A PROPOSED REGULATORY PERSPECTIVE ON THE SECURITY REQUIREMENTS FOR SPENT NUCLEAR FUEL

Z. F. HASSAN AKL
Egyptian Nuclear and Radiological Regulatory Authority
Cairo, Egypt
Email: eltasneem2007@yahoo.com

Abstract

Spent nuclear fuel (SNF) possesses potential security risks; consequently, nuclear security issues have to be considered and addressed for effective management of SNF. The vulnerability of SNF to theft, for constructing a radiological dispersal device, and to the terrorist attack during storage or transport is a major concern for States having such type of nuclear materials. Hence, the national policy and strategy for SNF management should include a set of goals and objectives to ensure the secure management of SNF, and should also set out the means for achieving these objectives. Egypt recognizes that a strong and efficient legal and regulatory framework is an important element of the national nuclear security regime; therefore, it has taken several steps to enhance its legislative and institutional frameworks. Currently, the Egyptian nuclear and radiological regulatory authority (ENRRA) is developing its regulatory system regarding nuclear security that includes developing the necessary regulations against which the various nuclear facilities will be assessed, setting out the licensing process and procedures along with definition of the corresponding documentation to be submitted by the applicant, and creating an inspection program. Regulatory requirements of the physical protection (PP) of nuclear material and associated facilities are considered as a cornerstone in ensuring the security of spent fuel. These requirements should be based on the current threat assessment or design basis threat (DBT) and should include provisions which if applied correctly, will ensure adequate security of SNF during storage either at reactor site or at an interim storage facility as well as during transport. The current work provides a proposal for security requirements of SNF taking into consideration the provisions of the Convention on the Physical Protection of Nuclear Material and its amendment, International Atomic Energy Agency (IAEA) guidance, and the best practices adopted by the international community.

1. INTRODUCTION

Spent fuel generated from the operation of nuclear reactors should be managed in a safe, secure, and effective way following its removal from the reactor core [1]. SNF may be considered as waste that is managed through direct disposal in some circumstances (open nuclear fuel cycle) or a potential future energy resource in others, managed through reprocessing (closed nuclear fuel cycle). Either option includes storage of the SNF for some period of time where SNF is preliminarily stored in the reactor fuel storage pool for cooling and then may be transferred to a designated wet or dry spent fuel storage facility for storage or reprocessing [2]. The State's strategy for the management of spent fuel will depend strongly on the overall energy strategy of the State (including nuclear energy strategy) and, in particular, on its requirements for security of energy supplies at an affordable cost. However, defining a policy for the management of spent fuel and radioactive waste is an essential cornerstone to ensure continuity in the necessary technological developments and related investments, and the consolidation of knowledge and competence [3]. Irrespective of the consideration of spent fuel (either waste or an energy resource), the safety and security aspects for storage remain the same [2]. Storage options of SNF include wet storage in some form of a storage pool or dry storage in a facility or storage casks built for this purpose. Storage casks can be located in a designated area on a site or in a designated storage facility. Security of SNF storage facility should be ensured throughout its lifetime stages (e.g. siting, design, construction, commissioning, and operation). At the design stage, due consideration also needs to be given to the future decommissioning of the facility.

Security concerns about using SNF for criminal purposes or utilizing it intentionally in an unauthorized manner should be addressed adequately within the State's nuclear security regime. A legislative and regulatory basis, with clearly assigned nuclear security responsibilities, is an essential pillar for effective protection and control of such material [4]. A regulatory body with prescribed responsibilities should be designated to ensure that the nuclear materials are used or nuclear facilities are operated in a safe and secure manner. The regulatory body is usually responsible for setting the requirements, standards, and associated procedures for evaluating applications and granting authorizations or licenses. In addition, it conducts inspections to verify that licensees are continuing to comply with the regulations and license conditions.

Licensing is a primary means to establish continual regulatory control for all activities and facilities associated with nuclear safety and nuclear security. Developing regulatory requirements or regulations is a prerequisite to the licensing process. Regulations are legally binding instruments developed to ensure the stability and consistency of regulatory control. Effective regulations represent a central part in managing the risks which should be addressed to protect nuclear material and associated facilities. It is the State's responsibility to define its own detailed security requirements and performance objectives. Nuclear security regulations should reflect the State's approach to risk management and assessment of the current threat [5]. The paper proposes regulatory requirements for PP of SNF based on the IAEA's nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5) [6] while taking into consideration the CPPNM and its amendment [7-8]. It could serve as a starting point for drafting a national regulation that reflects the national circumstances. In addition, the paper highlights the national licensing process and summarizes the on-going efforts put by ENRRA in the field of nuclear facilities' licensing from the nuclear security perspective.

2. EGYPTIAN NUCLEAR INFRASTRUCTURE AND REGULATORY FRAMEWORK

Egypt has different nuclear applications including nuclear facilities, activities, and practices. Currently, Egypt has 2 research reactors and fuel manufacturing pilot plant. In addition, it has radio-isotopes production unit and research and development facilities in the field of nuclear fuel fabrication and hydrometallurgy. Consequently, Egypt's concern is to enhance and improve the nuclear security systems in its nuclear applications as well as to enhance the national nuclear security regime. In this context, the Egyptian nuclear and radiation Law no. 7 of 2010 (Law) and its executive regulation have been issued [9-10]. This Law covers safety, security, safeguards, emergency, and liability for the whole peaceful applications of atomic energy. This was complemented by establishing an independent regulatory authority to monitor all nuclear and radiation facilities, activities and practices known as ENRRA. ENNRA carries out all regulatory and control functions related to the nuclear and radiation activities in the peaceful applications of atomic energy, to ensure the safety and security of human, property, society, and environment from the risks of exposure to ionizing radiation. ENRRA deals with all nuclear security-related activities (in cooperation and collaboration with relevant stakeholders) particularly in defining the anticipated threats, reviewing the design of the nuclear security systems and evaluating the performance of these systems, classification for the nuclear materials and radioactive sources from the nuclear security perspective, ensuring existence of adequate PP for nuclear material and associated facilities, approving import and export activities, monitoring measures and procedures applied to combat illicit trafficking of nuclear and radioactive materials, and establishing the State's database for nuclear material and radiation sources in all applications. ENRRA regulates nuclear materials including SNF and associated facilities by means of integration of regulatory requirements, licensing, oversight (including inspection and performance evaluation), and enforcement.

2.1. Nuclear facilities' licensing approach

Licensing or authorizing an applicant to use, handle, transport, export nuclear materials, or to operate a nuclear facility is a prerequisite to any activities related to nuclear material, as stated in the Egyptian nuclear law. The general licensing steps for nuclear facilities had been established by the Law in six steps, namely: site approval permit, construction permit, pre-operational testing permit, fuel loading and approach to criticality permit, operation license, and end of service permit (decommissioning and release from regulatory control). Documents to be submitted to ENRRA for oversight each licensing stage were mentioned in details in the Law and its executive regulation. ENRRA issues one license for each facility including safety, security, and safeguards. The licensing process for PP and safety are carried out by different groups of experts, however; stages for both the processes are consistent. Licensing process is accompanied by ENRRA oversight at all licensing stages as well as during operation to verify compliance with the licensing conditions. Joint review and assessment and/or inspection could be conducted by safety and security personnel to discuss and resolve safety-security interface issues.

2.2. Development of nuclear security regulations

The Law gave ENRRA the authority to draft and issue regulations, standards, and limits in connection to safe and secure peaceful uses of the atomic energy. Particularly in the area of nuclear security, ENRRA has to define PP requirements for nuclear materials and associated facilities that ensure their protection against unauthorized removal and sabotage [10]. Several ongoing activities are in place for developing and enacting different regulations in the field of nuclear security that will cover security requirements for nuclear materials as well as radioactive sources during their whole lifetime and associated facilities. As a first step, rules of classification of nuclear materials and radioactive sources form nuclear security perspective have been issued in order to build nuclear security requirements based on a graded approach, where nuclear material classification is in line with the INFCIRC/225 [11].

3. A PROPOSAL FOR SNF SECURITY REQUIREMENTS

3.1. Preamble

The system of regulations and guides should be in conformity with the national legal system, and the nature and extent of the facilities and activities to be regulated. Nuclear security regulations should specify the requirements and associated criteria for ensuring the protection of regulated materials and facilities. Establishing a well-developed regulation may be challenging to nuclear power newcomers and States those don't have a mature national regulatory infrastructure for PP, therefore international experience and best practices may provide a good basis for developing the national regulation. It can be helpful for embarking countries to adopt the IAEA documents in their regulatory systems, as the IAEA security publications provide a good global reference and establish a good level of nuclear security. Since INFCIRC/225 has been the de facto international standard for the PP of nuclear material for decades, it was excogitated and reflected in the following section. The current work comprises general requirements that if adopted by the regulatory body further guidance would be developed on how these requirements would be implemented. The following requirements shall be in addition to, and not in place of, other relevant applicable national laws and regulations, and none of these requirements are interpreted as relieving the licensee from complying with other applicable laws and regulations. The Law assigned the prime responsibility of PP of all nuclear and other radioactive materials and their associated facilities and activities to the licensee, so this will not be repeated in these requirements. The following proposal doesn't contain security requirements during SNF transport; as such requirements are covered by another regulation already drafted by ENRRA. Regulatory body and operators should consider working together to anticipate, as much as possible, future threats to SNF and to ensure that security requirements remain up-to-date in the face of constantly changing risk [12].

3.2. General requirements

— Licensee responsibilities.
  - Licensee shall establish and maintain a security program that is capable to provide high assurance that activities involving SNF do not create an unreasonable risk to public health and safety.
  - Licensee shall set up PP measures and systems that protect SNF against unauthorized removal and against sabotage during storage and transport.
  - Licensee shall comply with all relevant national laws and technical requirements or standards to ensure the safety and security of SNF.
  - Licensee shall fully cooperate and coordinate with all national organizations having security responsibilities.
  - Licensee shall implement any additional PP measures recommended by the authority, on the basis of DBT or Threat Assessment.
  - Licensee must not make major changes, additions, or modifications to the approved security measures without prior approval by the authority.
  - Licensee shall maintain control of and be able to account for SNF at all times.

— General performance objective and requirements of the Physical protection system (PPS).

- Licensee shall design a PPS that is effective against the theft and sabotage scenarios as defined in the DBT.
- PPS shall be designed with sufficient redundancy and diversity to ensure maintenance of its capabilities.
- Licensees shall evaluate the effectiveness of the PPS design and submit this evaluation to the authority to verify that it complies with the PP requirements. The licensee's evaluation shall include performance testing of the PPS and of the timely response of the guards and response forces. If the licensee's evaluation or authority's review determines that the PPS is ineffective, then the licensee shall redesign the PPS and re-evaluate its effectiveness.

— Security plan.
  - Applicant/licensee shall develop and maintain a detailed security plan that describes all security measures and procedures applied to protect SNF during storage and transport.
  - The plan shall describes how the licensee will meet the PP regulatory requirements and includes all technical, organizational, and resource information related to applied PPS e.g. security policy, security organization, security personnel (responsibilities, armament, training, and qualification), information management, location and maintenance of PP equipment, security procedures, contingency procedures, and response planning. The plan shall list the tests, audits, and inspections used to demonstrate compliance with PPS design requirements and to ensure the plan's continued effectiveness.
  - Licensee shall keep the security plan up to date so that it reflects the current conditions at SNF storage facility and the current threats.

— Interface with other systems.
  - Licensee shall asses and manages any interface of PP measures with safety measures in a manner to ensure that they do not hinder each other and that, to the degree possible, they are mutually supportive.
  - Licensees shall assess and manage the interface of PP measures with nuclear material accountancy and control activities in a manner to ensure that they do not adversely affect each other and that to the degree possible, they are mutually supportive.

— Sustainability program.
  - Licensee shall establish a PPS sustainability program that includes developing and updating the operating procedures, instructions, and manuals; developing and implementing PPS maintenance means and procedures; developing plan for equipment updating, repair, and calibration; developing and implementing PPS performance testing and operational monitoring; configuration management; human resource management and training; resource allocation, and operational cost analysis.
  - Licensee shall review and evaluate the applied PP measures, procedures, and plans on a periodic basis to ensure system effectiveness. The results of these reviews and any actions taken as a result of prior reviews shall be documented and maintained.

— Compensatory measures.
  - Licensee shall identify compensatory measures to be applied in case of inoperability, failure, or degradation of any PPS related equipment, structures, and components to assure that the effectiveness of the PPS is not reduced.

— Management system.
  - Licensee shall establish and maintain a management system and quality assurance program that covers all aspects of the security program.

— Security culture.
  - Licensee shall establish and maintain a dynamic and effective organizational culture where there is recognition that credible threat exists and every individual has a role in security.
  - Licensee shall regularly review the applied nuclear security practice and systems, conduct self-assessments, and draw lessons from real incidents and security exercises.

— Reporting.
  - In addition to rules and procedures set out in the Law and its regulation on the reporting, in case of security-related events the licensee shall;
    (i) Immediately take remedial actions and notify the authority.
    (ii) Submit a brief initial report to the authority on the causes and effects of the event within 24 hours.
    (iii) Submit a detailed report to the authority, within 30 days, on the event origin and consequences, corrective measures taken to minimize the consequences, and preventive measures taken to avoid event reoccurrence.

- In case of failure of any PPS equipment, licensee shall immediately apply the approved compensatory measures, investigate the failure along with its causes and consequences, and notify the authority.
- Licensee shall report all confirmed accounting discrepancies from licensee's system for nuclear material accountancy and control.

— Information protection.
- Licensee shall define and classify sensitive information which may add to adversary capability to perform sabotage or unauthorized removal of SNF.
- Licensee shall establish, implement, and maintain an information protection plan to ensure that sensitive information is protected against unauthorized disclosure and is disseminated only on a need to know basis for trustworthy personnel.
- Licensee shall define access rights and rights of use pertaining to information.

— Cyber security.
- Licensee shall protect the digital computers, communication system, and network associated with safety-related functions, PP functions, and nuclear material accountancy and control against compromise.

— Mitigating insider threat.
- Licensee shall establish, maintain, and implement a long-term insider mitigation program.
- Licensee shall establish and implement a trustworthiness assurance program, where appropriate security clearances shall be carried out in order to ensure the vetting of individuals granted unescorted access to a PA, VA, or sensitive information.
- Licensee shall establish and implement measures to minimize the potential for insiders' threats including facility workers, contractors, and subcontractors utilized by the licensee.

— Contingency planning.
- Licensee shall prepare a contingency plan to counter malicious acts effectively and to provide for appropriate response by guards or response forces.
- The contingency plan shall include a mechanism for detection and assessment of malicious acts that could lead to radiological sabotage and measures to prevent further damage, securing the SNF storage facility, and protection of emergency equipment and personnel etc. in case of sabotage.
- Licensee shall initiate its contingency plan after detection and assessment of any malicious act.
- Licensee shall ensure that arrangements and procedures are in place that warrants effective response and coordination with offsite response agencies, in case of a security event.
- Licensee shall ensure that proper communications and procedures are in place to provide offsite authorities with reliable information in case of a security event.

— Performance testing and exercises.
- Licensee shall conduct, in collaboration with response force, evaluations of the individual PP measures and of the PPS, including a timely response of the guards and response forces. Results of testing and exercises including significant deficiencies and action taken shall be documented and reported to the authority.

3.3. Technical measures

Based on the SNF storage choice (dry casks or pool), Licensee shall store SNF within one or more protected area (PA) or one or more vital area (VA) located inside a PA. Licensee shall provide storage area/s with appropriate equipment for detecting unauthorized intrusion, technical means and procedures to control access, and convenient provisions for response in case of unauthorized intrusion or any other security-related event.

3.1.1. Requirements related to protected area

Intrusion detection.

— The perimeter of the PA shall consist of a physical barrier and an isolation zone.
— PA shall be equipped by appropriate systems to detect and assess unauthorized intrusion of, or activities within the PA.
— The components of the intrusion detection and assessment systems shall be tamper indicating, self-checking, and provided by an uninterruptible power supply in order to be maintained in an operable condition in case of normal power absence.

— The PA shall be provided by adequate illumination that meets the PPS illumination requirements and allows an appropriate assessment of unauthorized intrusions of or activities within the PA. The illumination systems shall be maintained in operable condition.
— The PA perimeter shall be subject to continues surveillance and be protected by intrusion alarm system which is capable of detecting penetrations through the isolation zone and that is monitored in a central alarm station (CAS) and its backup assessment station.
— The All vehicles, personnel, packages, and materials entering the PA shall be checked for proper authorization and be subject to search to detect and prevent introduction of contraband or other prohibited items, before entry.
— Entry of vehicles into the PA shall be strictly minimized and limited to designated parking areas.
— Delay measures shall be designed and implemented to allow for a timely and appropriate response to any malicious act.

Access control.

— The number of access points into the PA shall be kept to the minimum necessary, and all points of potential access shall be appropriately secured and alarmed.
— Effective access control measures shall be implemented to the PA to ensure that only authorized personnel can gain access and unauthorized access will be detected and prevented.
— The PA access control means and measures shall be protected against compromise.
— A personal identification system and a controlled lock system shall be established and maintained to limit access to authorized individuals.
— Unescorted access to the PA shall be only limited to authorized personnel with predetermined trustworthiness.
— A log of individuals granted access to the PA shall be kept.
— All emergency exits in the PA shall be alarmed and secured by locking devices while allowing prompt egress during an emergency.

3.1.2. Requirements related to vital area

Intrusion detection.

— VA shall be equipped by appropriate systems to detect and assess unauthorized intrusion of, or activities within the VA.
  - VA shall be appropriately secured and alarmed when unattended.
  - The components of the intrusion detection and assessment systems shall be tamper indicating, self-checking and provided by an uninterruptible power supply in order to be maintained in an operable condition in case of normal power absence.
  - All vehicles, personnel, packages, and materials entering and leaving the VA shall be subject to search to detect and prevent unauthorized access, introduction of prohibited items and removal of nuclear material.
  - Access of private vehicles to VA shall be prohibited.
  - Licensee shall ensure detection of unauthorized acts by continuous surveillance, through the two-person rule or other equivalent means, whenever VA is occupied.
  - SNF storage area shall be hardened, locked, and alarms activated except during authorized access to the material.
  - Timely detection of tampering or interference with VA equipment, systems, or devices shall be provided, and during the maintenance period, strict access control to VA shall be maintained. Searches and testing shall be conducted to detect any tampering that may have been committed during maintenance.
  - VA shall provide delay against unauthorized access to allow for a timely and appropriate response to a malicious act. Delay measures shall be designed considering both insider's and external adversary's capabilities and be balanced for all potential points of intrusion.
  - Vehicle barriers shall be installed at an appropriate distance from the VA to prevent the penetration of unauthorized land or waterborne vehicles that could be used by an adversary for committing a malicious act. Attention shall also be given to providing protection measures against any airborne threat.

Access control.

- The number of access points into the VA shall be kept to the minimum necessary. All points of potential access shall be appropriately secured and alarmed.
- Effective access control measures shall be implemented to VA to ensure that only authorized personnel can gain access and unauthorized access will be detected and prevented.
- VA access control means and measures shall be protected against manipulation, falsification, or other forms of compromise.
- The number of authorized persons entering the VA shall be kept to the minimum necessary.
- The identity of authorized persons entering the VA shall be verified.
- Persons with authorized access to the VA shall be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined shall be provided access only when escorted by persons authorized unescorted access.
- Records of all individuals who access the VA or who have access to or possession of keys, keycards, and/or other systems, including computer systems which control access to the VA shall be established and kept.

3.1.3. Requirements related to protection against sabotage

- Licensee shall specify, in view of DBT information, credible sabotage scenarios by which adversaries, whether externals and/or insiders, could sabotage SNF or SNF storage facility, and submit these scenarios to the authority
- Licensee shall define equipment, structure, system or components, and/or material; the sabotage of which could directly or indirectly lead to high radiological consequences (targets).
- Licensee shall design a PPS that is effective against the defined sabotage scenarios and complies with the PP requirements.
- The PPS shall be designed to deny unauthorized access of personnel or equipment to the defined targets.
- The PPS shall be designed as an element of an integrated system to prevent the potential consequences of sabotage by taking into account the robustness of the engineered safety and operational features, and the fire protection, radiation protection, and emergency preparedness measures.
- The response strategy shall be based on denial of adversary access to the sabotage targets or denial of adversary task completion at the sabotage targets.

3.1.4. Central alarm station

- Licensee shall establish a constantly staffed CAS for alarms' monitoring and evaluation, response inception and communication with the guards, response forces, and facility management.
- Licensee shall establish redundant means that grantee continual CAS functions during emergencies, throughout a backup assessment station which is separated from CAS by means of distance and structural solutions.
- Information acquired at the CAS shall be handled and stored in a secure manner.
- The CAS shall be located within a PA and shall be hardened.
- Access to the CAS shall be strictly minimized and controlled.
- The CAS shall be provided with a timely means for alarms assessment, an uninterruptible power supply, and voice communication means (dedicated, redundant, secure, and diverse transmission systems for two way voice communication between CAS personnel, response forces and guards) for activities involving detection, assessment, and response.

3.1.5. Response planning

- Licensee shall afford a 24-hour guarding service and response forces to ensure an adequate and timely response to prevent an adversary from completing a malicious act.
- A security organization with well-defined responsibilities, sufficient personnel, and written procedures shall be established.

— Members of the security organization shall be adequately equipped, trained, qualified, and re-qualified to perform their assigned responsibilities in accordance with applicable national laws and regulations.
— Security staff shall be equipped with redundant communications capabilities allowing them to communicate with off-site security personnel.
— The CAS personnel and off-site response forces shall communicate at scheduled intervals.
— Written response procedures shall be established and maintained for addressing malicious acts.
— Response procedures shall be exercised on a periodic basis, to validate the readiness of the response force.

4. CONCLUSION

According to the Egyptian legislative and regulatory framework, authorization of nuclear facilities is one of the principal functions of ENRRA. Authorization requires review and assessment and inspections against the regulatory requirements. Therefore, regulations are required to establish nuclear security requirements for nuclear materials including SNF as well as nuclear facilities. Regulations should reflect the State's assessment of the threat and the potential consequences of malicious acts and State's approach to risk management by which it ensures that the nuclear security regime is capable of establishing and maintaining the risk associated with nuclear security events at acceptable levels through a risk-informed approach. The current work provides a proposal for security requirements of SNF.

REFERENCES

[1] COMMITTEE ON THE SAFETY AND SECURITY OF COMMERCIAL SPENT NUCLEAR FUEL STORAGE, National Research Council, Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report, The National Academies, Washington, D.C (2006)
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Storage of Spent Nuclear Fuel, SSG-15, IAEA, Vienna (2012).
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).
[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, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).
[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980).
[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10-GC (49)/INF/6, IAEA, Vienna (2005).
[9] EGYPT, Law no. 7, The law for Organizing Nuclear & Radiation Activities, Amiri Presses, Cairo, Egypt (2010).
[10] EGYPT, Executive Regulation of the Law no. 7, The law for Organizing Nuclear & Radiation Activities, Amiri Presses, Cairo, Egypt (2011).
[11] Egyptian Nuclear and Radiological Regulatory Authority, Classification Rules of Nuclear Materials and Radioactive Sources Form Nuclear Security Perspective, Egypt (2015).
[12] WINS International Best Practice, Guide Security of Spent Nuclear Fuel in Dry Storage (Revision 1.1), Vienna (2015).