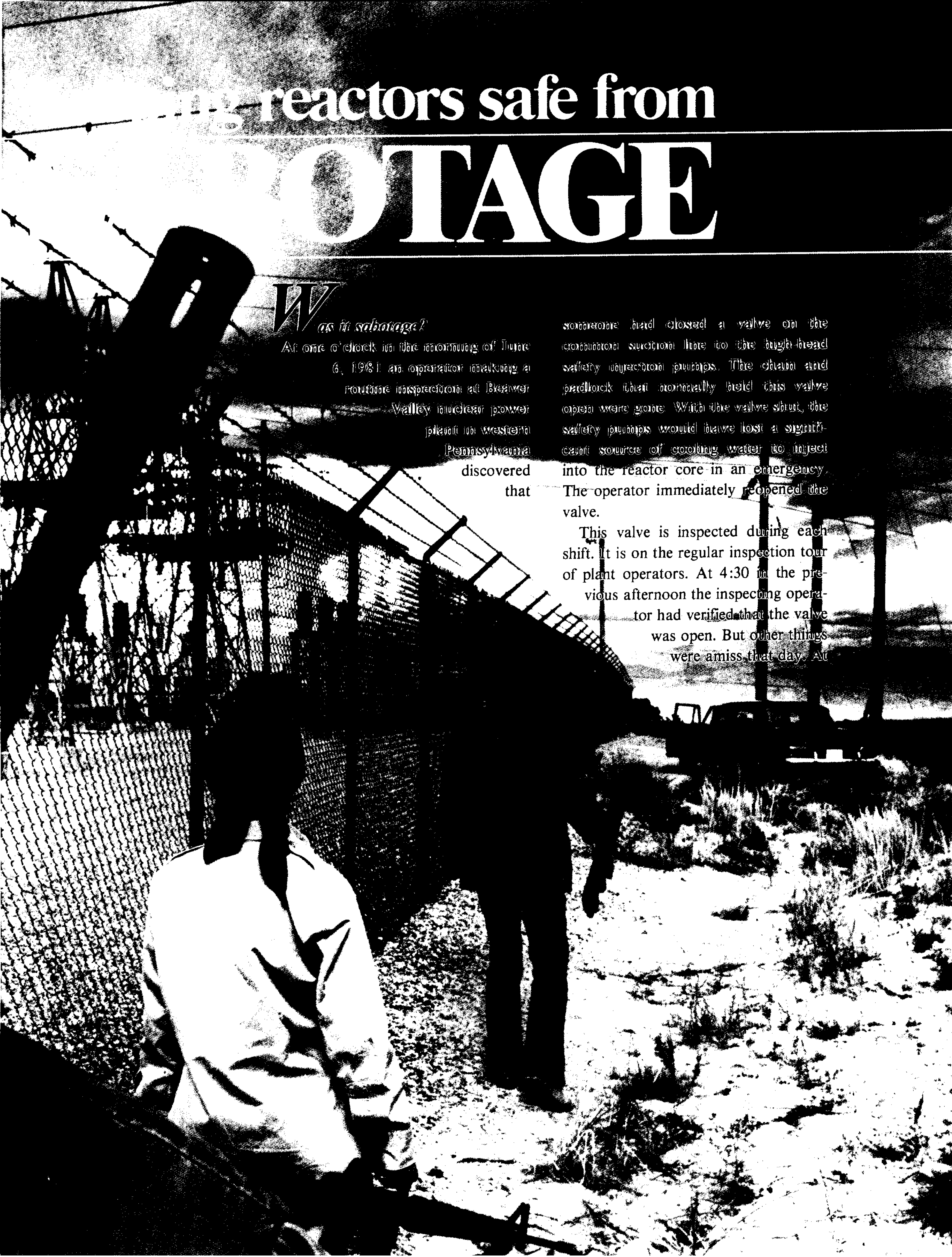


ing reactors safe from OTAGE

Was it sabotage?

At one o'clock in the morning of June 6, 1981 an operator making a routine inspection at Beaver Valley nuclear power plant in western Pennsylvania discovered that someone had closed a valve on the common suction line to the high-head safety injection pumps. The chain and padlock that normally held this valve open were gone. With the valve shut, the safety pumps would have lost a significant source of cooling water to inject into the reactor core in an emergency. The operator immediately reopened the valve.

This valve is inspected during each shift. It is on the regular inspection tour of plant operators. At 4:30 in the previous afternoon the inspecting operator had verified that the valve was open. But other things were amiss that day. At nine o'clock in the morning operators found that locks and chains had been removed from other valves on three auxiliary feedwater pumps, The valves, however, were all in the normal, open position. But neither these locks and chains nor the ones for the suction-line valve could be found.

Duquesne Light Company, licensee of the Beaver Valley nuclear plant, immediately isolated the plant's vital areas and stepped up security. Operators began checking key equipment every two to four hours. And the Pittsburgh office of the Federal Bureau of Investigation began looking for the culprit.

The valve incident at Beaver Valley is over. Whatever the actual cause was, there was no effect on the plant. The inspection system functioned as intended. The power plant continues to operate. But this successful detection of tampering and protection of plant vital areas has significance far beyond Beaver Valley.

Concern for Security

Protecting American nuclear power plants from internal sabotage and external attack has long been a major concern of the United States Nuclear Regulatory Commission. Studies performed in the early seventies indicated that nuclear power plants were not attractive targets for terrorism and that their construction was highly resistant to damage, yet there were conditions under which the radioactive containment features could be sabotaged. This conclusion prompted the Nuclear Regulatory Commission, in February 1977, to publish a revised section to the Code of Federal Regulations, Title 10 Part 73.55.

The new requirements were aimed specifically at countering any form of sabotage that could release radioactive material and thereby create a hazard for the general public. But implementation of the new law required reviewing and upgrading the security plans for more than 70 nuclear power plants each with unique nuclear and secondary systems and unique geographic and demographic environments. (There is no "standard nuclear plant" in the United States. Although a single manufacturer may provide the basic reactor system for a group of plants, the remainder of each plant is a composite provided by various contractors.)

The Nuclear Regulatory Commission recognized the complexity of the security review project from the very beginning and the Commission called upon Los Alamos for engineering support even before final adoption of the new regulations. Eight teams were formed to analyze individual plans for physical security. Each team had one Los Alamos engineer for mechanical systems and one for electrical systems and two Nuclear Regulatory Commission personnel. Over a period of 18 months, beginning in February 1977, these teams visited every operating commercial power reactor in the United States at least once and many several times. What these teams learned from site visits and from security plans provided by the licensees was analyzed to determine how well each plant fulfilled the requirements of the new security rule. When deficiencies were found, the licensees were required to correct them,

Early in 1978 the Nuclear Regulatory Commission organized three additional teams of two Los Alamos engineers each, with support from Science and Engineering Associates of Albuquerque, to pinpoint potential sabotage targets at all nuclear power plants in the country and thus identify exactly what was the vital equipment that needed to be protected. These teams have visited 50 of the 70 nuclear reactors in the U.S. and their work is still underway.

Altogether the review process has had a profound effect upon the planning for security at nuclear power plants, especially in defining what we are trying to protect, what kinds of threats we face, and how we can realize the largest return for our investment in nuclear plant security. The review process also has implications for nuclear plant safety.

Protecting Property or People?

Before designing a physical security plan, two basic questions need to be answered. First, what is to be protected? The Nuclear Regulatory Commission answered this very simply: in this case, protection is not for the power plant but for the health and safety of the public. The purpose is to prevent "radiological sabotage." Radiological sabotage is defined in terms of a maximum radiation level established in the Federal regulations for siting nuclear power plants. It is any deliberate act that causes a radiation release sufficient to provide a dose of more than 300 rem to the thyroid or 25 rem to the whole body of a person who remains at the edge of the plant exclusion area for 2 hours after the release.

The decision to protect against a radioactive material release rather than to protect the entire power plant is

conceptually important because it allows the plant area and the analysis of physical security to be divided into two parts. The large area containing all components of the nuclear power plant is commonly called the protected area, and it is at the boundary of this area where physical security measures start. An intruder may get into the protected area and inflict damage to plant systems that interrupts normal operation, yet his actions here do not cause a radioactive release. The security analysis of the protected area concerns mainly the response of a guard force to a detected intrusion.

Within the general protected area are specific areas that are vital to radiological security; disabling equipment or systems in these vital areas could either directly cause a radiological release or prevent mitigation of a threatened release caused by damage elsewhere. Typical vital equipment includes the reactor containment, the main reactor controls, and the pumps, piping, and valves essential for reactor cooling. Analysis of the plant involves identifying vital equipment, pinpointing the actual location of that equipment at the plant site, and predicting the response of the reactor to sabotage of that equipment.

A second question is equally important to the design of a physical security plan. What is the threat? The answer to this question is not easy. Real sabotage threats might range in size from a single person to a large paramilitary force. Motivations might include the illusions of the individual terrorist as well as the grand mission of an antinuclear movement. Methods might include direct external attack as well as covert operations by persons inside the plant. Before 1974, the postulated external threat to a nuclear plant was generally considered to be of the lone bank-robber type. However, because of the growing concern about terrorists, the regulations issued in February 1977 by the Nuclear Regulatory Commission defined the design-basis threat to nuclear power plants to be a small group of dedicated, well-equipped, and well-trained attackers with or without assistance from a person inside the plant.

The Commission's definition of the threat put plant security in another light. Ordinarily, nuclear power plants would seem to be very difficult sabotage targets. The plant components and structures are large and strong and have many redundant control, safety, and shutdown systems. Redundancy in the design comes from the "single-failure" concept; under this concept we assume that accidental single failures may occur in any component in a system and, therefore, we must have backup components. However, we now realize that a well-trained, knowledgeable team of terrorists could circumvent this inherent safety feature by deliberately causing multiple failures in a selected system. Such a postulated threat, of course, introduces further complexity into the system analysis. But it is this same kind of common-mode failure where a single event precipitates a simultaneous multiple failure of some key system that has been highlighted by the Three Mile Island accident.

Requirements for the Protected Area

Postulate a team of saboteurs trying to enter a power plant's protected area and reach a vital area. How are they detected? How do the guards know whether the alarm is real? Where is this team going and how strong are they? How should the guard force be deployed to intercept them? What type of armaments will best counter this threat? Which would be more effective in delaying this threat until the police arrive—stronger doors at vital areas or a larger guard force?

As these questions illustrate, a nuclear power plant security system has many elements: physical barriers, detection devices, alarm systems, communication systems, guard training, guard force levels, and armaments. The engineering teams found that the combination of security elements and their interactions were unique to each plant. The main task for the Los Alamos engineers was to assist personnel from the Nuclear Regulatory Commission in comparing and evaluating the technical aspects of each plant's security system with the Commission's published requirements for security.

Then, since all the individual components of a physical security system must function together, the teams postulated intrusion scenarios in the protected areas to see if the plant guard force could respond in time to prevent the saboteurs from gaining access to a vital area.

Here are examples of some of the security elements and interrelationships that needed to be considered by the Nuclear Regulatory Commission and the engineering teams. For the simulated attack shown in Fig. 1, at point A the attackers breach the protected area barrier, usually an 8-foot cyclone fence topped with three strands of barbed wire. How fast can they do this? The times needed to breach many types of barriers with a variety of mechanical and explosive tools have been determined by repeated experiments at Sandia. In this case a cyclone fence is not a very effective barrier and can be climbed or penetrated in seconds. Even though vibration sensors or other detection systems may be on the fence, its major purpose is simply to define and limit the boundary of the protected area.

In this example, more effective protective elements are just inside the fence. Here, sighting along a level area kept clear of herbage, is an intrusion-detection device, perhaps a microwave system combined with electric-field, infrared, or seismic detectors. When the attackers breach the protected area, this system signals two alarm stations with visual and audible alarms.

The alarm signals the guards, but is the penetration real? Also sighting along this cleared area are a number of closed-circuit television cameras. A view of the penetrated section of the fence is displayed automatically so guards can determine whether the alarm is real. If so, the station guards call out the response force and initiate other necessary actions, such as notifying outside law-enforcement agencies.

Several questions are addressed in this part of the security review. Is this area lighted well enough? Should a closed-circuit camera be placed to view this door? Are the guard patrols frequent and random enough in this area to keep the probability low that the attackers will reach point B while the guards are at other distant locations in the plant site? How long will it take a well-equipped team to penetrate the barrier at B?

Once inside the building, the attackers attempt to move to point C, breach this door and reach the vital component inside. Should the barrier at C be strengthened? What is the measure of the reliability of the guard force communications system used to cope with this situation? Does guard force training permit an efficient, coordinated attempt to prevent the saboteurs from reaching their objective?

One suggested analytic method for answering these questions was a computer code developed by Sandia National Laboratory for the Nuclear Regulatory Commission; it is called EASI (for estimate of adversary sequence interruption). In this code the properties of the protective systems, such as the efficiency of the intrusion-detection system, the reliability of communications, and the time for the guard force to respond, are balanced against the time it takes the attacker to penetrate the various barriers and perform his sabotage. The comparision produces an estimate of the probability that the response force can intercept the attackers before they can do their mischief.

Although the basic EASI calculations are relatively simple, the large number of different elements makes the task ideal for computer analysis. By manipulating the variables of attack and response, the teams could evaluate tradeoffs and determine which would give the greatest protection for the money invested. One version of the code runs on hand-held

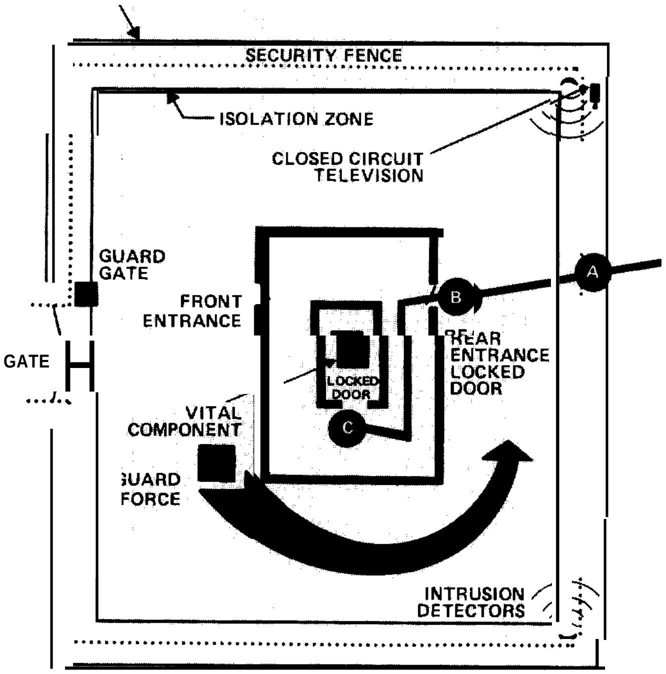


Fig. 1. Action sequence for a hypothetical sabotage attack.

computers: thus teams could evaluate facilities in the field and licensees could analyze their own plants.

The data needed for the EASI analysis-times for barrier penetration, distance traversed, guard response, and the reliability of communication and detection systems—cannot have exact values because they all have statistical fluctuations. Thus, the method can only provide a percentage estimate of guard success in interrupting hypothetical attackers. However. the method is ideal for evaluating the relative worth of several protective systems or the proposed improvements for a given system.

This type of analysis is illustrated in Fig. 2, a three-dimensional plot used to analyze one aspect of a protective system: the interruption probability versus the guard-force response time and the time to breach door B of Fig. 1. Point I toward the lower front corner represents a long guard response time (12 minutes). a short time for the saboteurs to breach door B (4 minutes), and thus, a low probability of interruption (5%). If this plot represented an actual data point for a plant, a Nuclear Regulatory Commission reviewer would note a physical security problem. The plant owner, looking at this same plot, could correct the defect by either shortening guard response time or increasing barrier strength at point B. In this particular case. he might decide that it would be more cost effective to strengthen the door and raise the breach time to 16 minutes (point II). thereby increasing the probability of interruption from 5% to nearly 90%. Whatever modification the owner makes. the Commission reviewer will be satisfied when the probability of interruption is high enough.

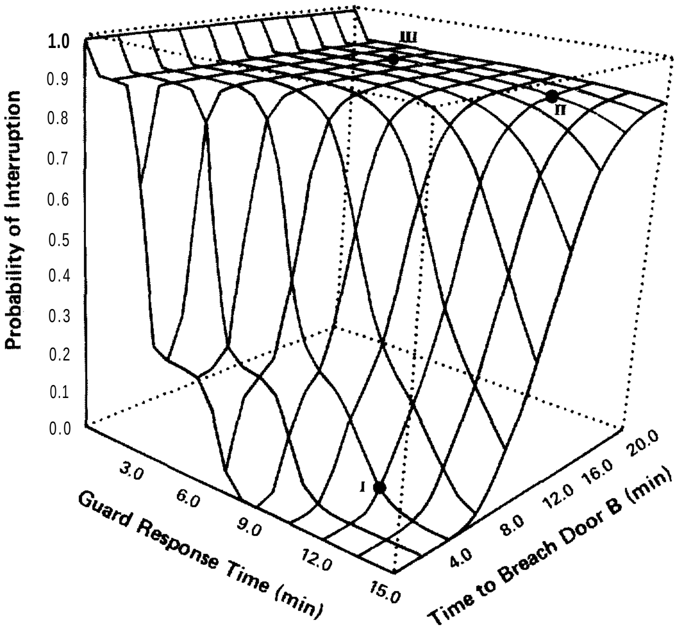


Fig. 2. Probability of interrupting hypothetical saboteurs as a function of guard response time and the time required to breach a locked rear door, as calculated with EASI.

Intrusion games can be played many times for each plant and the interruption probability can be plotted as a function of virtually any variable. Such analyses have allowed numerical assessment of complicated physical security problems. The three-dimensional aspect of these EASI plots is especially helpful in revealing either steep or flat regions on the probability surface. A steep region will cause dramatic increases in the probability of interruption for small improvements (such as from point I to point II), whereas a flat region (such as from point II to point 111) shows where further improvements may not be cost effective.

One important aspect of physical plant security not directly covered in our scenario is protection of the plant from the inside man, a plant employee in any position of responsibility or even a visitor. Three protection methods have been suggested to plant owners: limit access to vital areas; prevent anyone from being in a vital area alone (the two-man rule): and allow only cleared persons into vital areas. An example of the two-man rule as protection from an inside saboteur is the use of two alarm stations; since the stations have identical alarms and controls, the guard in either station can monitor the other.

A number of other measures protect against a potential saboteur, who may be either a visitor or an employee. Access to the protected area is through a single gate where all persons are identified and checked for contraband. The last door from the entry guard station to the protected area can only be opened by a guard behind a rifle-proof barrier. and another guard observes this operation to prevent an inside man from letting a collaborator in. Similar precautions are followed for entry of vehicles. In fact, all packages in delivery vehicles must be identified, the shipment administratively verified, and the packages off-loaded at a special receiving area near the perimeter of the protected area.

Defining Vital Areas

Suppose a team of saboteurs gains entrance to the plant despite the protective measures. Or suppose a saboteur is already in the plant as an insider. Which components would the saboteurs go after? Where are they located? If the sabotage attempt succeeds, will the crippled reactor release a significant amount of radioactive material? To answer these kinds of questions, the engineering teams had to start by locating potential targets. the plant's vital equipment. To assure complete protection, all vital equipment must be so designated. However, the designation of noncritical areas as vital would add unnecessarily to plant costs and the burden of the plant security force. Such unnecessary designations could also add to safety problems.

The Nuclear Regulatory Commission has defined two levels of vital areas. A Type 1 vital area is a single location where a saboteur could cause successful radiological sabotage (for example, the nuclear reactor containment building). A Type 2 vital area contains equipment insufficient in itself to achieve a suc-

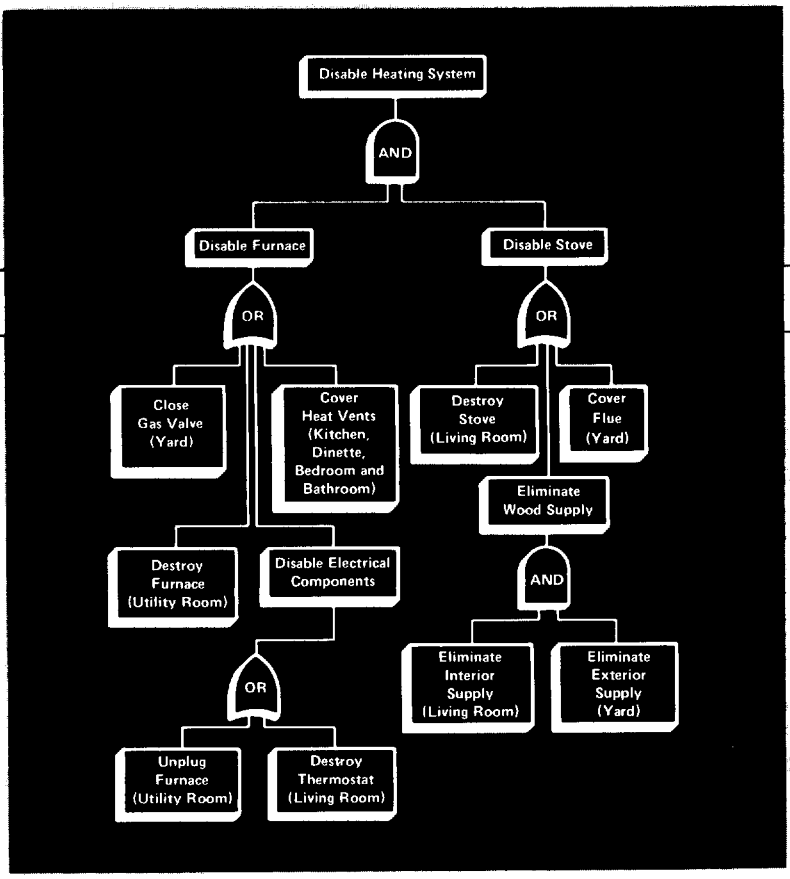
Sidebar: A FAULT TREE FOR HOUSEHOLD SABOTAGE

Consider an imaginary saboteur intent on disabling the heating system of a certain residence. First, of course, she gathers information about the system's components and learns that the house is equipped with a forced-air gas furnace in the utility room, a main gas valve in the yard, a thermostat in the living room, heat vents in the kitchen, dinette, bedroom, and bathroom, a wood-burning stove in the living room, and wood supplies in the living room and yard.

Because this particular saboteur has a rather analytic mind, she uses the following method to select a course of action. First, she draws a fault tree to show the possible paths to the goal. She uses the "and" symbol (⌓) to indicate actions all of which are required to produce the desired effect and the "or" symbol (⌂) to indicate actions each of which is sufficient in itself. Then, she ponders—analyzes-this fault tree and compiles a list of the various location scenarios, as she calls them, at which actions must occur to accomplish the crime, She also lists the various event scenarios, or necessary actions, associated with each location scenario.

The saboteur may now select a location scenario that seems most advantageous. Being sensible, she rejects those location scenarios requiring her presence in all or nearly all rooms of the house. A decision among the other possibilities will be made on the basis of her personal tastes and abilities,

Turning the tables on our imaginary saboteur, scientists at the Laboratory have applied this technique to one aspect of foiling sabotage at nuclear power plants—identification of "vital areas," those places or combinations of places at which radiological sabotage could be accomplished. Based on site-specific information, a fault tree for a particular plant is developed and analyzed with a computer program developed at Sandia National Laboratories, The program rejects those location scenarios requiring actions in an excessive number of places and provides a list of more credible location scenarios and associated event scenarios. These location scenarios may then be classified by the Nuclear Regulatory Commission as vital areas requiring implementation of various security measures. ■


Disable Heating System
AND
Disable Furnace
Disable Stove
OR
OR
Close Gas Valve (Yard)
Cover Heat Vents (Kitchen, Dinette, Bedroom and Bathroom)
Destroy Stove (Living Room)
Cover Flue (Yard)
Eliminate Wood Supply
Destroy Furnace (Utility Room)
Disable Electrical Components
AND
Eliminate Interior Supply (Living Room)
Eliminate Exterior Supply (Yard)
OR
Unplug Furnace (Utility Room)
Destroy Thermostat (Living Room)

LOCATION SCENARIO	EVENT SCENARIO
Yard	Close gas valve and cover flue
Living room	Destroy thermostat and destroy stove
Utility room and living room	Destroy furnace and destroy stove Unplug furnace and destroy stove
Utility room and yard	Destroy furnace and cover flue Unplug furnace and cover flue
Living room and yard	Destroy thermostat and cover flue Destroy thermostat and eliminate interior and exterior wood supplies Destroy stove and close gas valve Eliminate interior and exterior wood supplies and close gas valve
Utility room, living room, and yard	Destroy furnace and eliminate interior and exterior wood supplies Unplug furnace and eliminate interior and exterior wood supplies
Kitchen, dinette, bedroom, bathroom, and living room	Cover heat vents and destroy stove
Kitchen; dinette, bedroom, bathroom, and yard	Cover heat vents and cover flue
Kitchen, dinette, bedroom, bathroom, living room, and yard	Cover heat vents and eliminate interior and exterior wood supplies

cessful sabotage; a saboteur would have to commit destructive acts in more than one Type 2 area to cause a radioactive release.

But how can we determine what areas should be designated Type I vital areas? Before the vital area reviews, the auxiliary feedwater system in a pressurized-water reactor was considered critical enough to designate the locations of its components as Type I vital areas. However. some utility operators questioned this designation. They maintained that even with the loss of the auxiliary feedwater system, the reactor could still be cooled using the high-pressure injection pumps. Team engineers analyzed the problem using TRAC, the thermal-hydraulic computer code developed at Los Alamos. TRAC is discussed at length in the article “Accident Simulation With TRAC.” Results of the study verified the operators’ position; proper use of the high-pressure injection system could control the particular Babcock & Wilcox reactor studied and, thus, the locations of the auxiliary feedwater system were not necessarily Type I areas.

Since each American nuclear plant has a unique design. the engineering teams had to analyze each plant separately to locate its vital equipment. The key element in this analysis was another Sandia computer code* that acts as a “bookkeeper.” Using this code for keeping his records, the engineer can develop and solve fault trees in applications involving a large number of event paths. In this application the scenarios available to a saboteur involved thousands of possi-

**R. B. Worrell, “Set Equation Transformation System (SETS), ” Sandia Laboratories report SLA-73-0028A (July 1973).*

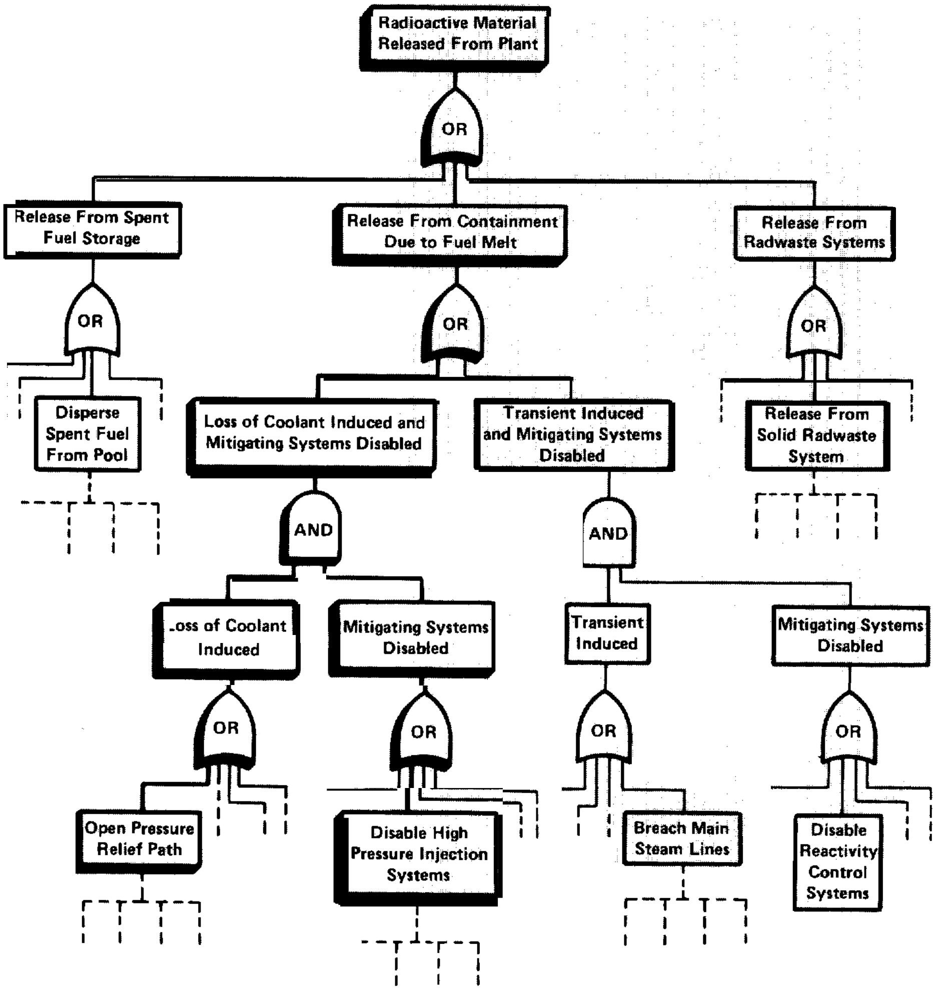

Radioactive Material Released From Plant
OR
Release From Spent Fuel Storage
Release From Containment Due to Fuel Melt
Release From Radwaste Systems
OR
OR
OR
Disperse Spent Fuel From Pool
Loss of Coolant Induced and Mitigating Systems Disabled
Transient Induced and Mitigating Systems Disabled
Release From Solid Radwaste System
AND
AND
.oss of Coolant Induced
Mitigating Systems Disabled
Transient Induced
Mitigating Systems Disabled
OR
OR
OR
OR
Open Pressure Relief Path
Disable High Pressure Injection Systems
Breach Main Steam Lines
Disable Reactivity Control Systems

Fig. 3. Portion of a hypothetical sabotage fault tree for a light-water reactor.

ble event paths. When printed out in full, such a fault tree can be over thirty feet long. What we see here (Fig. 3) is a small part of a generic sabotage fault tree for a light-water reactor.

The engineers' first step in the analytic process was to review each power plant's Final Safety Analysis Report to familiarize themselves with various plant details. The next step was to visit the plant to discuss operating procedures with plant engineers and operators. The purpose of these discussions was to gain insight into the ways a saboteur could initiate a radiological event and then disable the safety systems that could control or mitigate that event.

These visits focused on all loss-of-coolant possibilities and included examination of all water systems connecting to the reactor primary coolant system. Systems mitigating against this type of sabotage-induced event include the emergency core-cooling system, reactivity-control systems, and post-accident heat-removal systems. The engineers also reviewed sabotage scenarios that lead to transient incidents such as loss of off-site power or breaching of the main steam lines, and identified the reactivity-

control and heat-removal systems necessary to control the transients.

In one hypothetical sequence, the saboteur opened the valve on the pressurizer in an attempt to induce a loss-of-coolant accident. This initiating event is represented in our fault tree analysis (Fig. 3) by the box in the lower left corner labelled "open pressure relief path." However, the' reactor could still be controlled by the high-pressure injection system; in other words, this mitigating system would also have to be disabled if the sabotage is to be successful. Thus our sample fault tree leads from the appropriate two lower left boxes upward to an "and" gate. This means that both events must happen before the core uncovers and the threat of a fuel melt becomes real.

Including the reactor containment, there are three general areas where enough radioactive material might be found to cause a serious release; the other two are the spent-fuel storage pool and the radioactive waste treatment systems. Generally, the storage pool would be a significant source of radioactive material for some length of time after spent fuel assemblies were placed in it. The actual number of days this pool would be a threat depends on reactor core size, the stored fuel's power history, site meteorology, and the type of pool building; this length of time was calculated for each plant.

The study did not overlook theft of fissionable materials as another form of possible sabotage, but such theft was considered unprofitable on two accounts. First, the nuclear fuel used in light-water nuclear power plants is of such low enrichment that it cannot be used directly to construct nuclear explosives. Further, once the reactor is operating, the fuel is highly radioactive and cannot be handled without special equipment. A person attempting the theft of this fuel would quite likely receive a lethal dose of radiation. The liquid, gas, or solid radioactive waste contained in the waste treatment system also was considered in the analysis, but usually there would not be enough material in the system for it to be of real sabotage concern.

The major source of concern and potential for radiological release is in the reactor itself. If the saboteur can cause the fuel to melt significantly and cause the containment boundaries (fuel cladding, primary containment system, and containment building) to be breached or circumvented, then he can achieve successful sabotage. A direct breaching of the containment structure would be a difficult task because the walls are typically 4 to 5 feet of steel-reinforced concrete; however, there are other approaches the saboteur could envision to cause a radiological release that would be less difficult than breaching the reactor containment building.

Benefits of the Study

This review of plant security in the American nuclear power industry has given the Nuclear Regulatory Commission a sound, analytic basis for implementing its new security regulations. The interactions between systems were discussed with plant engineers and operators and verified by reference to the safety reports, emergency operating procedures, and various analyses done by equipment vendors, national laboratories, and the Regulatory Commission.

The reviewing process gave plant operators an insight into the analytic techniques used by Los Alamos team members and an appreciation for the value of these techniques. Many of the licensees were skeptical about the credibility of outside inspection teams until they saw that the analyses were simplifying rather than complicating their security operations.

Beyond the problems of plant security, the study has shown the potential of using TRAC to identify safety problems not detected by conventional safety analyses. The scenario that paralleled the Three Mile Island accident (see accompaying note "A Strange Coincidence") could as well have been undertaken in a safety analysis instead of the security analysis. The computer code does not distinguish between the loss of a nuclear plant component from sabotage and the loss of that same component from an accident. The value of this tool has been demonstrated and it is now available to the Nuclear Regulatory Commission for both security and safety evaluations.

Finally, in its role as an energy research laboratory, Los Alamos National Laboratory has also benefited from participation in this program to identify vital areas and to assist the Nuclear Regulatory Commission in implementing security regulations. Los Alamos engineers are gaining component-level familiarity with all nuclear power plants in the United States. Discussions of study results with plant engineers have helped in validating and refining analytic techniques. And the overall effort has demonstrated another application of the Laboratory's technological capabilities. ■

Sidebar:

A STRANGE COINCIDENCE

During the vital areas study, Los Alamos nuclear engineers performed a series of thermal-hydraulic transient analyses to determine the effect of two sabotage scenarios involving loss of the steam-generating function in a nuclear power plant.* A computer-based event tree had flagged the auxiliary feedwater system as Type I vital equipment because its destruction in conjunction with certain other acts might cause dangerous overheating of the reactor core. Some utilities questioned this designation. They maintained that even if the steam generator were out, water pumped into the nuclear core by the high-pressure injection system and then released as steam through the safety valves would remove the decay heat. But no one had made the mechanistic calculation that would prove or disprove the feasibility of this feed-and-bleed cooling. Hence the Los Alamos study. The results indeed supported the views of the utility operators concerning certain reactors systems; the high-pressure water injection system could take over and thus the auxiliary feedwater system would not be Type I equipment. By a strange coincidence, the scenarios also foreshadowed many of the key events of the Three Mile Island accident.

One scenario in this computer study postulated a loss of all ac power, which resulted in a number of events including the sudden shutdown of the turbines and the reactor and a loss of the steam generator’s heat-withdrawing properties. These events were duplicated at Three Mile Island by the initial accident sequence. The scenario assumed that the relief valve on the pressurizer was opened. This was the valve that accidently stuck open during the Three Mile Island accident. The study then examined how the reactor would behave if no auxiliary feedwater were available and the high-pressure injection pumps were not turned on for various time periods. The operators at Three Mile Island, believing their pressurizer vessel to be falling completely with water, or “going solid,” sharply reduced flow from the high-pressure injection pumps. A solid pressurizer would indicate too much water in the primary coolant system and risk loss of pressure control. In actuality the open valve acted as a leak (small loss-of-coolant accident) and the primary system was losing coolant. So the actions taken by the operators to counter the apparent solid pressurizer (cutting back on high-pressure injection) actually aggravated a relatively minor loss-of-coolant situation. This led to the creation of voids in the primary system and ultimately to the uncovering of the reactor core, This was the major cause of the reactor fuel damage at Three Mile Island. The misinterpretation by the operators about what was actually happening to their reactor hinged on the phenomenon of a solid, liquid-filled pressurizer coincident with a reactor core that was being uncovered. The response predicted by the Los Alamos computer analysis included the formation of a steam bubble in the reactor core that increased in size and uncovered the core centerline in 23 minutes. The close parallel between the hypothetical sabotage and the real accident demonstrates vividly the importance of detailed, computer-aided analysis in the evaluation of both the security and the safety of nuclear power plants. ■

J. W. Bolstad and R. A. Haarman, “Summary of Thermal-Hydraulic Calculations for a Pressurized Waler Reactor, ’’Los Alamos Scientific Laboratory report LA-8361-MS (May 1980).

Acknowledgments

The authors gratefully acknowledge the contributions made to the vital areas section of this article by Ronald L. Cubitt, Jerry J. Koelling, and John L. Rand.

Special thanks to the Dynamic Testing Division and to its Phermex Group for their contribution of photographer James E. Lewis's time and skill in developing the photograph on pages 120 and 121 of our "Sabotage" article.

Commendation by Nuclear Regulatory Commission

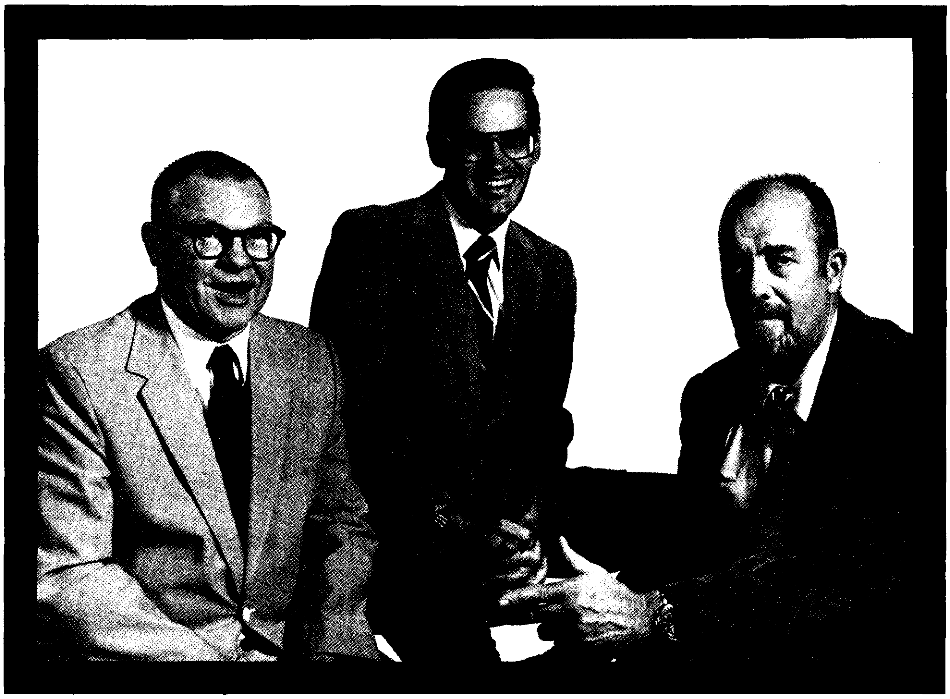
The following members of the Los Alamos technical staff assisted the Nuclear Regulatory Commission in the security analysis of nuclear power plants: Richard J. Bohl, William A. Bradley, Donald F. Cameron, Walter S. Chamberlain, Eddie R. Claiborne, Ronald L. Cubitt, Richard D, Foster, Paul M. Giles, Roy A. Haarman, Walter D. Hatch, James O. Johnson, Jerry J. Koelling, Richard W. Leep, Charges A. Linder, Joseph W. Neudecker, Jr., Alden T. Oyer, John L. Rand, Donald G. Rose, and Dean H. Whitaker. The Commission praised the men for "their dedication in spending considerable time away from Los Alamos to visit nuclear power facility sites and in devoting greater than normal effort in completing review assignments in a timely manner. . .“

Further Reading

Harold A. Bennett, "The 'EASI' Approach to Physical Security Evaluation," Sandia Laboratories report SAND76-0500 (January 1977).

G. Bruce Varnado and Roy A. Haarman, "Vital Area Analysis for Nuclear Power Plants," Los Alamos Scientific Laboratory unclassified release LA-UR-80-2407 (August 1980).

The Code of Federal Regulations, Title 10, Energy, (General Services Administration, Washington, D. C., 1980), pp. 514-520.



Authors Donald G. Rose (left), Roy A. Haarman, and William A. Bradley.