

**A Regulators Systematic Approach to Physical Protection for
Nuclear Facilities**

Stephan Bayer, PhD., Nicholas Doulgeris and Andrew Leask
Australian Safeguards and Non-Proliferation Office

Contracting, designing and construction are the large and obvious tasks when building new nuclear facilities. It could be easy to leave the less glamorous work of protecting nuclear facilities and nuclear materials until a time when the project is well advanced; but this would be a costly mistake. So, drawing on Australia's current experience of building a replacement research reactor near Sydney, this paper outlines the framework for a physical protection regime which needs to be incorporated into the design and construction phases of the nuclear facility. This is a risk based methodology which takes a whole-of-government approach.

Specifically, this paper considers:

- The consequences of malicious activity that are unacceptable to stakeholders, and
- The management of risk.

The methodology presented here offers the regulatory authority a rigorous, analysis based and defensible assessment and approval process.

To begin with, let me summarise the process. Nuclear facilities must have security which is effective and affordable. To this end, there are 7 basic steps: (1) determine the threat (2) determine an acceptable

level of risk (3) assess targets and rate the consequences of an attack on these targets (4) assess the resulting likelihood of success of the terrorist or insider and calculate the risk (5) evaluate remedial measures and re-check the risk (6) design and implement the security system, and (7) review the results regularly throughout the life cycle of the facility.

In the beginning

Physical protection considerations came during the life of Australia's present research reactor whose origins date back to the early 1950s. Consequently some measures were "add-ons". As a result, from the inception of the Replacement Research Reactor Project, when the design specification was being drafted, the Australian Safeguards and Non-Proliferation Office, ASNO, was involved—pressing for a comprehensive, detailed and costed approach to physical protection. This was a unique opportunity not to be missed.

Although the reactor is not complete yet, it is clear that involvement by the nuclear safeguards regulator from the outset will result in a highly effective, robust, security system at the new nuclear facility. Further, this security system will cater for the way in which the facility will be operated. The security system is comprehensive, involving policies, procedures, human resources and technology, many parts of which have to be considered from the outset if they are to be effective, while some elements have to be built into the fabric of the facility at an early stage. It is never too early to start security planning. Indeed, given that security and physical protection considerations will affect facility design—buildings, possibly location and the site itself—it is essential that security is viewed as a fundamental design requirement of equal status to safety, with which it has a symbiotic relationship.

While Australia is building a research reactor the principles espoused

in this paper are applicable equally to nuclear power reactors.

A Whole of Government Response

Australia takes a national, whole of Government approach to the protection of critical infrastructure which is coordinated by the Attorney Generals Department. Evaluation of security at the Replacement Research Reactor is evaluated using this organisational structure to ensure consistency and comprehensiveness across the whole of government. Within this framework, ASNO has managed an inter-agency process to ensure that the requirements of all stakeholders— ARPANSA¹, EMA², Health Authorities, the reactor operator and users—are satisfied.

The national approach in Australia is one based on risk analysis about which I will say more later.

Consequences other than the release of radiation are not considered by ASNO. Economic consequences, loss of confidence in government through denial of services to the community are assessed by Departments other than ASNO, although ASNO may advise on the likelihood of occurrence.

Modelling Tools

The security starting point is the physical protection model developed by the US DOE and the IAEA, which Australia has modified to suit its particular requirements and its broader methodology for the protection of critical infrastructure. Detailed guidance is supplemented by IAEA document INFCIRC225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities.

¹ Australian Radiation Protection and Nuclear Safety Agency

² Emergency Management Australia

Further guidance is obtained from Government policy documents, State and Territory authorities, security and risk assessments.

A key element arising from INFCIRC225/Rev.4 is use of the DBT—design basis threat—methodology. This offers a rigorous evaluation of realistic threats that the system should be designed to cope with. ASNO looks out over a period of some 15 years when setting the DBT. Using this approach, ASNO, in conjunction with the operator or licensee, has been able to develop a flexible, graduated security response built on a core system with a strong baseline capability.

A Risk Based Approach

We all manage risks everyday. Hazards such as lighting strikes, infectious diseases, traffic accidents, crime and accidents in the home confront all of us regularly, and intuitively we give them varying degrees of attention.

But more analytically, what is risk? It is a measure of potential hazards. Further, risk is a product of the probability that an adverse event may take place and the severity of the consequences should it occur.

Taking a whole of government approach, ASNO uses the following risk matrix which is the same as that used in Australian National Counter-Terrorism assessments.

RISK		CONSEQUENCE						
		Negligible	Insignificant	Minor	Moderate	Major	Extreme	Catastrophic
LIKELIHOOD	Certain	Medium	Medium	High	High	V High	V High	Extreme
	V High	Low	Medium	Medium	High	High	V High	V High
	High	Low	Low	Medium	Medium	High	High	V High
	Medium	V Low	Low	Low	Medium	Medium	High	High
	Low	V Low	V Low	Low	Low	Medium	Medium	High
	V Low	Neg	V Low	V Low	Low	Low	Medium	Medium
	Negligible	Neg	Neg	V Low	V Low	Low	Low	Medium

The aim here is to identify the events that could cause adverse consequences and to assign the appropriate level of risk based on the severity of the consequence and the likelihood of it occurring. In the case of the security assessment the events are sabotage or theft by an adversary on identified targets within a site, while the likelihood is the prospects of a successful attack.

The likelihood is derived from the probability of an attack occurring and then succeeding (termed vulnerability). The vulnerability in turn depends on the characteristics of the adversary—specified in a design basis threat—and the security systems at the facility. It should be noted that the security system may be enhanced as threat levels are raised to ensure the residual risk is kept below a threshold level. This is termed scalability, about which more will be said shortly.

Risk Factors

Having first considered risk in terms of likelihood and consequence, to ensure a robust security system we need then to examine system shortcomings, or vulnerabilities.

In the first instance we must be able to interrupt an attack. This means making early detection, which must be accompanied by an assessment to determine the required and appropriate response that should be taken. Then we require delay so that the necessary response can be made in good time—that is, before serious consequences arise.

Depending on the nature of the attack, after interruption it may be necessary to neutralise the threat by means of a response force.

This is where the DBT is so practical, and necessary. It should be noted that the DBT is not a particularly new concept being introduced and required by INFCIRC225/Rev.4 in 1999. While I will say more about the DBT in a minute, suffice it to note now that the DBT places a boundary about the level of response required since it defines the upper level of threat or adversary capability.

Nuclear Security Risk Assessment

Agencies are responsible for their own security to which end they must seek protective security risk reviews to help them meet this responsibility. A risk review is usually an assessment of current risks only. Such a review identifies relevant threats, events that could cause adverse consequences and their severity. The appropriate level of risk is assigned to each event based on the severity of the consequence and the likelihood of it occurring. The agency then receives a list of the events ranked by risk. The objective is to identify those priority areas which require attention and to take whatever action is necessary to reduce that risk to an acceptable level. Based on the overall risk matrix, the Regulator will approve construction and operation. If doubts linger, the Regulator may grant only a temporary or conditional approval to the facility operator.

Early Engagement: the Scalability Requirement

As the threat changes, the security system must be capable of being strengthened to meet a rising threat. Total security must be adequate to be able to protect against the DBT at an acceptable level of risk for all threat levels. This method relies on intelligence to provide accurate assessments of threat. While response forces may be capable only for the current threat, this capability must be adjustable to match the

adversary. As mentioned earlier, this is known as scalability. Some features of a security system can be easily scaled. For example, it is relatively easy to restrict access or increase the number of guards at short notice. Other features of the security system, however, are much more difficult to change in-service and must be designed and built to be effective throughout the expected life of the facility. Therefore, the DBT will drive features that must be installed during construction for the full range of threats covered in the DBT, for example the thickness of certain walls, or the layout of the facility.

So, clearly, consideration and design of the security system must be made early in the project's life.

Scalability Implementation

Scalability is a core element in the design of the security system. Scalable measures should be described in advance for all threat levels so that the accompanying risks can be calculated. Response force capability must be adequate for the current threat and, also, it must be scalable to meet an increased threat. But this is not an open-ended situation. The DBT has defined the upper boundary. Total security must be adequate to be able to protect against the DBT at an acceptable level of risk for each threat level.

But the DBT is at best an estimate based on current knowledge. Throughout the life of the facility, the DBT will have to be re-assessed and amended as required. Such changes could result in a major, and possibly costly, upgrading of security.

The Design Basis Threat

The potentially catastrophic consequences of malicious activity at civil nuclear facilities make it vitally important that security measures are both appropriate to the threat and fully effective. It is also important that resources are not wasted on ineffective or nugatory security

measures. Therefore, there is a need for a definitive statement of the possible hostile activity and capability that could be faced at a nuclear facility. The DBT is designed to meet this requirement.

The DBT is concerned with deliberate and malicious threats: it does not address the possible consequences of accidents or other potential failures of process. Neither is it predictive. It deals principally with threats to national security, public safety and the environment.

The DBT excludes hostile groups or capabilities that are judged not to be relevant to the civil nuclear industry and takes account of the availability of countermeasures and other precautions provided by others, usually national, authorities (e.g. contingency arrangements to interdict hijacked aircraft). As these are considered to be beyond the scope of the facility design they are termed “beyond design basis threat”.

At this point, a careful distinction needs to be made between a DBT and a Threat Assessment. The former is a planning criterion. The DBT is fixed until it becomes appropriate to change those planning assumptions. The security measures that derive from those plans should, and must, be capable of countering the current threat throughout the lifetime of the DBT.

By distinction, a Threat Assessment is a judgement of the likelihood of the occurrence of a hostile act within a specified usually short period of time based on specific intelligence and has no link to the security measures in place. A Threat Assessment should, thus, indicate which security measures—available because of the DBT—are currently the most relevant. Should the capabilities described in a current Threat Assessment begin to exceed those in the DBT, the latter would be in need of re-assessment.

It is a fundamental of this approach that security measures must be capable of meeting the threats described in the DBT. In that sense it is a *minimum* standard. However, that does not imply that all the designed-for security measures have to be fully operative at all times. In practice, physical protection will nearly always be at a standard to meet the DBT (security fencing, barriers, and electronic systems). Any variation is likely to come in security procedures. These procedures, especially guarding, need to be capable of meeting the DBT criteria at short notice but this is a more practicable, efficient and effective process than the alternative of never falling below a high state of alert. A guard-force complement and duties, for example, will be determined by the DBT but its deployment by the current Threat Assessment. In this sense, therefore, the DBT is the *maximum* necessary. It is the particular strength of this methodology that the regulated operators are not left reaching for an ill-defined level of perfection.

The severe consequences of failure demand a high level of confidence that security measures are appropriate and effective. The DBT will be used to review existing security standards and will influence decisions about changes in security arrangements. The DBT will be reviewed regularly to ensure its currency.

Consequences

The DBT, threat assessments and considerations of response help address the first part of the risk equation, likelihood. The next element is consequences.

Principally there are two threats: theft and sabotage causing unacceptable radiological consequences. In Australia, ASNO has the responsibility and authority for approving the physical protection systems at nuclear sites to guard against these threats. In this context, radiological consequences means radiation doses received by individuals or contamination of areas—harm caused directly by the

presence of radiation. Evacuation may be an important part of the security systems, but has its own consequences which must be taken into account.

Secondary consequences include economic loss, denial of services, loss of confidence in or by the Government and the public at large.

A first step is to define general parameters applicable to nuclear sites for generic consequences and risk level. Acceptable and target risk levels have been a feature, at least implicitly, of the Government's security assessment process for several years—but have not been explicitly linked to emotionally sensitive nuclear sites. The key here is to meld consequences, likelihoods, acceptable and target risk levels in a form which is acceptable to the whole of Government. This requires careful management of key stakeholders and the inter-agency process.

Consequence Scales

In Australia, national consequence scales are being developed for traditional critical infrastructure. The challenge here is to define a consequence scale for the reactor which is uniform in terms of harm to the nation; that is across different types of facility, for example, chemical plants as well as nuclear facilities. This is particularly important due to the politically sensitive nature of the subject—a nuclear reactor. Partly because it cannot be seen, radiation is regularly misunderstood and misrepresented. Consequently, governments and promoting agencies are often disbelieved and find it hard to build public trust. Furthermore, governments are wary of assigning consequences in terms of deaths and injuries. But a failure to calibrate severity appropriately will lead to a misallocation of protective effort and will distort responses to the point where projects may be stymied.

Rating scales for radiological consequences have been jointly developed by ASNO and ARPANSA and an illustrative example is shown below.

Example Consequence Scales

	Total collective dose received by all individuals receiving an individual dose greater than 1 Sievert	Area contaminated to a dose level greater than 200 μ Sv.hr ⁻¹	Theft of direct-use nuclear material
Catastrophic	20 000 P.Sv	100 km ²	1 SQ
Extreme	2 000 P.Sv	10 km ²	0.5 SQ
Major	200 P.Sv	Site and buffer zone	0.1 SQ
Medium	20 P.Sv	Site	0.05 SQ
Low	2 P.Sv	Building	0.001 SQ
Insignificant	1 P.Sv	Equipment	5X10 ⁻⁴ SQ
Negligible	0 P.Sv	Nowhere	1X10 ⁻⁴ SQ

Example Only

Consequence Scales: Development

Non-radiological consequences could be included in assessments, also, but these are rightly the responsibility of other agencies, although ASNO may advise on the likelihood of events occurring. Where possible suitable criteria were based largely on accepted intervention levels for radiation exposure or contamination. Consequence scales are usually logarithmic. ASNO checked the scales using examples of real disasters—mostly non-nuclear—to see how they would have rated on these or equivalent scales. For example, on the scales above the chemical plant disaster at Bhopal would clearly rate as catastrophic, while the Bali bombing attack would rate as major. Smaller scale events such as traffic accidents would be medium or low.

Threats and Threat Levels

Each site needs to identify theft and sabotage targets through a Site characterisation process, covering nuclear material storage and use locations and vital areas (see INFCIRC 225). Further, they must determine the consequences—both before and after remediation—of a successful attack on each identified target. Both the targets and

consequences need to be assessed and agreed to by the relevant radiation safety authority.

Australia operates a national threat level system that is related to the likelihood of an attack. These threat levels are the indicators used in physical protection plans to trigger scaling of measures as the likelihood of an attack increases. Therefore, the risk calculation must be repeated for the security system at each threat level, to ensure that the risk remains acceptable for each state. For example, if the threat level is low with no hostile activity predicted, guard levels may be routine and reactor operations normal. But, should there be a high likelihood of an armed attack, to maintain or lower the overall risk it would be necessary to reduce the consequences and decrease the chances of a successful attack, under which circumstances, guard levels would be increased, access controlled more tightly and consideration might even be given to shutting down the reactor.

Site Characterisation

The operator is responsible for identification of theft and sabotage targets through a Site characterisation process, covering nuclear material storage and use locations and vital areas. The aim is to identify what actions an adversary may seek to carry out including details of combinations of targets, sequences of actions, time and materials requirements and the potential consequences should they succeed.

The severity of the consequences of a successful attack on each identified target needs to be determined for risk assessment purposes and this may be understood from a study of the consequence scales table. This severity may be reduced by actions taken before, during or after an attack (for example evacuating people from the area while the attack is underway).

Vulnerability: The Probability of success

Where the risk from any combination of target and attack likelihood is greater than the predetermined acceptable level (i.e. a vulnerability), the proposed system must be modified to reduce the risk. Approaches to treating a vulnerability include reducing the probability of an attack or successfully reducing the consequence of a successful attack.

Reducing the probability of an attack being successful may involve interruption and neutralisation of the attacking force. Typically this involves earlier detection, increased delay, reducing the response time or increasing response effectiveness. Consequences can be treated to a limited extent through emergency management procedures of which evacuation is a common example. Other possible measures involve reducing exposure to radiation and may involve changing the operational mode of the facility and changes to transport or storage arrangements.

In addition to the risk assessment ASNO is also still bound to implement IAEA guidelines contained in INFCIRC/225, which outlines specific measures that should be included in the security (or physical protection) system.

Conclusion

This risk based methodology offers a sound approach for developing effective and cost effective security systems at nuclear facilities.

Based on best international guidance, this methodology quantifies risk and consequences, resulting in a rigorous, defensible approval process.