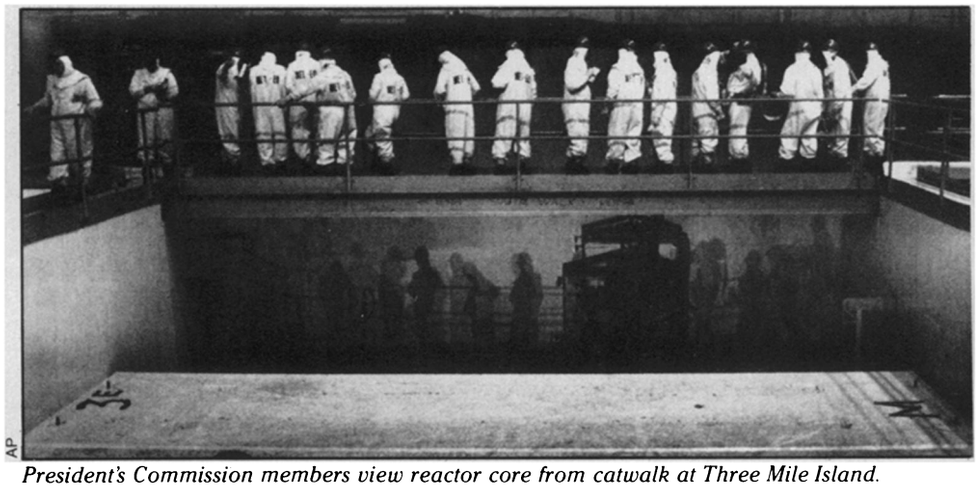
HUMAN ERROR:

The Three Mile Island accident suddenly brought home the importance of human performance in modern technology. And experts say it may be man, more than machine, that needs improvement.

BY JOEL GREENBERG


AP

President's Commission members view reactor core from catwalk at Three Mile Island.

The collaborative symphony performed by man and modern machine is filled with sour notes. Because most human errors are subtle and inconsequential, they pass unnoticed and do not influence most of present-day technology's complex tasks: Close to 5 million airplanes take off and land safely each year in the United States; trains usually manage to stay on their tracks and transport people and materials without incident, if not always on schedule; massive ships generally are able to navigate amongst one another through narrow harbors. And, at least until now, nuclear plants have been able to provide huge amounts of power to large areas without blowing up or melting down.

But last year's near-meltdown at the Three Mile Island nuclear plant in Pennsylvania is indicative of widespread and increasingly difficult problems of matching human performance and reliability with that of sophisticated machinery. As a rule, mistakes that do reach the public consciousness are so disastrously out of tune with the expected technological harmony that even the most untrained ear can pick them up. These errors usually lead to events that are fatal, or potentially so, to large numbers of people — the TMI accident; the derailment of trains carrying passengers or toxic chemicals; plane crashes that kill hundreds, such as those in San Diego, Chicago and the Canary Islands; the inexplicable collision of an oil tanker with a Coast Guard cutter on a clear, moonlit night in Tampa Bay.

Human factors are simply ignored at the design stage.

The vast majority of mistakes, however, do no harm because the system either compensates by itself or allows human operators time to correct the error. But whenever humans are involved, mistakes are bound to occur and do so with a frequency that some find disturbing. Even among commercial airline pilots, considered perhaps the best prepared of modern technicians, experts estimate an average of one to two errors — albeit minor, correctable ones — per hour.

For reasons made even more obvious than before by the near-catastrophe at Three Mile Island, the orchestration of nuclear power plants is the current priority among experts in "human factors" engineering. And at this point, their assessment of the state of the art might coincide with that of a critic who has just been forced to sit through a junior high school's rendition of Beethoven's Fifth Symphony.

Nuclear power is far too important to be left to nuclear engineers.

"The design of [nuclear plant] systems today is simply in an intolerable state," says Donald Norman, a University of California at San Diego psychologist who specializes in human performance in the operation of mechanized systems. "Good design and analyses of human factors are simply ignored at the design stage," he says. "Designers would never think of doing this in [the design of] equipment."

The underemphasis on the role of humans in plant operation probably would still be a non-issue had the TMI accident not occurred. But some experts say it would only have been a matter of time before a similar accident exposed the deficiencies. "For years we have been relying on operator adaptability to overcome design deficiencies," says Gregory B. Minor of MHB Technical Associates. "There is an urgent need for a human factors research facility to evaluate control room changes ... and provide hard data on their impact on operating effectiveness and safety *before* they are cast in concrete."

In the TMI aftermath, investigations by the Carter administration's Kemeny Commission and a Nuclear Regulatory Commission team, headed by Washington attorney Mitchell Rogovin, have depicted a scenario of system failure made possible only through a series of unforeseen lapses in judgment and communication. Such errors — primarily consisting of opening valves that were supposed to be closed and vice versa — are inevitable in any complex system that does not require its human performance standards to match those of its hardware components, according to some scientists. "As systems become larger and more energetic ... error [becomes] of violent ... lethal importance," says John W. Senders, an electrical engineer and psychologist at the University of California at Santa Barbara and the University of Toronto and a recognized authority in human performance in technology. "Nuclear power is far too important to be left to nuclear engineers."

The TMI analyses appear at least partially to support the contention of Senders and others that the near-meltdown could have been avoided through more common-sense plant design and improved training of workers. "Human factors engineering ... has blossomed in the aerospace, defense and aircraft industries," says the Rogovin report. "But nuclear utilities, vendors and architect-engineer


Metropolitan Edison Co.

Size and layout of TMI-2 control room may have confused workers.

Science Service, Inc. is collaborating with JSTOR to digitize, preserve, and extend access to *Science News*. www.jstor.org

THE STAKES ARE RAISED

firms have done very little to incorporate such learning into their designs, and the NRC has done virtually nothing to require them to do so.

"This failure reflects the preoccupation of the industry and the regulatory agency with hardware systems. The NRC gives short shrift in the design safety review process to determining how well operators will be able to diagnose abnormal events, based on what they see on their instruments, and respond to them. In part, the failure is also due to a lack of expertise."

Apparently, seeing their instruments in the first place has been a major problem for workers not only at TMI but at other nuclear facilities as well. "There is evidence that the operators of TMI-2 were confused by equipment indications available to them on March 28, 1979," says Ronald M. Eytchison in a technical staff analysis report to the President's Commission on the Accident at Three Mile Island. "The confusion ... may have resulted in part from the control room layout and design or from the equipment malfunctions. The control room was evidently designed more for normal operation than for accident conditions," he says. "The arrangement of controls and indicators for engineered safety features was not well thought out."

Reactor operators are not extensively trained to diagnose and cope with the unexpected.

TMI design deficiencies cited in the reports of Eytchison and the Rogovin committee apply to a significant number of nuclear plants, according to the investigators. The problems include: controls located far from instrument displays that show the condition of the system; cumbersome and inconsistent instruments that often look identical and are placed side-by-side, but control widely differing functions; instrument readings that are difficult to read, obscured by glare or poor lighting or actually hidden from the operator; contradictory systems of lights, levers or knobs—a red light may mean a valve is open in one plant area and closed in another, or pulling one lever up may close a valve, while pulling another lever down may close one. In one plant examined by Senders, a blue valve was used to control the heat system while a red valve controlled the cooling system — "I call that criminal," he says.

During the early stages of the Three Mile Island crisis, the TMI-2 control room was a cacophony of blaring alarms, accompanied by flashing lights. But because many of the more than 1,500 plant alarms are triggered under relatively "normal" operating conditions, it is difficult if not impossible to detect a real emergency within a reasonable time after it occurs, the technical staff analysis suggests. Moreover, "a single 'acknowledge' button silences all of the alarms, making it likely operators could not comprehend the significance of all alarm conditions," says the report.

In some cases, emergency control systems at TMI are haphazardly scattered throughout various plant locations and may not even be visible to key personnel. "For instance," says Eytchison, "the high pressure injection (HPI) throttle valves are operated from a front panel but the HPI flow indication is on a back panel and cannot be read from the throttle valve operating positions."

Reports Rogovin: "No visual alarm signaled that the emergency feedwater system was completely blocked off. This was not discovered for some eight minutes into the accident, apparently because poor panel layout makes systems misalignment difficult to spot, and because a paper tag hanging from a handle on the control panel obscured an indicator light that would have shown the operators the position of one of the block valves shutting out this system."

All accidents in one sense can be traced to the failure of human beings in complex systems.

In another confounding turn of events, the report continues, important visual alarms "that might have told operators the pressurize relief valve was stuck open, even though the control panel light showed it was closed ... are on a panel remote from the central console that *faces away* from the operator!" Those particular alarms were also keyed to temperature and pressure in the reactor coolant drain tank, into which hot water from the stuck-open valve was pouring for more than two hours after the accident started, the report states.

"Certainly, the initial meshing of this emergency machinery in the control room is something short of symphonic," Rogovin reports. "There is good reason for [the workers] to suspect that their operator training and years of experience are serving them badly in this event; none of the buttons they've pushed or the switches they've pulled have produced the needed magic. Intellect tells them they don't really know what is going on; ego tells them none of the rest of the guys do either; on the evidence, both are right."

It is likely that such widespread design inconsistencies would have hampered even highly knowledgeable, stringently trained technicians. But according to Rogovin and a separate analysis report by Eytchison, the training of workers at TMI and elsewhere appears to fall considerably short of that in other high technology fields, such as airline operations.

"There is no regulation regarding operator selection and training; the NRC has no minimum eligibility standards for the qualification of operators," Eytchison says in the report. "Reactor operator candidates do not have to meet any requirements concerning minimum education, experience, reliability, criminal record or stress fitness.... There is a lack of emphasis on the comprehensive knowledge of theory, principles of operation, kinetics, thermodynamics and so on, which would enable operators to correctly interpret information available to them in the control room. Review of typical [licensing] examination contents indicates the examinations are consistent with the regu-

Continued on page 125

Wide World Photo

In the wake of its puzzling crash with the Coast Guard cutter Blackthorn, *the grounded tanker* Capricorn *is pushed by tug boats near the Sunshine Skyway in Tampa Bay. Exactly how or why the two vessels collided on a relatively clear night Jan. 28 remains a mystery. The cutter sank almost immediately after the fatal crash.*

. . . Human error

lations; they do not ensure that license candidates have an in-depth knowledge of nuclear reactor theory, design and operation."

Rogovin compares the operation of an airliner with that of a power plant — much of the work is essentially routine, at times boring. But the major difference, he says, is that the airline pilot is trained not only to handle but to diagnose emergencies such as loss of an engine, sudden depressurization and hydraulic failure. "It is here that reactor operator training has been seriously deficient," says the report. "Other than being required to memorize a few emergency procedures, reactor operators are not extensively trained to diagnose and cope with the unexpected — equipment malfunction, serious transients [temporary electrical oscillations], events that cannot be easily understood."

Ironically, it may be that the generally high reliability of today's nuclear plants is in part responsible for deficiencies among workers. "If a system breaks down once every 10 years, will people have enough practice to handle it?" asks Senders. "If an operator is never called upon to act, the system must be 100 percent reliable — and they are," he adds with a smile. "We haven't had a blowout yet"; then, somberly: "God help us, we hope we'll never know what the reliability of systems really are."

Even were unlimited resources available for upgraded operator selection and training programs, just how much improvement could be achieved in safety and performance is uncertain for two reasons: the variability of human beings, particularly under stress, and the present shortage of data on human error. "A human can fail in so many ways, it almost defies description," says Alan D. Swain of Sandia Laboratories. Specifically he says errors may be placed in any of five categories: omission, commission, extraneous action, sequential and time error.

The TMI accident, which experts say probably incorporated several types of error, is by no means the only instance in recent years in which mental lapses have played a role in technological disasters or near-disasters. "All accidents in one sense can be traced to the failure of human beings in complex systems," says Senders.

According to psychologist Norman, "human processing is lazy — we process with as little depth as needed." He cites the example of a crash of two large commercial jets on a runway in the Canary Islands several years ago. The tower told one of the pilots he was "cleared for takeoff"; the pilot, apparently eager to return to his home base after an extended tour of duty, misinterpreted the message as a go-ahead to actually take off at that moment, precipitating the crash with the other plane, Norman says.

Senders, who was among those who formulated the design of military aircraft in the early 1950s, concurs that the human

AP

Worker checks radiation at TMI plant.

It is assumed that either humans won't make a mistake, which is idiotic, or that humans do not contribute to the performance of the system.

mind at times can be less than 100 percent reliable — sometimes with tragic results. He recalls a succession of crashes around that time when military planes plummeted to the ground for no apparent reason. It was later discovered that during routine maintenance, workers had reversed the airplanes' trim tab wires that controlled the flaps. To anyone less than totally familiar with the design of these specific planes, it may have seemed more logical to reverse the wires — which is exactly what some of the less knowledgeable workers did. Unfortunately, the naive placement of the wires in this "logical" position sent the flaps up when they were intended to go down, and vice versa.

"Preventive maintenance, if not done correctly, can be worse than no maintenance at all," says Senders, who also cites one study reporting the increase in auto accidents *after* mandatory inspections of steering and brakes. In the case of the military airplanes, Senders says designers could have made it physically impossible for the wires to be switched by requiring that the wire ends fit only into specific receptors. Similarly, he suggests that the risk of human error at power plants could be significantly reduced through straightforward designing — including more standardized colors and sizes for valves and levers — that meshes with human thought patterns and anticipates potential errors. It has been estimated that the probability of a plant worker failing to reopen a valve after closing it for inspection is 1 in 100. "That's just not acceptable," Senders says.

But any new, human-oriented designs or training procedures must be based on the types and frequency of mistakes made in nuclear plants — and, experts concede, there are woefully few data in that area compared with what is known about technological reliability. Part of the problem may be traced to what Senders calls a "self-protective attitude" and a "reluctance to release data" by plant managers concerned with their own performance records.

"Lack of data is the single most important factor impeding the development of HPR [Human Performance Reliability] indices and the utilization of mathematical models of human performance," says David Meister, senior staff specialist at the Naval Personnel Research and Development Center in San Diego. Adds Swain: "Human reliability analyses are rarely performed; it is assumed that either humans won't make a mistake, which is idiotic, or that humans do not contribute to the performance of the system."

Despite the paucity of such information, Norman says even the current available knowledge is "good enough" to have helped develop techniques that might have "prevented many errors and accidents up to now."

Swain and his colleagues have developed the currently "most widely used" human reliability model, called THERP — Technique for Human Error Rate Prediction. Although THERP may be the most sophisticated method yet developed of predicting human error rates and evaluating "the degradation to a man-machine system likely to be caused by human errors," even Swain allows that its accuracy and value could be substantially improved if more solid, scientific data were available.

Senders stresses that models for obtaining data on human error have "been available for 25 years." Such study techniques — used primarily in the military up to now — could be applied to the operation of nuclear power plants, he suggests. "All that has been done [in relation to nuclear plants] is to count errors — and that information has been used to indicate a problem with the *equipment,*" he says. "No one knows, in fact, what kind of errors *people* will make."

Senders proposes to study the combined effects of time stress and training level on the rate and types of error in power plants. This would be done by "synthesizing a job" — as simulated by a computer — where the experimenter would have "complete and absolute control over the job. You would determine the percentage of errors generated from within the system and from outside of it . . . you look for consistency of errors and performance on the job."

Until a large-scale commitment is made to this and other types of investigation into human error, Senders says, "we will continue to get biased numbers . . . overestimating the safety" of nuclear plants because "most errors are absorbed by the systems, and very few actually result in accidents."

Even now, he says, probably enough is known about human factors to eliminate "a whole class of potential errors" — including some of those that contributed to the Three Mile Island accident. "At TMI, the cost of human error was made evident; it is clear that people in great positions of power do not always do the right thing," he says. "But when things fail you do need people — and things do fail." □