PROTECTING NUCLEAR MATERIAL: 'COMBATIVE' RESEARCH

Scientists, engineers and computers have begun to vigorously exploit the resources of modern technology to develop a formidable obstacle course of safeguards

BY MICHAEL A. GUILLEN

President Carter's recent approval to build a uranium enrichment plant at Portsmouth, Ohio, will increase the United States' capacity to make uranium reactor fuel by about one-third. Overtaxed with foreign and domestic demands, the country's three facilities annually process about 3.75 million kilograms of enriched uranium (U-238 with 3 percent U-235).

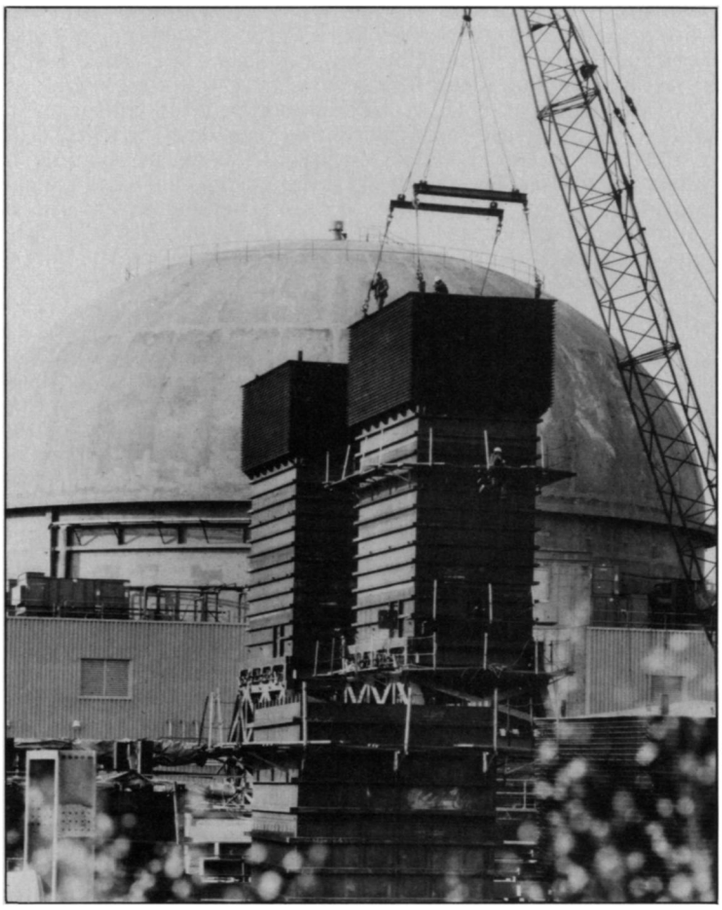
Construction of the new plant will commence in late 1978 and preliminary operations in 1986. It will use high-speed centrifuges to separate U-235 (the "active ingredient" in reactor fuel) from gaseous raw uranium (about 99.3 percent U-238). The three existing U.S. plants accomplish this separation by forcing gaseous uranium through thousands of "strainers."

Carter's public decision also referred to his concern about worldwide proliferation of nuclear technology. He hopes that this extra U.S. capacity will equalize supply and demand and thus obviate the incentive for other countries to build their own plants. Until recently, the United States supplied about 95 percent of the enriched uranium needed by non-Soviet-bloc countries.

A tacit assumption in Carter's philosophy, of course, is that the United States can be safely entrusted with the enormous obligation of maintaining reliable safeguards against criminal acquisition of nuclear material, especially enriched uranium and plutonium.

Last month, the Nuclear Regulatory Commission announced proposed improvements of some existing nuclear security regulations (SN: 7/16/77, p. 38). Concurrently, the Institute of Nuclear Materials Management held its annual meeting in Washington with the theme: "Safeguarding the Nuclear Fuel Cycle."

Michael A. Guillen is a Ph.D. candidate in physics and astronomy at Cornell University and writes a weekly science column for a chain of California newspapers. He is working on the staff of SCIENCE NEWS for the second summer in a row.



Battelle-Northwest Photo

Some new plutonium-handling safeguards are being tested on the premises of the liquid sodium-cooled reactor at Hanford, Wash. Two large heat exchangers loom in front of the main dome housing the test reactor.

During the three-day affair, research groups discussed their latest efforts including major prototypes of a plutonium-handling security facility and a perimeter security layout. Both of these, designed and built by engineers from Sandia Laboratories in Albuquerque, N.M., recently became partly operational and are being evaluated.

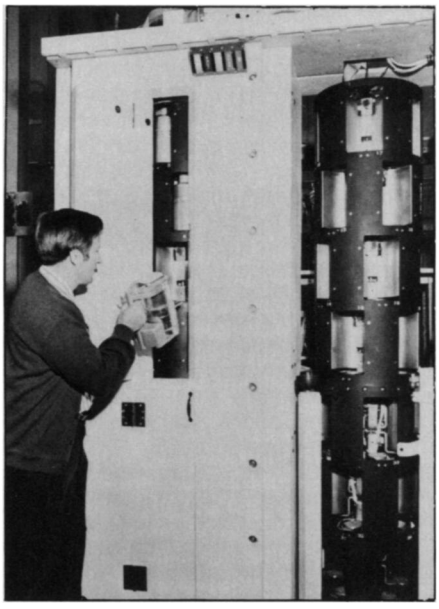
Other INMM conferees described the current generation of security systems, which as it happens, are largely comprised of commercially available technology. There are fences festooned with a formidable array of intrusion alarms; elaborate computerized systems that keep track of personnel and nuclear material; and television cameras, radiation detectors and seals that betray any effort to tamper with them.

The more futuristic, yet also largely over-the-counter contrivances identify a person by his or her voice, handwriting pressure or card key. Still others can sense body heat, metal, motion or small vibrations in a floor.

Complementing the talks on experimental hardware were those that described theoretical efforts to create a safer nuclear facility or transport. There were a plethora of hypothetical models purporting to depict ambushes, sabotages and general malevolence perpetrated by conventional means. Adversaries were typically portrayed effecting their heists with standard armaments.

None of the models explicity considered the role of such potent criminal devices as seizing hostages, enlisting airborne support or extortion. This was less a matter of oversight, however, than an indication of the field's embryonic stage of development.

A dubious aspect of the theoretical modeling, illuminated during many of the meeting's question and answer periods, is the quantification of human factors. If a conspirator witnesses the defeat of several companions, will he retreat or surrender? Experiencing difficulty picking the first lock, will an intruder be sufficiently unnerved that his ensuant distress will affect the outcome of his plans? These and other critical considerations might never be adequately accounted for, some argue, by



Sandia Laboratories

Plutonium storage vault restricts access.

numbers in a computer program—not even probabilistically.

Questionable as their results may now be, the computer simulations will ultimately assist administrators on how best to allocate a security budget. They will help establish priorities: more guards or more alarms, more checkpoints or more television cameras, better communications or better escort armament.

One model deals with the safe conveyance of nuclear material across open highways. Using it, R.J. Gallagher, K.G. Stimmel and N.R. Wagner of Sandia Laboratories in Livermore, Calif., investigated the casualties sustained by variously organized convoys. The basic model pits a parade of trucks laden with nuclear cargo against a small, well-armed group of ambushers.

The model predicts different attrition rates depending on the number, spacing and speed of a convoy's trucks and the strength and weaponry of the adversaries. Although not conclusive, one result indicated a slight advantage for randomly spaced trucks.

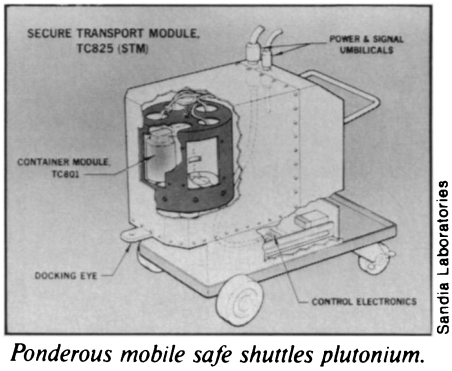
Another Sandia theoretical model was developed by Kathryn P. Berkbigler to predict the number of available law officers along any contemplated convoy route. Berkbigler, using data from the U.S. Bureau of the Census and FBI, can apply it to many routes actually in current use.

One was the subject of some controversy several months ago. Some critics publicly questioned whether there was adequate protection of a nuclear shipment enroute from the enrichment plant at Oak Ridge, Tenn., to Chicago's O'Hare airport. (From there the cargo was bound for West Germany.) According to Berkbigler's model, there are more than 25 police available within 50 kilometers of any point along that particular itinerary. In general, a primary objective of the model is to identify and remedy those locations deficient in local police protection and thus undesirable as transport routes.

Currently, government-owned nuclear payloads are carried in penetration-resistant trailers towed by armored tractors. The special container, developed by the U.S. Energy Research and Development Agency, is called a Safe-Secure Trailer and resembles a standard semitrailer. Its walls, ceiling and floor, however, are designed to resist vigorous attack.

A besieged transport vehicle can be automatically immobilized—its tires flattened, for instance—to preclude its being driven away illegally. Each shipment is protected by armed escorts who ride in vehicles specially designed to keep them comfortable and alert during long journeys.

A key to the ERDA transport system is the nationwide computerized communication network that keeps track of all active shipments. The digitized system is capable of monitoring the status of all convoys simultaneously.



Sandia Laboratories

Ponderous mobile safe shuttles plutonium.

Since 1972, the fleet of ERDA trailers has logged about 1 million miles without a reported theft or sabotage attempt.

Substantially more attention was paid at the INMM conference to safeguards useful in stationary facilities.

Researchers at Sandia in Albuquerque have built a full-scale perimeter security system somewhere "in the southern

Computers: Lock and key of nuclear safeguards

Nuclear safeguards roughly divide into two major categories: physical security and materials accountability. The former refers to security hardwarelike fences, alarms and ID's; the latter, to elaborate accounting systems designed to oversee a facility's inventory of nuclear material.

This dual line of defense, of course, is vital, potent and most effective against conventional thieves. Worrisome, however, is the ubiquitous role of computers in the safeguard network.

At the INMM meeting, for example, computers were charged with every imaginable security task: from monitoring alarms to counting plutonium-filled modules. Manifold studies of hypothetical, coercive adversaries were described, but similar efforts involving sophisticated, "white-collar" criminals were notably lacking.

A single rapporteur addressed the potential threat to the nuclear industry of offenders, who by guile and deception use "the characteristics of a system to subvert it and [do] not subject it to frontal attack." The talk was based on a report prepared for the Nuclear Regulatory Commission in January. Its authors, Herbert Edelhertz and Marilyn Walsh of the Battelle Human Affairs Research Center in Seattle, conclude that security against the subtle criminal is "not likely to be found in expensive protective devices or in elaborate procedures."

A common belief, expressed by many attendees and Clifford V. Smith Jr., director of the NRC's Office of Nuclear Material Safety and Safeguards, is that the shrewd malefactor can generally be thwarted via stringent materials-accounting systems. These typically require massive computer programs, however—one of the very aspects of safeguards most vulnerable to the white-collar criminal.

A materials accountability scheme "is not the be-all and end-all," says Edelhertz. The level of security it offers is readily subverted by the skillful offender's extensive repertoire, as revealed during recent history.

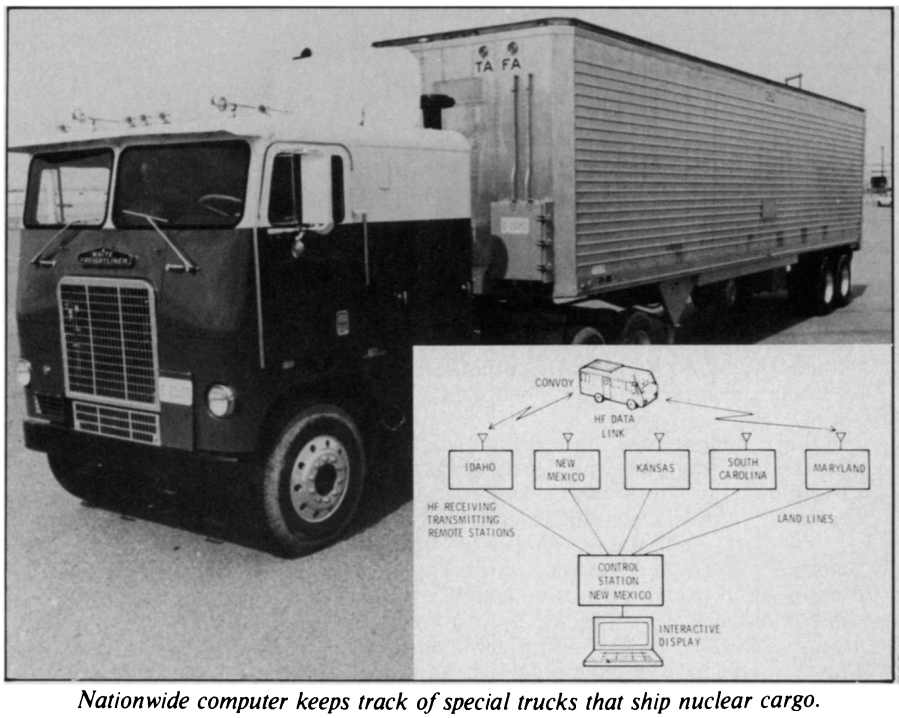
The public record abounds with cases of computer fraud, but "practically all [of them] have been discovered by accident," says Edelhertz. One bank's computer programmer, who fixed it so the machine ignored overdrafts of his personal checking account, was not caught until the computer broke and the bank was temporarily forced to operate manually.

The U.S. Chamber of Commerce estimates that at least $40 billion per year is lost to white-collar crime in the United States. A substantial portion of this involves computer fraud. Notwithstanding the unreliability of this estimate, "these dollar losses dwarf into insignificance those of ordinary crime," says Edelhertz.

For some foreign countries and overzealous political gangs, nuclear material of bomb quality may suit their schemes better than even money. In this regard (motivation), current statistics on white-collar crime are relevant in evaluating the possible threat to the nuclear industry.

Any computer—the machine—is supremely scrupulous. It also can be profoundly naive, and in skillful but perfidious hands, it can readily be manipulated to deceive humans, other computers and even itself.

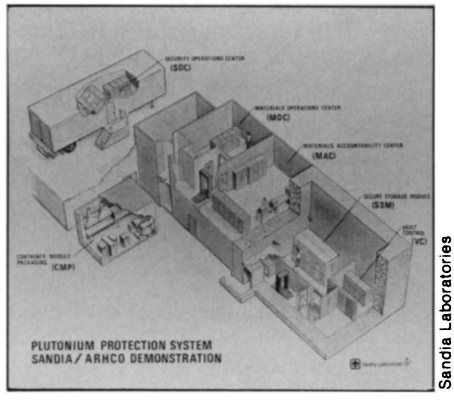
—M.A.G.



ERDA

Nationwide computer keeps track of special trucks that ship nuclear cargo.

Great Plains." The rectangular area enclosed by two chain-link fences has a perimeter of 3 kilometers. Between the fences is an illuminated "isolation zone" (at least 30 meters wide) constantly surveyed from above by microwave motion detectors and television cameras. Buried 45 centimeters below ground are electrical cables sensitive to ground vibrations, like those that would be caused by an intruder's footfalls. Two large sentry towers at diagonally opposite corners also house an elaborate alarm control system.



Sandia Laboratories

Prototype plutonium facility: Partly built.

Simple mercury switches are placed on the inner fence to detect motion caused by a trespasser trying to scale it. This fence is also rigged all around by two horizontally parallel wires, between which is an electric field that reacts in a measurable way to any presence.

At first, the security compound was susceptible to frequent false alarms. The main culprits were jack rabbits, wind that rattled fences and raindrops that set the ground into motion. Some of these nuisance alarms were eliminated simply by reducing the sensitivity of the devices affected, without appreciably jeopardizing security.

Other recurrent spurious alarms are taken care of as they happen by an organized scheme of alarm priorities. This partly relies on the philosophy that a bona fide intruder will trigger a pattern of alarms distinguishable from the ones caused by "imposters" like jack rabbits.

The validity of any alarm is decided on by a computer that takes second-by-second account of prevailing weather conditions. So if a specific sensor vulnerable to the wind triggers while a sufficiently strong gust is blowing, the computer will "ignore" the alarm.

Besides screening out likely nuisance alarms, the computer will also assess the relative urgency of several simultaneous alerts. Using the information, guards will know to which alarms to respond first.

Sandia's plutonium protection system, on the other hand, is designed primarily to assure the integrity of a nuclear facility's internal operations. E.A. Bernard, D.S. Miyoshi and F.D. Gutierrez of Albuquerque are testing two prototypes—one at the reactor site in Hanford, Wash., and one at Albuquerque—by going through the motions of handling plutonium and deliberately challenging the security measures. The former activity, actually using plutonium, is being emphasized at the Hanford plant; the "devil's advocate" tests at the other.

The heart of this security operation are computers that continually oversee the traffic of personnel and nuclear substances within and between compartmentalized working areas. All transactions involving nuclear material are prescheduled, and computers—via information from interlocks, checkpoints and various other detectors—verify that each step was completed in the time allotted it.

The nuclear material is handled largely in heavily shielded modules, each with its attendant electronics package that monitors temperature and pressure and stores a security code. This identifies a container and reveals if it has been mishandled.

The plutonium receptacles are stored in carousel-vaults resembling ponderous automated food vendors. A vault's individual compartments are staggered so as to allow access to only one of them at a time. The system's computerized accountant keeps an overall running inventory of the plutonium.

An electronic "credential" transmits an identifying code each time its wearer passes a special portal so that the computer always knows where a nuclear plant's personnel are. This scheme, under development by a separate but cooperative group within Sandia, is entirely automatic, unlike popular card key systems that require user participation.

For each of many INMM conferees, the challenge to develop safeguards is a personal brain teaser. Their expressed enthusiasm is best compared to the faithful who believe they can build a perpetual-motion machine despite the odds. The odds, in this case, are primarily affected, as one conferee privately noted, by the preassurance that better safeguards will not only improve security but also provide others with some brain teasers. □