Year-2000 Chip Danger Looms Large

With less than a year left to avert failures, computer experts and engineers are finding that year-2000 computer chip and software problems may be much more severe than had been anticipated.

The trickiest situations involve not software but integrated-circuit chips built into a wide variety of products, ranging from thermostats and valves to wristwatches and pacemaker monitors. "The more we work on the problem, the bigger it gets," says Michael P. Harden of Century Technology Services in McLean, Va.

Harden spoke at a meeting sponsored by the World Future Society last month in Washington, D.C., on preparing for potential disruptions caused by systems that stop working or produce erroneous output as the year 2000 nears.

The so-called Y2K problem stems from the pervasive use of two digits instead of four to represent the year in digital programs. Systems still using that shortcut by this time next year will have trouble interpreting whether 00 means 1900 or 2000.

A computer program sorting entries in a financial spreadsheet, for example, might put new data entered in the year 2000 at the beginning of a chronological list rather than the end. A bank might calculate that interest on a deposit made in 1999 and withdrawn in 2000 was earned over a period of –99 years instead of 1 year. Depending on how one part of a system affects another, such errors will have unpredictable consequences (SN: 8/7/93, p. 88).

"It is no minor programming glitch," says Jonathan Spalter of the U.S. Information Agency. "If we don't take action, it could threaten economic stability."

When the Y2K problem first came to light more than a decade ago, it was thought to be confined to large computers running software written many years ago, Harden says. "As we learned about the issue, we began to understand that any organization with a computer had a problem."

Major corporations, the federal government, and other organizations have already expended considerable effort and spent large sums fixing their computer systems. They have so far given less attention to computer chips installed in electronic equipment, including industrial machinery, monitoring devices, traffic lights, security alarms, and consumer products.

Control-system chips often need to keep track of time. Traffic-light and heating-system schedules, for example, change according to the day of the week. Monitoring devices are sometimes designed to shut down if they are not recalibrated at regular intervals.

Although certain applications may not require knowledge of the year, many general-purpose timing chips incorporate such a counter, says Mark A. Frautschi of Shakespeare and Tao Consulting in Lutherville, Md. It isn't always obvious whether a particular chip tracks the year.

Because instructions typically are encoded in chips permanently, the only solution in many pieces of equipment is to replace the chip. "You've got to go to where the problem is," Frautschi says. That may be impossible, however, if the chip happens to be in equipment deep underwater or embedded in concrete.

Harden and his coworkers have compiled a database, containing more than 1 million items, of information gleaned from manufacturers detailing how different chips perform. Only a tiny fraction of the roughly 70 billion chips manufactured since 1972 has a Y2K date problem, Harden notes. Identifying those with the problem, however, is an immense task.

A recent audit of the Seabrook nuclear power plant in New Hampshire revealed that 1,304 software items and embedded chips are affected by Y2K problems. The Nuclear Regulatory Commission report described 12 of them, including a reactor coolant-level indicator, as having "safety implications."

The complexity of the Y2K problem in both computers and chips—and the late start by many organizations—mean that many fixes will not be done in time. In some cases, "people aren't doing things the right way, and problems are not actually being solved," Harden contends.

A United Nations draft resolution emphasizes "the importance of contingency planning . . . to address the potential for large-scale failures in the public and private sectors."

"This is a major emergency," insists Harrison W. Fox, a staff member of the House of Representatives Management, Information, and Technology Subcommittee. Yet "there is still a lack of awareness of the problem." —*I. Peterson*

Water comes clean with new purity test

Water from a pristine mountain spring may be fine to drink, but it's not clean enough for drug and computer-chip manufacturers. Both need huge amounts of ultrapure water, which is filtered so clean that it contains only one or two bacteria in a liter of liquid.

Researchers from Organo Corp. and Fuji Electric Corporate Research and Development in Japan have developed a new, quick way to detect bacteria in ultrapure water, down to individual cells. Using this method, the group finds that contamination in ultrapure water is much higher than existing tests show.

The pharmaceutical industry uses ultrapure water in sterile products such as intravenous solutions. In computer-chip manufacturing, ultrapure water flushes away chemicals between processing steps. Stray particles could bridge the tiny connections etched onto the chip, causing a short circuit.

"The microelectronic requirements are even more demanding than the pharmaceutical requirements," says Theodore H. Meltzer, a water-filtration consultant in Bethesda, Md. Because one organism can multiply, "you can't be casual about even the lowest amounts."

Up until now, the best way to determine bacterial contamination has been to pass a water sample through an ultrafine filter, grow any captured cells for 2 to 7 days, and then count the number of colonies that form. This process is slow and "inadequate in terms of selectivity and sensitivity," says microbiologist Marc Mittelman of Altran Corp., an engineering firm in Boston. The Japanese group's method improves on all these aspects, he notes.

The researchers created a novel probe for bacteria by using antibodies that attach themselves to any DNA they come across. These antibodies were derived from mice genetically engineered to model the autoimmune disease lupus. When the antibodies are attached to an enzyme that catalyzes a light-producing chemical reaction, the complex glows in the presence of DNA.

To assess contamination, the researchers capture bacteria on a filter, break the cells apart to release their DNA, then apply the probe. A sensitive camera records the tiny spots of light from the filter, the team reports in the Dec. 15, 1998 ANALYTICAL CHEMISTRY.

The new technique detected up to 225 times more cells in ultrapure water than the traditional technique did, at least in part because the method counts dead bacteria as well as living ones. Chip makers can use this information, since even dead cells can cause a short circuit. Pharmaceutical companies, however, would need additional tests to distinguish between live and dead organisms, Mittelman says.—*C. Wu*