The Salem Case: A Failure of Nuclear Logic

The "impossible" happened twice in three days when a fail-safe device failed at a New Jersey plant

Near the southern end of the New Jersey Turnpike, on the marsh of Alloway Creek, the Salem-1 reactor did one of those things on 22 February that a nuclear plant is not supposed to do. It refused to stop the fission reaction in its core when ordered to do so by a safety control system. An operator had to intervene, turning a manual switch to shut off the reactor. This kind of failure, the nuclear industry had long believed, has a negligible chance of occurring, on the order of once in a million reactor operating years. Yet it has happened several times already.

By official count, the incident at Salem was the third time in commercial history that this safety failure has occurred. It has happened at military reactors as well, but no one has revealed how often because the data are secret. It happened for the fourth time in commercial history on 25 February, again at Salem. It was only after the second incident that the federal government learned of the trouble.

The plant's owners, Public Service Gas and Electric of Newark, New Jersey, reported only the second failure. The reason, the company said, was that the operating staff had shut down the reactor on 22 February and restarted it a day later without understanding that there had been a safety failure. They apparently could not decipher a computer printout that recorded it. Company officials agree that, in hindsight, it is easy to spot the malfunction in the record. Indeed, Salem's staff spotted it almost immediately on the morning of 26 February when inspectors from the Nuclear Regulatory Commission (NRC) visited the control room and asked to see the printout. But they said they could not spot it before because they "weren't looking for it."

The NRC began an investigation. On 15 March, the chief of reactor regulation, Harold Denton, declared that the safety implications were "the most significant . . . that we have had since Three Mile Island." Their importance reaches beyond the problems at Salem and touches on the broader issue of how to shut down a reactor ("scram") when the safety system fails to do so during a routine anomaly in operations (a "transient") such as the one at Salem. This kind of failure is known to the experts as Anticipated Transient Without Scram (ATWS). The events at Salem show that a breakdown of the plant's electronic safety system is not so implausible as the industry has claimed in NRC proceedings on ATWS over the last decade. They also reveal, as NRC commissioner Victor Gilinsky said, an intolerable degree of carelessness.

ATWS has been studied as a hypothetical problem for more than 13 years and has been the subject of proposed regulations by NRC since 1973. The NRC staff thought it would be wise to build in extra damage-limiting equipment to prevent an ATWS from becoming an accident. No ATWS regulations have been adopted, however, because industry has opposed them, arguing that an ATWS is so unlikely to occur that no new protective measures are needed. The NRC summarized this opposition in a paper (NUREG 0460) written in 1978:

> The basic industry position is that the high reliability of reactor protection systems makes the probability of an ATWS event negligibly small and not worthy of consideration as a design basis. It is also maintained that if consideration of ATWS events is necessary in reactor safety evaluations, the requirements expressed in the staff status reports are excessively conservative. Such views were expressed in letters from individual applicants and industry groups including AIF [Atomic Industrial Forum] and EPRI [Electric Power Research Institute]. . . . The industry further contended that the cost of the changes required by the staff position to mitigate ATWS events would be significant and not justified.

One vocal advocate of this view, until 1980 when the NUREG 0460 proceeding died, was Westinghouse, designer of the Salem nuclear plant.

Harold Denton declared that the safety implications were "the most significant . . . that we have had since Three Mile Island."

During the first full briefing on Salem for the NRC commissioners on 15 March, staffers and commissioners spoke of careless management. Salem's owner was stung by this and responded at an NRC meeting on 24 March. The company chairman, Robert Smith, said, "We fully recognize the seriousness of the incidents . . . when a basic safety system failed to operate automatically." The NRC's findings "indicate to me and senior management of the company that there are areas which can and will be improved." However, Smith argued that other backup safety systems would have prevented any major mishap and said the hazards had been exaggerated.

Another company official said that the plant would be ready to resume operating within a few days and asked for the NRC's concurrence. The NRC did not agree. A detailed review is in progress, and it is unlikely that there will be any decision on restarting Salem before mid-April. The shutdown is costing the company $330,000 a day for makeup power alone.

While the Salem plant did not come near having an accident, it did deteriorate to a condition in which a serious accident could have occurred in different circumstances—for example, if both feedwater pumps (rather than just one) had been out, if the plant had been on full power, if the turbine had been left on, and if the emergency cooling system had failed to switch on. The operators handled the situation well, but another time they might not. This is what worries the NRC.

The risk in depending on the operators is twofold. First, they must realize within seconds that a scram is required. Second, a manual scram demands some form of active intervention—an electric impulse sent from the control room to the main shutoff switches two floors below, the physical manipulation of the downstairs switches, or the use of other plant functions to bring power under control. A loss of control room electricity would make this part of the job difficult, even if the operators knew what to do. Fortunately, on 22 February there was only a partial and temporary blackout of the control room, the reactor was

running at 20 percent of capacity, and the operators responded correctly.

The reactor was shut down in both incidents within 30 seconds of the need for a scram. Clearly the operators moved quickly but not extraordinarily so when measured against the demands of an ATWS in a Westinghouse plant such as this. According to the NRC's calculations, a delay of 100 seconds could lead to serious damage.

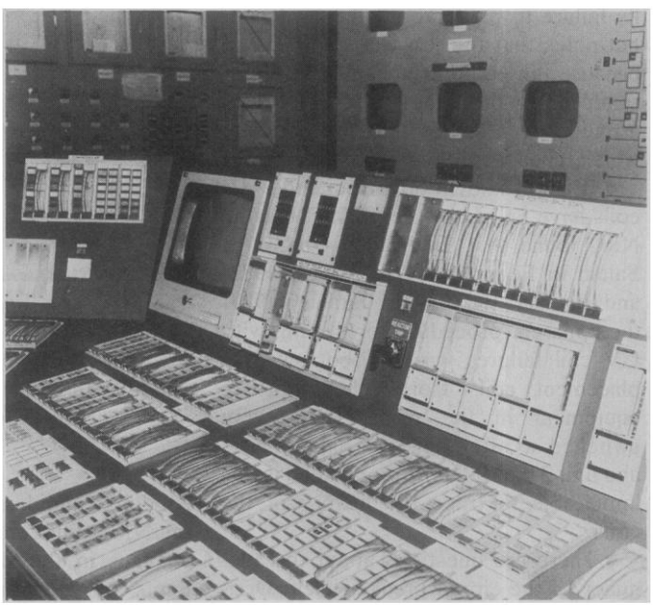
Because the margin for error is so small, nuclear plants are wired in a "fail-safe" fashion so that any major disturbance of the controls, including loss of power, is supposed to trigger an automatic shutdown. It is this automatic logic which is supposed to fail no more than once per million reactor years. But the one-in-a-million event happened twice in three days at Salem. Why?

The problem centers on a pair of huge circuit breakers which are meant to disconnect during an emergency. These Westinghouse devices, known as DB-50's, supply power to the mechanism that raises and lowers the core control rods which regulate the speed of the fission reaction. Under normal circumstances, the power flows through the DB-50's, the rods are lifted and held in the "up" position, and the core generates heat. Any of a number of danger signals can trigger an alarm in the plant's electronic logic telling the system to scram. When this happens, the electronic brain sends a message to the DB-50's telling them to break the circuit. They open, releasing the rods, which drop by gravity into the core. For added safety, DB-50's are used in pairs, wired in series, so that if one fails the chances are good that the other will work. It only takes one to break the circuit. At Salem, both DB-50's received the automatic message to scram and both failed to open. This happened on 22 February and on 25 February.

Other things happened on 22 February which are peripheral to the ATWS but revealing about the environment surrounding it. A major circuit in the control room failed, cutting off electricity to a reactor coolant pump and to the control room itself. The lights went out briefly, until emergency power came on. Some control indicators stopped working. An operator, realizing the reactor should be turned off, reached for the main "reactor trip" switch. This sends a stronger scram signal than the one from the automatic logic. (The safety logic had already sent a message, without effect.) The switch handle came off in his hand. The company explained later that the operator was new on the job and unfamiliar with the control board. It took him a few seconds to insert the handle and turn the reactor off. In the confusion, the operators never appreciated the fact that the automatic shutoff system had failed and that they had experienced an ATWS.

The second event was less chaotic, but like the first it left the operators with the impression that nothing extraordinary had happened. It was only after the plant had been shut down and the circuitry checked—according to the NRC, 30 to 60 minutes later—that they realized an ATWS had occurred. Their first thought was that they had experienced a false alarm, and this is why the electricians were called in to check the circuitry.

There have been several detailed reviews of Salem's troubles, two by the NRC regional office in King of Prussia, Pennsylvania, and one by the Franklin Research Center in Philadelphia, which was asked to examine the part of the DB-50 that failed. Some of the more important findings are as follows:



Where man meets machine

Part of the control board at Salem, showing rod level indicators (middle right) and the main trip switch (center), which the operator must turn to stop the fission process manually. When the operator reached for the switch on 22 February, the handle came off.

- The fundamental fault was in a device called an undervoltage (UV) coil in the DB-50. It failed to activate the breaker when it received a message to do so from the control room. It is supposed to switch off the power not only when it receives a signal from the plant's automatic logic, but also whenever there is a sudden loss of power. As it turns out, the UV coil, the heart of the fail-safe system, has a long history of trouble.

As early as 1971, because of malfunctions in a UV coil at the H. B. Robinson plant in South Carolina, Westinghouse recognized that this device needed special attention. Westinghouse sent out a technical bulletin in December 1971 warning owners of this fact and urging them to have the device replaced with a modified version. Because of a repeated failure of a UV coil at Robinson in December 1973, Westinghouse sent out two more letters in 1974, giving important instructions on the twice-yearly cleaning and lubrication of UV coils.

On 9 December 1971 the NRC sent out its own bulletin describing how UV coils had failed on three occasions in two different plants. One of the cases involved a double failure, like Salem's, during testing. The NRC described the causes of failure as "dirt accumulation on exposed linkages," and "mechanical binding of the trip lever."

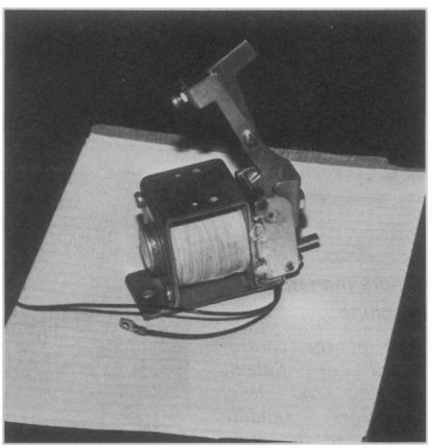
- Gary Toman, senior engineer at the Franklin lab who inspected a UV coil taken from Salem (he does not know whether it was one of those that failed), identified three general faults in the device. He found mechanical binding of the trip lever, excessive wear of linkages, possibly due to poor lubrication, and uncalled-for adjustment of a spring that would tend to make the device less likely to trip off. He speculated that the adjustment may have been made because operators found that the DB-50's were shutting down the reactor on false alarms.

- Maintenance of the breakers at Salem was poor. They were never listed as safety equipment, which baffled the NRC. They never got the critical attention they deserved. In addition, Salem somehow failed to get or keep the important Westinghouse bulletins on the UV coil. The company agrees that there was *no* maintenance of the UV coils between their installation in the 1970's and August 1982, when they began to fail repeatedly. When NRC investigators visited Salem in March, they found that the

breakers had been taken out of the switchgear cabinet and that "the inside of the switchgear had a heavy layer of dust on the bottom of each breaker position."

- It was difficult to verify whether or not the improved coils were installed in the breakers, for the utility had no record of this happening. However, several days after the NRC asked for evidence of this work, Salem officials turned over documents given them by Westinghouse a week earlier, indicating the work had been done in 1972. The author of the NRC report on Salem says he does not know where the failed UV coils have gone, although he knows that Westinghouse collected at least one immediately after the incident. A responsible NRC official in Washington faults the staff for its failure to preserve all the evidence, but notes that the job was complicated because the equipment had been disassembled by the time NRC inspectors arrived. He assumes that the breakers which failed were the improved version.
- It is not known how frequently UV coils have failed at other plants, but the NRC found that they failed (singly) at Salem in February 1979, August 1982, and January 1983. Until January 1983, the apparent procedure for dealing with UV coil failures was to "borrow" replacement coils from other working equipment in the plant. Parts were switched so often between Salem unit 1 and unit 2 that the NRC concluded it was impossible to trace the history of the coils.
- There are questions about the adequacy of the circuit breaker itself. Originally built in the 1940's for use in conventional electric plants, the DB-50 has been modified somewhat for nuclear systems. Some NRC staffers believe there ought to be a larger margin of force in the UV mechanism to insure that it will be able to break open the circuit in all circumstances. This is under study.
- There were several signs of careless management. The operators were accustomed to experiencing false alarms, the NRC believes, and this may have led them to be unaware of the seriousness of the ATWS on 22 February. Some were confused about the meaning of the alarm lights in the control room, for they could not tell NRC inspectors whether a signal meant that the reactor had been tripped by the automatic logic, or ought to be tripped.
- The staff was careless about the postincident analysis on 22 February. Even though there was an open disagreement about how the reactor had been shut down, no one made a thorough review of the record to find out exactly whose memory was correct. As a result, the reactor was restarted the next day—contrary to standing instructions—without a clear understanding of what had malfunctioned.

Westinghouse maintains that there were several protective systems still intact when the ATWS occurred that would have prevented an accident. Even if these had failed, Westinghouse says, the plant has a large capacity to remove heat and withstand internal pressures, enough to avoid core damage. However, the NRC staff concluded that with a few changes in the situation, the pressure limits of the primary coolant system could have been surpassed, going over 3200 pounds per square inch, since one of the pressure relief valves was blocked shut on 25 February. Had this happened, safety related valves might have been overstressed, leading to a loss of coolant, overheating, and possibly core damage.



Ten years of trouble

This UV coil taken from Salem was worn and bound by friction, like others studied in 1971 and 1973. This device (on an 8 by 11 inch pad) carries out the automatic command to break the rod control circuit in an emergency.

The events at Salem have changed the NRC's outlook on ATWS. But it is not clear what the practical result will be. Earlier ATWS proposals have been smothered by industry opposition. The first policy paper in 1973 (WASH 1270) suggested a number of revisions in safety shutdown systems and proposed that a construction schedule be in place by the end of 1976. This was resisted. Instead, the NRC undertook a broader investigation in four volumes (NUREG 0460), which in 1978 came up with several alternative proposals for modifying shutdown systems. It offered data to refute arguments that the proposed changes would cost too much. It suggested that they could be made in the early 1980's. The industry voiced strong opposition to this plan as well, and as one NRC staffer puts it, the staff was "beaten into a retreat" by the highly regarded statistical analysis submitted by EPRI, showing that the likelihood of an ATWS was small. In addition, the staff coordinator of the NRC proceeding was badly injured in an accident and relieved of the ATWS assignment.

In the meantime, the utilities and reactor vendors wrote an ATWS rule of their own and, by a quirk in the law, had their idea published by the NRC as a proposed rule in the *Federal Register* in November 1980. The following spring, the NRC task group under a new leader came up with a new staff rule. It was a compromise between the utility rule and the proposals made in NUREG 0460. Next, the chairman of the NRC at the time, Joseph Hendrie, waded in with a proposed rule of his own. Both were published in the *Federal Register* in November 1981. Now, there were three official proposals for dealing with ATWS and utter confusion among the regulators.

In April 1982, the NRC pulled itself together and gave the ATWS assignment to Robert Bernero, director of the division of risk analysis in the research office. He convened a group of experts, met with industry representatives, and drafted another proposed ATWS rule. It required almost no changes at Westinghouse plants, because they were thought to have sufficient capacity to relieve the pressure surge that could occur following an ATWS. But the rule did propose significant changes in other systems. Owners have already objected that the costs would be too high. "The rule was drafted and reasonably complete," says an NRC staffer, "and then Salem came along."

Now another task force under Roger Mattson, director of the division of systems integration, has been asked to think about Salem and its implications for future NRC regulation. The Mattson and Bernero groups are supposed to collaborate and do something about ATWS.

NRC staffers who have worked on this problem are understandably eager to bring it to a conclusion. The last thing they want is another in-depth analysis, for they fear it could lead to another delay. Yet in the aftermath of the double ATWS at Salem it seems sensible to review the odds and reconsider the measures needed to prevent an ATWS. Perhaps this time, with so much experience under its belt, the NRC will be able to be both quick and comprehensive in its decision.—**ELIOT MARSHALL**