**International Policies and Tools for Protecting Against**

**Radiological Sabotage**

*Leitch, R.1; Stanford, D.; 1Brigantic, R. 1*

1Pacific Northwest National Laboratory, Richland, Washington

*E-mail contact of main author:* *Rosalyn.Leitch@pnnl.gov*

**Abstract:** This paper provides a comprehensive overview of international policies and tools that can be used for protecting against radiological sabotage at nuclear and radiological facilities. This analysis is uniquely relevant for international nuclear security because there are few materials available which provide a broad overview of the policy and technical context associated with sabotage. The paper will be geared toward policy makers and managers who do not necessarily have a strong understanding or familiarity with the concept of sabotage and the roles and responsibilities of various stakeholders. Through describing the rising threat of non-state and unconventional actors, we provide historical context for the threat of nuclear terrorism and sabotage After providing historical context for the rising threat of sabotage, we describe several international policies and guidance documents geared toward addressing the threat of sabotage, including Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) and the Convention on the Physical Protection of Nuclear Material (CPPNM).

We describe and provide an analysis of the factors which influence the scale of sabotage threat, including material type and quantity, type of radioactive material release (single or sustained), and type of sabotage scenarios. Several potential sabotage scenarios which can be identified in a threat assessment or design basis threat include direct versus indirect attacks and a blended cyber-physical attack. Through highlighting the roles and responsibilities for the Competent Authority and site operator, the paper illustrates how respective authorities conduct threat assessments, determine thresholds for unacceptable and high radiological consequences, and identify vital areas within a site or facility which may warrant further protection. In addition, we analyze how regulators and operators can cooperate to implement mitigation measures or contingency plans in response to various sabotage scenarios.

Finally, the paper reviews several software tools used to analyze sabotage threats and consequences, including the U.S. Nuclear Regulatory Commission’s Radiological Assessment System for Consequence Analysis (RASCAL), Sandia National Laboratory’s Turbo Federal Radiological Monitoring and Assessment Center (FRMAC) software, the National Atmospheric Release Advisory Center’s (NARAC) HotSpot Health Physics code, and the Quick Look Radiological Assessment Methodology (QLRAM) developed by Pacific Northwest National Laboratory for the National Nuclear Security Administration.

**Key Words:** radiological sabotage, nuclear terrorism, international policy, software tool

# Introduction: The Threat of Nuclear Terrorism and the International Response

In September 2001, International Atomic Energy Agency (IAEA) Director General Mohamed ElBaredei stated that “the tragic terrorist attacks on the United States were a wakeup call to us all. We cannot be complacent. We have to and will increase our efforts on all fronts - from combating illicit trafficking to ensuring the protection of nuclear materials – from nuclear installation design to withstand attacks to improving how we respond to nuclear emergencies.” The September 11 attacks in New York City made it clear that the threat of large, well-organized global terrorist groups is serious and imminent. In addition to preventing terrorists from acquiring weapons-usable material, a central element of combatting nuclear terrorism is protecting nuclear facilities and materials from sabotage. [1] Radiological sabotage is any deliberate act directed against a nuclear facility or nuclear material in use, storage, or transport which could directly or indirectly endanger the health and safety of personnel, the public, or the environment by exposure to radiation or release of radioactive substances. [2] More specifically, nuclear power plants and spent fuel pools present the greatest risk for nuclear sabotage, as they have large concentrations of intensely radioactive material and allow possible scenarios for generating nuclear or chemical energy to disperse that radiation. Research reactors, nuclear and radioactive material transport shipments, and waste storage facilities may also present significant sabotage risks. While most physical protection systems are designed with redundant safety features to prevent an adversary from overcoming the security system, the possibility of a terrorist attack or insider sabotage scenario overcoming those systems is still a realistic threat. [3]

Other world leaders and organizations have acknowledged the grave threat of nuclear terrorism as well. United States President Barack Obama spearheaded an initiative for a global summit on nuclear security in 2010 as part of an effort to “secure all vulnerable nuclear material around the world within four years.” The goal of the summit process is to address the threat of nuclear terrorism by enhancing international cooperation to prevent the illicit acquisition of nuclear material by non-state actors such as terrorist groups and smugglers. The United States will host the fourth summit in 2016. Among other goals and deliverables, summit leaders have worked to promote ratification of the Convention on the Physical Protection of Nuclear Material, which calls for a stronger focus on prevention of sabotage at nuclear and radiological facilities. [4]

In July 2006, the United States and Russia established The Global Initiative to Combat Nuclear Terrorism (GICNT), an international partnership of 85 nations and four official observers who are committed to working individually and collectively to implement a set of shared nuclear security principles. The mission of the GICNT is to strengthen global capacity to prevent, detect, and respond to nuclear terrorism by conducting multilateral activities that strengthen the plans, policies, procedures, and interoperability of partner nations. The United States and Russia serve as co-chairs of the GICNT, and the Republic of Korea serves as coordinator of the Implementation and Assessment Group.

# International Policies and Guidance

The IAEA plays a key role in combatting nuclear terrorism and sabotage by drafting and implementing technical guidance to promote best practices internationally. The IAEA Nuclear Security Series of publications, and in particular *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5), address the objectives of a State’s physical protection regime. While previous revisions of INFCIRC/225 included information about protecting nuclear material and nuclear facilities against sabotage, Rev. 5 was the first revision to include reference to the key concept of defining thresholds for both unacceptable and high radiological consequences. Additional guidance related to sabotage in INFCIRC/225/Rev. 5 specifies that States should conduct an analysis for each nuclear facility to determine whether the radioactive inventory has the potential to result in unacceptable radiological consequences. Furthermore, the operator should identify equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to this condition as potential sabotage targets and protect them accordingly. [5] In summary, a State is to assess the potential radiological consequences of sabotage at a nuclear facility and determine if this potential exceeds the State’s unacceptable radiological consequences. These consequences are typically expressed as a release exceeding an established dose threshold at some distance from the facility, generally the site boundary. Unacceptable radiological consequences and levels may vary from State to State because each State’s competent authority is responsible for defining that threshold. [6]

Other IAEA guidance documents that focus on the threat of sabotage include:

* NSS-16, *Identification of Vital Areas at Nuclear Facilities*, presents a structured approach to identifying the areas that contain equipment, systems, and components to be protected against sabotage, particularly in high-consequence facilities.[7]
* NSS-4, *Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage*, provides guidelines for evaluating the engineering safety aspects of the protection of nuclear power plants against sabotage, such as a defense in depth approach to sabotage protection and self-assessment in cooperation with the competent authorities, for example. [8]

The Convention on the Physical Protection of Nuclear Material, which entered into force in February 1987, is the only legally binding international agreement focusing on the physical protection of peaceful-use nuclear materials. The original Convention on the Physical Protection of Nuclear Material applied only to nuclear material used for peaceful purposes while in international nuclear transport and did not apply to nuclear materials used for military purposes or to those used for peaceful purposes but not in international transport. Following the terrorist attacks of September 11, States expressed increasing security concerns related to large-scale terrorism. In order to address this concern, States initiated an amendment process that sought to expand the Convention's scope to cover the physical protection of nuclear material in domestic use, storage, and transport, and the protection of nuclear materials and facilities against sabotage. The amendment process also sought to facilitate cooperation among States and the IAEA to locate and recover stolen nuclear material. [9]

The International Convention on the Suppression of Acts of Nuclear Terrorism (ICSANT) entered into force in 2007 in response to several arguments that Convention on the Physical Protection of Nuclear Material did not adequately address the issue of nuclear terrorism. ICSANT establishes an international framework to combat nuclear terrorism and prevent the proliferation of weapons of mass destruction, including measures that will strengthen cooperation between States in the field of nuclear security, criminalize the planning and performing of nuclear terrorism, and provide a formal definition for nuclear terrorism. [10]

# Physical Protection of Nuclear Facilities Against Sabotage

As States and policy makers consider the threat of and prevention measures for sabotage, it is important that they understand several key concepts related to sabotage. Potential consequences of sabotage at a nuclear facility include radiological release, environmental contamination, injury to persons, loss of use of a facility, and potentially negative economic and political consequences. Sabotage threats for nuclear facilities can be classified broadly into two different categories. The first sabotage threat category is a direct access attack, or a threat posed to the nuclear facility by insiders or by outsiders who intrude into the facility (with or without insider assistance). In a direct attack, an adversary applies energy directly to the nuclear or radioactive material to cause dispersal, so the adversary must gain access to an area in which material is located. The second is an indirect or standoff attack, which is a threat that is initiated outside the plant boundary and does not require the presence of the adversaries on-site, such as shoulder launched missiles, vehicle bombs, and malicious aircraft impacts. In an indirect attack, the adversary uses energy present in the material or process system to cause dispersal, which requires initiating a process upset condition and disabling the systems designed to mitigate the upset. [11]

The State’s Competent Authority is responsible for coordinating with various stakeholders, including operators and intelligence organizations, to implement and maintain a comprehensive threat assessment procedure. As part of a comprehensive threat assessment, the Competent Authority should analyze and document each potential adversary scenario applicable to the State’s nuclear facilities, including those related to motivation, intention, and capabilities. [12] INFCIRC/225/Rev. 5 requires that a State establish a design basis threat (DBT) for Category I nuclear material facilities and facilities that could be sabotage targets. [13] The DBT document defines the threat characteristics against which the operator should provide protection. In regards to sabotage, the State competent authority uses the DBT and vital area identification process to design a physical protection system capable of preventing or neutralizing a sabotage scenario. [14] For all other nuclear facilities, such as Category II and III facilities, the State has the prerogative to choose whether it will use a formal DBT or just a threat assessment. One potential element of a threat assessment or DBT is the definition of an Insider Threat. An Insider is any individual with authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who could aid outsiders to do so. Other threat scenarios that the Competent Authority should consider during development of a threat assessment or DBT are a stand-off attack in which weapons such as rocket-propelled grenades and a computer-based attack which may compromise safety and security functions. [15]

As a key element of sabotage analysis, vital area identification is the process of identifying the areas in a nuclear facility around which protection will be provided in order to prevent or reduce the likelihood of sabotage. INFCIRC/225/Rev. 5 indicates that nuclear material in an amount which, if dispersed, could lead to high radiological consequences and a minimum set of equipment, systems, or devices needed to prevent high radiological consequences, should be located within one or more vital areas, and be located inside a protected area. [16] As indicated in Figure 1, a protected area should be inside a limited access area. It should also have a perimeter equipped with a physical barrier and a means of intrusion detection, have a limited number of access points, require search of vehicles or people entering the area, limit access to authorized people, and require random guard patrols. [17]



*Figure 1. Site Diagram, Including Limited Access, Protected, Vital, and Inner Areas*[18]

IAEA guidance recommends that States use a graded approach to physical protection against sabotage, under which the level of protection required at a facility should be related to potential level of radiological consequences. States must determine consequence levels for unacceptable radiological consequences, or the level above which implementation of physical protection measures is warranted, and high radiological consequences, the level above which vital areas must be identified and protected. Only certain types of facilities, such as Category I facilities and potential sabotage targets, require vital area identification and a high radiological consequence threshold. The physical protection measures appropriate for vital areas are highlighted in INFCIRC/225/Rev. 5, but States must specify their own protection requirements for facilities with consequences between unacceptable and high. [19]

The Competent Authority can define an unacceptable radiological consequence level based on a variety of factors including unacceptable dose level, unacceptable radioactive material release level, or unacceptable plant state. If a State’s unacceptable radiological consequences are identical with its threshold for nuclear safety considerations, the safety analyses performed for the facility could also be used for security analyses. [20] This guidance also assumes the worst case scenario in analysis of sabotage, so mitigation factors are not initially taken into account in determining the baseline threat of sabotage. Mitigation measures are considered part of the more comprehensive sabotage analysis outlined in INFCIRC/225/Rev. 5.

A sabotage threat analysis requires that the operator obtain an inventory of nuclear and radiological material on site, specifically noting the form, activity level, and location on site for each inventory item. Security personnel should coordinate with nuclear material accountancy and control personnel at a site to obtain accurate material inventories. The operator must evaluate whether the complete release of any or all inventories could exceed the unacceptable radiological consequences criteria. The operator must also identify critical safety functions and potential sabotage targets for the nuclear facility, such as shielding, criticality prevention, cooling, confinement, fire prevention, and structural integrity. [24] The operator must also analyze the site and installation characteristics, the elements of which may be sufficient to exclude or increase the likelihood of certain sabotage scenarios. A plant’s location in a mountainous area, for example, may limit the feasibility of a large aircraft being able to approach the site from the angle necessary to cause damage. [21]

The operator should look at the distance from each critical facility or vital area to the site boundary to understand the severity of potential radiological consequences at the site boundary. [22] Even further, the operator should consider the population density and weather patterns in the vicinity of the facility and other site characteristics which would influence the severity of consequences for a potential radiological release. [23] The operator must also consider the type and number of facilities at the site. A nuclear power plant, for example, may have several reactor units on site as well as other critical facilities such as spent fuel storage pools or dry cask storage. The design of a facility must be taken into account, as some facilities have built-in features to defend against design basis internal and external events such as fire, earthquakes, explosions, or aircraft impacts. Finally, the operator must consider off-site security measures which are independent of the facility. These could range from local law-enforcement capabilities in the vicinity to security measures in the aviation industry. While these will not affect a worst case scenario analysis, they may influence an analysis of mitigation measures. Upon completion of all the above activities, the operator should generate a report documenting the analysis for the Competent Authority’s approval. [24]

As part of the vital area identification process, the Competent Authority must identify any possible initiating events of malicious origin (IEMOs) that could lead to unacceptable radiological consequences as well as identify any IEMOs that exceed the capability of existing mitigation systems to protect against sabotage. Many of these IEMOs are addressed in existing safety analyses, so the Competent Authority should consider that before starting from scratch to identify IEMOs. For each IEMO, the Competent Authority and site operator should identify specific systems, structures, and components needed to mitigate negative consequences, particularly critical safety functions which would prevent a release of radioactive material. This evaluation will determine which components/systems require additional protection by locating them within a vital area. [25]

In addition to identifying mechanisms to protect against sabotage, the State and operator should coordinate closely to develop and implement detailed mitigation procedures for responding to acts of sabotage. NSS-13 explains that each should develop its own contingency plan including measures which focus on preventing further damage, securing the nuclear facility, and protecting emergency equipment and personnel. [26] The Competent Authority and operator should also develop an emergency plan which consists of measures to ensure the mitigation or minimization of the radiological consequences of sabotage as well as human errors, equipment failures, and natural disasters. [27]

A few key characteristics of an effective physical protection system for preventing and/or responding to a sabotage scenario include balanced protection, defense-in-depth, and reliability. There are many unique physical paths to each target at a facility. Because a system is only as effective as its weakest path, it is critical that operators provide adequate and balanced protection against all potential threats along all adversary paths. The goal of defense in depth is to establish a security system in which an adversary must defeat or avoid a number of protective devices in sequence in order to gain access to a vital area. An effective defense in depth strategy should increase an adversary’s uncertainty about the system, require more extensive preparations and equipment by an adversary prior to attacking system, and create additional steps through which the adversary may fail or abort the mission. Finally, reliability involves redundant equipment, such as multiple complementary sensors, central alarms stations, and response force locations. Competent Authority’s and operators should coordinate to conduct regular exercises of physical protection system effectiveness. This involves verifying that the physical protection system satisfies requirements, identifying system deficiencies, and analyzing system upgrades. [28]

# Tools for Analyzing Radiological Release and Consequences of Sabotage

A variety of useful tools exist for analyzing the threat and potential consequences of radiological sabotage. The Radiological Assessment System for Consequence Analysis (RASCAL) was developed for the U.S. Nuclear Regulatory Commission and is designed for use in the independent assessment of dose projections during response to radiological emergencies. RASCAL can be used by response personnel to conduct an independent evaluation of dose and consequence projections and for training and drills. RASCAL consists of seven tools, four of which are used for consequence assessment, and the remaining three for flexible scenarios such as reactor-specific assessments, simultaneous accidents, and assessment based on real-time meteorological observations and forecasts. [29]

Sandia National Laboratory’s Nuclear Incident Response Program provides research and technical solutions, expert analysis, and highly trained emergency response professionals to support the federal government's response to an accident or act of terrorism involving radiological, chemical, or biological material. Sandia developed the Turbo Federal Radiological Monitoring and Assessment Center (FRMAC) software program, a publicly available software tool which automates the calculations described in *The Federal Manual for Assessing Environmental Data during a Radiological Emergency*. Using values generated by field samples, instrument readings, or computer dispersion models, Turbo FRMAC assesses the generated results into values that are meaningful and useful for a decision maker at a radiological emergency. Turbo FRMAC provides calculated results to determine whether radiation values exceed city, state, or federal limits; whether crops can they be utilized after a release; whether residents need to be evacuated or sheltered in place; and how long emergency workers can safely work in a given area. [30]

The National Atmospheric Release Advisory Center (NARAC), a national support and resource center for planning, real-time assessment, emergency response, and detailed studies of incidents involving a wide variety of hazards, including nuclear, radiological, chemical, biological, or natural emissions, is located at the Lawrence Livermore National Laboratory and provides tools and services that map the probable spread of hazardous material accidentally or intentionally released into the atmosphere. [31] One particular software tool that NARAC developed is the HotSpot Health Physics code®, which was created to provide emergency response personnel and emergency planners with a fast, field-portable set of software tools for evaluating incidents involving radioactive material. The software is also used for safety analyses of facilities handling nuclear material. The HotSpot atmospheric dispersion models are designed for near-surface releases, short-range dispersion, and short-term release durations in unobstructed terrain and simple meteorological conditions. These models provide a fast and usually conservative means for estimation of the radiation effects associated with the atmospheric release of radioactive materials. HotSpot is publicly available, but users must register with NARAC before they are granted access to download the tool. [32]

While HotSpot is a valuable tool in analyzing incidents involving nuclear material, it can be rather time intensive to calculate each set of environmental circumstances and data independently. In 2015, Pacific Northwest National Laboratory developed a software tool called Quick Look Radiological Assessment Model (QLRAM) for the Department of Energy National Nuclear Security Administration Office of Global Material Security. QLRAM uses data sets generated from HotSpot but simplifies the process by generating results for a wide range of scenarios in a few seconds. It would take hours to generate these same results with HotSpot. The purpose of QLRAM is to provide a decision support tool for users to easily determine if a credible threat from a sabotage event exists or if the threat can be eliminated from further evaluation based on an initial worst-case estimate of dose rate related to material dispersed. In QLRAM, worst-case assumes all material is dispersed into the atmosphere by a conventional high explosive and no mitigation measures are in place. The primary intended users of QLRAM are international users who are not necessarily experts on conducting a sabotage analyses or the underlying source models. The data used in QLRAM is based on the HotSpot model, but the evaluation process is much simpler than using HotSpot because QLRAM synthesizes information into one process instead of requiring the user to input countless numbers of data sets to get the same result. In order to use the QLRAM tool, the user must determine his or her own unacceptable radiological consequences to plug into the tool and know the nuclear and radiological material inventory at the respective facility. [33]

# Conclusion

A central element of combatting nuclear terrorism is protecting nuclear facilities and materials from sabotage. As States and policy makers consider the threat of and prevention measures for sabotage, it is important that they understand the potential consequences of sabotage at a nuclear facility, including radiological release, environmental contamination, injury to persons, loss of use of a facility, and potentially negative economic and political consequences. State Competent Authorities and Operators rely heavily on international guidance to implement effective nuclear security measures designed to protect against sabotage. IAEA guidance such as INFCIRC/225/Revision 5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, plays a key role in providing guidance and best practices for states to protect against possible sabotage scenarios. Software tools such as HotSpot and QLRAM also facilitate more accurate analysis of sabotage scenarios for responsible stakeholders. While international guidance and relevant software tools provide an effective platform for States to develop and implement nuclear security programs to protect against sabotage, there is still a great deal that needs to be done to establish more robust international policies and tools which are both accessible and practical for relevant stakeholders. The IAEA can play a key role in promoting best practices and facilitating international collaboration to develop these policies and tools.

**REFERENCES**

[1] Bunn, M. and G. Bunn, Reducing the Threat of Nuclear Theft and Sabotage, Symposium on International Safeguards Verification and Nuclear Material Security, Vienna, Austria, International Atomic Energy Agency. (2001), Vol: 367: p. 18.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 1.1, p. 18.

[3] Bunn, M. and G. Bunn, Reducing the Threat of Nuclear Theft and Sabotage, Symposium on International Safeguards Verification and Nuclear Material Security, Vienna, Austria, International Atomic Energy Agency. (2001), Vol: 367: p. 18.

[4] ARMS CONTROL ASSOCIATION, “Nuclear Security Summit at a Glance,” (April 2014), Retrieved 20 March 2015 from <http://www.armscontrol.org/factsheets/NuclearSecuritySummit>.

[5] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities. INFCIRC/225/Revision 5 (2013), Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf>.

[6] Brigantic, Robert et.al., U.S. National Nuclear Security Administration, Quick Look Radiological Assessment Model (QLRAM) - User’s Guide and Documentation v1.0 (January 2015).

[7] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities (2012), Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[8] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (2007), Retrieved 20 March 2015 from <http://www-pub.iaea.org/books/IAEABooks/7574/Engineering-Safety-Aspects-of-the-Protection-of-Nuclear-Power-Plants-against-Sabotage>.

[9] Convention on the Physical Protection of Nuclear Material (CPPNM), NUCLEAR THREAT INITIATIVE, Retrieved 21 March 2015 from <http://www.nti.org/treaties-and-regimes/convention-physical-protection-nuclear-material-cppnm/>.

[10] Kane, Sam and Reif, Kingston, Fact Sheet: The 2005 Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) and the International Convention on the Suppression of Acts of Nuclear Terrorism (ICSANT), Arms Control Association, Retrieved 21 March 2015 from <http://armscontrolcenter.org/fact-sheet-the-2005-amendment-to-the-convention-on-the-physical-protection-of-nuclear-material-cppnm-and-the-international-convention-on-the-suppression-of-acts-of-nuclear-terrorism-icsant/>.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 4.1., p. 5.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 5.1, p. 4-7.

[13] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities. INFCIRC/225/Revision 5 (2013), Section 3.37, p. 13, Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf>.

[14] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities (2012), p. 8, Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 5.1, p. 6-16.

[16] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities (2012), p. 8, Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 6.1, p. 8.

[18] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities. INFCIRC/225/Revision 5 (2013), Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf>.

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 6.1, p.3.

[20] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities (2012), p. 6, Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[21] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (2007), p. 9, Retrieved 20 March 2015 from <http://www-pub.iaea.org/books/IAEABooks/7574/Engineering-Safety-Aspects-of-the-Protection-of-Nuclear-Power-Plants-against-Sabotage>.

[22] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (2007), p. 9, Retrieved 20 March 2015 from <http://www-pub.iaea.org/books/IAEABooks/7574/Engineering-Safety-Aspects-of-the-Protection-of-Nuclear-Power-Plants-against-Sabotage>.

[23] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities (2012), p. 8, Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[24] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (2007), p. 9, Retrieved 20 March 2015 from <http://www-pub.iaea.org/books/IAEABooks/7574/Engineering-Safety-Aspects-of-the-Protection-of-Nuclear-Power-Plants-against-Sabotage>.

[25] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities (2012), Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[26] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities. INFCIRC/225/Revision 5 (2013), p. 18, Retrieved 20 March 2015 from <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf>.

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 0.2, p. 13.

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Regional Training Course on Protection of Nuclear Facilities against Sabotage (2014), Vol. 2.1, p. 15-19.

[29] U.S. NUCLEAR REGULATORY COMMISSION, RASCAL: Radiological Assessment System for Consequence AnaLysis (2015), p. 2.

[30] SANDIA NATIONAL LABORATORIES, National Incident Response Program (NIRP) (2014), Retrieved 17 Feb 2015 from <https://nirp.sandia.gov/Software/TurboFRMAC/TurboFRMAC.aspx#Overview>.

[31] National Atmospheric Release Advisory Center, NARAC Overview (Sept. 2012), Retrieved 3 March 2015 from <https://narac.llnl.gov/narac_overview.html>.

[32] National Atmospheric Release Advisory Center, HotSpot Health Physics Codes for the PC (May 2013), Retrieved 3 March 2015 from <https://narac.llnl.gov/HotSpot/HotSpot.html>.

[33] Brigantic, Robert et.al., U.S. National Nuclear Security Administration, Quick Look Radiological Assessment Model (QLRAM) - User’s Guide and Documentation v1.0 (January 2015).