



Union of Concerned Scientists

Citizens and Scientists for Environmental Solutions

April 28, 2003

DOCKETED
USNRC

Annette L. Vietti-Cook
Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

May 2, 2003 (10:00AM)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Attention: Rulemakings and Adjudications Staff

PRM-50-80
(68FR35585)

Dear Ms. Vietti-Cook:

On behalf of the San Luis Obispo Mothers for Peace (MFP) and the Union of Concerned Scientists and pursuant to 10 CFR 2.802, I submit the enclosed petition to U.S. Nuclear Regulatory Commission (NRC) to amend 10 CFR 50.59, *Changes, tests, and experiments*, 10 CFR 50.54, *Conditions of Licenses*, and 10 CFR ~~Part~~ 50, *Domestic Licensing of Production and Utilization Facilities*. The purpose of this petition is to provide better protection against radiological sabotage at U.S. nuclear power plants.

Prior to 09/11, the NRC staff was pursuing revisions to its regulations and associated implementing procedures intended to manage the risk from radiological sabotage. Obviously, those **undertakings** grew in both scope and urgency following 09/11. But whereas UCS was an active participant in the NRC's public discussions on proposed changes to its regulations and procedures before 09/11, the NRC **has** steadfastly denied UCS access to such policy discussions since 09/11. In fact, the NRC has formally declined to even listen to our concerns and recommendations.

Left with no other recourse, the petitioners submit this petition for rulemaking **as** a vehicle for injecting what we believe are practical solutions to radiological sabotage problems into the NRC's deliberative process. We request that we be permitted to attend any and all meetings the NRC and NRC *staff* have with non-governmental, external stakeholders (i.e., nuclear industry representatives) dealing with this petition and the matters addressed by this petition.

Pursuant to 10 C.F.R. § 2.802(d), petitioner MFP requests that the Commission suspend the licensing proceeding for an Independent Spent Fuel Storage Installation at the Diablo Canyon nuclear power plant, while it is considering this petition. Suspension of the proceeding is warranted, because consideration of the petition has the potential to bring about a significant redefinition of the fundamental design requirements that are considered adequate to protect independent spent fuel facilities (ISFSIs) against radiological sabotage. In addition, the petition seeks to upgrade the safety evaluation process in 10 CFR 50.59, which would likely be used by the Diablo Canyon licensee in developing and revising procedures for dry cask loading and movement. In order to ensure that the proposed Diablo Canyon ISFSI is adequately designed to accommodate these changes, conclusion of the licensing proceeding should await the outcome of the rulemaking proceeding.

Sincerely,

David Lochbaum
Nuclear Safety Engineer
Washington Office



union of
Concerned
Scientists

Citizens and Scientists for Environmental Solutions

PETITION FOR RULEMAKING

This petition for rulemaking is submitted pursuant to 10 CFR 2.802 by the San Luis Obispo Mothers for Peace (MFP) and the Union of Concerned Scientists (UCS). It is patterned after the layout and structure of a recent industry petition that was accepted by NRC. The petitioners request that the U.S. Nuclear Regulatory Commission (NRC), following notice and opportunity for comment, amend 10 CFR 50.59, *Changes, tests, and experiments*, 10 CFR 50.54, *Conditions of Licenses*, and 10 CFR Part 50, *Domestic Licensing of Production and Utilization Facilities*, to provide better protection against radiological sabotage of U.S. nuclear power plants.

I. STATEMENT OF PETITIONER'S INTEREST

UCS is a nonprofit partnership of scientists and citizens combining rigorous scientific analysis, innovative policy development, and effective citizen advocacy to achieve practical environmental solutions. UCS had 61,300 members in 2002.² UCS was an active participant in a series of public meetings conducted before 09/11 by the NRC with its external stakeholders regarding security regulations and implementing procedures for nuclear power plant reactors and their spent fuel. Among other things, those discussions produced two policy papers submitted by the NRC staff to the Commission in June 2001.³ Although the NRC closed its doors to UCS and other non-industry, public stakeholders regarding security policy matters after 09/11, we continued to articulate potential problems and recommended solutions in other public arenas. In April and June of 2002, UCS testified before the U.S. Senate on nuclear power plant security issues. In March of 2003, UCS testified before the U.S. House on nuclear power plant security issues. UCS stands ready to resume discussions with the NRC should the agency opt to re-open its doors to stakeholders other than the nuclear industry.

In 1969, a group of women founded the San Luis Obispo Mothers for Peace (MFP) to speak out *against* the Vietnam War. At the war's end, the group's mission shifted to advocating for safety and protection of the environment against the dangers of the Diablo Canyon Nuclear Power Plant (DCNPP). For 30 years, staffed entirely by volunteers, MFP has been the foremost DCNPP watchdog group, and a nationally respected voice on nuclear safety issues. MFP has sponsored hundreds of educational forums, litigated to obtain precedent-setting decisions from the U.S. Nuclear Regulatory Commission (NRC) and state regulatory agencies, and testified before Congress and the State Legislature. MFP *has* been the subject of books and films, and many MFP members have been interviewed for documentaries, radio, and TV programs (including *60 Minutes*). MFP believes that individuals and groups can and should make a difference on local, national and global levels. MFP focuses on the interconnected issues of peace, social justice, and a safe environment. MFP takes action on all of these issues, working in every available way to make the world safer and more humane for generations to come.

II. BACKGROUND

Safety and Security Evaluation Intern-ation

Section 50.59, *Changes, tests, and experiments*, to 10 CFR was promulgated in 1962 by the U.S. Atomic Energy Commission, forerunner to the NRC. It contains requirements for the process through which plant owners *can* modify their facilities and procedures without prior NRC approval. The objectives of 10 CFR 50.59 are to ensure that plant owners evaluate proposed changes to facilities and procedures for their effects on the licensing basis of the plant and obtain prior NRC approval for changes having potential

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

impact on the basis for issuance of the operating license. "Potential impact" is explicitly defined in the regulation as any proposed change, test, or experiment that would:

- (i) result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the final safety analysis report (FSAR),
- (ii) result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component important to safety previously evaluated in the FSAR,
- (iii) result in more than a minimal increase in the consequences of an accident previously evaluated in the FSAR,
- (iv) result in more than a minimum increase in the consequences of a malfunction of a structure, system, or component important to safety previously evaluated in the FSAR,
- (v) create a possibility for an accident of a different type from any previously evaluated in the FSAR,
- (vi) create a possibility for a malfunction of a structure, system, or component important to safety with a different result than any previously evaluated in the FSAR,
- (vii) result in a design basis limit for a fission product barrier described in the FSAR being exceeded or altered, or
- (viii) result in a departure from a method of evaluation described in the FSAR used in establishing the design bases.⁴

In practice, §50.59 typically involves a three-tiered review of proposed changes to a nuclear power plant or its procedures. The first tier screens the proposed change against the above-cited regulatory criteria. When the proposed change clearly invokes none of the criteria, the change can be made at the plant owner's discretion. If at least one criterion might be satisfied by the proposed change, the second tier is a more rigorous evaluation. When the evaluation determines that none of the criteria are invoked, the change can be made at the plant owner's discretion. Otherwise, the NRC must approve the change in advance, the change must be revised such that none of the criteria are invoked, or the change must be abandoned.

Section 73.55, *Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage*, to 10 CFR requires plant owners to "establish and maintain an onsite physical protection system and security organization which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in §73.1(a)." The design basis threat is being revised in the wake of 09/11, but currently specifies protection against:

- (i) a determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (A) Well-trained (including military training and skills) and dedicated individuals, (B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and (E) a four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment to the proximity of vital areas, and
- (ii) an internal threat of an insider, including an employee (in any position), and

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

- (iii) a four-wheel drive land vehicle bomb.

The physical protection system features elements such as perimeter fences, locked doors, access controls, intrusion detection systems, and armed responders. Comparable to 10 CFR 50.59, paragraph (p) to 10 CFR 50.54, *Conditions of licenses*, permits plants owners to change their physical protection equipment and procedures without prior NRC approval as long as the changes do not decrease their effectiveness. In practice, a security evaluation process determines if a proposed change to physical protection equipment or procedures can be made, can be made with NRC's prior approval, or cannot be made.

Aerial Hazards

U.S. nuclear power plants were designed and licensed to provide reasonable assurance that an accidental aircraft crash would not adversely harm public health and safety.' The process involved a mathematical exercise to determine the likelihood that an errant aircraft could damage vital part(s) of the plant by impact. The inputs to the number-crunching were the proximity of the nuclear power plant to aircraft flight paths, the amenity of the site to aircraft crashes, and any spatial parameters (e.g, vital plant areas being shielded by non-vital areas that the aircraft could destroy without consequence).

U.S. nuclear power plants were also designed and licensed to provide reasonable assurance that an accidental fire within the facility would not adversely harm public health and safety. But a very serious fire at the Browns Ferry nuclear plant showed that the original regulations and associated implementing procedures were insufficient as the following history details:

During the initial implementation of the U.S. nuclear reactor program, regulatory acceptance of fire protection programs at nuclear power plants was based on the broad performance objectives of General Design Criterion 3 (GDC 3) in Appendix A to 10 CFR 50. Appendix A to 10 CFR 50 establishes the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety. GDC 3 addresses fire protection requirements and specifies, in part, that: (1) structures, systems, and components important to safety shall be designed and located to minimize the probability and effects of fires and explosions; (2) noncombustible and heat-resistant materials be used whenever practical; and (3) fire detection and suppression systems be provided to minimize the adverse effects of fires on structures, systems, and components important to safety. However, during this early stage of nuclear power regulation, the level of fire protection was generally found to be acceptable if the facility complied with local fire codes and received an acceptable rating from its fire insurance underwriter.

A fire at the Browns Ferry Nuclear Power Plant, Unit 1, on March 22, 1975, was a pivotal event that brought fundamental change to fire protection and its regulation in the U.S. nuclear power industry. The fire started when plant workers in the cable spreading room used an open flame to test for air leakage through a non-fire-rated (polyurethane foam) penetration seal that led to the reactor building. The fire ignited both the seal material and the electrical cables that passed through it, and burned for almost 7 hours before it was extinguished using a water hose stream. The greatest amount of fire damage actually occurred on the reactor building side of the penetration, in an area roughly 12.2 m (40 feet) by 6.1 m (20 feet). More than 1600 cables, routed in 117 conduits and 26 cable trays were affected and, of those cables affected, 628 were important to safety. The fire damage to electrical power, control systems, and instrumentation cables impeded the functioning of both normal and standby reactor cooling systems, and degraded plant monitoring capability for the operators. Given the loss of multiple safety systems, operators had to initiate emergency repairs in order to restore the systems needed to place the reactor in a safe shutdown condition.

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

In May 1976, the NRC issued BTP APCS 9.5-1 which incorporated the recommendations from the Browns Ferry fire special review team, and provided technical guidelines to assist licensees in preparing their fire protection programs. As part of this action, the staff requested each licensee to provide an analysis that divided the plant into distinct fire areas and demonstrated that redundant divisions of equipment required to achieve and maintain safe shutdown conditions for the reactor were adequately protected from fire damage. However, the guidelines of BTP APCS 9.5-1 applied only to those licensees that filed for a construction permit after July 1, 1976.

In September 1976, in an effort to establish defense-in-depth fire protection programs, without significantly affecting the design, construction, or operation of existing plants that were either already operating or well past the design stage and into construction, the NRC modified the guidelines in BTP APCS 9.5-1, and issued Appendix A to BTP APCS 9.5-1. This guidance provided acceptable alternatives in areas where strict compliance with BTP APCS 9.5-1 would require significant modifications. Additionally, the NRC informed each plant that the guidance in Appendix A would be used to analyze the consequences of a postulated fire within each fire area of the plant, and requested licensees to provide results of the fire hazards analysis performed for each unit and the technical specifications for the present fire protection systems.

Early in 1977 each licensee responded with a fire protection program evaluation which included a fire hazard analysis. These analyses were reviewed by the staff using the guidelines of Appendix A to BTP APCS 9.5-1. The staff also conducted inspections of operating reactors to examine the relationship of structures, systems, and components important to safety with the fire hazards, potential consequences of fires, and the fire protection features.

In November 1980, the NRC published the "Fire Protection" rule, 10 CFR 50.48, which specified broad performance requirements, as well as Appendix R to 10 CFR Part 50, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979" which specified detailed regulatory requirements for resolving the disputed items. ... 10 CFR 50.48 and Appendix R to 10 CFR Part 50 became effective on February 17, 1981.⁶

While the initial regulations attempted to provide adequate protection, the Browns Ferry fire demonstrated their deficiencies and caused a more formal, structured approach. That more formal, structured approach was recently detailed by the owner of the plant that started it all, Browns Ferry:

[Browns Ferry] performed an Appendix R evaluation to ensure that safe shutdown capability can be maintained during and after a fire in accordance with Section III.G, III.J, and III.L of 10CFR50 Appendix R. Based on this evaluation, the Appendix R Program for Units 2 and 3 was developed along with the Safe Shutdown Instructions (SSIs) to provide the operators with the necessary actions to shutdown the reactor in the event of an Appendix R fire.

This program has two objectives. The first objective is to ensure that the equipment relied upon to shutdown Units 2 and 3 during or after a fire will be available when called upon by the SSIs. This objective is achieved by identifying equipment testing criteria regardless of whether or not the required equipment is encompassed by Technical Specifications. The second objective is to provide a mechanism to ensure safe shutdown equipment is available, or compensatory actions are taken, if any required safe shutdown equipment is not available. This objective is accomplished through the establishment of appropriate compensatory measures (i.e., fire watches, etc.) when required safe shutdown equipment is not available.'

The equipment specified within the Safe Shutdown Instructions has the following functions: 8

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

- The reactivity control function should be capable of achieving and maintaining cold shutdown reactivity conditions.
- The reactor coolant makeup function should be capable of maintaining the reactor coolant level above the top of the core for BWR's and within the level indication of the pressurizer for PWR's.
- The reactor heat removal function should be capable of achieving and maintaining decay heat removal.
- The process monitoring function should be capable of providing direct readings of the process variables necessary to perform and control the above functions.
- The supporting function should be capable of providing the process cooling, lubrication, etc. necessary to permit the operation of the equipment used for safe shutdown.
- One division of the equipment and system used to achieve and maintain hot standby conditions (hot shutdown for a BWR) should be (1) free of fire damage; (2) capable of maintaining such conditions for an extended time period longer than 72 hours if the equipment required to achieve and maintain cold shutdown is not available due to fire damage; and (3) capable of being powered by an onsite emergency power system.
- Equipment and systems used prior to 72 hours after the fire should be capable of being powered by an onsite emergency power system; those used after 72 hours may be powered by offsite power.

U.S. nuclear power plants are protected from aerial hazards by pre-09/11 and pre-Browns Ferry fire regulations that rely in large part on the low probability of an aircraft impacting the site.

111. PROPOSED ACTIONS

Safety and Security Evaluation Integration

10 CFR 50.59 and 10 CFR 50.54(p) should be revised to require plant owners to formally evaluate whether proposed changes, tests, and experiments cause protection against radiological sabotage to be decreased and, if so, that such actions only be conducted with prior NRC approval.

Aerial Hazards

10 CFR Part 50 should be revised to require plant owners to formally evaluate their facilities against specified aerial hazards and make changes as necessary to provide reasonable assurance that the ability of the facility to reach and maintain safe shutdown would not be compromised by an aerial assault, whether accidental or intentional. The requested changes to 10 CFR Part 50 for aerial hazards are analogous to the regulations promulgated by the NRC to rectify the fire protection regulation shortcomings exposed by the Browns Ferry fire (i.e., the addition of 10 CFR 50.48 and Appendix R to 10 CFR Part 50).

IV. RATIONALE FOR THE CHANGES

Safety and Security Evaluation Integration

10 CFR 50.59 requires plant owners to evaluate proposed changes, tests, and experiments and to obtain prior NRC approval for those having more than minimal adverse impact on the licensing basis. Likewise, 10 CFR 50.54(p) requires plant owners to evaluate proposed changes to their physical protection equipment and procedures and to obtain prior NRC approval for those that decrease effectiveness.

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

As presently promulgated and practiced, these safety and security change control regulations have minimal overlaps. For example, a proposed modification to the decay heat removal system typically does not involve a formal evaluation of whether it makes radiological sabotage easier unless it directly affects a piece of physical protection equipment or the response capability of an armed guard. Many changes, tests, and experiments have no affect, direct or indirect, on nuclear plant security. But some may, particularly those involving short-term and temporary applications.

Degraded conditions and off-normal configurations are often deemed acceptable from a safety evaluation perspective because of the low probability that an initiating event occurs during the brief period of the impairment. Initiating events like pipe breaks, earthquakes, etc. are low probability events assumed to occur randomly such that the chances of the initiating event happening during any short time period are a mere fraction of an already small number.

But that same impairment, judged from a radiological sabotage perspective, may be unacceptable because the initiating event for sabotage is not random. The saboteur(s) can cause actions to happen precisely at the time of the impairment. Thus, the chances of an initiating event occurring, instead of being reduced to a mere fraction of a small number, increase towards 100 percent. The NRC's design basis threat is supposed to consider both an act of malice perpetuated by an insider acting alone and an act by an insider aided by several outsiders. As long as one or more insiders remains part of the design basis threat, it is reasonable to assume that sabotage will be timed to coincide with the plant configuration being most, or at least more, vulnerable.

Consequently, it is imperative to evaluate proposed changes, tests, and experiments from both a safety and a security perspective. The security perspective won't necessarily prevent proposed actions from being performed. In the case of short-term or temporary applications, the security perspective review might flag a heightened vulnerability to radiological sabotage but accept it based on compensatory measures put in place. The compensatory measures might entail posting armed guards around the in-service safety widget while the redundant safety widget is removed from service for extended maintenance.

Without the regulation change sought by this petition to integrate the safety evaluations performed pursuant to 10 CFR 50.59 with the security evaluation performed pursuant to 10 CFR 50.54(p), changes, tests, and experiments may continue to occur at U.S. nuclear power plants with proper consideration of safety implications, but with insufficient consideration of their security implications. The regulatory changes sought by this petition would not necessarily prevent the changes, tests, and experiments from happening. The requested regulatory changes would, in all likelihood, (a) allow many changes, tests, and experiments to proceed as planned, (b) require some changes, tests, and experiments to proceed with compensatory measures in place to offset the radiological sabotage risk, (c) require a very few changes, tests, and experiments to be approved by the NRC because they decreased the effectiveness of physical protection equipment and/or procedures, and (d) prevent a very, very small number of changes, tests, and experiments on grounds of undue risk from radiological sabotage.

Aerial Hazards

None of the 103 nuclear power plants operating in the United States at the time were designed to withstand suicide attacks from the air as we tragically experienced on September 11, 2001. This vulnerability prompted the Federal Aviation Agency (FAA) to establish no-fly zones around nuclear plants in the fall of 2001. This response was largely symbolic since FAA sanctions would probably not deter a suicide bomber, but it marked an implicit concession by the federal government that nuclear plants were vulnerable to air assault.

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

Nuclear plant owners would like us to now believe their facilities are hardened structures virtually immune to attack from the air. For example, they recently reported:

[T]he nuclear power industry is confident that nuclear plant structures that house reactor fuel can withstand aircraft impact, even though they were not specifically designed for such impacts. This confidence is predicated on the fact that nuclear plant structures have thick concrete walls with heavy reinforcing steel and are designed to withstand large earthquakes, extreme overpressures and hurricane force winds. The purpose of this study is to validate that confidence.⁹

But the thick, reinforced walls do not surround all vital parts of a nuclear power plant. One study of aircraft hazards, jointly prepared by the owners of two similar nuclear power plants more than 20 years ago, concluded “*The control building is the only single building which, if hit, could lead to core melt.*” The control buildings at every nuclear plant in the US are located outside the robust structures described by the industry. Thus, the nuclear industry’s proclamations about the robustness of thick, reinforced walls may be accurate, but they fail to tell the entire story. The incompleteness of their story is further evidenced by the fire hazards analyses required by NRC’s regulations. The NRC did not restrict the scope of the fire hazards analyses to only those areas within the reactor containment structure. The regulations recognize the reality that reactor core damage can result from fires outside the reactor containment structure.

Security tests conducted since 1991 under the NRC’s Operational Safeguards Readiness Evaluation (OSRE) program also detail why the nuclear industry’s current assurances are incomplete. Each OSRE involved force-on-force exercises with a small group of mock intruders going up against the facility’s armed responders. As the NRC individual responsible for the OSRE program testified to Congress last year:

Eighty-one OSREs have been conducted to date. At 37 of them, the expert NRC team identified a significant weakness; significant being defined as the adversary team simulating sabotaging a target set, which would lead to core damage and in many cases, to a probable radioactive release.”

The “target set” attacked and defended by the adversary team and the security force respectively during the force-on-force exercises is defined by the NRC as follows:

A target set is a minimum combination of equipment or operator actions which, if prevented from performing their intended safety function or prevented from being accomplished, would result in core damage.”

Target sets vary from plant to plant. As implied by name, a target set generally involves more than a single pump, a single valve, or a single wall (however thick and reinforced). The Nuclear Energy Institute (NEI) issued guidance to assist plant owners in developing their target sets. NEI described the process for determining target sets as follows:

Analysis identifies target sets that, if all targets within a target set are destroyed, could lead to significant core damage. Using these target sets provides a basis for evaluating the protective strategy and assessing the significance of issues based on the risk involved.¹³

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

To illustrate the concept—without revealing any plant-specific safeguards information—NEI provided sample target sets in Table A-1. Ten (10) target sets are shown as Columns numbered 1 through 10. Reactor core damage can be prevented if cooling water is supplied from any one of four possible sources listed: normal (High Pressure supply), safety back-up (Emergency High Pressure supply), another safety back-up (Low Pressure supply), and an additional back-up (Alternate Low Pressure supply).

Structures, Sys. & Comps.	1	2	3	4	5	6	7	8	9	10
High Pressure supply										
Power					X			X		
Control	X	X				X				
Suction				X						X
Discharge			X						X	
Location							X			
Emergency HP supply										
Power	X				X			X		
Control		X				X				
Suction				X						X
Discharge			X						X	
Location							X			
Low pressure supply										
Power	X									
Control				X		X				
Suction		X			X			X		X
Discharge			X							
Location							X		X	
Alternate LP supply										
Power	X				X					
Control				X		X				
Suction		X						X		X
Discharge			X							
Location							X		X	

Table A-1 Sample Target Sets

In this sample, each cooling water supply can be disabled by any one of five ways: (1) power for the pump motor can be interrupted, (2) control for the pump and/or valves upstream and downstream of the pump can be lost, (3) the pathway from a water source to the pump can be eliminated, (4) the pathway from the pump to the reactor vessel can be eliminated, and (5) the location of the pump itself can be rendered unusable such as by fire.

As NEI reported, only one of the four ways of cooling the reactor need survive the attack:

Each target set is developed to provide assurance that, if any element is protected, public health and safety will not be endangered by a significant radiological release.¹⁴

In the sample case, the adversary team must “knock out” at least one element for all four water supplies to successfully attack a target set while the security force need only protect one element for one water supply to be successful. The NRC evaluates security during an OSRE by this performance measure:

The licensee’s performance for a particular exercise scenario should be judged a success if the response force effectively protects against the adversary disabling and/or destroying all pieces of equipment and preventing the operator actions in a target set; and the licensee’s performance will be judged unsuccessful for the scenario if the response force is not able to prevent the adversary from disabling and/or destroying all pieces of equipment/actions in a target set.¹⁵

In 37 of the 81 OSREs conducted, the security forces were unable to successfully defend even one element of the target set from simulated ground assaults.* Some of the recent failures:

Quad Cities (IL): *In accordance with this interim guidance, the findings of the Quad Cities OSRE appear to have low to moderate safety significance as described in Section 4.3 of this report because there were losses of target sets in two scenarios due to specific deficiencies associated with procedures, training and the protective strategy.”*

Farley (AL): *The licensee’s protective strategy failed during force-on-force exercises in that the licensee failed to prevent the mock adversaries from gaining access to target sets in two of four*

* The math gets a little complicated. The typical OSRE features four force-on-force exercises. For this statistic, 37 of the plants tested had at least one exercise where the target set was completely eliminated.

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

*exercises and the simulated destruction of the significant plant equipment during a third exercise.*¹⁷

Oyster Creek (NJ): *On May 8-9, 2001, the NRC OSRE team observed and evaluated four force-on-force exercises. In one force-on-force exercise, your response strategy was insufficient to successfully interdict an adversary force. Consequently, there was a loss of a complete target set that was necessary to prevent or mitigate core damage.*¹⁸

Vermont Yankee (VT): *As noted in our inspection report, the finding was considered preliminarily Yellow because response strategy weaknesses found during the conduct of the OSRE were considered generally predictable, repeatable and indicative of a broad programmatic problem. This determination was based on potential response strategy vulnerabilities that were identified during the conduct of table-top drills, and subsequently confirmed by the results from two of the four force-on-force exercises”.*

The sample target sets illustrate the conclusion reached more than 20 years ago about the control building being an Achilles’ heel. Target Set 6 shows that knocking out the control element for all four water supplies can result in core damage. An aircraft hitting the control building may destroy the control elements for all four water supplies, and much more.

These target sets should be used to evaluate nuclear power plants for destruction caused by postulated aircraft impact and subsequent fire. This aircraft hazard evaluation approach mirrors the approach taken for in-plant fire hazards. Following the extremely serious fire at the Browns Ferry nuclear plant in 1975, NRC required all plant owners to evaluate their facilities room-by-room assuming a postulated fire completely engulfs the room destroying all equipment and cabling in it. The fire hazards analysis must show that sufficient equipment exists outside the room to enable the reactor to be shut down and adequately cooled. Many plant owners had to relocate equipment and/or cabling in order to get successful results from their fire hazards analyses. These fire hazards analyses are ‘living documents’ in that proposed changes to plant procedures and proposed modifications to plant structures must be formally reviewed against them to verify that protection against fires will not be lessened.

The real way to ensure adequate protection of nuclear plants from aerial threats would be to replicate the fire hazards analysis process.’ The NRC should define, as part of its design basis threat, the size and nature of aerial threat that the plant must be protected against. As a minimum, it would seem to include general aviation aircraft since the post-09/11 airport security measures generally overlook general aviation. The aerial threat may also entail explosives delivered via mortars and other means (e.g., rocket propelled grenades) as deemed appropriate by the NRC. If the aerial hazards evaluation determines that all targets within a target set are likely to be disabled, at least three options are available to the plant’s owner to remedy the vulnerability:

- 1) Other equipment outside of and not affected by the impact zone could be added to the target set. Using the sample target sets, a fifth makeup water supply system could be added if it were outside the impact zone and could adequately cool the reactor core.

[#] While the existing fire hazards analyses will be useful input to the aircraft hazards analyses, they do not eliminate the need for further study for two reasons: (1) the fire hazards analyses assumed that the postulated fire would be confined to a single room, whereas the aircraft impact and resulting fire(s) may affect multiple rooms, and (2) many rooms were summarily accepted as-is by the fire hazards analyses due to insufficient combustibles being present to sustain a fire — assumptions invalidated by the large amount of fuel carried by aircraft. The fire hazards analyses will expedite the aircraft hazards analyses by defining the equipment needed to cool the reactor if a room is hit. If that equipment could also be disabled by an aircraft impacting the room, action will be required to eliminate that vulnerability.

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

- 2) Protection in place for at least one of the targets within the existing target set could be provided. Using Target Set 9 from the sample target sets, if an aircraft impact at the location of the low pressure supply system and the alternate low pressure supply system potentially caused collateral damage to the discharge pathway for the emergency high pressure supply system, it might be possible to install a shield wall or screen to protect the exposed pathway.
- 3) Affected portions of a system could be relocated to a safe place outside the impact zone. Using Target Set 5 from the sample target sets, if the only part of the Emergency High Pressure Supply System within the impact zone was the power cable for the pump, that power cable could be rerouted.

The aerial hazards analysis would not only establish adequate protection at nuclear plants, for those that may not already be there, it would also provide the means to ensure that future changes to plant structures and procedures do not compromise that protection.

Absent such aerial hazards analyses, nuclear power plant protection against aerial threats is a Nuclear Maginot Line – a defense that looks good on paper but is easily circumvented in practice. Thick, reinforced reactor containment walls might not be breached by a fully loaded 767 aircraft. But that's not enough as documented by the NRC:

The heart of this program [OSRE] is nuclear power plant security force demonstrations of their armed response capability in onsite force-on-force exercises. Significant weaknesses were identified in 27 of 57 plants (or 47%) evaluated to date. "Significant" here means that a real attack would have put the nuclear reactor in jeopardy with the potential for core damage and a radiological release, i.e., an American Chernobyl. ... For example, 14 of these plants were unable to prevent mock adversary forces from gaining (simulated) access into reactor containment!²⁰

At that time (February 1999), the adversary teams had simulated the destruction of at least one target set at 27 different nuclear plants. Roughly half of the time (i.e., at 13 of the 27 plants), the adversary team did not enter the reactor containment in order to destroy every target within the target set. Whether arriving on foot or by air, adversaries should not be able to wipe out an entire target set.

V. CONCLUSION

The proposed changes to 10 CFR 50.59 and 10 CFR 50.54(p) integrate the safety and security evaluations performed for proposed changes to plant safety equipment and procedures, thereby providing better protection against radiological sabotage.

The proposed changes to 10 CFR Part 50 provide a formal, structured approach for managing the risk from aerial hazards comparable to the regulatory approach already adopted for managing the risk from fire hazards. Had 09/11 featured one of the hijacked aircraft hitting a U.S. nuclear power plant, the formal, structured approach being sought by this petition would have been undertaken as a necessary step to prevent another event. If these changes are good measures to prevent recurrence, they represent even better measures to prevent occurrence in the first place

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

Cited Sources:

¹ Letter dated February 6, 2002, from Anthony R. Pietrangelo, Director – Risk & Performance Based Regulation, Nuclear Energy Institute, to Annette L. Vietti-Cook, Secretary, U.S. Nuclear Regulatory Commission.

² Union of Concerned Scientists, Cambridge, MA, “Annual Report 2002.”

³ Memo dated June 4, 2001, from William D. Travers, Executive Director for Operations, Nuclear Regulatory Commission, to the Commissioners, Nuclear Regulatory Commission, SECY-01-0100, “Policy Issues Related to Safeguards, Insurance, and Emergency Preparedness Regulations at Decommissioning Nuclear Power Plants Storing Fuel in Spent Fuel Pools,” and Memo dated June 4, 2001, from William D. Travers, Executive Director for Operations, Nuclear Regulatory Commission, to the Commissioners, Nuclear Regulatory Commission, SECY-01-0101, “Proposed Rule Changes to 10 CFR 73.55: Requirements for Physical Protection of Licensed Activities at Nuclear Power Reactors Against Radiological Sabotage; 10 CFR Part 72: Licensing Requirements for the Independent Storage of Spent Nuclear Fuel and High-Level Radioactive Waste; and 10 CFR 50.54(p): Conditions of Licenses.”

⁴ Regulatory Guide 1.187 dated November 2000 by the NRC’s Office of Nuclear Regulatory Research, “Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments.”

⁵ Standard Review Plan Chapter 3.5.1.6, Draft Rev. 3, dated April 1996 by the NRC, “Aircraft Hazards.”

⁶ Draft Regulatory Guide DG-1094 dated October 1999 by the Pacific Northwest National Laboratory, “Regulatory Guide: Fire Protection for Operating Nuclear Power Plants.”

⁷ Letter dated May 25, 1999, by Tennessee Valley Authority, “Browns Ferry Nuclear Plant (BFN) Units 1, 2, and 3 Fire Protection Plan and Fire Hazards Analysis.” [Available in the **NRC** ADAMS internet collection under Accession No. ML993340417.]

⁸ Draft Regulatory Guide DG-1094 dated October 1999 by the Pacific Northwest National Laboratory, “Regulatory Guide: Fire Protection for Operating Nuclear Power Plants.”

⁹ Nuclear Energy Institute report dated December 2002, “Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant’s Structural Strength.”

¹⁰ Report from Spring 1982 by the Power Authority of the State of New York and the Consolidated Edison Company of New York, Inc., “Indian Point Probabilistic Safety Study,” Section 7.6.2, “Aircraft Hazards Analysis.”

¹¹ Testimony on April 11, 2002, by David N. Orrik, Reactor Security Specialist, Office of Nuclear Security and Incident Response, Nuclear Regulatory Commission, before the US House Subcommittee on Oversight and Investigations, “A Review of Enhanced Security Requirements at NRC Licensed Facilities.”

¹² NRC memo dated November 17, 2000, from Glenn M. Tracy, Chief – Operating Licensing, Human Factors and Plant Support Branch, to John R. White, Chief – Radiation Safety and Safeguards Branch, Region I; Kenneth P. Barr, Chief – Plant Support Branch, Region II; James R. Creed, Team Leader – Safeguards Staff, Region III; and Gail M. Good, Chief – Plant Support Branch, Region IV, “Conduct, Agenda, and Rules of Engagement for Operational Safeguards Response Evaluations,” page 4.

¹³ Nuclear Energy Institute draft report dated October 2000, “Safeguards Performance Assessment Program.”

¹⁴ Nuclear Energy Institute draft report dated October 2000, “Safeguards Performance Assessment Program.”

¹⁵ NRC memo dated November 17, 2000, from Glenn M. Tracy, Chief – Operating Licensing, Human Factors and Plant Support Branch, to John R. White, Chief – Radiation Safety and Safeguards Branch, Region I; Kenneth P. Barr, Chief – Plant Support Branch, Region II; James R. Creed, Team Leader – Safeguards Staff, Region III; and Gail M. Good, Chief – Plant Support Branch, Region IV, “Conduct, Agenda, and Rules of Engagement for Operational Safeguards Response Evaluations,” page 6.

¹⁶ NRC letter dated February 1, 2001, from Glenn M. Tracy, Chief – Operating Licensing, Human Factors and Plant Support Branch, to Oliver D. Kingsley, President – Nuclear Generation Group and Chief Nuclear Officer, Commonwealth Edison Company, “NRC Operational Safeguards Response Evaluation (Inspection Report Nos. 50-25412000-201 and 50-265/2000-201).”

¹⁷ NRC letter dated June 21, 2001, from Charles A. Casto, Director – Division of Reactor Safety, Region II, to D. N. Morey, Vice President, Southern Nuclear Operating Company, Inc., “Farley Nuclear Plant – NRC Inspection Report 50-348101-07 and 50-364101-07.”

¹⁸ NRC letter dated June 22, 2001, from Wayne D. Lanning, Director – Division of Reactor Safety, Region II, to Ronald J. DeGregorio, Vice President – Oyster Creek, AmerGen Energy Company LLC, “Oyster Creek Generating Station – NRC Inspection Report 0500021912001-011.”

¹⁹ NRC letter dated March 25, 2002, from Hubert J. Miller, Regional Administrator, Region I, to Michael A. Balduzzi, Senior Vice President and Chief Nuclear Officer, Vermont Yankee Nuclear Power Corporation, “Final

Petition for Rulemaking: Better Protection Against Radiological Sabotage of Nuclear Power Plants

Significance Determination for a Yellow Finding at the Vermont Yankee Generating Station (NRC Inspection Report 50-271101-O1O)."

²⁰ NRC memo dated February 3, 1999, from Captain David N. Orrik, Security Specialist, to William D. Travers, Executive Director for Operations, "Differing Professional Opinion Regarding NRC's Reduction of Effectiveness and Efficiency in the "Staff Recommendations" of the Follow-on OSRE Program for Nuclear Power Plants."