing a channel of communication with users on security issues.
g) Frequent periodic trials of individual security knowledge [16].

5. Conclusions

Recognizing that a utilization plan must inherently consider security issues, a comprehensive approach is strongly recommended. Adherence to administrative requirements involving use of proven procedures will enhance security levels. It is also essential to note that specific attributes in some aspects may result in conflicts between utilization and security. This should be solved by effective coordination and harmonization of approaches and methods and by following proven operating procedures. When conflicts are unmanageable, the problem should be resolved based on minimizing the overall radiological risk and security threats to the workers, public and the environment.

The development of an integrated management system for a research reactor facility is a fundamental requirement for enhancing utilization and ensuring security. This system integrates all quality, health, utilization and environmental issues along with safety and security into a unified consistent framework to effectively manage the interactions and interfaces between various disciplines, activities and requirements, and could be developed at the level of the reactor itself or be contained within the management system of the operating institute.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

I would like to thank King Abdulaziz City for Science and Technology (KACST) for supporting this work. I would also like to thank the anonymous reviewers for their comments and recommendations.

References

[1] A.M. Shokr, et al., Considerations and milestones infrastructure for a research reactor project, in: Proc. Research Reactors: Safe Management and Effective Utilization, Rabat, 2011.
[2] International Atomic Energy Agency, Nuclear Security Management for Research Reactors and Related Facilities, IAEA-TDL-004, Vienna, 2016.
[3] International Atomic Energy Agency, Research Reactors: Purpose and Future, 2016. Vienna.
[4] International Atomic Energy Agency, Nuclear Technology Review, 2012. Vienna.
[5] J. Vyshniauskas, Utilization of Research Reactors for Nuclear Education and Training: Overview of Activities, IAEA, Vienna.
[6] International Atomic Energy Agency, The Applications of Research Reactors, IAEA-TECDOC-1234, Vienna, 2001.
[7] International Atomic Energy Agency, The Role of Research Reactors in Introducing Nuclear Power, [Accessed 31 July 2020].
[8] D. Ridikas, Developing strategic plans for effective utilization of research reactors, EUROPEAN NUCLEAR SOCIETY 48 (2015).
[9] International Atomic Energy Agency, Strategic Planning for Research Reactors, IAEA NUCLEAR ENERGY SERIES No. NG-T-3.16, Vienna, 2017.
[10] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA NUCLEAR SECURITY SERIES No. 4, Vienna, 2007.
[11] International Atomic Energy Agency, Management of the Interface between Nuclear Safety and Security for Research Reactors, IAEA-TECDOC-1801, Vienna, 2016.
[12] A.M. Shokr, et al., A New IAEA Document on Managing the Interface between Safety and Security for Research Reactors, Proc. European Research Rectors Conference, Bucharest, 2015.
[13] International Atomic Energy Agency, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, Vienna, 2008.
[14] V. Bezzubtsev, B. Krupchatnikov, Interface of nuclear safety and security, safety and security culture, in: Proc. International Conference on Effective Nuclear Regulatory Systems: Further Enhancing the Global Nuclear Safety and Security Regime, 2009, Cape Town, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 2010.
[15] K. Horváth, et al., Cut the costs and enhance efficiency in nuclear safety and security culture self-assessments: considerations that should Be taken to merge nuclear safety and security culture assessments, HADMÉRNÖK 12 (2017) 115–122.
[16] International Atomic Energy Agency, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, Vienna, 2015.