Day 9: Inviting Disaster Ch 2

Saturday, October 3, 2020 11:54 AM

Inviting_Disaster_Ch2

ODECO had not trained him in emergency operations of the ballast system, and he was doing as well as any of us could have done in that position on such an evil night.

"In all the years it drilled," Hylund says, "*Ocean Ranger* never produced a drop of oil."

"The hubris of it all just strikes me," says Don Rathbun's sister Diane. "We heard it was the largest oceangoing rig, it was unsinkable and on and on. And look what ended it—a stupid little porthole."

The *Ocean Ranger* disaster shows how difficult it is for people to sort problems out from the control room, on the fly, as failure starts to spread through a complex system. The people who were supposed to be in control didn't know at least two important things that night: the strange workings of the ballast system when the rig was tilted, and how a storm might take a small off-balance condition and make it much worse. And the slow and ambiguous response of the ballast controls made managing them very difficult once the rig left the familiar boundaries of civilized machine behavior. The next chapter explores the problem of machines whose critical workings were even more deeply hidden from the operators.

2: BLIND SPOT

BAFFLED AND BEWILDERED INSIDE THE MASSIVE SYSTEM

On January 8, 1989, a British Midlands 737 was flying shuttle service from London to Belfast. The captain and copilot heard a bang at twenty-nine thousand feet and felt the airframe shaking at a high frequency. These occurrences, in combination with the smell of overheated metal in the fresh air gathered by the engines' compressor stage, made the captain and copilot suspect an engine problem.

The flight crew checked out the engine problem not by eye—the limited visibility prevented anyone in the cockpit from seeing back to the engines on the wing—but according to a manufacturer's checklist and by using engine controls and instruments. When the captain switched off the autopilot and pulled back on the throttle to the right-hand engine, the vibration and noise eased greatly.

The situation suddenly seemed much clearer now. Vibration had eased soon after they reduced power on the right-hand engine, so the problem must be there. The crew radioed to air controllers that the flight needed to land nearby and agreed on the East Midlands airport. There was no need to declare an in-flight emergency, because the 737 was fully able to divert and land with a single good engine. They reduced power on the left-hand engine on the way down and the vibration diminished further.

In fact they had leaped from initial hypothesis straight to a fatal conclusion, because they couldn't easily check reality by looking at the engines. The right-hand engine wasn't in trouble: it had been doing fine until they shut it down two minutes after the first noises. Passengers were puzzled by the captain's announcement that he had shut down the right-hand engine, since some could see the *left*-hand engine throwing off sparks and flame. Mechanically, the problem had started when fan blade number 17 had broken as a result of metal fatigue and had thrown fragments into the rear part of the engine, causing more damage.

Nobody from the passenger cabin came forward or contacted the flight deck. It was the captain speaking, after all, and he was sure that it was the right-hand engine that had the problem. The airplane joined the glide slope to East Midlands, and the vibration lessened further. The airliner descended like this for a quarter-hour, the left-hand engine slowly chewing itself up but still providing just enough power to deceive. Two miles short of the runway, the left-hand engine went to pieces, slinging fan blades over a wide area. Now the fire warning went off on the left side. The captain did his best to restart the right-hand engine, but the airplane was only nine hundred feet off the ground and he ran out of time. The jet hit a field, bounced up, and slammed into an embankment of the M1 motorway near Kegworth. Forty-seven people died.

The investigating board found that even without a fire alarm from the bad engine, one small indicator on the cockpit video-display screens could have set the crew straight, namely, a vibration readout for the left-hand engine. Its reading was at five, meaning maximum vibration. But it was a small indicator and out of the way, mostly for engine-trend monitoring and not able to set off its own alarms.

All vague blind spots

The Kegworth crash shows how problems can happen in any system with a blind spot. This means a machine whose inner workings are hidden from the operator's view and whose instruments do not show up plainly enough to overcome a powerful human tendency to jump to conclusions when under stress. The pilots had a full fifteen minutes to consult the engine vibration monitor or simply to ask the flight attendants whether they could see any visible signs of engine trouble by looking out the side windows. The engine failure would have been no more than a jotted note in a flight log if the operators had taken the time to "consult reality" rather than jumping to conclusions. Another midair crisis occurring out of view doomed ValuJet Flight 592, in 1996, because the pilots had no smoke alarm or any other way of detecting an oxygen-boosted fire in the cargo compartment below in time to return to the airport.

People can do remarkably well in controlling complex machines whose workings are fully understood and open to view. One example is how crews manage to land airplanes on the decks of aircraft carriers at one-minute intervals or less with very few accidents, especially considering the hazards. When meeting a new system, people need time to know its workings under good conditions and bad. The most dangerous time is when the operators don't know what they don't know.

ATOMS FOR PEACE

The most expensive blind spot in history happened on March 28, 1979, at the power plant called Three Mile Island Unit 2, near Harrisburg, Pennsylvania. Though the plant looked fine on the outside after the crisis was over, on the inside the reactor core was a complete wreck. Half the fuel in the reactor vessel had melted, and most of the rest had tumbled into a heap of rubble on top of that. Still, the thick-walled stainless steel reactor vessel held the fuel from breaking out the bottom, just long enough.

The President's Commission on Three Mile Island concluded that the reactor core came within a half hour of total meltdown. Notwith-

standing the media's excitement over the "hydrogen bubble" after the first day, it's clear now that the first three hours at TMI-2 were the most critical. While it's possible that the reactor core could have melted into the ground in the so-called China Syndrome, it's equally likely that fuel melting out the bottom of the reactor vessel would have set off a mighty steam explosion when it hit the pool of water in the bottom of the thick concrete containment building, breaking open the building to release a massive cloud of radioactive steam across the towns and farms of southern Pennsylvania. Though news media excitement peaked a few days later, the worst danger had passed on the same day it started and certainly was over by April 1, when President Jimmy Carter arrived at Harrisburg, Pennsylvania, to reassure the public. According to Walter Mondale, during the visit a woman spoke up after Carter said that the danger was over. "I believe you," she said, "because if there was any danger the vice president would be here instead."

The apparent bumbling in the control room inspired cartoonist Matt Groening to give Homer Simpson the job of reactor operator at the Springfield Nuclear Power Plant. Three Mile Island Unit 2 cost General Public Utilities and the rest of us more than $4 billion, making it the nation's worst industrial disaster in cash terms. It was so big that two decades later, lawyers are still fighting over who should pick up the cost.

Beforehand, the Nuclear Regulatory Commission had declared any such "loss of coolant accident," occurring while the reactor was at full power, as so unlikely as to not require consideration in safety plans. And it was a bizarre case of automated equipment trying to save itself, while operators blocked its moves at every turn for the first two hours and twenty minutes. Was it the case of "stupid error" that a British government official called it afterward?

The operators' actions will make more sense after knowing how key parts of the plant were hidden from view, how many instruments gave false readings, and how operators' early training had given them a mindset to close off the emergency cooling. They saw this last, desperate measure as the only way to keep the reactor pipes from bursting. Studies of human behavior in other disasters have often shown this

"cognitive lock" phenomenon, where those on the scene decide on a course of action and hold to it against all contradictory evidence. Cognitive lock is a perfect match with an opaque and complex system. Together they have the power to turn a minor problem into a very dangerous situation.

According to measurements at the site, TMI-2 didn't get far enough down the disaster road to release fatal levels of radiation to the outside. In the lingo of the field, TMI was more of a near miss than a catastrophe. TMI vented about fifteen curies of radiation; the Chernobyl disaster seven years later turned out millions of times more. The number one reason the containment building didn't break open was Brian Mehler, a supervisor who wasn't even supposed to be in the TMI-2 control room that day. In fifteen minutes, he figured out what was wrong.

A malfunctioning device straight out of the steam days called the pilot operated relief valve (PORV) was the feather that broke TMI's back. Steam technology was so important to the reactor's troubles during the first, critical three hours that a riverboat engineer from 1850 would be able to understand most of what happened at TMI-2 very well. He would probably call it a blowdown, though, rather than a meltdown. "Blowing down the boiler," in steam lingo, means to dump the steam out through a valve, either preparatory to shutting the boiler down or as a way to loosen mineral deposits from its inside walls.

As much as he would marvel at the fabulous expense and size of a reactor, the old-timer would be amazed at how little the operators could see or hear of what was going on in the reactor building. The reactor building was only a minute's walk away from the control room, but because it was there to contain any leaks of radioactive steam and water, it was not the kind of place you'd work in daily. Operators had no instrument telling them how much water was in the pipes cooling the reactor, and several key instruments would give them dangerously false readings in the crisis.

By contrast, from his post in the engine room while the engine was running, an operating engineer from the steam era could see and hear and feel pretty much everything, short of crawling into the boiler while the

engine was running. And he could go even there after he blew down the boiler and let it cool. Sometimes he didn't wait that long.

When the tramp steamer *Tripoli* lost power and drifted toward the rocks of Gibraltar in the late 1800s, the chief engineer crawled inside the firebox while it was still too hot to touch, relying on coveralls soaked with seawater to keep himself alive just long enough to get out. Staying on a plank to keep himself off the grates, he stood up in the chamber to install a washer. The engineer knew to face the firebox door as he did so, so that if he collapsed from the heat, he might fall on the plank. That way other men outside in the engine room could pull him out before he boiled to death.

They had valves showing whether the boiler had enough water, and later, "sight glass" tubes to get the same information more quickly. By the 1850s they had gauges to judge boiler pressure; before that they had to judge pressure by whether the safety valve opened. Some engineers said they could judge pressure by watching the heaving of the riveted boiler walls, in and out, as the cylinders drew steam. Such engineers, then, would be distinctly nervous about the idea of sitting all day in a control room and running a monstrously big boiler by remote control, operating at a steam pressure twenty times greater than the highest pressure of the steam era boilers without being able to see and hear what the machinery was doing.

But, after all, we're only talking steam. When civilian uses for atomic power first hit the public stage after World War II, making plain old water into steam looked like the crude beginnings, just a short bridge to the new era of plenty. According to legend, Hungarian-born physicist Leo Szilard first conceived of a sustaining chain reaction in 1936 when standing on a European street corner. Szilard obtained a patent and secretly assigned it to the British government, but nobody paid attention to him until the bomb-building Manhattan Project. In the early stages of the project, Enrico Fermi headed a group to assemble a crude reactor under the stands of the University of Chicago football stadium, and he welcomed Szilard's input. The world's first reactor was uranium arranged in a pile, with a larger pile of graphite bricks around it. The purpose of the "atomic pile" was strictly experimental,

to see what it would take to scale up a bigger reactor to harness energy from a sustaining nuclear chain reaction.

Fermi's pile worked because uranium atoms have a nucleus of neutrons and protons that is easily broken apart when hit by a neutron from outside. In breaking up, the atoms release showers of more neutrons, which in turn break up more atoms. During the Manhattan Project physicists learned how to regulate the number of loose neutrons so the reaction in the pile would turn out a steady heat but not spew out of control; one of their discoveries was that some materials, such as cadmium, indium, and boron, absorbed neutrons easily and if inserted into the pile could damp down a runaway reaction. A reaction running totally out of control was fine if you wanted a bomb, but not otherwise.

After two bombs ended the war against Japan, most Americans felt better about the atomic age angle. It sounded wonderful, particularly to the writers of books like *The Atomic Revolution* (Robert D. Potter) and *Atomics for the Millions* (Maxwell L. Eidinoff and Hyman Ruchlis). Atomically heated open-air stadiums would be nice. Also, according to Pulitzer Prize–winning science writer David Dietz, cars would run on tiny uranium pills, each pill powerful enough to heat a house through the winter. Factories would transmute base metals to gold so cheaply that pipes used in their operating systems might be made of gold to reduce maintenance costs.

We would certainly need rockets and airplanes fueled by uranium. How about diamonds in trainload quantities, forged out of carbon by the irresistible pressure of an underground blast? Or melting the icecaps with the heat from H-bomb blasts? Officials in four southeastern states tried to talk the federal government into using H-bombs to excavate thirty-nine hilly miles for their Tennessee-Tombigbee barge-canal project. In the process of checking all these ideas out, the Atomic Energy Commission (AEC) exploded underground bombs as far west as Alaska and as far east as Mississippi.

But it was harder than it looked on the magazine covers, and it always cost more than imagined at first. The Air Force's delay in building a nuclear-powered airplane "has been of grave concern to many of our clearest thinking airmen," fretted the editors of *Flying* in 1959. In

fact, worried the magazine, the delay suggested pre-Sputnik head-in-the-sand penny-pinching.

The AEC's plans for blasting its way across the Western Hemisphere with strings of H-bombs died with the Test Ban Treaty of 1963. And who can say whether science-fiction editor Hugo Gernsback was ever serious about his idea of winter clothes engineered like wearable electric blankets, powered by personal reactors small enough to fit in a pocket? The closest some citizens ever got to seeing the age of wonders, firsthand, was the fluoroscope installed in some shoe stores in the 1950s, for the benefit of customers dying to see a full-motion X ray of how their new shoes fit when they wriggled their toes.

Atomic power plants jumped out of the wish list and into production because the military, needing them for propulsion on board long-range ships, worked out the key details first. The first commercial nuclear power plant, at Shippingport, Pennsylvania, began running in 1957 and was built around a submarine reactor. Things were far enough along now, ten years after the first burst of enthusiasm over nuclear power, to inform the public that some risk was involved. Physicist Edward Teller, while a booster of nuclear power's benefits, had warned an August 1955 international conference in a scientific paper that reactors would always pose some risk of catastrophe, including turning the site of the plant into a no-man's land. And plant officials played up the importance of safety when reporters visited the sixty-megawatt Shippingport plant while it was under construction. Most of it was underground for safety; "Every piece of equipment down to the last nut and bolt is scrutinized with fantastic care," said *Life* magazine. This was important, the article said, because the gear would be sealed out of sight and out of the reach of repair.

The Shippingport power reactor opened for business in 1957. Though very high operating costs dogged that plant from its first day, the nuclear power plant industry grew at an astonishing pace over the next decade, spurred by fuel subsidies from the government and below-cost pricing by reactor builders. Builders and buyers agreed: make the plants big, because bigger would be cheaper per kilowatt-hour. By 1966, the country had fifteen nuclear power plants running, nine more under construction, and twenty-two on order. Some of

those orders were for 1,100-megawatt plants, almost twenty times the size of Shippingport.

One of the late-coming enthusiasts was a holding company called General Public Utilities (GPU), which owned three big utilities, including Metropolitan Edison in Pennsylvania. GPU started its push by requesting permission to build a single nuclear power plant on Three Mile Island, the name referring to the length of the gravelly bar in the wide Susquehanna River, ten miles down from the state capital of Harrisburg. Unit 1 was completed in 1974. Then GPU wanted another plant.

Unit 2, completed in March 1978 and the one headed for infamy, had two cooling towers, a building for fuel storage, a two-hundred-foot-high containment dome to confine leaks from the reactor vessel inside, and two large rectangular buildings for turbines and auxiliary equipment. The cooling towers were one very visible sign that, well before the 1979 crisis, the trends in favor of nuclear power just ten years before were shifting fast. *Sports Illustrated* published an article in 1969 claiming that nuclear power plants were killing off fish by dumping their waste heat in rivers and bays; after the controversy caught on, power companies found themselves building cooling towers at extra expense, which dumped heat into the air instead. Combined with public protests against nuclear power that led to more requirements for safety equipment, every new plant after the first wave saw its costs go way up. TMI-2's final cost went from the original estimate of $130 million to more than $700 million. This had to cause real pain at General Public Utilities. According to some who have studied the origins of the meltdown there, part of the explanation for its mechanical problems may lie in the owner's rush to get the plant into electricity production by December 31, 1978, so it could qualify for tax credits.

FEEL THE HEAT

Just as journalism-school students learn to follow the money, it helps to follow the heat in understanding the layout of TMI-2 (see Figure 3). We can think of TMI as three sets of pipes linked together like loops of

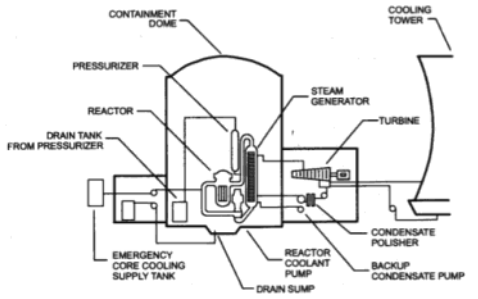
a chain, working together to move heat from the reactor core to the outside world, taking it through generators along the way that harnessed the heat and turned it into electric power. We'll call the first set of piping the "reactor coolant" pipes. The reactor coolant pipes took high temperature, high pressure water to extract heat from the one hundred tons of hot uranium in the reactor core. The reactor coolant pipes were entirely inside the containment dome, out of view. Traveling inside these pipes, highly pressurized water extracted heat from the reactor pressure vessel and carried it off to a heat exchanger. Inside the heat exchanger, what we'll call the "steam-making pipes" accepted the handoff of heat and carried it from the containment building. Inside the steam-making pipes, ultrapure water flashed into steam. Arriving at the turbine building, the steam passed through a set of turbines and generators, making 880 megawatts of electricity to sell.

Then a third set of pipes, which we'll call the "external cooling" pipes, conducted the waste heat away from the steam-making pipes and carried it outside the turbine building to the top of giant concrete cooling towers. As the hot water trickled down the inside of the towers, some of it evaporated, and in doing so it cooled the water that remained; pumps sent the cooled water back through the external cooling pipes, back into the turbine building to remove more heat. Of the three piping loops, the external cooling pipes were the most visible and accessible to people working at Three Mile Island; even nearby residents could see when that part of the system was operating to bring heat out of the plant, because of the plumes of condensed water vapor that the cooling towers gave off.

The operators and maintenance people were less in sync with the steam-making pipes, since those pipes carried high-pressure steam and very hot water and were not accessible where they passed through the containment building. But the maintenance people could see and even touch this set of pipes where they passed through the turbine building. And by closing isolation valves they could even separate out some of the steam-making pipes from the rest of the system and work on them while the reactor was operating.

Both these loops of piping were visible to the human eye and

FIGURE 3: THREE MILE ISLAND UNIT 2



PROBABLE SEQUENCE

1. Malfunction during maintenance work causes condensate valves to close.
2. Reactor coolant heats up and pressure rises; pilot operated relief valve (PORV) on pressurizer opens.
3. PORV does not close on automatic command.
4. Coolant begins draining out of reactor through pressurizer.
5. Operators cut back on emergency cooling system and drain more coolant, thinking reactor coolant level is dangerously high.
6. Problem is discovered after half of reactor core melts.

Adapted from Senate Committee on Environment and Public Works

open to the wrench, then, in their own ways. Not so the third, the reactor coolant pipes, which held the hottest, most radioactive water. These were entirely out of sight from operators and maintenance workers, buried deep inside the containment building. These pipes and vessels could not be worked on while the reactor was operating, since the pressure, radioactivity, and heat would have made the work unsafe. Not even cameras revealed what the reactor coolant pipes would be doing in an emergency.

Yet all three links of this chain were equally important. The analogy works because a chain is only as strong as its weakest link; at TMI-2, all three loops had to work if the reactor was to stay within its temperature limits. If any of the three loops of piping failed, the reactor would go into an emergency condition, relying solely on short-term supplies of cooling water. The emergency could happen even after a reactor shutdown, after control rods had stopped the critical mass of full-power fission. For hours after a shutdown, the one-hundred-ton reactor core kept producing so much decay heat that the thermal energy could not safely remain inside the pressure vessel without some kind of cooling.

In the early hours of March 28, 1979, the situation on Three Mile Island was as follows. The Unit 1 power plant was down for repairs and testing; Unit 2 was running at 7 million horsepower, enough to supply a city of five hundred thousand people. Big systems like this always have at least a few things out of whack, or maybe more than a few. Down in the hot and cavernous basement of the turbine building at Unit 2, Don Miller and Harold Farst had opened up a part of the steam-making loop for maintenance. It may seem to you like an odd time to do maintenance, but the system had valves to isolate this area from the high pressures and temperatures of the rest of the steam-making pipes.

The problem concerned one of the giant water filters (called a "condensate polisher") in the steam-making loop. All night the men had been trying to shake loose tons of tiny plastic beads in one of the demineralizer tanks. The beads, with the consistency of coarse sand, had jammed into a pipe leading out of filter tank number 7. The bead-jamming problem had plagued the operators on and off for months;

before it had always yielded to blasts of compressed air through a pipe stuck in from underneath. Miller had been trying this for hours, to no avail. The problem was not critical; there were seven other filtering tanks to handle the five thousand gallons of water needed every minute at the steam generator. The reactor was running at 97 percent full power.

At some point during the frustrating hours of fooling around with the compressed air jet and the filter tank, a few ounces of water seeped backward into the compressed air lines, undetected by those on the scene. It took a little while for the water to snake its way into the instruments that relied on compressed air, but then things happened quickly. At 36 seconds past 4:00 A.M., the leaking water from the polisher repair attempt reached the control line to the big valves controlling all the condensate polishers. The automatic controls interpreted this tiny bit of water in their air lines as a deviation from proper conditions and so shut all the valves that let coolant through. This acted like an instant roadblock in the steam-making pipes. The inertia of five thousand gallons of water a minute, stopping so quickly, tore one of the big pipes loose in the turbine building, pulled out controls, and sprayed the place with scalding water. Without water, pumps downstream cut off, so steam stopped flowing from the heat exchanger in the containment building; that made the generating turbines shut down, too.

In 1893, Rudyard Kipling published a poem called "M'Andrew's Hymn," which called for a poet to sing the "Song o' Steam." Three Mile Island sang its own song: every month or so, over the single year from its first operation, escape pipes had howled like an enormous whistle as valves inside the turbine building opened to dump excess steam. That morning, the reactor played its last song as the turbines shut down. For at least a mile in every direction, anyone awake in the Middletown, Pennsylvania, area could hear the sound of a million pounds of high-pressure steam, shrieking into the sky. It woke up one woman a quarter mile away.

So it happened that the three-link chain of cooling pipes suffered a broken link. With the steam-making pipes shut off, the water in the reactor coolant loop had no place to dump its heat. Following auto-

matic "scram" commands from a computer, cadmium control rods plummeted into the reactor, ending the nuclear chain reaction and cutting back heat production at the core to a few percent of full power. Still the temperature rose and the water began expanding, as things will do when heated. The expanding water made the pressure climb from the usual value of 2,150 pounds per square inch.

The reactor coolant loop had only one open space for the water to expand into. It was called the pressurizer tank, and it was forty-two feet high, located inside the containment building along with the rest of the coolant piping. The pressurizer tank acted like a shock absorber to the reactor coolant piping. On an ordinary day the tank was supposed to be about half filled with reactor coolant water at the bottom, leaving steam as a cushion in the upper part. Automatic controls maintained the right balance of water and steam by either cooling or heating the contents of the pressurizer tank.

At the very top of the pressurizer was a safety valve to let off steam if pressure rose too fast for the automatic controls. Deep inside the containment building, the pilot operated relief valve (PORV) opened as intended, reducing pressure by letting steam out the top of the pressurizer when the water level rose. That sent a mix of water and steam down a drainpipe to a storage tank on the floor of the containment building.

THE RUBBLE MAKER

There were many problems at Three Mile Island Unit 2 that morning, but the PORV was the one that reduced the reactor core to slag and rubble. When the pressure stabilized a few seconds later and the electronic command came to close the PORV, the valve stuck open instead. That left a hole about the diameter of a Ping-Pong ball in the reactor coolant system. It wasn't discovered until more than two hours later.

That a safety valve could open and prevent a steam explosion but still somehow cause a terrible problem would have sorely surprised the valve's inventor. His name was Denis Papin, born in France in 1647 and

educated as a physician. Papin opened a doctor's practice in Paris but devoted his spare time to his real love, physics. In 1675, Papin moved to England to develop the science of pressurized air. Four years later Papin invented the pressure cooker, initiating a line of thinking that contributed much to successful high-pressure steam engines in the early 1800s.

Papin worked on many projects throughout his life, from air guns to steam-powered pumps to grenades, but arguably the pressure cooker was his gift to the ages. He referred to it often when writing letters to the wealthy, asking them for financial support. He called it the "New Digester or Engine for Softening Bones." Papin recognized that if food cooked reasonably well in boiling water, it would cook even better if the temperature was higher. That means he had to understand steam and how to control it. The ancients knew about steam. According to good authority, Hero of Alexandria directed steam from a teapotlike device and got it to spin a little pinwheel.

Papin understood that the way to make water cook things better is not to build a bigger fire under the kettle. Adding heat only makes the water boil more briskly, without raising the boiling temperature, which at sea level is 212°F. Instead Papin closed off the kettle. That way the water would hit a higher temperature before boiling. Papin fitted a stout U-shaped metal frame over his kettle and equipped it with a screw clamp that pressed the kettle lid down tight. It looked something like an old-fashioned printing press.

It doesn't take much brainpower to realize that a clamped-down pot of water with a fire under it is going to blow up sooner rather than later, so Papin invented the safety valve. Had historians named it the Papin valve people might have remembered him better. Because his most striking inventions remained on paper, Papin never made it into today's pantheon of scientific greats. As it was, he died in London around 1712, penniless and mostly forgotten except in his hometown of Blois, which erected a statue.

To make his safety valve Papin drilled a hole at the top of the New Digester, and arranged a metal weight to sit on the hole to prevent steam from leaking out. To situate the weight he rested a long

metal bar on top of the hole, one end of the bar hinging on the cooker. The other end stuck out over the side and was free to swing up and down. Having arranged a lever, Papin hung a metal weight on the free end. By changing the poundage of the weight or by sliding it along the bar, Papin changed the leverage bearing down on the hole of the cooker. This arrangement allowed him to set the pressure that would build before the steam power was strong enough to hoist up the metal bar and vent the kettle. People had used a lever-and-weight arrangement for other devices—it's similar to a balance scale, after all—but Papin was the first ever to use it with steam valves. Today's home cookers are functionally similar to his, operating at about fifteen pounds per square inch with the water temperature at 250°F.

Industrial-size steam valves use springs or motors now instead of weights and beams, but the principle is much the same. The maker of the safety valve that caused trouble at TMI-2 was Dresser Industries, under its Electromatic trade name. The pilot operated relief valve was an electrically operated device, weighing 175 pounds and costing about thirty thousand dollars. At its heart it had a sliding metal cylinder that normally covered a hole into the pressurizer. A spring held the cylinder in place until an electric command slid the cylinder and uncovered the hole, letting steam out of the pressurizer. Babcock & Wilcox used PORVs on its nuclear reactors as a way to help them run more smoothly, to dump steam before the pressure got high enough to open two other safety valves, which were required by law.

Come inside the beige-paneled control room at TMI-2, eight seconds after the valves slammed shut and blocked off the steam-making pipes. The intense investigation into TMI gave us the best record, ever, of how things look to the people trapped inside the fast-moving, scary world of a major system failure. Like Alice inside the rabbit hole, the operators did their best to impose order onto seeming chaos. And they might have succeeded had they been able to see what was really happening inside the containment building only a few dozen yards away.

TMI-2 had four Nuclear Regulatory Commission–licensed reactor operators on the 11:00 P.M. to 7:00 A.M. shift, plus extra men to work on machinery maintenance. The licensed men in the control room at 4:00

A.M. were shift supervisor Bill Zewe and two operators, Craig Faust and Ed Frederick. The shift foreman, Fred Schiemann, was still down in the basement of the turbine building with Don Miller and his partner, trying to fix the condensate polishers.

A two-tone control room warning horn went off shortly after 4:00 A.M., and Faust saw lights warning him that pumps in the steam-making pipes had shut down. Zewe came out of his glass-walled office to join the others at the panel. It showed that three emergency pumps were coming on-line automatically, to keep water moving along in the steam-making pipes and thus assist the flow of heat out of the reactor.

Pressure was going up in the reactor coolant loop; that was to be expected at this point, because of all the heat trapped by the blockage in the steam-making pipes. A bright red glowing light showed that an electric signal had ordered the PORV to open and vent any pressure over 2,255 pounds per square inch. Shortly afterward the pressure dropped and the PORV light went out. Operators thought this meant that the PORV had closed, but all it really meant was that the command had been sent to close it. Nothing showed them that the valve had actually stuck open. The false PORV light was the first deceptive control reading that morning, but not the last.

During the first minute, the level of water showing in the pressurizer tank was dropping, too; also to be expected as the reactor heat dropped and the water cooled. Working from his books of emergency procedures, Frederick turned on high-pressure pumps to throw some extra water into the reactor coolant pipes. This would replace some of the volume lost as the coolant water shrank. The pressurizer water level began to creep upward from its low point of 158 inches. That gauge showed the water level compared to the length of the pressurizer tank, which was a vertical tube. The highest possible reading on the gauge was four hundred inches. Schiemann arrived, having run up eight flights of stairs from the turbine building basement. Schiemann took a seat at a panel on the left side of the console, where he could watch the water level in the pressurizer.

The rising water should have stopped but didn't. When it hit three hundred inches at four minutes into the crisis, Frederick cut back

on the water injection pumps, but the water level still went up even though pressure was dropping. TMI-2 was now cruising somewhere outside the operators' familiar world. Past four hundred inches on the gauge, the operators knew, there would be nowhere for rising water volume to go.

Think of filling a closed set of metal pipes with water, right to the top, leaving no air space at all, then sealing them up tight. Reactor operators call that condition "going solid." If you heated those filled pipes just a little more, the increasing water volume would create so much pressure that the pipe would have to burst. In a reactor the coolant water would turn to steam, and the voids left in the pipes would let the core overheat. It would be the much-feared "loss of coolant accident." Said the TMI operating manual in unusually clear words for a technical manual, the pressurizer "must not be filled with coolant to solid conditions (400 inches) at any time except as required for system hydrostatic tests."

Based on what the operators knew at the time, and given the readings from the pressurizer's water gauge, their fear made sense. Training on the Babcock & Wilcox computerized simulator at Lynchburg, Virginia, had never shown this behavior, and in fact the training had stayed away from showing the operators any complex, multiple-failure scenarios like the real one the four men faced here, a scenario that required them to fly blind. In all this big control room, there was not a single instrument or gauge that told them how much water actually sat in the reactor vessel, or in the convoluted piping with its high points and low points, or in the steam generator. Only the pressurizer tank, with its relief valves sitting at the top, had a water level indicator. It was a gauge with a needle showing against a vertical scale, and it was labeled "PZR Level." It lay just inches from the pressure gauge for the pressurizer.

Meanwhile, undetected, the PORV on the pressurizer was blowing down the boiler, letting steam out at the rate of 220 gallons of water per minute. It was this leak at the top of the pressurizer that was sending the water level so high, fooling the operators. There were other people, though, outside the plant, who had already found out how the water level

in the pressurizer could fool operators, given how hard it was to see inside the containment building. To these people the apparently contradictory behavior (pressure dropping and water level rising) would not have seemed so strange. Well before March 1979, word had come to Babcock & Wilcox, and the Nuclear Regulatory Commission, as well, of a near miss at the Davis-Besse Unit 1 reactor near Toledo, Ohio. On September 24, 1977, an electrical glitch there had opened and closed a PORV so many times that it stuck open; this caused the water level in the pressurizer to go up as the pressure went down.

Just as would happen at TMI, the Davis-Besse reactor operator had followed his training and shut off the emergency cooling out of fear that the reactor coolant piping was about to go solid. Why no disaster at Davis-Besse? That plant had been running at low power, and the operator had seen his error after just twenty minutes. The Davis-Besse plant changed its in-house procedures after this to warn against shutting off the emergency cooling. But on the reasoning that this brand of relief valve was unique to Davis-Besse and thus of no interest to other power plants, Babcock & Wilcox and the NRC sent out no warnings to operators of other B&W reactors about the erratic reactor behavior that a stuck-open relief valve would cause. Nor did the manufacturer change its manuals or reactor training regimen to warn operators during training that if a relief valve ever stuck open, it could mislead them into thinking the reactor coolant was going solid when it was not.

So, without the benefit of this lesson from Ohio, Zewe and his operators guarded vigilantly against any tendency of TMI to go solid. As the water level continued to go up, they cut back the flow of high-pressure cooling water from five hundred gallons a minute to a bare twenty-five gallons a minute. Feel free to criticize their decision to shut off the high-pressure cooling, but also know that the operators did not design the control room that gave them so many problems that morning. Ed Frederick had sent a memo a year before to management, saying the control room layout was going to cause a severe problem some day. Nothing substantial was done to fix the problems in the control room's alarm system during the months leading up to the final

accident, Frederick testified later, and the meeting he asked for never happened.

And still the water level rose on the pressurizer gauge. Zewe and the others now faced a full-fledged mystery.

"A GIGANTIC AND SENSELESS FEAR"

Although the operators' lives were not in immediate jeopardy, what the reactor was doing was fully as unnerving as other incidents have been along the machine frontier, like the moments leading up to the crash of AeroPeru Flight 603 on October 2, 1996. The 757 airliner took off that night from Lima with its left-side "static port" sensor tubes taped over. Removing the tape was a forgotten task after the plane's preflight washing. None of the mechanics or pilots had detected this extremely serious problem before flight. It was serious because those few inches of tape blocked in an erratic fashion the air supply needed by critical flight instruments, particularly the airspeed indicator and altimeter. As recorded on the cockpit tape recording, the AeroPeru crew struggled mightily to make sense out of the lies their instruments were telling them. They were experiencing what sociologist Karl Weick calls *vu jade* (the opposite of *déjà vu*), the profoundly frightening impression that the world no longer makes sense and that one has blundered into a place or circumstance so alien that no one has ever been there before. Weick quotes Freud on this: "a gigantic and senseless fear is set free" when things get bad enough.

The Peruvian airplane swerved, climbed, and descended almost at random as the pilots struggled with the controls and the autopilot. Distracted by constant alarms, the crew members never figured out why the airspeed indicator and altimeter varied wildly though the airplane was flying well. Even with assistance from an air traffic controller, the plane crashed into the Pacific after a desperate half hour's struggle, killing sixty-eight. Its altimeter read 9,700 feet.

The TMI operators stuck with their theory that the reactor was going solid. Maybe a pump or valve somewhere had gotten stuck and was forcing more water in, defying all commands. If cold water was

coming in, that might explain why the pressure was dropping. It was hard to concentrate, with the main alarm Klaxon going and more than a hundred alarm lights flashing. So the operators began letting water out of the primary coolant piping at the rate of 160 gallons a minute.

Finally, having cut off the inflow of nearly all emergency cooling water, and having opened a valve to let more water out, at 4:06 A.M. the operators saw the water level stop climbing as it reached the top of the gauge. It looked like a hairsbreadth escape from the do-not-exceed point of four hundred inches. For the next two hours, the water level gauge would hold the operators' attention like a cobra in a basket. It would drift down when they let more water out of the primary system; then it would creep back up toward four hundred inches. It was so strange that Zewe sent his assistants to cross-check the other instruments, to see whether the water level gauge was showing bad information. The word came back later that the gauge was correct.

Other workers and managers on the graveyard shift began to gather, consulting in low tones and offering to watch panels under Zewe's direction. The control room had only a single phone line to the outside world. Even the computer was far away: although the computer was capable of recording key information about hundreds of alarms as fast as they came in, it could only print out fifteen lines of information per minute. The printer fell more than two hours behind at one point in the emergency.

By 4:20 A.M., the combination of choked-down emergency pumps and coolant water flowing out the letdown valve seemed to be working well enough because the pressurizer water level was hovering somewhere around 370 inches. So Zewe left the control room to see if he could straighten out the mess at the condensate polishers. But when Zewe got back at about 5:00 A.M., affairs had taken a very serious and unexpected turn. The four giant pumps in the containment building that forced water through the reactor coolant pipes were shaking themselves to pieces as the pump impellers met cavities of steam, sped up, then slammed into solid water and slowed down.

Pumps and fittings could not survive this abuse without cracking. Worse, this didn't fit at all with the operators' prevailing theory that the

primary system was nearly full of water. Instead it was a strong signal that the water was full of steam, meaning that the water level might be dropping below the top of the reactor core. Following standard procedures once again, at 5:14 A.M. the operators shut off two of the pumps, and the last two a half hour later.

It was about 5:00 A.M., when the four reactor coolant pumps began shaking, that an engineer used the precious single phone line from the control room to call Brian Mehler at his home in Palmyra, Pennsylvania. They needed him as backup and wanted him to come as soon as possible. Mehler was not assigned to Unit 2 at the time; the duty roster for the day showed Mehler coming in at 7:00 A.M. to work as a shift supervisor at Unit 1. Mehler had been working over at Unit 2 the day before, and someone must have thought he might have an opinion as to what was going wrong.

Mehler got in his car and hurried down Pennsylvania 421 to the plant, stopping at the gate to check with the guards and pick up his radiation badge. The guards didn't know anything about the emergency, but Mehler could see that the power generators had stopped because no white plumes rose from the cooling towers. Mehler drove to the control building and walked into the Unit 2 control room shortly after 6:00 A.M. The station manager gave him a short briefing.

It was a wild scene: at least fifty engineers, supervisors, and shift workers had crowded into the control room, all trying to make sense of what the controls were telling them. The panels showed 110 alarm lights flashing. The master alarm siren was still driving people crazy. Free for a few minutes to pursue his own train of thought, Mehler pondered how it could be that water pressure was down if the pressurizer's water level was up. Nothing in the manuals had explained it, so something else must be going on.

MEHLER'S DISCOVERY

Mehler approached the problem a little differently from most of the operators. Zewe, Schiemann, Frederick, and Faust, caught in the center

of the storm since it started, were all navy men of at least five years' experience and had operated reactors in submarines or on aircraft carriers. Mehler had served his military time in the air force. The only reactor Mehler had ever operated before TMI Unit 1 had been the little open-pool training reactor behind the hockey arena at Penn State University, doing startups and shutdowns.

Fifteen minutes after arriving at the control room, Mehler had two theories in mind. One explanation could be a blown circuit breaker that had knocked out the electric heaters in the pressurizer tank. These heaters were supposed to come on if pressure dropped, making more steam at the top of the pressurizer. Mehler figured that if the heaters weren't working, the system would have trouble keeping the water level down where it was supposed to be. Mehler sent a man to check on the breaker panel.

Without waiting for an answer about the circuit breakers, Mehler turned to the other possible explanation, a fairly small leak somewhere in the reactor coolant system, and one that had opened very early in the sequence. It wasn't practical for him to run over to the containment building, throw open the door, and look for spurting steam. Any clues would have to come from the same two-thousand-plus instruments and controls that had been baffling the others for more than two hours.

Mehler knew that the air pressure in the containment building was up, and it was getting warm in there, which indicated a steam leak somewhere in the domed building. He went to the computer terminal and called up temperature readings for the drain line coming off the PORV. The computer indicated the drain temperature from the PORV was higher than normal, at 280°F, but far short of the reactor coolant temperature of almost 600°F. Mehler could have stopped here, reasoning that since the line was well below the coolant temperature, he was only seeing evidence of the same old slow leak that had been in progress since October; in fact it had first been written up more than a year before, when the plant was still in testing. All the operators knew about the PORV's slow leak and also that the plant had been unable to fix it.

Actually the drain line was much hotter, but a programmer had instructed the computer not to show any drain line temperature over

280°F. Still, even that struck Mehler as too hot under the circumstances. Could this be the leak? Not according to the men thronging the control room before Mehler arrived. Bill Zewe had already asked for a report on the PORV drain temperature earlier. The man who checked on it mistakenly told Zewe that it was close to the usual temperature. And, Zewe believed, the control panel proved that the PORV had shut. Finally, Zewe had twice asked for information about the drain tank that the PORV emptied into, and twice he was told that it didn't seem to be filling. That had been enough for a very busy and harried supervisor. Zewe had not pursued the issue any further.

Mehler asked the supervisors in charge if they minded if he went ahead and closed an electrically operated valve that would isolate the pressurizer tank from the PORV. The actuating switch for the valve was within reach, right there on the central console alongside the indicator for the PORV. If steam was blowing out the PORV, whether a little or a lot, the "block valve" would choke off the leak. They told him to go ahead; nothing else had worked.

One operator told federal investigators later that Mehler's idea was a last-ditch measure, but it wasn't. Blocking off the pilot-operated relief valve posed no risk because the pressurizer tank had two more safety valves, completely separate from the PORV. The two valves, which operators called the "code safeties," were required by the Boiler Code of the American Society of Mechanical Engineers. By law, operators cannot block off the code safety valves or mess with them in any way. The code safeties were set to open at twenty-five hundred pounds per square inch, well below the measured strength of the piping.

At the time Mehler got his clearance to proceed, the system pressure had dropped to nine hundred pounds per square inch. He leaned over to Fred Schiemann and asked him to close the block valve. Within seconds, a gauge in the control room relayed news about the first good thing to happen on Three Mile Island in the last two hours and eighteen minutes. The primary coolant pressure was heading back up.

Core damage was well under way by then and would continue for much of the day; and it would be eleven hours more before the operators brought the water level up enough to cover the core, but

TMI's worst overheating had been stopped less than an hour from disaster. At least one other man had been sniffing along the trail of subtle clues that led toward the stuck PORV, a Babcock & Wilcox engineer named Lee Rogers who was in touch by phone, but it's impossible to know what would have happened had Mehler not spotted the problem when he did.

"I brought a fresh pair of eyes into the room," Mehler says now, but it took more than that to divine the machine at its worst moments and stop the leak that the others had let go for more than two hours. He had the time and the inclination to take his two theories and test them fully against the facts, rather than stopping halfway as the others had done. He could see no further into the containment dome than anyone else. Mehler was doing what economist Herbert Simon called "satisficing," which means coming up with a workable and fast-acting solution without complete information. In an emergency, satisficing is better than "optimizing," which means trying for a solution that is close to perfect.

The primary system had lost about two-thirds of its coolant, allowing half the core to melt; perhaps twenty tons of uranium had melted into a slag pool at the bottom of the reactor vessel. The first direct sign of how serious the damage was became apparent the next day when a water sample was taken. It was loaded with black grit and radioactive particles from the ruptured fuel rods. The full story of the first day's chaos in the containment building would take fourteen years and a billion dollars to sort out completely.

There's still no agreement among TMI experts about why the PORV stuck open; possibly a buildup of boron compounds from the reactor coolant water, or an electrical malfunction—called chatter—that made the valve cycle open and close so many times that it wore out.

OF NORMAL ACCIDENTS AND HIGH-RELIABILITY ORGANIZATIONS

The bizarre events of TMI-2's man-machine struggle attracted much attention from system-safety thinkers. One of them was Charles

Perrow, who cited the events at Harrisburg to open his landmark book, *Normal Accidents*. Perrow concluded that some classes of technology are inherently open to chains of failure, whether sooner or later. With such machines, adding more safety systems only raises their levels of complexity. He said the systems of most concern are those involved in transforming dangerous substances (such as in a recombinant DNA lab or a nuclear reactor) and that show the characteristics of "tight coupling" and high "interactive complexity."

"Tight coupling" means a time-driven system in which one event leads to another in short order. A down-home example of tight coupling would be a line of fast-moving cars in traffic with too little separation between bumpers. Even a small problem with the front car, such as a flat tire or the driver's inattention, can cause a massive pileup among all the rest. An interactive and complex system is one that is subject to chains of unexpected failure. It resists thorough understanding by its managers and operators, like the reactor at TMI-2. Perrow believes the only sure way to manage the situation is to shelve the technologies that are too complex and too likely to fail catastrophically (he had nuclear power plants and gene splicing labs in mind), and to run any marginal ones with a very disciplined organization.

On the other side of the aisle are several sets of researchers who believe that people can safely handle just about any risky business if they organize themselves into "high reliability organizations," with employees who are empowered and trained in special ways. According to the high-reliability school, these groups all share a few key elements: a priority on safety from top to bottom; deep redundancy so the inevitable errors or malfunctions are caught in time; a structure that allows key decisions at all levels; workers who keep their skills sharp with practice and emergency drills; and a premium on learning lessons from trials and errors. These guidelines arose out of observations at such demanding places as air traffic control centers, nuclear power plants, aircraft carrier landing control centers, and nuclear submarines. These researchers zeroed in on plants whose operations have the worrisome elements listed by Perrow but who nonetheless have impressive safety records.

The feeling that mastery over machines is possible has inspired companies like DuPont, Lever Brothers Worldwide, and the INCO Corporation mining conglomerate to adopt a "zero injury" goal for their employees. DuPont reports that some of its plants have gone more than twenty years without any lost-workday accidents.

Though it's generally true that old and tested systems lie more open to view than new ones, my point is not that all modern systems are opaque and mysterious, whereas all old systems are visible and safe to operate. Certain machines of our time are already close to perfection. Today's gas turbines provide much more reliable propulsion for airliners and helicopters than the piston power plants they replaced, for example.

The problem of the blind spot can show up in any system with misreading instruments, hidden equipment, and a sluggish response to the controls. The problem grows much worse when crews don't know how little they are seeing into the machine, and then in a crisis they erroneously cobble up a theory and stick to it against all evidence. The next chapter looks at another hazardous mindset: the zeal to finish a great project before its time.