Root causes of the Three Mile Island accident

Designers of new nuclear power systems can learn from the TMI accident. They should assure the quality and completeness of the plant's safety analysis early in the design phase.

By Zoltan R. Rosztoczy

The accident at Unit 2 of the Three Mile Island nuclear power plant, at that time operated and partly owned by Metropolitan Edison Company, occurred 40 years ago, on March 28, 1979. Following the accident, two major investigations were conducted, one by the President's Commission on the Accident at Three Mile Island[1], appointed by President Carter, and the other by the Nuclear Regulatory Commission's Special Inquiry Group.[2] The investigations documented the timeline of the accident and the availability and failure of equipment, and addressed operator actions during the accident, the training of operators, and NRC procedures that applied to the event. The design process for the plant and the designer's responsibilities, including the plant's safety analysis, were not addressed. Many additional studies and papers have been published over the past 40 years, none of which have addressed the design process or the safety analysis of the plant.

The only effort specifically addressing the design of the plant and responsibility for the accident was Metropolitan Edison's lawsuit against Babcock & Wilcox (B&W), the designer of the plant. A trial began but was terminated, and the case was settled out of court. The court records are sealed; information is not available.

More than 10 years prior to the TMI-2 accident, B&W was designing its first nuclear power plant. In the designation of safety systems and in the safety analysis of the plant, there were two relatively minor but important omissions. These omissions turned out to be the root causes of the accident. If just one of them had been corrected during the intervening years, the accident would have been avoided.

The TMI design was reviewed by utilities purchasing plants from B&W and by the NRC. The omissions remained undetected. The safety role of the pilot-operated relief valve (PORV) and the PORV block valve were not fully appreciated. The manufacturer of the PORV was not notified of the valve's safety function, namely that it has to be able to close after being exposed to accident loads.[2] Also, the plant's safety analysis report (SAR) did not address loss-of-coolant accidents (LOCA) initiated by very small breaks. Unfortunately, the plant responds very differently to an event initiated by a stuck PORV than to the small-break events presented in the SAR. At the time, this was unknown.

Lessons learned from the omissions in the TMI design are timely today, when new types of reactors, such as small modular reactors, are on the drawing board. The designers of these new systems can learn from the TMI experience.

The initiating event

Operators attempting to clean a condensate polisher tripped the steam generator feedwater pumps. Then, the plant safety system tripped the turbine. The turbine was no longer removing heat from the reactor coolant system (RCS), the temperature and pressure of the RCS started rising rapidly, and the PORV opened, as designed.

Upon shutdown of the feedwater pumps, the plant's safety system turned on the emergency feedwater pumps. Due to a maintenance error, both emergency feedwater block valves, which are supposed to be open when the plant is operating, were closed, so no emergency feedwater reached the steam generators. The closed valves caused the RCS to heat up faster than in the case of a normal turbine trip, and the PORV was exposed to a larger load than normal, most likely a heavy two-phase flow (steam and water mixture) or water discharge. Thus, the closed valves could have played a role in causing the accident. This possibility is not addressed in the literature.

As RCS pressure increased, the reactor protection system shut the reactor down, after which the RCS pressure dropped. The PORV should have closed, but instead it stuck open, and the plant faced a LOCA. The obvious question is, "Why did the PORV fail to close?"

Designers of nuclear power plants have a dual responsibility. They must design the plant not only for normal operation of generating electricity, but also for safe performance in case of events that might occur during the lifetime of the plant and in case of postulated accidents.

Components of systems that have both an operating function and a safety function have to be identified and designed to perform both functions in a reliable man-

Zoltan R. Rosztoczy <zoltanrosztoczy@comcast.net> was Manager of the Safety Analysis Department of Combustion Engineering's Nuclear Division in its formative years. He later joined the Nuclear Regulatory Commission and was a charter member of the commission's Senior Executive Service.

Photo: The Jimmy Carter Presidential Library and Museum

From right to left: President Jimmy Carter, Pennsylvania Gov. Richard Thornburgh, and the NRC's Harold Denton tour the TMI-2 control room on April 1, 1979.

ner. The PORV is a good example of such a component. During normal operation, the PORV maintains RCS pressure below specified limits by opening and closing and by discharging steam from the pressurizer. During abnormal events, as in the TMI-2 case, the PORV could be discharging two-phase flow or water. The valve must be designed to perform its safety function—namely, to close following a two-phase flow or water discharge. Apparently, this was not the case at TMI. The PORV was not designed to perform its safety function. The purchase order failed to specify this requirement, and the supplier of the valve did not know that the valve had a safety function and that it had to close following two-phase flow or water discharge.[2]

Designers are also responsible for incorporating operating experience into their design. Prior to the TMI-2 accident, PORVs failed to close seven times at B&W plants.[2] Despite this record, the PORV itself was not modified or replaced. Instead, an indicator light was installed to show whether the block valve upstream of the PORV had received a signal to close, but there was no indication in the control room that the valve had actually closed.

PORVs opened relatively frequently on B&W-designed pressurized water reactors. The thermal hydraulic design of the reactor core was closer to acceptable limits than other PWR cores, and the amount of water contained in the secondary side of the steam generators was very small—only 25 percent of some other PWRs' water content.[2] These differences made the system react faster to changes. With quick plant response, the PORV came into action relatively frequently. More frequent use of the PORV led to more frequent failures. The PORV failure at TMI-2 was the eighth at a B&W plant, more than an order of magnitude higher than PORV failures with other reactor designs.[2]

The NRC has specific requirements for equipment related to safety. Equipment essential to accident mitigation and equipment whose failure can cause or aggravate an accident are considered "safety related." A stuck-open PORV causes a breach in the boundary of the RCS, creating a LOCA. Among postulated accidents, LOCAs are considered to be the most serious, and therefore they receive special attention. Nuclear power plants are designed with three barriers to protect the public from radioactive material release: The fuel is enclosed in a sealed cladding, the reactor core is within the closed RCS, and the RCS is covered by a containment building. Among all postulated accidents, there is only one—the LOCA—where two of the barriers are predicted to be damaged. In the case of a LOCA, the event itself breaches the RCS, and the predicted consequences of the accident are expected to damage some of the fuel cladding. Protection of the public is reduced to a single barrier, the containment building. Furthermore, valve failures are more likely than pipe breaks. Thus, the most likely LOCA is the stuck-open PORV.

Surprisingly, the PORV was not identified by the designer as safety-related equipment. The design was reviewed by Metropolitan Edison and evaluated by the NRC. Neither objected to the PORV not being designated as safety related, and the NRC approved the construction permit application. Had the PORV been designated as safety-related equipment, it would have had to meet reliability requirements and be tested under accident conditions. If the TMI-2 PORV had been tested, it most likely would not have passed. Following the accident, the manufacturer of the valve stated that the TMI-2 PORV was not qualified to close following a two-phase flow or water discharge.[2] If the PORV had been designated as safety related, it would have been replaced or modified.

The reason given for not designating the PORV as safety related was the presence of a block valve upstream of the PORV. If the PORV is stuck open, the block valve can be closed, terminating the accident. Thus, the block valve is essential for the mitigation of a PORV failure accident, and it is also considered safety-related equipment. It must have automatic safety-grade actuation initiated from the stuck-open PORV or, if the initiation is manual, safety-grade position indication must be available in the control room with sufficient time for operator action. Neither of these conditions existed at TMI-2.

Consequences of PORV failure

Part of the designer's responsibility is to conduct a complete and detailed safety analysis of the plant. The analysis must include transients that might occur in the plant. The analysis of transients must show that continued operation of the plant following these events is justified. The plant's safety analysis also has to address all potential accidents, both system failures and operator errors that the plant could be subject to, unless they are considered to be extremely unlikely (severe accidents). It is the designer's responsibility to identify all accident types specific to the design of the plant. In the case of water-cooled reactors, one of these accident types is a breach in the RCS—a LOCA.

For PWRs such as TMI-2, it is an NRC requirement that a complete spectrum of breaches in the RCS be analyzed, starting from the double-ended break of the largest pipe in the RCS down to the break size that the makeup water system can keep up with. Unfortunately, it was not emphasized that a breach in the system includes stuck-open valves if the valve's discharge area is within the size range of the postulated accident. The PORV falls within the size range. Complete spectrum also means all possible break locations. The consequences of a stuck-open valve on the top of the pressurizer could be different from a same-size break at a lower elevation.

Typically, prior to the TMI accident, the large-break LOCA analysis included break sizes in both the hot and cold legs of the RCS, starting from a double-ended break down to a 0.5 square-foot break. Usually, the consequences were most severe at one of the larger breaks. From there on, smaller sizes resulted in more favorable consequences. The small-break LOCA analysis ran from 0.5 square foot down to about 0.1 square foot. The trend was the same; smaller breaks had less severe consequences. Breaks even smaller were not analyzed for

two reasons: (1) the calculations ran long on the computer and the analyses were expensive, and (2) the trend was already established. Instead, the assumption was made that the trend would continue down to the smallest required size. Also, small-break LOCA analysis was assumed to be independent of break location. Thus, breaks less than 0.5 square foot were not analyzed at different locations, and breaks less than 0.1 square foot were not analyzed at all.

The safety analysis of the plant serves many purposes. It provides both the designer and the operator of the plant with an understanding of how the plant responds to a specific event or accident, indicates potential damage if mitigating actions are not taken, guides the designer in the design of the needed safety systems, and provides information for training the operating staff. The analysis shows how reactor operators can recognize a specific event and what actions they must take and provides the needed information for the preparation of emergency procedures. The results of the analysis also show compliance with applicable regulations. It shows that potential damage has been mitigated and the safety of plant personnel and the public is ensured.

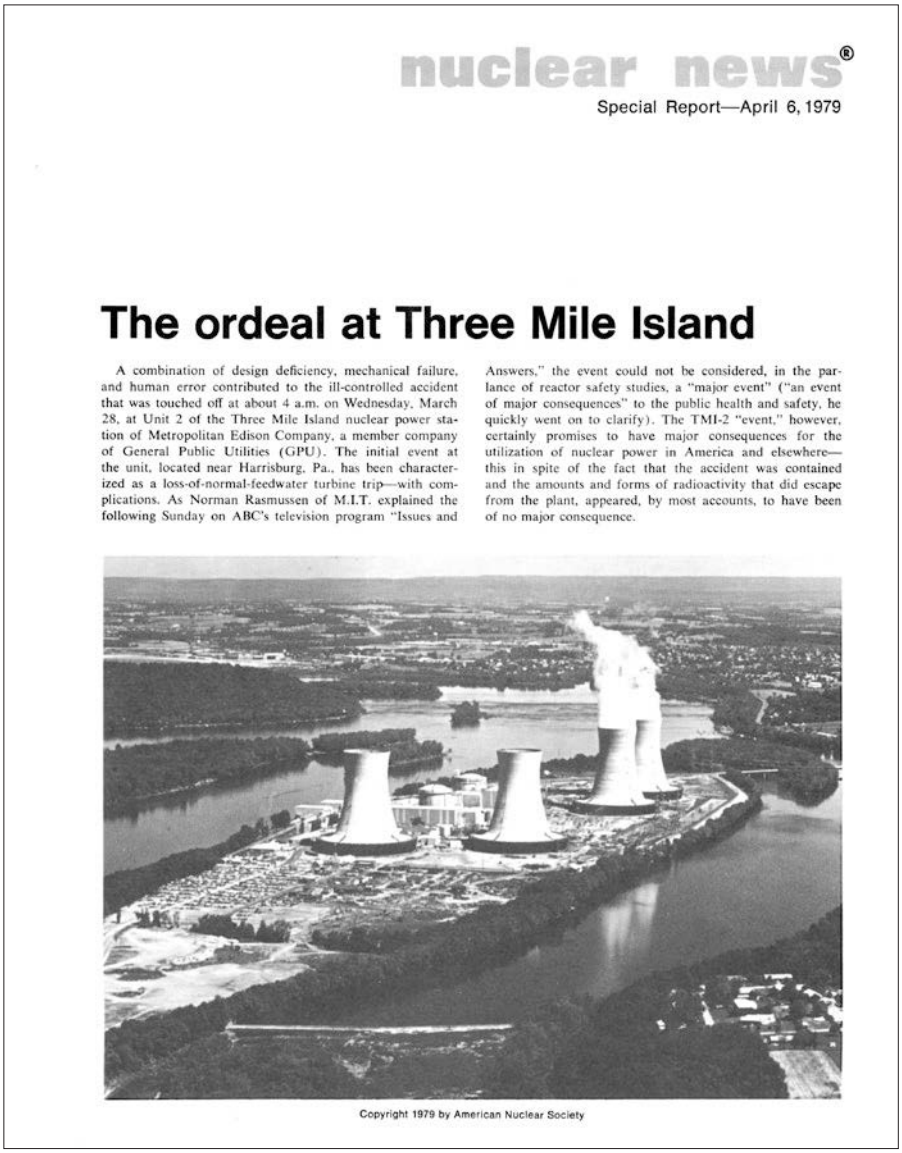
The TMI-2 LOCA analysis was performed by the designer. It was rather elaborate but was incomplete in the sense that it failed to show that very small breaks behave differently and have more serious consequences than small breaks. As part of the TMI-2 licensing process, no LOCA analysis was performed by the designer, and no LOCA analysis was submitted to the NRC by the utility for a break size anywhere close to the size of the discharge opening of the PORV (about 2 square inches). No analyses were performed for any size break at the top of the pressurizer or for a LOCA caused by a stuck-open PORV.

Unfortunately, as was learned from the TMI accident and from analysis performed after the accident, a stuck-open PORV LOCA is very different from the small-break LOCA analyses presented for TMI-2. Analysis of smaller breaks showed that the trend reverses and the consequences increase with decreasing break size. The plant responds differently, reliance on safety systems and instrumentation changes, and different operator actions are required.

The consequences of a PORV failure are even more different. RCS pressure can drop while the water level in the pressurizer is rising. Void can form in the reactor core and accumulate at high locations of the RCS while the pressurizer water level is high. Furthermore, the water level can drop below the top of the core, resulting in core damage, while the pressurizer water level is still high. Obviously, pressurizer water level indication is not a useful tool for the handling of this accident.

A special design feature of B&W plants further aggravates this effect. The pressurizer surge line is designed with a loop seal to prevent steam from entering the pressurizer. Eliminating steam flow to the pressurizer prevents water level drops in the pressurizer, keeping the water level high, while void is accumulating in the RCS.

Due to the lack of analysis, the consequences of a PORV failure were unknown. As it turned out, the actual consequences without proper mitigation were a lot worse than one would expect. The assumption that consequences get better with decreasing break size was incorrect. The actual consequences of the accident equally surprised the designers, the owner/operator of the plant, and the regulators. The plant's response to the PORV failure was totally unexpected.



nuclear news®

Special Report—April 6, 1979

The ordeal at Three Mile Island

A combination of design deficiency, mechanical failure, and human error contributed to the ill-controlled accident that was touched off at about 4 a.m. on Wednesday, March 28, at Unit 2 of the Three Mile Island nuclear power station of Metropolitan Edison Company, a member company of General Public Utilities (GPU). The initial event at the unit, located near Harrisburg, Pa., has been characterized as a loss-of-normal-feedwater turbine trip—with complications. As Norman Rasmussen of M.I.T. explained the following Sunday on ABC's television program "Issues and Answers," the event could not be considered, in the parlance of reactor safety studies, a "major event" ("an event of major consequences" to the public health and safety, he quickly went on to clarify). The TMI-2 "event," however, certainly promises to have major consequences for the utilization of nuclear power in America and elsewhere—this in spite of the fact that the accident was contained and the amounts and forms of radioactivity that did escape from the plant, appeared, by most accounts, to have been of no major consequence.

A six-page special report—*Nuclear News*'s initial coverage of the TMI accident—was mailed separately to subscribers and ANS members in April 1979.

Accident management

Early in the morning of March 28, 1979, four young operators at TMI-2 realized that something had happened, but they had no idea what it was. The turbine shut down, the reactor scrammed, and a cascade of alarms sounded and flashed. The plant was acting strangely. RCS pressure was decreasing while the pressurizer water level was increasing. The operators had not faced this situation before. It was not covered in their training. They did not know what to do.

The event facing the operating crew was a stuck-open PORV and a very small LOCA. They did not know that was the case. There was no direct indication of PORV position in the control room. They could not see that the PORV was stuck open.

Not knowing what was going on and not having familiarity with the event, the operators were improvising, trying to maintain water level in the RCS within prescribed limits. They relied on the pressurizer water level reading, as they were trained to do. Unfortunately, they took a

few inappropriate actions, which included turning off the high-pressure emergency core cooling system, opening the letdown line, ignoring signs of overheating of the reactor core, and pumping radioactive water to the auxiliary building. All of this occurred before they learned—two hours and 20 minutes into the accident—that the PORV was stuck open. Then they took corrective action and closed the block valve.

The obvious question is, "Why were the operators in the dark, and why did they lack familiarity with this event?" Their training covered mitigation of postulated accidents, including LOCAs. There was only one set of accidents missing, very small LOCAs, including PORV failure. Since the designer did not analyze this event, it was not included in operator training. Not knowing the plant's response to a PORV failure, the designers and the training staff instructed the operators to always rely on the pressurizer water level indication for water level measurements in the RCS. The operators followed their training on that morning.

Despite the total lack of training for a stuck-open PORV event, could the operators have realized what was going on and taken appropriate action? The answer is yes.[1] The temperature of the PORV drain pipe was monitored and showed high readings, an alarm signaled high water level in the containment building sump, high neutron level indications were observed in the reactor core, temperature and pressure were rising in the containment building, and the reactor coolant pumps were vibrating. Any of these observations, typical of a LOCA, could have brought attention to a stuck-open PORV. The remedy should have been obvious: Close the block valve.

Once the block valve was closed, the LOCA was terminated. The next step was to cool the core by natural circulation of the water in the RCS. This was not possible, however, due to the large amount of void that had accumulated in the RCS. The operating staff had to improvise again to reduce the void and the bubble in the RCS, and then to establish neutral circulation. It took a couple of days' work for them to accomplish this.

Both the plant's designer and operator lacked the knowledge of how the plant would respond to a stuck-open PORV. What they did not know, they could not pass on to the operators. The operators' training was misleading, and the emergency procedure was incorrect for the incident they were facing.

Industry practice and oversight

B&W's two omissions—safety-related classification of the PORV and the PORV block valve, and the lack of PORV failure analysis—were not unique to B&W. The other U.S. PWR designers, Westinghouse and Combustion Engineering, made the same omissions. How could three independent sets of engineers make the same mistake? Licensing of the plants was a major consideration. The SAR was the centerpiece of the licensing review. Precedent provided guidance for the preparation of the report. Analyses presented in previous applications were included in the report; analysis that was not required was ignored.

Dozens of utilities received SARs with the same omissions. The omissions had a direct and major effect on the training of reactor operators. The operators received training on a plant simulator, with postulated accidents programmed into the simulator. One accident, the PORV failure, was missing. Nobody noticed it or took corrective action. After PORVs failed seven times at B&W plants, this accident was still missing from the operator training program and from the simulator.

In the case of PWR evaluations, the NRC had the distinct advantage of reviewing SARs from three independent designers. Comparisons among the three designs frequently helped in the reviews. The NRC, however, failed to recognize its own effect on plant design and analysis. A nuclear power plant is a complex system. A regulatory review and evaluation cannot address all aspects of the design, and priorities have to be set. There was a tendency not to require more from an applicant than was required from previous ones. Spending time reviewing areas of the design that weren't reviewed in the past was discouraged. Consequently, regulators and designers addressed the same areas of the design and the safety analyses over and over again and ignored other areas.

Conclusions

Failure to incorporate the safety function of the PORV and the block valve in the design of the plant created the condition for the TMI accident. With no positive indication in the control room of an open PORV and no positive position indication of the block valve, the operators were left to guess what was going on and what needed to be done.

Not having addressed PORV failure in the plant safety analysis, the designers, as well as the training and operating staff, were unfamiliar with the plant's response to this type of accident. They did not know that the plant conditions the operators were facing were possible, and as a result, training and instructions were inadequate.

When similar plant designs are being reviewed or evaluated one after the other, there is a tendency to address the same issues in each case. Plants are very complex, and not everything can be evaluated as part of one review. It is appropriate to shift emphasis in subsequent reviews and to address issues previously not covered.

Appropriate NRC regulations relative to LOCAs to control the design and operation of the plants' safety systems and develop operator training programs and emergency procedures were evolving when B&W designed its first plants, but they were in place at the time of TMI-2's licensing. The problem was that some of the regulations were not followed.

The two omissions—not recognizing the safety function of the PORV and the block valve, and the failure to analyze the stuck-open PORV event—were the root causes of the TMI-2 accident. Correcting the first omission would have prevented the accident. Correcting the second omission would have resulted in prompt and effective mitigation of the accident.

Lessons learned

Understanding the root causes of the TMI accident provides valuable guidance for nuclear power plant designers, especially for designers of new plant types, such as small modular reactors. The recognition of safety-related components and design-specific accidents is more complex and more difficult than it appears to be. It is the designer's responsibility to identify all safety-related systems and components and to analyze all accident types.

Many systems and components of a plant have both an operational function and a safety function. In the design of every system, the question must be raised as to whether a system or component has a safety function. Then, if applicable, it must be designed for both the operational function and the safety function.

Plant response during accidents can be abnormal and never seen during normal operation. The plant's safety analysis must be complete, and it must describe all potential plant responses.

Designers cannot depend on utilities' reviews and regulatory evaluations to correct shortcomings. The design must be done right in the first place, and the quality assurance process should guarantee perfection of the design.

References

1. John G. Kemeny, et al.: *Report of the President's Commission on the Accident at Three Mile Island* (October 30, 1979).
2. Mitchell Rogovin, George T. Frampton Jr.: *Three Mile Island: A Report to the Commissioners and to the Public* (January 1980).

Acknowledgment

I am grateful to Sheldon Trubatch for his valuable suggestions, review of this article, and thoughtful comments and insight into the era from the legal perspective surrounding the accident. I have derived great benefit from our stimulating discussions. NN