Risk– Based Approach for Security Management

D.R. Ek

Sandia National Laboratories (SNL), Albuquerque, NM, USA

drek@sandia.gov

Abstract. Developments in the approach to nuclear security over the past 45 years have resulted in a much more sophisticated, methodical, and systematic discipline. The efforts behind these developments were inspired by several security and safety events that occurred over this time period, and the resulting approach is for a large part a product of these events.

This paper will outline the relationship between these events and the resulting security development, and will describe the resulting risk-based nuclear approach to security management.

1. Introduction

Nuclear security addresses two specific global concerns: (1) the initiation of unacceptable radiological consequences through the intentional, malicious dispersal[1] of nuclear and/or other radioactive materials and (2) the unauthorized removal of nuclear and/or other radioactive materials with the intent to construct a weapon of mass destruction. Thus, a properly established nuclear security program simultaneously addresses program objectives that are shared with nuclear safety and program objectives that are shared with nuclear safeguards. In fact, nuclear security is a necessary complement to both of these global programs in order to ensure that the societal benefits of nuclear/radioactive materials are preserved by protecting the public against adversary-induced unacceptable consequences.

Currently, the international community places significant emphasis on the implementation of a robust nuclear security regime. For those not intimately involved with nuclear security, the basis for this emphasis may not be obvious; however, it is clearly demonstrated by:

- the large number of international instruments that highlight obligations/responsibilities and/or provide guidance to States with respect to their nuclear security programs;
- the availability of international conferences and training courses focused on nuclear security;
- the popularity of IAEA nuclear security missions and guidance documents; and
- the number of donor States investing significant capital and resources to promote the global strengthening of nuclear security.

This presentation provides a background of what led to the international emphasis on nuclear security and describes how nuclear security is effectively implemented so as to preserve the societal benefits of nuclear and radioactive materials.

2. What is Nuclear Security?

Security is not a new field developed only in response to the nuclear age. Security has existed as long has mankind has had property to protect. Security was historically achieved by the rather brute-force

[1] Such as a sabotage of the reactor

approach of "gates, guns, and guards". However, over the past 45 years, this traditional approach has been studied and refined into a more sophisticated, systematic, integrated security approach that not only incorporates consequence severity assessment and risk management approaches but also includes a methodology for estimating security effectiveness.

As mentioned, the objective of nuclear security[2] is to prevent unacceptable consequences resulting from intentional, malicious acts involving nuclear or other radioactive materials. Nuclear security accomplishes this by pursing a philosophy of separating potential adversaries from areas where unacceptable consequences could be initiated[3]. The focus of adversaries who are attempting a malicious act could be the nuclear or radioactive material, or it could be the equipment, structures or systems, the disablement of which could indirectly result in unacceptable consequences. The collection of these materials, equipment, structures and systems to which an adversary would focus their malicious acts are called "targets". Separation of adversary and targets is achieved by surrounding the target areas with a continuous layer(s) of security measures that collectively comprise a nuclear security system.

Every effective security system possesses three fundamental capacities:

1. Reliably ***detect*** an undesirable activity in order to alert those who would respond,
2. ***Delay*** the progression of an undesirable activity long enough to permit those alerted to respond, and
3. Effectively ***respond*** to an undesirable activity so as to prevent its completion.

A successful security system is one that surrounds targets with effective and integrated detection and delay measures, which provides a continuous security boundary around the targets. Effective detection measures reliably alert responders of any adversary activity early in the scenario development; while delay measures, which are only effective after detection occurs, slow the progress of the adversary's activity for a sufficiently long time to permit security responders to organize, travel, deploy, and effectively stop the malicious activity. In this sense, detection and delay measures need to be coordinated with response measures in a systematic manner. The overall effectiveness of the resulting security system is defined by: (1) the individual robustness of each of these three fundamental capacities (detection, delay, response) against the adversary, (2) the efficiency of integration of these three capacities for all adversary scenarios, and (3) the effectiveness of the systematic approach to security management, which includes quality controls.

3. Background: Where did the emphasis on nuclear security originate?

The euphoria that accompanied the "Atoms for Peace" initiative of the 1950's and early 60's obscured nuclear security considerations. During this time, the design and construction of research reactors was limited to the optimization of their intended operations. However, beginning in the late 60's and early 70's, concerns about the security of nuclear material began to arise due to changes in the global threat

[2] INFCIRC225/Rev5-NSS#13 uses the term "physical protection" when referring to nuclear security of nuclear material and nuclear facilities; whereas, NSS#14 uses nuclear security when referring to radioactive materials or associated facilities and activities. This paper is focused on research reactors and associated facilities, which are subject to both NSS#13 and NSS#14. In this paper, the term "nuclear security" will be employed rather than "physical protection" to refer to nuclear security of nuclear material and nuclear facilities under regulatory control.

[3] This approach is most relevant to outsider adversaries. For insiders, the approach is a bit more complex, involving means to detect malicious actions.

environment, based particularly on incidents of politically oriented terrorism. In October of 1970, a nuclear bomb threat was made to blow up a major city unless a ransom was paid. The threat was accompanied by a drawing of the device. The drawing had merit, and the ransom was nearly paid. The threat turned out to be a hoax; however, the event caught the attention of leaders around the world. Near the end of 1971, in response to concerns by several Member States and motivated by malevolent activities of several militant groups around the world[4] combined with reports on the effects of radiation[5] and on the ease with which a nuclear explosive device could be constructed[6], the Director General of the IAEA invited security experts to develop the first international security recommendations. The resulting document, "Recommendations on the Physical Protection of Nuclear Material," was published by the IAEA in June 1972; however, the document was only shared upon written request, due to concerns by some that the document infringed on State sovereignty. This document dealt with the primary concern of theft of nuclear material for use in an improvised nuclear device and was seen as a supplement to Nuclear Safeguards. It was not long after the release of the document, however, that the concerns limiting document distribution seemed to diminish; perhaps, in part due to the worldwide live coverage of the hostage events during the Munich Olympics in July of 1972. In 1975, a revised version of this first document, which focused mainly on nuclear material theft (but also first mentioned sabotage), was published as INFCIRC225. This was followed by the development of the International Convention on the Physical Protection of Nuclear Materials in 1980, an undertaking with legally binding measures to prevent and punish offenses related to nuclear material.

Subsequent events, such as truck-bomb attacks on buildings, suicide bombers in public locations, the Chernobyl accident, and nuclear material trafficking in the early 1990's led to steady increases in the attention given to nuclear security for the prevention of theft or sabotage. The attacks on the World Trade Center in New York on September 11, 2001 prompted the development of several international nuclear security instruments, an even greater emphasis on nuclear security at the IAEA (including a much stronger emphasis on sabotage), and a greatly increased level of assistance offered by donor States. Further, the attacks of September 11th served as the catalyst for concerns about the security of radioactive materials.

In parallel to the increased attention on nuclear security over these years, the concepts and approaches to nuclear security were incrementally developed and improved. This included the introduction of design basis threats, a more structured approach to sabotage analysis, methods to effectively address insider adversaries, a quantified and performance-based system vulnerability assessment approach by which benefits of proposed improvements can be measured, and a security risk management approach to inform decision makers. As a result, we now have a mature, structured, and systematic approach to nuclear security that includes both security responsibilities and the coordination of State bodies and operator organizations under a nuclear security regime.

The nuclear security approach now considers the contribution of technical and administrative security measures to achieve the fundamental security functions of detection, delay, and response in an integrated and balanced manner that serves to both deter and prevent theft or sabotage. The approach incorporates a graded philosophy, whereby more attractive targets are afforded more robust security. Finally, the

[4] Such as: the Red Army Faction, the Red Brigade, the Provisional Irish Republican Army, etc
[5] Influenced by, among other events, the atmospheric nuclear tests of the USA and USSR
[6] Nuclear Theft: Risks and Safeguards, Willrich and Taylor, 1974

nuclear security approach now provides a validated performance-based methodology that enables site operators and State authorities to assess the effectiveness of the security system against credible adversary threats, thereby providing confidence that the security system is both appropriate and adequate.

4. Structured, Systematic Approach to Nuclear Security

This systematic, performance-based approach lends itself to establishing risk-informed security levels for a research reactor facility. Potential security risks posed by a research reactor and its associated facilities can be assessed by understanding:

(1) the potential radiological consequences of intentional malicious acts,
(2) the ease with which consequences can be intentionally initiated,
(3) the ability to which these consequences can be mitigated, and
(4) the effectiveness of the security system in preventing malicious acts or in complicating the ease of initiating such acts.

Once understood, security risks can be "managed" by increasing or decreasing the robustness of the nuclear security system. By modifying the components of the system and measuring estimated risk changes, one can optimize the parameters that affect achievement of an "ideal" security system. These parameters are:

- the risk posed by security threats (adversaries),
- the costs of installing and operating a nuclear security system to adequately mitigate these risks, and
- the operational impacts of specific security measures.

A nuclear security system has several characteristics. These characteristics will be discussed in the succeeding sections to provide insight into the systematic approach to security that was developed in response to the increased concerns.

4.1 Nuclear Security Targets

Targets through which an adversary would intend to initiate unacceptable consequences include not only nuclear and radioactive material but also include those operations, systems, equipment, or structures that collectively ensure that unacceptable radiological consequences cannot occur during the operation of a nuclear facility.

Safety analysis is conducted to identify initiating events that could upset safe facility operations and addresses mitigating safety systems that would prevent subsequent unacceptable consequences. It is tempting to assume that these credible, identified initiating events and the safety systems that mitigate their consequences would define a complete set of sabotage targets. However, due to the intentional nature of security events and the ability of an adversary to upset or defeat systems that might not otherwise be possible or credible in an accidental or unintentional manner, and due to the introduction of external energy (e.g. explosives) that could exacerbate consequences of dispersal, it is a mistake to assume that a safety analysis has identified the complete set of security-related sabotage targets. A separate sabotage analysis is required to review and build upon the existing safety analysis, as appropriate, so that all credible adversary sabotage scenarios are identified.

4.2 Balanced Security

An adversary will likely select the scenario, time, path, and target(s) that best meet their objective and that provide their perceived highest probability[7] of success. Therefore, the security system must be balanced across the security layer that surrounds the target so that the probability of detection, delay time, and response effectiveness remains the same whatever scenario, time, path, and target are selected by the adversary. Accomplishing balanced security can be quite difficult, as the security layers typically will include diverse structures and barriers (i.e., walls, ceiling, floor, doors, windows, fences, gates, vents, etc.). Maintaining uniform detection and penetration delay across these structures and barriers for a given adversary can be complex. Access control systems for entry/egress points across a layer can be particularly difficult to address when achieving balance, as these must often address the competing criteria of minimizing detection and delay of authorized personnel, and maximizing detection and delay for unauthorized personnel. Therefore, security strives to minimize the number of entry/egress points to restricted areas in order to facilitate balance across the security layer.

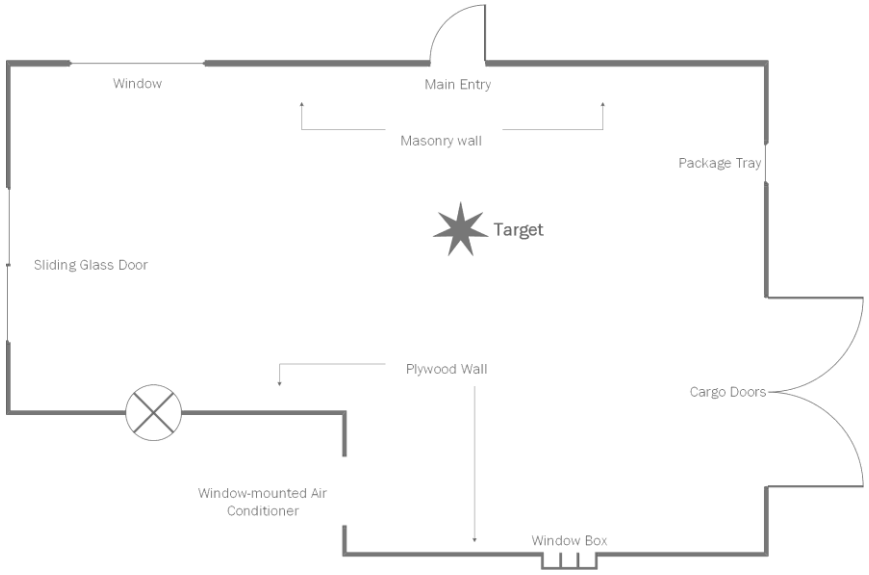

Figure 1: Example of a security layer surrounding a target that is composed of diverse barriers

4.3 Threat-Based Security

The confidence that an undesirable activity will be detected, delayed, and/or appropriately responded to depends on the capabilities of the adversary undertaking the activity. A security measure that will adequately and reliably detect one adversary with high confidence may completely fail against an adversary with different capabilities. This is also true for barrier delay times and response force neutralization effectiveness. Therefore, a full understanding of the capabilities of the expected adversary as well as customizing the security system to address these capabilities is necessary to develop an effective security system.

Unfortunately, adversaries are numerous and diverse, and their characteristics are ever changing. Due to this, the nuclear security community has pursued development of State-specific regulatory threat criteria,

[7] Probabilities used in this paper may only be known imprecisely and perhaps even ambiguously, such as when one speaks, for example, about a low probability

in which the capabilities of a *hypothetical* adversary[8] are described. For nuclear facilities, this description is typically known as the Design Basis Threat (DBT), but more simplified threat-based criteria, known as a "threat statement", can also be employed. The DBT or threat statement is based on the State's threat assessment.

4.4 Robustness of Security Measures

The effectiveness of a detection measure relates to its appropriateness within the expected environment, the probability that it will detect the hypothetical adversary capabilities, and the quality of its installation and maintenance.

The probability that a detection measure will detect an adversary's activity can be determined by analysis and testing of the actual detection measure (e.g. equipment or procedure), in the actual environment, against expected adversary scenarios employing defined adversary capabilities.

The time that is required for an adversary to defeat a delay measure should be assessed for multiple credible defeat methods by conducting an analysis of barrier characteristics and by performing tests. The analysis and tests are completed assuming adversary capabilities as outlined in the DBT or threat-based criteria.

The time required for a response force to assemble, transport, and tactically deploy at the target location can be measured by conducting response time tests under varied operational situations. The robustness of the deployed response force to permanently stop the adversary activities can be estimated using analysis tools, such as tabletop exercises and force-on-force engagement techniques. These analysis tools assume adversary capabilities as described in the DBT or threat-based criteria.

In each case, the robustness of the security measures requires an understanding of adversary capabilities as defined in the State's DBT or threat-based criteria.

4.5 Integration of Detection, Delay and Response into a Security System

An effective security system requires that all technical and administrative security measures supporting detection, delay, and response capacities be integrated into a cohesive system. This requires that:

- adequate and reliable detection of a adversary's malicious act before any adversary delay barriers;
- total adversary task including delay times (for every credible adversary scenario) exceed the total security response time (i.e., time required to communication to the response force as well as assembly, transport, and deployment of the response force); and
- a responding security force that is sufficiently trained, deployed, and equipped to subdue or otherwise stop the adversary from completing its malicious act.

Figure 2 below depicts an adversary scenario with barriers and sensing elements that would be encountered.

[8] To simplify discussion, we will refer to the "adversary" with the assumption that the hypothetical adversary may consist of a group of several people, possibly including insiders who have access to the facility.

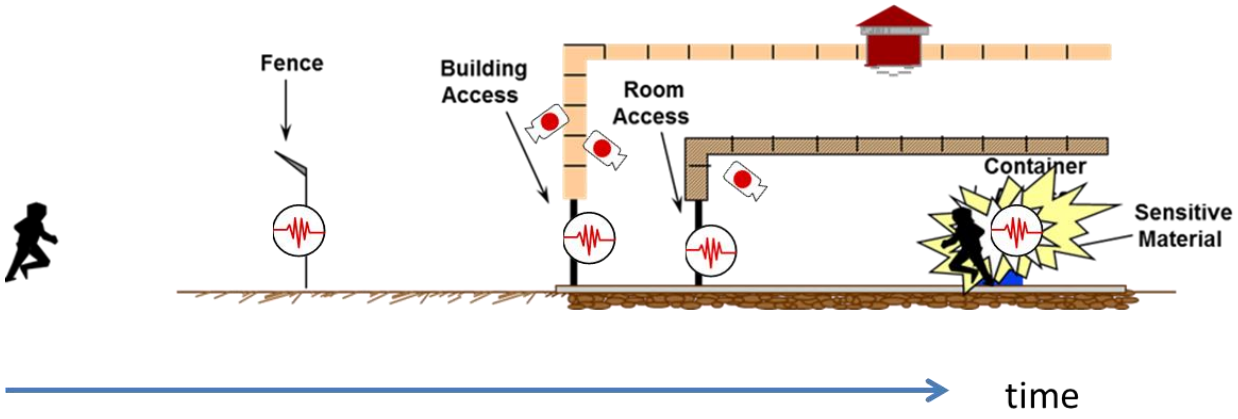

Figure 2: Adversary scenario with detection and delay measures along the path

The overall effectiveness of a security system is complex to measure, but it can be estimated by measuring the specific effectiveness of the security system against individual adversary scenarios. The key metric to effectiveness of a security system against an adversary scenario is the cumulative probability that the adversary's activities are detected and reliably communicated to the response force in a timely manner (i.e., in time to permit an adequate response to arrive and stop the progress of the adversary's scenario prior to its completion). So, a security system is deemed "effective" against a specific adversary and scenario IF this cumulative probability is adequate (e.g., exceeds a minimum threshold as defined by the State). This minimum threshold can be a qualitative or quantitative level.

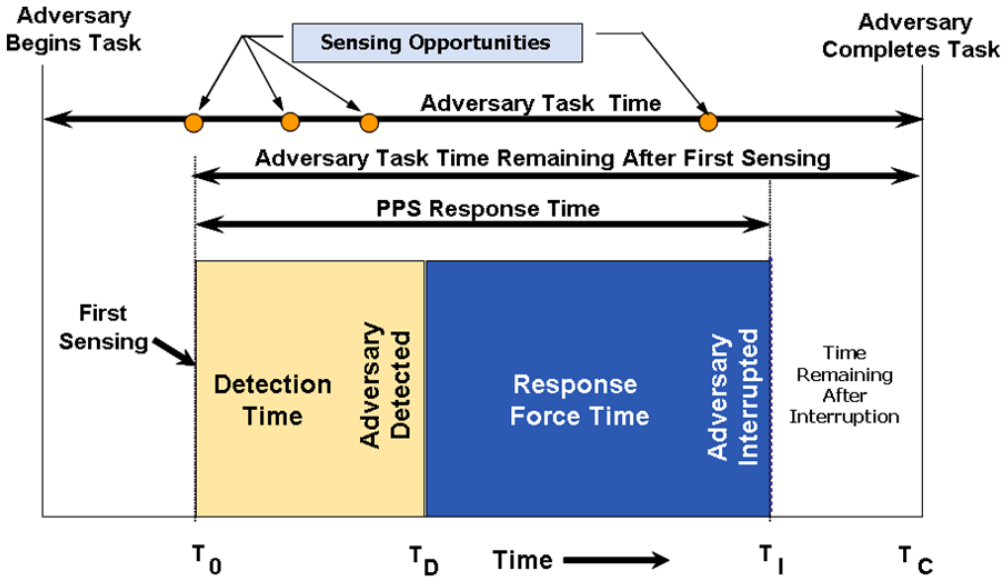

Figure 3: Adversary scenario timeline diagram illustrating the timely detection

Figure 3 translates the adversary scenario in Figure 2 into a timeline to look at what are called sensing opportunities where detection could occur, the delay time for the adversary, and the time for response

forces to deploy. The last moment at which the response force must be notified in order to interrupt the adversary (so as to have a chance at stopping them) is depicted by T_D (because T_D is the last instant when a notification to response will result in timely response to interrupt the adversary). The first three sensing opportunities preceded T_D and, therefore, are timely; whereas, the forth sensing opportunity is too late to initiate a response to stop the adversary. This indicates that the metric for determining the effectiveness of the security system against this particular adversary scenario is the cumulative probability of detection at only the three timely sensing opportunities. If this cumulative detection probability exceeds the State's minimum threshold, then the specific system effectiveness for this scenario is deemed adequate. By assessing the security effectiveness over a suite of challenging scenarios, an overall conservative estimate of security effectiveness can be made.

To ensure the proper effectiveness of the security measures within the system, an adequate security infrastructure of maintenance, training, and component testing needs to be established, implemented, and maintained. This security infrastructure is typically supported by a security management system that ensures quality and promotes an effective security culture.

5. Security Management

The technical and administrative security measures that lead to the detection, delay, and response are a necessary component of the site's nuclear security regime--but they are not the only components. A nuclear security management system represents the overall security effort at a site, and encompasses not only the operation of the security system but also the infrastructure to assure that the system is and continues to be effective. Elements of the security management system include:

- Policies and programs to operate, maintain, and test security systems and components;
- Security system installed and security personnel to operate it
- Security procedures needed to operate and maintain the security system;
- Security training to ensure personnel competence;
- Analysis of consequence severity due to a security event (and identification of security targets);
- Programs to ensure effect security system performance against regulatory requirements;
- Security plans to address security events;
- Quality assurance program to continuously review security-related programs to ensure that they are effective; and,
- Coordination with other entities within the facility and with security stakeholders outside of the facility; and,

The nuclear security management also includes policies and actions that foster a strong security culture within an organization.

6. Nuclear Security Risk Management

Any adverse nuclear security event is undesirable, but not all undesirable events are severe enough to justify the expenditure of security resources to prevent their occurrence. There is a threshold of severity of undesirable events above which it is prudent to invest resources to prevent or reduce the probability of their occurrence. This threshold divides 'undesirable' consequences from 'unacceptable' consequences. The threshold between undesirable and unacceptable is a State decision.

Further, not all unacceptable consequences are equally severe and, therefore, not all unacceptable consequences warrant the same investment of security resources to prevent them. A graded approach to the application of security resources should be taken to ensure that the investment in security resources is commensurate with the consequence severity. The graded approach is a primary tool in the management of risk.

6.1 Nuclear Security Risk

Along with a structured approach to nuclear security, an understanding of security risks is important to ensure that resources are appropriately allocated to protect the public from adversary-induced unacceptable consequences.

The risk of a nuclear security event to society is influenced both by the probability of the event's occurrence and by the severity of the resulting consequences.

Security Risk = (Consequence Severity) x (Probability of Consequence Occurrence)

The probability of consequence occurrence resulting from malicious activity is, in turn, a function of the probability of an adversary attempt and the probability that the adversary succeeds in the attempt (or the probability that the security system does not succeed).

Likelihood of Consequence Occurrence =	*(Likelihood of Adversary Attempt) x (Likelihood of Adversary Success if Attempted)*

The probability of an adversary attempt depends completely on the dedication and motivation of the adversary, but it is also heavily influenced by their perceptions of the consequence severity and their belief that these consequences can be achieved. Motivation, dedication, and perception are very difficult to predict with any confidence or estimate with any precision; however, this probability can, in theory, be reduced both by sharing with the public that security systems are robust, and by restricting communication that implies high severity consequences or system vulnerabilities. It is for this reason that the security community would like to classify any information that implies potential for severe consequences or indicates potential vulnerabilities.

The probability of adversary success if attempted is 1 – the probability of security system success. This component of risk is far easier to estimate and control. As mentioned above, the probability of security system success is estimated as the probability of timely detection and communication to capable response forces.

It can be useful to numerically estimate security risk in order to understand the degree to which a facility possess liability, to compare the risk of different facilities, and to measure the value and benefit of the existing security system on risk reduction. The mathematical representation of numerical security risk is estimated to be:

Security Risk	=	*(Severity of Consequences) x (Probability of Adversary Attempt) x (1 – Probability of Security System Success)*

Developing numerical estimates for the factors of security risk, however, can be more complex and involve more uncertainty than those of safety. This is essentially because a security event is intentional (and intentions can be rational or irrational), consequences encompass more than just those of safety, and system effectiveness is complex and difficult to represent with a single number. This complexity leads to the concept of conditional risk.

Conditional risk recognizes that estimates of adversary attempt probability and therefore excludes this factor. It instead composes a "conditional" security risk that provides insight into the security risk at a facility IF an adversary with capabilities as described in the DBT were to make an attempt. The equation which represents this conditional security risk is:

Conditional Security Risk ≈ (Severity of Consequences) x (1 – Probability of Security System Success)

It is this conditional risk equation that is employed to provide insight into security risk.

6.2 Risk-Based Security Management

Information concerning risks can be used to influence approaches to achieve adequate security. By incorporating risk information of facility targets, management is able to optimize the use of security resources to maximize overall facility risk minimization. Use of risk-based security management provides value by:

- Increasing security effectiveness to reduce all facility risks to acceptable levels.
- Balancing risk levels across all facility targets
- Re-assessing the risk if targets, threats, facility security, consequence severity or thresholds for acceptable levels of risk change.

7. Summary

Security is an integral part of ensuring that the societal benefits of nuclear and radioactive materials can be enjoyed without the fear of unacceptable consequences. Security-related events over the past 45 years have necessitated an improvement in nuclear security sophistication to ensure that the risk of a security event involving nuclear or radioactive materials is minimized. This improvement is a result of collaboration by international community, and has resulted in a mature, systematic, and structured approach to nuclear security management. The improvements enable the international community to have confidence that nuclear security risks are addressed in an optimal manner: risk minimized, benefits achieved, and costs optimized.