Microchip Problems Plague DOD

Inadequate testing of millions of integrated circuits by Texas Instruments has sown new anxiety about the performance of weapons and spacecraft

On Monday, 4 September, senior executives of Texas Instruments (TI) brought politically alarming news to Washington. An internal corporate investigation had disclosed that millions of integrated circuits, assembled at a Texas Instruments factory in Taiwan and subsequently implanted in several hundred major U.S. military aircraft and weapons systems, had not been properly tested. High-level Pentagon officials say they were told that although the problem was traced as far back as 1975, its enormity had been recognized by the company only in late August.

The disclosure is embarrassing to the Defense Department because it comes on the heels of similar revelations involving two other major manufacturers of computer chips for use in U.S. armaments. And it also comes at a time when the Reagan Administration is doing its utmost, in the midst of a presidential campaign, to subdue congressional indignation over reports of defects in a wide-ranging series of sophisticated and costly weapons systems.

As a result, public relations specialists at both the Defense Department and TI have done their best to downplay the gravity of the company's oversight. Publicly, they have stated that the deficient testing involves 15 million microcircuits sold to IBM, as well as an indeterminate number sold to TI's other corporate customers for use in modern weapons. Richard DeLauer, the Pentagon's top scientist, told the press that the fault apparently lay with the management of TI's plant in Taipei. And he emphasized that the quality of TI's chips was not at issue. "The manufacturing process is not under suspicion at all," he said. "The quality of the product is very good." This point is reiterated by James Harroun, a spokesman for IBM. "To the best of my knowledge, the Defense Department has not had a single complaint" about the weapons in which the circuits were installed, he told *Science*. "We have not had a mention of any problem that has to do with performance or reliability of our systems."

But a different account emerges from conversations with government officials actively investigating the case, most of whom would talk only on the condition that they not be identified by name. Several characterize it as the worst and most extensive incident of its kind. Although the total number of chips involved remains unknown, one defense official predicts that "we'll probably tally 100 million before it's over, maybe more." The official adds that the chips were used in more than 270 major weapons systems, made by more than 80 defense contractors. "All of the biggies are included: Hughes, Sperry, General Dynamics, Boeing, Rockwell, McDonnell-Douglas, and so on," the official says. A complete list of the weapons involved was still being drawn up last week, but Trident submarines, B-52 and B-1 bombers, F-15, F-111, F-4, A-6, and A-7 aircraft, and Harpoon and HARM missiles are known to be included.

TI executives are just now beginning to discuss the testing irregularities with each of their customers. Already, they have determined that responsibility does not lie with management in Taiwan, but with improper directions from TI's military semiconductor headquarters in Midland, Texas. The details will presumably be fleshed out by a team of investigators from the Defense Logistics Agency and each of the three military services, now poring over the books in Midland.

The largest controversy surrounds the assertion by IBM and TI that the quality and reliability of the microcircuits is manifest, despite admitted discrepancies between the tests requested by customers and those actually performed in Taiwan. The claim has recently been challenged by officials at the National Aeronautics and Space Administration (NASA), which directs the development of numerous space systems that use microcircuits assembled at the same location. The agency has traced the failure of two IBM computers aboard the space shuttle Challenger last December, for example, to short circuits caused by loose silicon or metallic particles inside two TI integrated circuits, according to Harry Quong, the agency's director of reliability and quality assurance. Similarly, the failure of another IBM computer aboard the space shuttle Discovery last June has been traced to the contamination of another TI microcircuit by either saliva or perspiration, Quong says.

Quong adds that the revelation of these problems caused the space agency to order tests in August of 13 additional TI microcircuits slated for use in the space shuttle program. Four were immediately found to be contaminated with minute but highly conductive balls of solder, formed during the installation of protective covers atop the circuits. Upon further analysis, all 13 were found to be contaminated with either saliva or perspiration. "Obviously it came during the assembly operation," Quong says. TI says that it received this data only recently, and that a preliminary analysis indicates that all 13 chips were of a single type. But Quong points out that the contaminated circuits in question—used in the two shuttles as well as in the latest tests—are actually of several different types, and were manufactured in 1977, 1978, 1982, and 1983, indicating that the plant's quality control has been lax for many years. "As of now, anything produced by TI is of major concern to us," Quong says. Asked if he thinks similar chips were supplied to the Defense Department, he replies, "I would imagine it would be about the same. I see no reason why it should not be."

Due to the unwillingness of IBM and TI officials to discuss the problem in detail, the circumstances surrounding its discovery remain somewhat fuzzy to outsiders. Harroun of IBM says that a portion of it came to light during a 1983 IBM "quality" audit of TI's Midland plant. "When we looked at TI's documentation that said here are the tests that were run as ordered, the test numbers were different. As it turned out, they had not run the tests that we had asked for." The purpose of the tests, he explains, was to prove that circuits produced primarily for civilian uses are capable of withstanding the extraordinary stresses experienced in military applications: unusually high or low temperatures, extreme vibration, enormous acceleration, exposure to moisture, and so on. Completion of such tests can take weeks.

Neither TI nor IBM will say what triggered the audit or why the irregularities were not detected years earlier.

According to Pentagon officials, military suppliers such as IBM are contractually responsible for auditing subcontractors such as TI at government expense. DeLauer of DOD says that IBM was indeed paid for such work. "My concern is with IBM," he says. "I'm going to check on them . . . I want to know why they charged us that and didn't catch this. . . We're going to dig into the bottom of this." He and others working on the investigation note that TI's other customers were also responsible for ensuring that the tests were properly performed. "It is clearly their responsibility, and they weren't doing it: the IBM's, the Hughes's, the Sperry's," says a senior investigator. "They made a contract with the government and didn't follow it."

DeLauer says that in some cases TI relaxed the test requirements and, in others, it eliminated tests altogether. Norman Neureiter, a TI vice president and manager of corporate relations, emphasizes that every chip was given some testing at the commercial production line, which churns out billions annually. He adds that "only a small number of test elements were not conducted as they should have been." Both firms assert that defective chips would probably have been detected anyway during tests at a later stage in the manufacturing process. "Before our systems go out into the field, they are tested as subassemblies, then as completed weapons. So if a TI chip is not going to work, we're going to know about it," Harroun insists. Paradoxically, he adds that proper testing at the microcircuit level is still important, and that TI should have done it.

Several Pentagon officials suggest that these assertions by TI and IBM are somewhat misleading. One points out, for example, that the testing of completed weapons is frequently as inadequate as that performed by TI. Another notes that the Pentagon's mechanism for detecting part failures is also somewhat unreliable. "'No one will really know if we have a problem with these parts for another 4 to 5 weeks, when TI's customers answer a special survey that we ordered," the official said.

Even then, the complete picture may not be known, notes a senior Defense Department engineer with extensive experience in semiconductor reliability. Some of the chips have been installed in weapons intended for one-time use in combat, the engineer notes. Others may be so deeply embedded in a weapon that a complete failure analysis is impossible, the engineer adds. Consequently, many problems may not be traced to their source, and the contractors' upbeat claims may not be easily challenged. Thus far, he says, "we don't have absolute across-the-board evidence that indicates TI circuits are failing more often than they should. But if you go out and look at these weapons systems, there are plenty of malfunctions—even more than we anticipated. The sorry news is that TI parts may not be better or worse than any others and still be pretty bad."

Others point out that even if TI circuits are operating flawlessly now, there is little assurance that they will continue to do so in coming years, because the neglected tests might have weeded out chips that wear out quickly. DeLauer, for example, says he is "concerned about this from a mean time-between-failure standpoint. . . . We haven't had any failures yet, but the time hasn't gone far enough." Another senior Defense Department official agrees. "Although the early performance of the devices [may be] accounted for, there is no way to tell until years from now what the long-term reliability effect is going to be. At that time, nobody will know what the cause is. We will have forgotten about this by that time."

"As of now, anything produced by Texas Instruments is of major concern to us," a NASA official says .

One of the topics under investigation by the Defense Department is why IBM failed to inform the government of the results of its TI audit until last January, 8 months after it took place. Harroun of IBM will say only that his firm spent that period "working with TI to define the problem, to determine whether this was a single purchase order problem or something else. We were checking records at TI and [at IBM's office in] Owego, New York. It is not something that you just turn around in a week and 10 days." A senior investigator says this explanation is inadequate. "We've suggested to them that they should have told us a lot sooner. Is that a kind enough way of putting it?"

Within 3 days of IBM's disclosure, the Pentagon issued a decree that no further equipment would be accepted from Owego until the matter was cleared up. Several weeks ago, this order was extended to all of TI's corporate clients. But both orders had considerably more bark than bite. Harroun reports that to date, not a single IBM part with TI chips has been turned away. Most of the chips have been "revalidated," he says, and others have been granted waivers. "If the part is critical, meaning that you've got to have [it] for a B-52, you can get a waiver," explains DeLauer. "So, planes aren't stopping flying and missiles aren't stopping testing."

The ongoing process of microchip "revalidation" is also somewhat suspect. Harroun declines to describe it at all. "I just don't have that information. It's very detailed, very technical," he says. Neureter of TI says only that revalidation consists of detailed analysis of the "test documentation—to ascertain if there are discrepancies in testing procedures, and possibly to rewrite test programs." It is up to the customer, he says, "to decide what the implications are for his system." Thus far, according to both TI and the Defense Department, analysis of tests conducted on 2200 of the 4700 types of microcircuits in question has resulted in their successful revalidation.

Again, there may be less here than meets the eye. Defense Department officials say privately that nearly 10,000 different types of microcircuits are involved, but that TI has decided to restrict its analysis to the 4700 now in active use. Revalidation, they say, consists largely of TI persuading its corporate clients to accept the chips as is, and of the clients persuading the military services to accept the weapons in question as is. No additional tests of microcircuits in military applications have been conducted as yet, according to a senior investigator, although he feels certain that some will occur eventually. The senior Defense Department engineer is more skeptical. "A lot of bucks are tied up in this," he says. "A lot of relationships are involved. Besides, in most cases, you do more damage than you prevent by ripping these circuits off a board, even if the board is filled with lousy parts. Almost everybody is reluctant to do it."

At NASA, Quong says, "We're still trying to get our arms around the problem. We are in the same position as the Defense Department, with 90 percent of our business done through prime contractors who may or may not have used TI chips." Last January, the agency ordered IBM to conduct its own tests for particle contamination in TI circuits. Several aboard the three shuttle craft were replaced as a result. But Quong continues to worry because such testing is "not an exact science, it's an art." And he notes that some of the TI microchips used in the space shuttle program

malfunctioned at critical moments—during landing and shortly before takeoff. The agency is presently examining the vulnerability of every space system component with TI parts. "If it's not in a critical path, if we have redundancy, we would feel very comfortable. If we don't have redundancy, we'll have to go in and replace it."

Like the Defense Department, NASA has no idea what all this will cost. DeLauer, at a press conference, said that "it's too early to tell" if criminal prosecution is possible, probable, or warranted. When asked if the Defense Logistics Agency should also have detected the breadth of the problem earlier than it did, the senior investigator says, "Yes. Absolutely. So could the Air Force, so could the Army, so could the Navy. Any one of them. They all knew about it [after the notification in January]. There were meetings with IBM, and all those guys were invited to participate."

Some government officials believe that in the long run, problems such as this can only be avoided through the use of standardized computer circuits, manufactured under rigorous government supervision, for virtually all military applications. Industry has resisted the idea, the officials say, because the creation of circuits like TI's with unique capabilities—as ostensibly proven in tests—is far more profitable. Competition is all but eliminated, because only one microchip supplier exists, both when the weapon is manufactured and when it is repaired. But some feel that recent highly publicized discoveries of microchip testing irregularities at several companies, in addition to TI, cannot help but motivate the Pentagon officials to press harder for standardization.

—R. JEFFREY SMITH

Universities Vie for DOD Software Center

The chance to operate a major software engineering center for the Pentagon has kindled keen competition among universities who regard the center as a high-technology plum. The winning proposal will bring a contract worth $103 million over 5 years to establish and run a facility to be called the DOD Software Engineering Institute (SEI).

The SEI idea is a product of growing concern within the military that, as software has grown more important, more complex, and more expensive, emerging software ideas and technologies are not being incorporated satisfactorily into the systems being developed for the Department of Defense (DOD). Establishment of SEI was put forward as a way to improve the transfer of new software technology to government and defense industry users and to help overcome a shortage of software professionals.

The center will take the form of a federally funded research and development center (FFRDC), operating as a nonprofit organization managed by a university or consortium of universities. Its independent status would permit the institute to perform classified work, which is proscribed for on-campus laboratories by many universities. SEI's relation to government agencies will be similar to that of Lincoln Laboratories, an MIT spin-off, which mainly does electronics R&D for the military.

The Pentagon has not identified the bidders who met the deadline for proposals in early August, but seven contenders confirm that they submitted proposals and made presentations to a DOD evaluation panel. The aspirants include several combinations and permutations of universities and nonprofit organizations.

The Texas Engineering Experiment Station of the Texas A&M University system is taking the lead in a group that includes the University of Texas at Austin as an affiliate plus the University of Houston at Clear Lake, hard by the Johnson Space Center; Prairie View A&M University; and, outside Texas, the University of Southwestern Louisiana and the University of Southern California. The University of Michigan has formed a consortium with three other Big Ten universities: Illinois, Ohio State, and Purdue. Ohio State is also a major partner along with Wright State University in Dayton in a consortium that includes the University of Dayton and Sinclair Community College, as well as the University of Central Florida. The University of Maryland has joined with IIT Research Institute to propose establishment of the institute in the Washington, D.C., area. Carnegie–Mellon University in Pittsburgh has put in a solo bid, but has the "support" of the other major research universities in Pennsylvania. Georgia Institute of Technology is another single institution entry. And Northeastern University in Boston has offered a further variation by bidding to operate the institute itself but including pledges of participation from senior researchers from Brown, Harvard, MIT, and the Wang Institute for Advanced Graduate Study.

Although the contract has only a 5-year term, creation of a new FFRDC implies DOD intentions to underwrite a long-term effort. SEI's mission, according to one DOD description is "to accelerate the transition of emerging or advanced software technology into use in the development of DOD weapons systems." University sources say that the center is not expected to do direct applications work, but to make it possible for the Pentagon to use the most sophisticated software systems to meet a wide spectrum of demands.

In this cause, SEI will be called on to survey the software field for state-of-the-art developments useful to DOD systems. DOD is asking that SEI create a "showcase environment incorporating these techniques and methods" to aid the transition of new software technology to industry users. SEI will be expected to establish a so-called software factory capable of providing software tools and reusable software parts that can be employed as building blocks in various DOD computerized systems. For the universities, snaring the institute is seen as a way to provide a major inducement in recruiting faculty and to offer challenging work for graduate students, as well as being an opportunity to push an institution to the forefront of an important and highly competitive field.

DOD is keeping the procurement process under tight wraps. It is known that congressional delegations have mobilized to press the case in behalf of their constituents and there is some anxiety among the applicants that political muscle rather than merit might prevail. The decision on the contract was originally scheduled for 1 November but has been delayed to late in the month at the earliest. Slippage is not unusual in such cases, but in this instance, the move beyond election day might reduce the intensity of political pressure.—JOHN WALSH