Order Code RS21131
Updated August 9, 2005

Nuclear Power Plants: Vulnerability to Terrorist Attack

Carl Behrens and Mark Holt
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 new 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" that nuclear security forces must be able to defeat.

Security Regulations

Under the regulations in place prior to the September 11 attacks, all commercial nuclear power plants licensed by NRC must be protected by 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.[1]

Design Basis Threat. The severity of attacks to be prepared for are specified in the form of a "design basis threat" (DBT). 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 requires each nuclear power plant to conduct periodic security exercises 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 new 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. Each plant is required to conduct NRC-monitored force-on-force exercises once every three years.

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, the Government Accountability Office (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.[2]

---

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

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

Congress imposed statutory requirements for the DBT and force-on-force exercises in the Energy Policy Act of 2005, signed August 8, 2005. The act requires that each nuclear plant undergo force-on-force exercises at least once every three years (NRC's current policy), that the exercises simulate the threats in the DBT, and that NRC "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."

The new law requires NRC to revise the DBT within 18 months, after considering a wide variety of potential modes of attack (physical, chemical, biological, etc.), the potential for large attacks by multiple teams, potential assistance by several employees inside a facility, the effects of large explosives and other modern weaponry, and other specific factors.

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.

Another controversial issue regarding emergency response to a radioactive release from a nuclear power plant is the distribution of iodine pills. A significant component of an accidental or terrorist release from a nuclear reactor would be a radioactive form of iodine, which tends to concentrate in the thyroid gland of persons exposed to it. Taking a pill containing non-radioactive iodine before exposure would prevent absorption of the radioactive iodine. Emergency plans in many states include distribution of iodine pills to the population within the EPZ, which would protect from exposure to radioactive iodine, although giving no protection against other radioactive elements in the release. NRC in 2002 began providing iodine pills to states requesting them for populations within the 10-mile EPZ.

Nuclear Plant Vulnerability

Operating nuclear reactors contain large amounts of radioactive fission products which, if dispersed, could pose a direct radiation hazard, contaminate soil and vegetation, and be ingested by humans and animals. Human exposure at high enough levels can cause both short-term illness and death, and longer-term deaths by cancer and other diseases.

To prevent dispersal of radioactive material, nuclear fuel and its fission products are encased in metal cladding within a steel reactor vessel, which is inside a concrete "containment" structure. Heat from the radioactive decay of fission products could melt the fuel-rod cladding even if the reactor were shut down. A major concern in operating a nuclear power plant, in addition to controlling the nuclear reaction, is assuring that the core does not lose its coolant and "melt down" from the heat produced by the radioactive fission products within the fuel rods. Therefore, even if plant operators shut down the reactor as they are supposed to during a terrorist attack, the threat of a radioactive release would not be eliminated.

Commercial reactor containment structures — made of steel-reinforced concrete several feet thick — are designed to prevent dispersal of most of a reactor's radioactive material in the event of a loss of coolant and meltdown. Without a breach in the containment, and without some source of dispersal energy such as a chemical explosion or fire, the radioactive fission products that escaped from the melting fuel cladding mostly would remain where they were. The two major meltdown accidents that have taken place in power reactors, at Three Mile Island in 1979 and at Chernobyl in the Soviet Union in 1986, illustrate this phenomenon. Both resulted from a combination of operator error and design flaws. At Three Mile Island, loss of coolant caused the fuel to melt, but there was no fire or explosion, and the containment prevented the escape of substantial amounts of radioactivity. At Chernobyl, which had no containment, a hydrogen explosion and a fierce graphite fire caused a significant part of the radioactive core to be blown into the atmosphere, where it contaminated large areas of the surrounding countryside and was detected in smaller amounts literally around the world.

Vulnerability from Air Attack. Nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events, but attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not contemplated 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 NRC Chairman Nils Diaz. However, NRC is considering studies of additional measures to mitigate the effects of an aircraft crash.[3]

Spent Fuel Storage. Radioactive "spent" nuclear fuel — which is removed from the reactor core after it can no longer efficiently sustain a nuclear chain reaction — is stored in pools of water in the reactor building or in dry casks elsewhere 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. Spent fuel pools and dry cask storage facilities are subject to NRC security requirements.

---

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

The primary concern is whether terrorists could breach the thick concrete walls of a spent fuel pool and drain the cooling water, which could cause the spent fuel's zirconium cladding to overheat and catch fire. A report released in April 2005 by the National Academy of Sciences (NAS) 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.[4]

Both the House- and Senate-passed versions of the FY2006 Energy and Water Development appropriations bill (H.R. 2419, H.Rept. 109-86, S.Rept. 109-84) would provide $21 million for NRC to carry out the NAS recommendations. The House Appropriations Committee was particularly critical of NRC's actions on spent fuel storage security: "The Committee expects the NRC to redouble its efforts to address the NAS-identified deficiencies, and to direct, not request, industry to take prompt corrective actions."

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, which critics contended should be increased to include a number of separate, coordinated attacks. Critics also contended that nearly half of the plants tested in NRC-monitored mock attacks before 9/11 failed to repel even the small forces specified in the original DBT, a charge that industry sources vigorously denied. 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.[5] 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.

In February 2002, NRC implemented what it called "interim compensatory security measures," including requirements for increased patrols, augmented security forces and capabilities, additional security posts, installation of additional physical barriers, vehicle checks at greater stand-off distances, enhanced coordination with law enforcement and military authorities, and more restrictive site access controls for all personnel. The further

---

[4] 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.

[5] 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."

orders issued April 29, 2003, expanded on the earlier measures, including revising the DBT, which critics continue to describe as inadequate. Continuing congressional concerns resulted in the new criteria in the Energy Policy Act of 2005 for further DBT revisions.

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. On June 17, 2003, NRC established the position of Deputy Executive Director for Homeland Protection and Preparedness, whose purview includes the Office of Nuclear Security and Incident Response.

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; and
- requiring NRC to consult with the Department of Homeland Security on the vulnerability to terrorist attack of locations of proposed nuclear facilities before issuing a license.

A number of legislative proposals introduced since 9/11 to increase nuclear plant security were not included in the new law, including the creation of a federal force within the NRC to replace the private guards at nuclear power plants, requiring emergency planning exercises within a 50-mile radius around each nuclear plant, and stockpiling iodine pills for populations within 200 miles of nuclear plants. Other measures proposed but not enacted include a task force to review security at U.S. nuclear power plants and a federal team to coordinate protection of air, water, and ground access to nuclear power plants.