In mid-1998, a nuclear utility in Sweden decided to see what would happen if it switched the clocks in its reactor’s computers to read January 1, 1999. The response surprised utility officials, who had expected business as usual. The reactor’s computers couldn’t recognize the date (1/1/99) and thus turned the reactor off. If the utility had waited to run this test, last New Year’s Eve would have been rather cold in Sweden. The Y2K computer bug caused the problem.

The Y2K computer bug has the potential to affect the safety and operation of the 433 nuclear power reactors in the world today, other major nuclear facilities, and the entire electrical power distribution grid, all of which may depend directly or indirectly on electronic components. Even in countries where reactor operators are working to correct Y2K vulnerabilities, it is not clear that all problems will be fixed in time. Of great concern are the many countries where this job has barely begun. Citizens can play an important role in ensuring that Y2K-related risks and disruptions are minimized by encouraging their utilities, state and local governments, and federal regulators and officials to devote the resources necessary to address the issue and to make appropriate contingency and emergency plans to cope with unexpected circumstances.

BACKGROUND

The Y2K computer bug stems from the early days of computers, when memory was very expensive. Software designers saved on memory costs by writing date-sensitive functions with a two-digit year (i.e. 99 instead of 1999). Thus, when the program reaches the year 2000, it may read it as 1900, with unpredictable ramifications. Many of these early programmers assumed their programs would be obsolete by 2000. Unfortunately, the practice continued for many years, and affects not only the early mainframe computers, but also personal computers and other electronic devices that use preprogrammed “embedded chips.”

In addition, depending on how programs were written, other dates may set off problems, including September 9, 1999, February 29, 2000, and others.

Y2K AND NUCLEAR SAFETY

The systems which take a reactor from active production of electricity to “off-line” seem to be free from electronic components that could malfunction with the arrival of 2000. This is the basis for national and international regulator’s claim that the Y2K bug does not affect the safety of atomic reactors. There are however computerized systems and electronic components on which reactor operators depend for monitoring and controlling the function of the reactor. Bad data can lead to human error, like at Chernobyl and Three Mile Island.

For example, a U.S. Nuclear Regulatory Commission audit of the Seabrook reactor in New Hampshire, released November 6, 1998, found, in this single power plant, 1,304 separate software items and embedded chips that were affected by the Y2K bug. Twelve of these were described as having “safety implications,” including the critical Reactor Vessel Level Indication System; another 13 could cause the reactor to trip (itself a potential safety issue); 160 affected systems required by regulations; and 800 were “significant to business. Only about 40% of the items were described as having “minimal” or “no impact” on plant operations. Yet, even this extensive review neglected to turn up the fact that the reactor’s back-up power system was not operational.

Reactors in Eastern Europe and Russia have fewer digital components, but the inherent design-based instability of the reactors, electrical problems, fires, lack of containment, lack of funding for maintenance coupled with the aging of the overall system as well as the fuel assemblies make the Y2K challenge of particular concern. The potential for problems with taking RBMK reactors offline suddenly (scram) compound problems if the electrical grids fail in the areas serving those reactors.

In addition, the unpredictable nature of computer and embedded chip responses to an unreadable date means that some failures of systems not directly related to safety could adversely affect safety systems or operator responses to unrelated emergencies (e.g., by providing incorrect data).

REACTION NEED ELECTRICITY

The Y2K bug threatens to disrupt the delivery of power via electrical grids, and could cause local or regional blackouts. Some have predicted national electrical blackouts. Failure of some small utilities could cause instability in the electrical grid, leading to localized blackouts; failure of one or more larger utilities could lead to regional blackouts. While this would be inconvenient at best
for most people, it is potentially disastrous for nuclear reactors.

A little-known reality of nuclear power is that atomic reactors need a steady source of electricity to cool their cores and irradiated fuel pools even when they are shut down. Without this cooling ability, even closed reactors would melt down; fuel pools would boil and release their highly-radioactive inventories. The U.S. Nuclear Regulatory Commission says this “station blackout” scenario accounts for 50% of the total risk of operating a reactor.

To compensate, nuclear plants are required to have back-up power sources. These are normally giant generators that run on diesel oil and each reactor is required to have two of them (although some multi-reactor sites share generators). But these diesel generators can be unreliable. In the United States, the national regulator says they are 95% reliable. That means that if all 200 or so U.S. generators were required at one time, 10 may fail. Moreover, there is reason to believe, given the operating history of these generators, that the 95% level in the U.S. is little more than wishful thinking. It is not clear what the status of back-up power is in other parts of the world.

In 1998 there were 2 reactors that were minutes away from a major accident because of lack of back-up power, combined with a loss of grid delivery. The Davis Besse reactor in the U.S. lost power from the grid due to a tornado. One generator would not start. The second generator ran but then overheated. The first was started, then it also overheated. The reactor was without power, but thankfully, off-site power was restored within minutes. In Scotland an ice storm brought down power lines serving the Heysham reactors. There neither generator would start. The reactor alarms were going off and fire trucks were heading to the site before they were able to accomplish a manual reset of the generators and obtain power.

**Preparing for Y2K**

Ideally, all computer and electronic systems are tested for date sensitivity and then work is done to upgrade those systems to make them Y2K compliant, and then testing is done to insure that the “fix” worked and did not create any new problems. A crucial next step is to assess the entire system for weakness, such as back-up power generation.

Finally, the human element and interaction with other services should be assessed through emergency drills. NIRS has submitted three petitions for new rules in the U.S. that would require nuclear utilities to meet these basic requirements. Most countries in Eastern Europe have responded to a questionnaire from the International Atomic Energy Agency on Y2K but there is little funding for actually implementing Y2K preparations. Russia has not yet responded to the IAEA.