Order Code RS21131
Updated October 4, 2006

Nuclear Power Plants: Vulnerability to Terrorist Attack

Mark Holt and Anthony Andrews
Specialists in Energy Policy
Resources, Science, and Industry Division

Summary

Protection of nuclear power plants from land-based assaults, deliberate aircraft crashes, and other terrorist acts has been a heightened national priority since the attacks of September 11, 2001. The Nuclear Regulatory Commission (NRC) has strengthened its regulations on nuclear reactor security, but critics contend that implementation by the industry has been too slow and that further measures are needed. Several provisions to increase nuclear reactor security are included in the Energy Policy Act of 2005, signed August 8, 2005. The law requires NRC to conduct "force-on-force" security exercises at nuclear power plants at least once every three years and to revise the "design-basis threat" that nuclear plant security forces must be able to meet, among other measures. This report will be updated as events warrant.

Nuclear power plants have long been recognized as potential targets of terrorist attacks, and critics have long questioned the adequacy of the measures required of nuclear plant operators to defend against such attacks. Following the September 11, 2001, attacks on the Pentagon and the World Trade Center, the Nuclear Regulatory Commission (NRC) began a "top-to-bottom" review of its security requirements. On February 25, 2002, the agency issued "interim compensatory security measures" to deal with the "generalized high-level threat environment" that continued to exist, and on January 7, 2003, it issued regulatory orders that tightened nuclear plant access. On April 29, 2003, NRC issued three orders to restrict security officer work hours, establish new security force training and qualification requirements, and increase the "design basis threat" (DBT) that nuclear security forces must be able to defend against.

In the Energy Policy Act of 2005 (EPACT), Congress imposed a statutory requirement on the NRC to initiate rulemaking for revising the design basis threat.[1] The current DBT describes general characteristics of adversaries that nuclear plants and nuclear fuel cycle facilities must defend against, including radiologic sabotage and theft

[1] P.L. 109-58, Title VI, Subtitle D — Nuclear Security (Secs. 651-657). Sec. 651 adds Atomic Energy Act Sec. 170E. Design Basis Threat Rulemaking.

of strategic special nuclear material. EPACT requires that NRC now consider 12 factors in revising the DBT, including but not limited to an assessment of various terrorist threats, sizable explosive devices and modern weapons, attacks by persons with sophisticated knowledge of facility operations, and attacks on spent fuel shipments. NRC announced a notice of proposed rulemaking to amend 10 CFR Part 73 (Design Basis Threat) on November 7, 2005.[2]

Plant Physical Security. Under the regulations in place prior to the September 11 attacks (10 CFR 73 — Physical Protection of Plants and Materials), all NRC-licensed commercial nuclear power plants must have a series of physical barriers and a trained security force. The plant sites are divided into three zones: an "owner-controlled" buffer region, a "protected area," and a "vital area." Access to the protected area is restricted to a portion of plant employees and monitored visitors, with stringent access barriers. The vital area is further restricted, with additional barriers and access requirements. The security force must comply with NRC requirements on pre-hiring investigations and training.[3]

Design Basis Threat. The design basis threat is used by NRC licensees as the basis for implementing defensive strategies of a specific nuclear plant site through security plans, safeguards contingency plans, and guard training and qualification plans. One of NRC's April 2003 regulatory orders changed the DBT to "represent the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law," according to the NRC announcement. The details of the revised DBT, which took effect October 29, 2004, were not released to the public.

NRC's November 2005 proposed rule for revising the DBT, as directed by the Energy Policy Act, has the principal objective of making the security requirements imposed by the April 29, 2003, DBT orders generically applicable. The proposed rule would

- clarify that physical protection systems are required to protect against diversion and theft of fissile material;
- expand the assumed capabilities of adversaries to operate as one or more teams and attack from multiple entry points;
- assume that adversaries are willing to kill or be killed and are knowledgeable about specific target selection;
- expand the scope of vehicles that licensees must defend against to include water vehicles and land vehicles beyond four-wheel-drive type;
- revise the threat posed by an insider to be more flexible in scope; and
- add a new mode of attack from adversaries coordinating a vehicle bomb assault with another external assault.

Allowing 18 months for completing rulemaking as directed by the Energy Policy Act, NRC's final rules on the DBT are due in May 2007.

---

[2] *Federal Register*, Nov. 7, 2005 (vol. 70, no. 214), Proposed Rules, pp. 67380-67388.

[3] General NRC requirements for nuclear power plant security can be found in 10 CFR 73.55.

In 2006, the Government Accountability Office (GAO) reviewed the upgrades in nuclear plant security and found a generally logical and well-defined process. Though NRC staff trained in threat assessment monitored information provided by intelligence agencies, and screened the information to evaluate particular terrorist capabilities for inclusion in the DBT, GAO found that the NRC produced a revised DBT that generally, but not always, corresponded to the threat assessment staff's original recommendations.[4] In GAO's view, NRC's process created the appearance that changes from the recommendations were based on what the nuclear power industry considered reasonable and feasible to defend against rather than an assessment of terrorist threats, and the absence of reviewable criteria reduced the transparency of NRC decisions to make changes based on the threat assessment staff recommendations.

Force-On-Force Exercises. EPACT codified an NRC requirement that each nuclear power plant conduct security exercises every three years to test its ability to defend against the design basis threat. In these "force-on-force" exercises, monitored by NRC, an adversary force from outside the plant attempts to penetrate the plant's vital area and damage or destroy key safety components. Participants in the tightly controlled exercises carry weapons modified to fire only blanks and laser bursts to simulate bullets, and they wear laser sensors to indicate hits. Other weapons and explosives, as well as destruction or breaching of physical security barriers, may also be simulated. While one squad of the plant's guard force is participating in a force-on-force exercise, another squad is also on duty to maintain normal plant security. Plant defenders know that a mock attack will take place sometime during a specific period of several hours, but they do not know what the attack scenario will be. Multiple attack scenarios are conducted over several days of exercises.

Full implementation of the force-on-force program coincided with the effective date of the current DBT in late 2004. Standard procedures and other requirements have been developed for using the force-on-force exercises to evaluate plant security and as a basis for taking regulatory enforcement action. Many tradeoffs are necessary to make the exercises as realistic and consistent as possible without endangering participants or regular plant operations and security.

NRC required the nuclear industry to develop and train a "composite adversary force" comprising security officers from many plants to simulate terrorist attacks in the force-on-force exercises. However, in September 2004 testimony, GAO criticized the industry's selection of a security company that guards about half of U.S. nuclear plants, Wackenhut, to also provide the adversary force. In addition to raising "questions about the force's independence," GAO noted that Wackenhut had been accused of cheating on previous force-on-force exercises by the Department of Energy.[5] EPACT requires NRC

---

[4] GAO, *Nuclear Power Plants — Efforts Made to Upgrade Security, But the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved*, GAO-06-388, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, March 2006.

[5] Government Accountability Office. *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants.* Statement of Jim Wells, Director, Natural Resources and Environment, Government Accountability Office, to the Subcommittee

(continued...)

to "mitigate any potential conflict of interest that could influence the results of a force-on-force exercise, as the Commission determines to be necessary and appropriate."

As of September 2006, NRC had completed force-on-force exercises at 40 of 65 nuclear plant sites.

Emergency Response. After the 1979 accident at the Three Mile Island nuclear plant near Harrisburg, PA, Congress required that all nuclear power plants be covered by emergency plans. NRC requires that within an approximately 10-mile Emergency Planning Zone (EPZ) around each plant, the operator must maintain warning sirens and regularly conduct evacuation exercises monitored by NRC and the Federal Emergency Management Agency (FEMA). In light of the increased possibility of terrorist attacks that, if successful, could result in release of radioactive material, critics have renewed calls for expanding the EPZ to include larger population centers.

A controversy arose over plans to distribute iodine pills in the event of radioactive release. Because iodine tends to concentrate in the thyroid gland of persons exposed to it, taking non-radioactive iodine before exposure would prevent absorption of the radioactive iodine, but would afford no protection against other radioactive elements in the release. Emergency plans in many states include distribution of iodine pills to the population within the EPZ, and in 2002, NRC began providing iodine pills to states requesting them for populations within the 10-mile EPZ.

Nuclear Plant Vulnerability

The major concern in operating a nuclear power plant, in addition to controlling the nuclear reaction, is assuring that the reactor core does not lose its coolant and "melt down" from the heat produced by the radioactive fission products within the fuel rods. U.S. plants are designed and built to prevent dispersal of radioactivity, in the event of an accident, by surrounding the reactor in a steel-reinforced concrete containment structure. Two major meltdown accidents have taken place in power reactors, at Three Mile Island (TMI) in 1979 and at Chernobyl in the Soviet Union in 1986. Though both accidents resulted from a combination of operator error and design flaws, TMI's containment structure effectively prevented a major release of radioactivity from a fuel meltdown caused by the loss of coolant. Chernobyl's lack of containment contributed to a widespread dispersal of radioactivity and loss of life when a hydrogen explosion and a fierce graphite fire caused a significant part of the radioactive core to be blown into the atmosphere. The containment structure represents the intrinsic safety feature in mitigating the consequence of an accident or intentional act.

Vulnerability from Air Attack. Nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events. Their containment structures were not designed to withstand the impact of a jet airliner larger than a Boeing 707, the largest airliner in operation at the time. Attacks by larger airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not contemplated

---

[5] (...continued)
on National Security, Emerging Threats, and International Relations, House Committee on Government Reform. September 14, 2004. p. 14.

when design requirements were determined. A taped interview shown September 10, 2002, on Arab TV station al-Jazeera, which contains a statement that Al Qaeda initially planned to include a nuclear plant in its 2001 attack sites, intensified concern about aircraft crashes.

In light of the possibility that an air attack might penetrate the containment building of a nuclear plant, some interest groups have suggested that such an event could be followed by a meltdown and widespread radiation exposure. Nuclear industry spokespersons have countered by pointing out that relatively small, low-lying nuclear power plants are difficult targets for attack, and have argued that penetration of the containment is unlikely, and that even if such penetration occurred it probably would not reach the reactor vessel. They suggest that a sustained fire, such as that which melted the structures in the World Trade Center buildings, would be impossible unless an attacking plane penetrated the containment completely, including its fuel-bearing wings.

Recently completed NRC studies "confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low," according to former NRC Chairman Nils Diaz. However, NRC is considering studies of additional measures to mitigate the effects of an aircraft crash.[6]

Spent Fuel Storage. When no longer capable of sustaining a nuclear chain reaction, "spent" nuclear fuel is removed from the reactor and stored in a pool of water in the reactor building or in dry casks on the plant grounds. Because both types of storage are located outside the reactor containment structure, particular concern has been raised about the vulnerability of spent fuel to attack by aircraft or other means. If terrorists could breach a spent fuel pool's concrete walls and drain the cooling water, the spent fuel's zirconium cladding could overheat and catch fire.

The National Academy of Sciences (NAS) released a report in April 2005 that found that "successful terrorist attacks on spent fuel pools, though difficult, are possible," and that "if an attack leads to a propagating zirconium cladding fire, it could result in the release of large amounts of radioactive material." NAS recommended that the hottest spent fuel be interspersed with cooler spent fuel to reduce the likelihood of fire, and that water-spray systems be installed to cool spent fuel if pool water were lost. The report also called for NRC to conduct more analysis of the issue and consider earlier movement of spent fuel from pools into dry storage.[7] The FY2006 Energy and Water Development Appropriations Act (P.L. 109-103, H.Rept. 109-275) provides $21 million for NRC to carry out the site-specific analyses recommended by NAS.

Regulatory and Legislative Proposals

Critics of NRC's security measures have demanded both short-term regulatory changes and legislative reforms. A fundamental concern was the nature of the DBT,

---

[6] Letter from NRC Chairman Nils J. Diaz to Secretary of Homeland Security Tom Ridge, September 8, 2004.

[7] National Academy of Sciences, Board on Radioactive Waste Management, *Safety and Security of Commercial Spent Nuclear Fuel Storage, Public Report* (online version), released April 6, 2005.

which critics contended should be increased to include a number of separate, coordinated attacks. Critics also pointed out that licensees are required to employ only a minimum of five security personnel on duty per plant, which they argue is not enough for the job.[8] Nuclear spokespersons responded that the actual security force for the nation's 65 nuclear plant sites numbers more than 5,000, an average of about 75 per site (covering multiple shifts). Nuclear plant security forces are also supposed to be aided by local law enforcement officers if an attack occurs.

Because of the growing emphasis on security, NRC established the Office of Nuclear Security and Incident Response on April 7, 2002. The office centralizes security oversight of all NRC-regulated facilities, coordinates with law enforcement and intelligence agencies, and handles emergency planning activities. Force-on-force exercises are an example of the office's responsibilities.

Legislation. Since the 9/11 attacks, numerous legislative proposals, including some by NRC, have focused on nuclear power plant security issues. Several of those ideas, such as the revision of the design-basis threat and the force-on-force security exercises, were included in the Energy Policy Act of 2005, which also includes

- assignment of a federal security coordinator for each NRC region;
- backup power for nuclear plant emergency warning systems;
- tracking of radiation sources;
- fingerprinting and background checks for nuclear facility workers;
- authorizing use of firearms by nuclear facility security personnel (preempting some state restrictions);
- authorizing NRC to regulate dangerous weapons at licensed facilities;
- extending penalties for sabotage to cover nuclear facilities under construction;
- requiring a manifest and personnel background checks for import and export of nuclear materials;
- requiring NRC to consult the Department of Homeland Security on the vulnerability of proposed nuclear plant sites before issuing a license; and
- requiring the Energy Secretary to conduct a research and development program on cost-effective technologies for increasing the safety of nuclear facilities from natural phenomena and the security of nuclear facilities from deliberate attacks.

---

[8] 10 CFR 73.55 (h)(3) states: "The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards."