SAND99-1850C

SABOTAGE AT NUCLEAR POWER PLANTS

James W. Purvis, Sandia National Laboratories
P.O. Box 5800 MS-0759 Albuquerque, NM 87185 USA 505-844-3975 jwpurvi@sandia.gov

Abstract

Recently there has been a noted worldwide increase in violent actions including attempted sabotage at nuclear power plants. Several organizations, such as the International Atomic Energy Agency and the US Nuclear Regulatory Commission, have guidelines, recommendations, and formal threat- and risk-assessment processes for the protection of nuclear assets.

Other examples are the former Defense Special Weapons Agency, which used a risk-assessment model to evaluate force-protection security requirements for terrorist incidents at DOD military bases. The US DOE uses a graded approach to protect its assets based on risk and vulnerability assessments. The Federal Aviation Administration and Federal Bureau of Investigation conduct joint threat and vulnerability assessments on high-risk US airports. Several private companies under contract to government agencies use formal risk-assessment models and methods to identify security requirements.

The purpose of this paper is to survey these methods and present an overview of all potential types of sabotage at nuclear power plants. The paper discusses emerging threats and current methods of choice for sabotage—especially vehicle bombs and chemical attacks. Potential consequences of sabotage acts, including economic and political—not just those that may result in unacceptable radiological exposure to the public, are also discussed. Applicability of risk-assessment methods and mitigation techniques are also presented.

INTRODUCTION

A discussion of the emerging threats and current methods of choice for sabotage of all types against nuclear power plants (NPPs)—especially vehicle bombs and chemical attacks—is the focus of this paper. The potential consequences of sabotage acts are not limited to just those that may result in unacceptable radiological exposure to the public; the far-reaching effects on the economic and political arenas are also discussed. Applicability of risk-assessment methods and mitigation techniques are also presented. The goal is to expand awareness of all types of potential sabotage, to emphasize the need for increased physical protection measures, and to begin a dialogue on risk assessment methodology for evaluating protection against sabotage.

Basis for Concern

The recent noted increase in violent actions worldwide can be grouped into five categories:

- internal or domestic actions
- actions against neighboring states
- international acts
- war or threat of war
- nonproliferation acts

In any of these categories, documented incidents of sabotage at NPPs can be found [1].

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

DISCLAIMER

Domestic acts are those carried out by citizens of a state against their fellow citizens or the governing authority. Recent examples include the Oklahoma City vehicle bombing in the United States, the nerve gas attacks in Japan, and militant Islamic fundamentalist actions in Egypt and Algeria. Neighboring states' conflicts are most noted in the regions of the former Eastern Bloc countries and the Newly Independent States, such as Bosnia and Chechnya. International terrorist activity has been around for some time. In the 60s and early 70s, it involved mainly aircraft hijackings. In the late 70s and 80s, there was a transition to the bombings of aircraft. The 90s thus far has been characterized by hidden bombs in public places, armed attacks such as the Embassy in Peru, and vehicle bombings such as the World Trade Center, the Marine barracks in Beirut, and the Khobar Towers in Saudi Arabia. War and threats of war are everywhere—from Kosovo to Iraq to Pakistan to North Korea. Many of these situations are related to international nonproliferation actions.

Potential for Sabotage

In response to the number and type of documented incidents, and in combination with evolving threat capabilities, the International Atomic Energy Agency (IAEA) has recently issued Revision 4 of INFCIRC225 with a new section devoted to sabotage [2]. Assuming that an adequate armed response is available, facilities adhering to IAEA recommendations for current physical protection systems should be able to detect and neutralize both armed attacks and attempts to smuggle bombs into inner areas. However, there are other types of sabotage, which have not been discussed to which these facilities may be vulnerable. The evolving threat now includes armed suicide attacks, vehicle bombs, high-technology military explosives, homemade man-portable explosive devices, and chemical/biological capabilities. To explore this complex area, we will generally follow the Design Evaluation Process Outline (DEPO) as presented in Reference 3 and will discuss targets, threat, threat actions, consequences, analysis, and risk estimation.

In the international arena, perhaps it is time to expand the sabotage area. As evidenced in References 4–6, the vehicle bomb problem has become a serious sabotage concern for many facilities and agencies. The expansion could include not only all types of sabotage, but could establish consequence values for each type of target/sabotage combination, and should logically link each type of sabotage to a specific threat type, threat level, threat motivation, and target. By creating such a matrix for sabotage, it will then be possible for the physical protection system (PPS) designer or analyst to accurately identify exactly what needs protection and how to best to allocate funds in the wisest possible manner.

TARGET IDENTIFICATION

Target identification includes not only SNM at NPPs, but also vital areas, equipment, processes, classified material, critical economic information, and personnel. To accurately identify targets, it helps to keep in mind all possible threat objectives; i.e., all types of sabotage. DOE has a well-developed graded safeguards table for weapons and other nuclear material that establishes consequence values for theft of various materials [7], as well as other similar tables for both radiological sabotage and industrial sabotage. As the types of sabotage to be considered are expanded, proposals will be discussed to define the consequences of various types of sabotage numerically. As these consequence values and threat objectives are considered, identification and prioritization of targets are more easily accomplished. It should be emphasized that the Central Alarm Station, Secondary Alarm Station, response force barracks, and critical NPP personnel are also potential targets for sabotage.

THREAT DEFINITION

The threat may consist of outsiders, insiders, and insiders colluding with outsiders. The well-established outsider threat types [3,7] are: terrorist, organized criminal, white-collar criminal, disgruntled employee, psychotic, and extremist. The extremist type would include in its definition the political activist as well as the environmentalist. In considering an expansion of the sabotage area, it is prudent to establish a threat level within each threat type that ties specifically to the type of sabotage. For example, the white-collar criminal, psychotic, and disgruntled employee would almost always be a group of one. The organized criminal category would likely be a small group. Extremists, on the other hand, could be analyzed in terms of either a small, dedicated, highly trained, highly motivated group of two to four, or a large unruly, mindless crowd of misguided individuals. The former would be more likely to plan in detail and execute an attack on a vital area, while the latter may be content to cut fences and smash windows. Terrorists, acknowledged as the worst category, should probably be considered in terms of three levels: high, medium, and low. Each level would be defined in terms of numbers, objective, motivation, and specific sabotage type. For example, a group of six individuals willing to kill or risk death would not be sent on a mission to turn off a research reactor cooling valve or disperse a handful of plutonium oxide into the atmosphere at a facility. In other words, there should be some logical guidance, with examples, on how to develop an accurate design basis threat for different types of sabotage. This guidance may include the determination of a probability of action, which is similar to the probability of attack which is now assumed to be 1.0 in every case.

Threat Objectives, Purpose, Motivation, Strategy, and Equipment

When the threat objective is theft of special nuclear material—for the ultimate purpose of building a nuclear weapon—the motivation must be either financial or political/ideological. Obviously, this would be the highest level threat, and the strategy would include overt use of force with a willingness to kill and risk death. But what about the threat against a nuclear power plant that is crucial to the economic survival of a region or a sovereign state, for example, where extremist political parties are conducting campaigns? The threat objective could be political sabotage, the purpose would be to sway public political sentiment, the motivation is of course political ideology, the strategy may be covert force, and the equipment may include vehicle or anti-personnel bombs. We are breaching the gap between physical protection and security here, but this situation is becoming a reality in many parts of the world, and perhaps we should expand the process to address such situations with both guidance and examples. At the least, we can point out that DEPO analysis works for all of these areas, not just physical protection systems, and we can at some future point address the differences and similarities between physical protection and security.

DEFINITIONS OF SABOTAGE

Webster's Collegiate Dictionary (10th Edition):

> 1: destruction of an employer's property or the hindering of manufacturing by discontented workmen
>
> 2: destructive or obstructive action carried on by a civilian or enemy agent designed to hinder a nations war effort
>
> 3: an act or process tending to hamper or hurt

NRC:

> **radiological sabotage** means any deliberate act directed against a plant or transport in which an activity licensed pursuant to the regulations in this chapter is conducted, or against a component of such a plant or transport which could directly or indirectly endanger the public health and safety by exposure to radiation

IAEA:

> **SABOTAGE**: Any deliberate act directed against a nuclear facility, nuclear transport cask or nuclear material and associated fission products which could directly or indirectly endanger the health and safety of the worker, the public, and the environment by exposure to radiation.

DOE:

> **radiological/toxicological sabotage**: a malevolent act that results in the release of hazardous materials stored, produced, or used at DOE facilities, that may adversely impact the health and safety of employees, the public, or the environment
> **industrial sabotage**: any deliberate act, not involving radiological releases, which could have unacceptable impact to DOE programs

Types or Categories of Sabotage

As noted above, both the IAEA and the Nuclear Regulatory Commission (NRC) are concerned primarily with radiological sabotage, while the DOE considers toxicological, and industrial as well. Are there more types that should be considered? What about personal, political, technical, environmental, informational, diversionary and economic sabotage? Or are these subsets of the original three? Maybe sabotage acts should just be categorized as lethal, violent non-lethal, and non-violent. The tendency to get too complex and inundate the analyst with too much specificity should be avoided, unless it addresses an area of analytical deficiency. At the least, a discussion of these types, tied to a consequence value determination exercise, should be attempted. Specific acts of sabotage could include the basics: vehicle bombs, explosive attacks against a reactor core, cooling system shutdowns, diversionary arson, kidnapping or murder of critical personnel, etc. It is proposed that, at a minimum, three general categories of sabotage should be considered: radiological, operational, and personnel.

PRIMARY TARGETS AND THREAT OBJECTIVES

Following the above proposal to consider three categories of sabotage, the next step should be to identify the primary targets and threat objectives. For radiological sabotage, the primary target is SNM, which at an NPP includes fresh fuel, the reactor core, and spent fuel. The threat objectives in attacking this target include irradiating people and contamination of the site and the environment. Sabotage against personnel would include as targets: critical NPP personnel, such as the plant manager or the control room operators, other plant personnel, and any other people that might be on the site. Attacks against personnel targets have the objectives both of causing fatalities and impacting plant operations. For operational sabotage, the target would be any equipment that would impact power production or other operations of the plant, or perhaps cause econmic problems for the facility.

Consequence Values

Establishing consequence value tables for targets and types of sabotage has many benefits. A consequence value is a measure of the value of the target to the NPP. This allows targets to be prioritized for protection, and also aids in risk assessment. The table given below is an example of a consequence value table used by DOE for radiological and toxicological sabotage. It is proposed that similar but correlated tables be devised for each target type and sabotage category.

Table 1. Radiological and Toxicological Sabotage Consequence Values

Consequence Value	Impact	Effects on the Public, Employees, and the Environment from Acts of Radiological or Toxicological Sabotage
1.0	Catastrophic	On- and off-site fatalities and injuries, long-term denial of facility (>2years) due to damage or radiation contamination, and off-site denial of food, water, or habitat due to contamination for more than 1 year
0.8	High	Off-site injuries and on-site fatalities and injuries, on-site facility denial for 1 to 2 years, and off-site denial of food, water, or habitat due to contamination for less than 1 year.
0.5	Moderate	On-site injury (no off-site injury), on-site facility denial for 6 months to 1 year, and denial of food, water, or habitat due to contamination for less than 6 months.
0.2	Low	On-site injury, on-site facility denial for less than 1 month, and no impact on food, water supply or habitat.

ANALYSIS

In the DOE community, the DEPO model for designing and analyzing PPSs was developed with the nuclear weapons complex in mind. Consequently, the targets for the DEPO threats include weapons, special nuclear material for weapons, and production or research facilities for both. In the DEPO model, each threat type has two objectives: either theft or sabotage. In the case of sabotage, only either radiological/toxicological or industrial. Sometimes toxicological is broken out as a third independent category. The DEPO process is used with the Graded Safeguards Table to evaluate risk.

In general, the DEPO process or any similar methodology is satisfactory for analyzing the physical protection system at an NPP. There are many path models available, such as EASI and SAVIin the United States, and EVA in France, for use in the analysis process. These path models are used to construct Adversary Sequence Diagrams, which predict the most vulnerable pathways into a facility, the detection probability, and the time for an adversary to access the target. The analysis is usually stoppped when the saboteurs reach the target, and denial is the response force strategy. However, there may be some elements in the target/threat matrix where escape, prior to initiating the sabotage act, is a desired part of the attack. In this case, denial may not necessarily apply and containment may be an acceptable alternative.

As an enhancement to the usual analysis, NPPs might consider including reactor safety and accident prevention experts in the process. Considering the proposed new target types and sabotage categories,

their input could be invaluable in identifying new "vital" areas. In addition, it should always be borne in mind that any human error, equipment malfunction, or procedure that could result in problems for the NPP might also be used by a saboteur.

RISK ESTIMATION AND UPGRADES

Several organizations, such as the IAEA and the US NRC [2,8–11], have guidelines, recommendations, and formal threat and risk-assessment processes for the protection of nuclear assets. Some other examples include the former Defense Special Weapons Agency, which used a risk-assessment model to evaluate force-protection security requirements for terrorist incidents at DOD military bases. The US DOE uses a graded approach to protect its assets based on risk and vulnerability assessments. The Federal Aviation Administration and Federal Bureau of Investigation conduct joint threat and vulnerability assessments on high-risk US airports. Several private companies under contract to government agencies use formal risk-assessment models and methods to identify security requirements. If the sabotage considerations are expanded for NPPs, it might be useful to examine in detail all of the existing risk assessment methodologies and then use the most applicable ideas. A uniform, consistent national or international risk assessment process could be beneficial in areas other than just physical protection.

Analysis data, along with consequence values and response force capabilities, should be used to make risk predictions. However, risk calculations might also take into account the proposed new consequence tables for the various targets and types of sabotage. As previously mentioned, there are many agencies and organizations which use risk analysis. A consistent, standardized risk assessment methodology using consequence value tables appears to be the most desirable.

If analysis and risk evaluation show that a facility has an unacceptable risk level against a certain type of sabotage, the physical protection for the target should be upgraded. For example, if a target is at risk from a vehicle bomb attack, the installation of vehicle barriers at least 120 meters away [4] should mitigate the problem.

Analysis Examples

As a simple example, consider the spent fuel pools (SFPs) at two separate NPPs. Both NPPs were undergoing decommissioning and wanted to implement a security plan that addresses potential sabotage during this process. At NPP #1, most of the pool was below grade, while at NPP #2, the fuel cannisters were above grade. The vulnerability analysis at NPP #1, with emphasis on explosive sabotage, indicated that, due to the pool configuration, sophsticated military explosives could not penetrate the SFP walls and rupture a fuel cannister causing radiological contamination. Further, a vehicle bomb parked next to the SFP wall would, at most, fracture an upper part of the wall and cause it to fall into the pool. Neither attack could drain the pool enough to cause a radiological hazard. The addition of a simple vehicle barrier at an appropriate standoff distance was sufficient to mitigate the vehicle bomb problem and yet not impact deconstruction during the decommissioning process.

The situation was somewhat different at NPP #2. The pool contents were found to be potentially vulnerable to both sophisticated military explosisves and vehicle bombs. Either a specialized explosive device or a vehicle bomb could penetrate the pool wall with the potential to rupture a fuel cannister. Even without a cannister rupture, the pool could drain to a level which would expose the tops of the fuel cannisters and release radiation. While the radiation release would be limited to the site and not endanger the public, the plant management decided that they did not want to allow the possibility of additional radiation exposure to their employees, even during a cleanup operation. The management

took an unprecedented action to spend plant resources to install a specially designed blast wall to mitigate both types of attacks. Their concern and subsequent actions on behalf of both their employees and the reputation of the nuclear power industry merits international recognition and appreciation.

SUMMARY AND CONCLUSIONS

In this "Information Age" nuclear power plants are a vital source of power for many nations and will become even more so in the future. Threats are ever evolving to these facilities, which have new capabilities and motivations for sabotage. The IAEA has recently released Revision 4 of INFCIRC225 with a comprehensive new section devoted to sabotage. This release underscores the increasing international concern about sabotage at NPPs. This paper proposes a continuing effort to support the IAEA position. It is recommended that sabotage categories, target types, and consequences be revised, and a standardized analysis and risk assessment methodology be developed for this area of physical protection at NPPs. Many agencies and organizations worldwide use risk assessment methodologies which may be applicable to this problem. Uniform risk assessment techniques, in combination with recommended physiacl protection upgrades, can only lead to a safer world for us all.

REFERENCES

1. "Nuclear Terrorism—Sabotage and Terrorism of Nuclear Power Plants," http://www.pipeline.com/~happen/.
2. International Atomic Energy Agency, INFCIRC/225/Rev.4: *The Physical Protection of Nuclear Material and Nuclear Facilities*, Vienna, Austria, March 1999.
3. Sandia National Laboratories, The International Training Course: Physical Protection of Nuclear Facilities and Materials, Vol. III. *Evaluating the Physical Protection System Design,* Albuquerque, NM, March 1998.
4. US Nuclear Regulatory Commission, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants—Vehicle Barrier System Siting Guidance for Blast Protection," NUREG/CR-6190, Vol.1, Rev. 1, December 1994.
5. US Nuclear Regulatory Commission, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants—Vehicle Barrier System Selection Guidance," NUREG/CR-6190, Vol.2, Rev. 1, December 1994.
6. US Nuclear Regulatory Commission, "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Vol.I, January 1981.
7. B. Erkilla, D. Fidler, J. Larson, and J. Markin, *Guidelines for Material Protection, Control and Accounting Upgrades at Russian Facilities,* US Department of Energy, Washington, DC, December 1998.
8. US Nuclear Regulatory Commission, Code of Federal Regulations,Title 10 Part 100, January 1992.
9. US General Accounting Office, "COMBATING TERRORISM—Threat and Risk Assessments Can Help Prioritize and Target Program Investments," GAO/NSIAD-98-74, April 1998.
10. US General Accounting Office, "COMBATING TERRORISM—Opportunities to Improve Domestic Preparedness Program Focus and Efficiency," GAO/NSIAD-99-3, November 1998.
11. US Nuclear Regulatory Commission, "NRC Design Basis Threat and Vulnerability Performance Testing—International Training Course," May 1998.