PART FIVE
DECADE
90
The future of system design

Fault-tolerant design spans terrestrial and space applications

The growing commercialization of space will boost many more electronic systems into orbit in the 1990s. Fault-tolerant design techniques developed originally for aerospace systems will pervade the electronics industry as customers demand the utmost in reliability from every electronic product, even those intended for use on Earth.

Steven H Leibson, *Regional Editor*

Space has been a commercial frontier for more than 20 years, thanks to communications satellites. In the 1990s, a lot more hardware is headed off Earth both to enhance existing communications facilities and to expand the commercial use of space into other areas. President Reagan recently revealed a new space initiative that calls for increased commercialization of space, and several companies are now deeply involved in plans to make that vision real. As a result, during the next decade, engineers will design many more electronic systems for spaceborne applications than they have in past years.

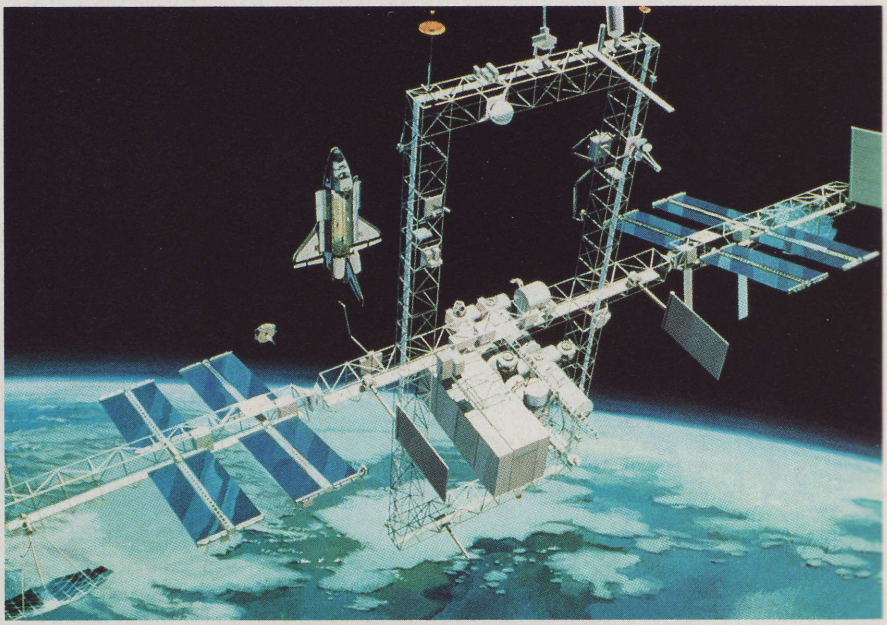
Systems for use in space must meet stringent reliability requirements. They must also withstand the unusual environmental hazards present in space, such as temperature extremes and radiation. What's more, as electronics spreads throughout earthbound applications, any system that plays a vital role in the health and welfare of human beings will have to meet requirements similar to those for spaceborne systems. Whether they're designing systems for use in space or on Earth, therefore, more engineers will have to become better acquainted with fault-tolerant design.

Space presents immediate challenges

The US's permanently manned space station, which NASA plans to make operational by 1997, represents a major opportunity for progress in space electronics. Just for its construction, the station requires extensive development of automated systems that manage data, environmental-control, life-support, thermal, and power systems. NASA divided the space-station project into four work packages and, last December, awarded contracts for these packages to Boeing Aerospace Co (Huntsville, AL), McDonnell Douglas Astronautics Co (Huntington Beach, CA), the Astro-Space Div of General Electric Co (Valley Forge, PA), and the Rocketdyne Div of Rockwell International (Canoga Park, CA).

In February 1988, President Reagan revealed a new space policy that plays up the role of private companies in US space efforts. In fact, firms in the US such as Space Services Inc (Houston, TX), with its Conestoga Series small boosters, are already attacking the first major hurdle—cost-effective access to orbit—by developing independent launch systems to supplement US

PART FIVE
DECADE
90
The future of system design



The US's permanently manned space station, *which is scheduled to become operational in 1997, presents several opportunities for designing fault-tolerant systems that manage data, environmental-control, life-support, thermal, and power systems. In addition, the space station will provide a platform for conducting manufacturing-related investigations, which will also require fault-tolerant systems to oversee the experiments. (Photo courtesy NASA)*

government vehicles. One forward-looking company, Orbital Transport Services Inc (Phoenix, AZ), is developing an electromagnetic catapult that employs superconducting storage rings to provide the electrical energy for launching a payload into orbit.

A space station smaller than NASA's planned one, the industrial space facility (ISF) designed by Space Industries Inc (Houston, TX), is scheduled to become operational in 1991, much earlier than the manned space station. The unmanned ISF will provide a platform for materials research and automated manufacturing. Unlike the manned space station, it will not incorporate life-support systems, but will be visited occasionally by the space shuttle for repairs, supplies, and retrieval of manufactured products.

Many other countries, attracted by the potential profits in satellite delivery, have entered the space-transportation business. The European Space Agency (ESA) has already launched several payloads with its Ariane booster series, and has recently decided to build an improved model—the Ariane 5—as well as the Hermes space shuttle and the Columbus manned space laboratory. China and the USSR have also entered the competition by selling rides on their respective Long March and Proton heavy-lift boosters. Japan, though not yet in the fray, is currently developing a commercial launch vehicle of its own. Consequently, a lot of electronic hardware will be heading for space during the 1990s.

Though more electronic systems will end up in space during the 1990s, many engineers today lack the expertise to design systems for extraterrestrial environments. Electronic systems in space applications must tolerate radiation, and few engineers are familiar with the components and techniques necessary to build radiation-resistant circuitry (see **box,** "Proofing electronic systems against radiation").

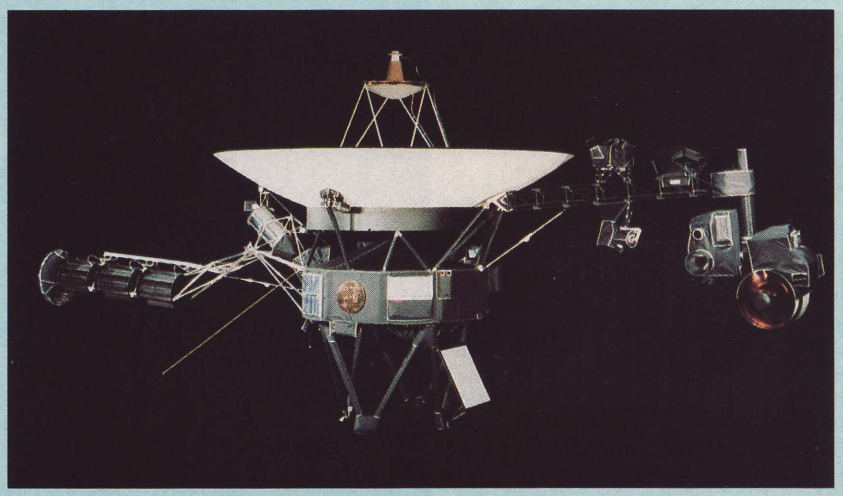
Space hardware must also be very reliable, because on-site service is either very costly or unavailable. Furthermore, most space equipment must be robust enough to handle unplanned problems without human intervention. Today, engineers developing equipment for aerospace applications are some of the world's leading experts on fault-tolerant, redundant design.

Aircraft need fault tolerance

According to Gary Kravetz, vice president of engineering at Fail-Safe Technology Corp (a consulting firm specializing in reliable-system design), engineers first started using fault-tolerant and fail-safe designs for aircraft flight-control systems in the 1960s. At that time, aeronautical engineers were starting to design inherently unstable airframes, such as that of the F-16 fighter, that required a computer to dynamically position the control surfaces for stable flight. The control computers had to be absolutely reliable, because computer failure in such applications results in catastrophic consequences—the plane will fall out of the sky.

Proofing electronic systems against radiation

Besides requiring reliability, redundancy, and robustness, spaceborne systems encounter an environmental hazard not common to most terrestrial applications: radiation. All ICs tolerate radiation to some extent, but because manufacturers are always trying to optimize other characteristics such as yield or speed in their commercial parts, chips that are not specifically hardened against radiation may not have repeatable radiation tolerance from lot to lot. Engineers confer hardness on a design by using special device geometries and spacings and by fabricating the chips with carefully controlled processes.



Voyager's mission posed some tough challenges *for designers trying to harden the spacecraft's electronic systems against radiation. One such challenge presented itself in the form of reports from Pioneer 10 and 11—a year after the Voyager design was finished—that the radiation intensity in the vicinity of Jupiter was 1000 times greater than experts had estimated. The discovery required Voyager's designers to provide the craft with additional radiation hardening. (Photo courtesy JPL/NASA)*

Spurred by the US government's requirements for radiation-hardened devices in military and space applications, several companies now offer ICs specifically built for high-radiation environments. For example, Harris Semiconductor (Melbourne, FL), offers several lines of rad-hardened analog and digital ICs. The company even offers a hardened version of the Intel 8086 μP, which Ball Aerospace Systems Div (Boulder, CO) has incorporated in its subsystem processor, a computer subsystem that Ball plans to use as a controller in future spacecraft designs.

The United Technologies Microelectronics Center Inc (UTMC, Colorado Springs, CO) also offers rad-hardened ICs. The company makes both standard parts and ASICs for systems that must tolerate radiation. Recently, UTMC introduced the UTD-R family of gate arrays, which meets all of its data-sheet specifications after absorbing a 1M-rad (Si) dose of radiation. That's about the radiation dosage an unshielded system must endure while orbiting the Earth for 10 years.

Different types of radiation (neutrons, ionizing radiation, and heavy ions) affect semiconductors differently. In addition, different dose rates create varying effects. Because device physicists don't yet fully understand all of the changes that different types of radiation produce in semiconductors, few standards for testing an IC's radiation hardness exist. Most of the existing standards were created by the US Department of Defense.

Rad-hardened-system design has remained a rather esoteric field that's limited mostly to military and space applications. However, because of the growing number of electronic systems in space, more engineers will need to develop expertise in rad-hard design. The IEEE's Nuclear and Plasma Sciences Society serves as an excellent source of information concerning radiation effects on electronic devices. The society sponsors an annual Nuclear and Space Radiation Effects Conference (NSREC) that includes a short course on rad-hard design methods for the uninitiated. This year's conference will take place in Portland, OR, from July 11 to 15. For more information about the 1988 NSREC, contact Bobby Buchanan at Spire Corp (Bedford, MA, (617) 275-6000).

PART FIVE
DECADE
90
The future of system design

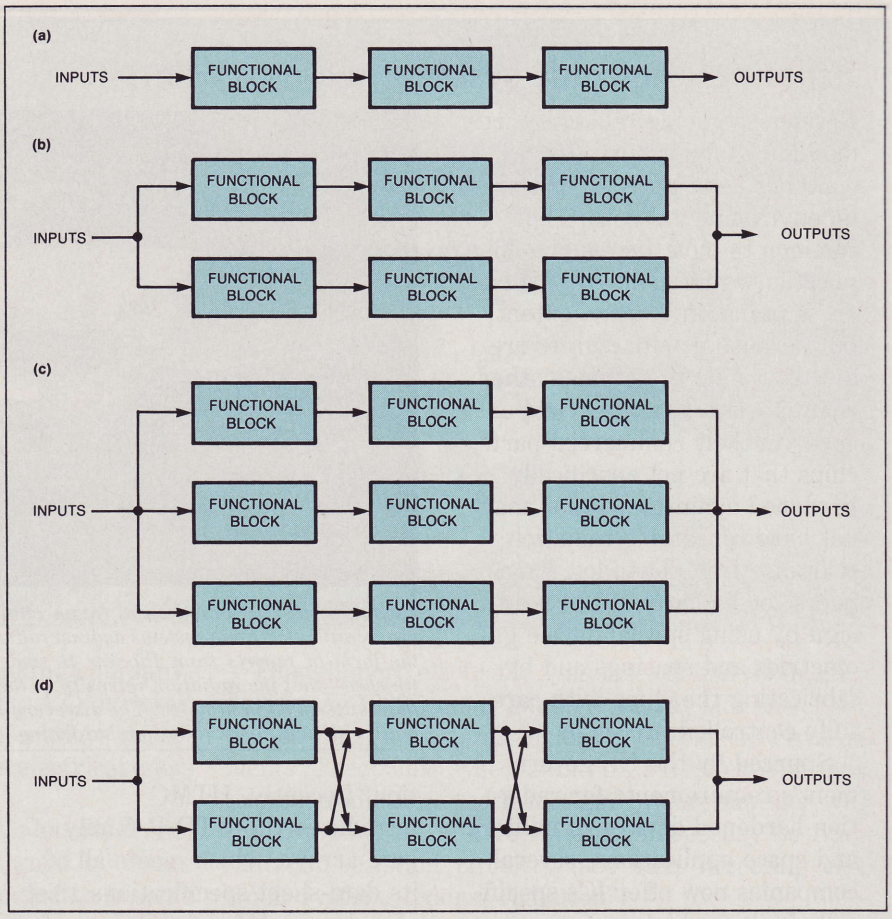


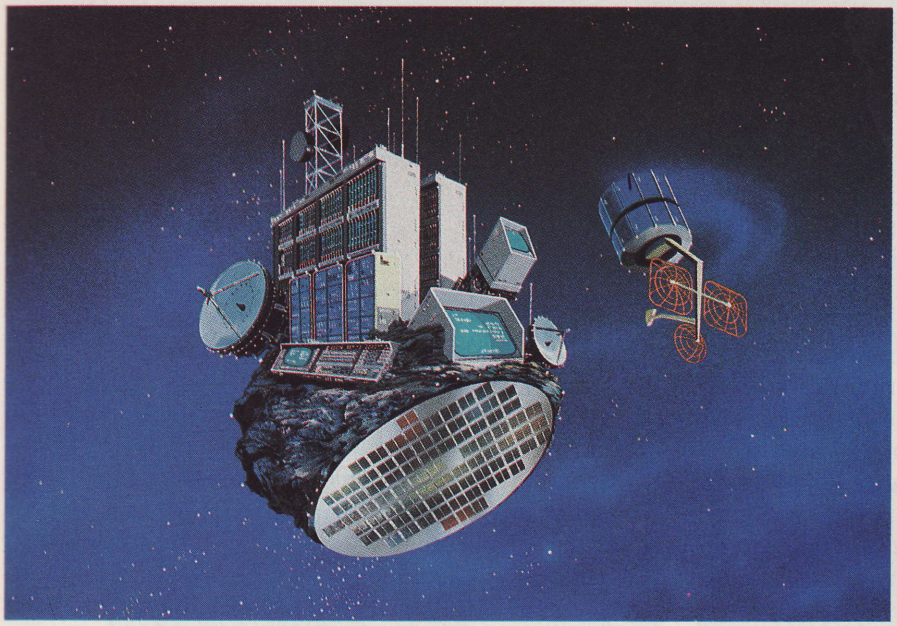
Fig 1—You can represent a complex system as a string of functional blocks, *assign the string a reliability figure, and then compute the expected failure rate for the entire string* ***(a).*** *Should that figure not meet your system specs, you can add a parallel, redundant system* ***(b),*** *or even two of them* ***(c),*** *to boost the overall system reliability. To achieve even greater reliability, usually at lower cost, spacecraft designers often use cross-strapping, which allows one system to use functional components from another system in case of a failure* ***(d).***

Kravetz says that spacecraft requirements for electronic control systems vary according to the mission. The first orbiting satellites had fairly simple electronic systems, because they could rely on human ground controllers to rectify problems by radio control. Attitude controls, however, were made fail-safe so that a control-system failure would not plunge the satellite into the atmosphere before the ground crew could correct the fault.

Ball Aerospace Systems Div (Boulder, CO) specializes in building unmanned orbital spacecraft. William H Follett, deputy director of spacecraft systems at Ball, says that the aerospace industry has developed several approaches to improving system reliability. For example, you can represent a complex system as a series of functional blocks, assign a reliability figure for the string, and then compute the expected failure rate for the entire string **(Fig 1a)**. Should that figure not meet your system specifications, you can add a parallel, redundant system **(Fig 1b)**.

If that step does not achieve the desired system reliability, you could add another redundant system to the design **(Fig 1c)**, but spacecraft designers often use a different approach, cross-strapping, which allows one system to use functional components from another system in case of a failure **(Fig 1d)**. Cross-strapping achieves better reliability than simple replication, and it does so at a lower hardware cost than you'd incur by building systems with triple redundancy.

For orbital spacecraft, ground controllers can manually switch components into operation by using cross-strapping. Planetary probes such as the Voyager and Galileo spacecraft developed by the Jet Propulsion Laboratory at the California Institute of Technology (Los Angeles, CA), however, can't depend on ground control, because planets and other celestial objects occasionally block radio transmissions. Such spacecraft require electronic control systems that are not only fail-safe, but redundant, self-repairing, and autonomous as well.



Commercial space development in the 1990s will strengthen *the communications systems already in orbit and will initiate the era of manufacturing in space. Such enterprises require robust, reliable, redundant electronic systems that can manage operations, providing a less-expensive alternative to constant human attention. (Photo courtesy Motorola Inc, Phoenix, AZ)*

Robust, redundant, highly reliable systems certainly are critical for space applications. But they're important for applications on Earth, too. For example, by the early 1990s, at least one auto manufacturer will offer vehicles with drive-by-wire steering, in which there's no mechanical linkage between the steering wheel and the front wheels. Such a system requires less energy to operate than a hydraulic power-steering system does. The electronic steering subsystem in a drive-by-wire car had better be as robust, reliable, and redundant as any of the circuitry in a planetary space probe. In addition, as electronics become more pervasive in medical equipment, redundant and reliable design will be needed to safeguard a patient's health and well being.

Other applications in which lives hang in the balance include automated transportation, such as San Francisco's BART (Bay Area Rapid Transit) system, and industrial process control. Such applications demand fault-tolerant electronic systems. Moreover, after the USSR's Chernobyl disaster and the Three Mile Island scare in the US, many utility companies are retrofitting manual control systems in nuclear power plants with fault-tolerant, computer-based controls.

Computers in the loop

In the past, most designers resisted using computer-based control systems in critical control loops because the computers simply weren't reliable enough. Now, however, the highly reliable design techniques developed for aerospace applications greatly reduce that problem. Further, industrial disasters, such as explosions or fires in refineries or chemical plants, underscore the utility of fault-tolerant backup computers in emergencies that a human operator can't cope with.

In fact, even lower-risk applications benefit from fault-tolerant and fail-safe design. Tandem Computers (Cupertino, CA) has offered its highly reliable NonStop minicomputers for many years. The machines find use in such applications as transaction-processing systems (computers that process the information from automatic tellers, for instance), in which the financial institutions often determine that it's less expensive to pay for a very reliable system than it is to re-enter data lost because of a computer failure.

Reliability is cheap enough for μCs

Fail-Safe Technology Corp believes that microcomputer-based applications can also benefit from highly reliable design techniques. The company will start shipping its FS-66 series of 80286- and 80386-based, fault-tolerant, PC-compatible computers later this year. Each FS-66 incorporates two μPs and an ASIC that monitors the operation of both processors. If one processing subsystem should fail, the ASIC switches operations over to the second μP.

Fail-Safe claims that the FS-66 computers will provide 99.99% uptime and an MTBF of three years, yet will cost about the same as equivalent PCs from IBM.

Fail-Safe says that its machines will find use in critical data-processing equipment such as file servers, where the loss of one machine could stall or lose data from several tasks. In fact, NASA has expressed interest in using FS-66 computers to control experiments aboard the space shuttle, where a computer failure could destroy a multimillion-dollar experiment. Fail-Safe Technology also plans to incorporate the FS-66 technology in a single-board computer for embedded applications.

Many of the systems designed over the next decade will borrow freely from the fault-tolerant design techniques developed for space. Because of the greater number of electronic systems on Earth, because so many Earth systems need fault tolerance, and because technology of the 90s will make fault tolerance much less expensive to build into systems, you can expect designers of earthbound systems to take over the lead from aerospace designers in creating such rugged systems during the 1990s, further driving system engineers to adopt fault-tolerant design universally.

You can employ fault tolerance today

The tools and technologies needed to create highly reliable electronic systems are appearing rapidly. Soaring IC integration levels, for instance, are helping to make redundant design easier than ever for engineers who can wield the proper design techniques. And system-level CAD tools can simulate the performance of alternative designs; thus, you can iteratively improve a design to create the optimal solution. By rapidly creating software simulations of a prototypical system and testing them in simulated environments, you can find and eradicate many flaws before they creep into your hardware. Simulation also allows you to pit your designs against situations that could be very difficult or impossible to create in a physical test, but that could occur in the systems' target environment.

Testability is another key to reliable design: It lets you quickly verify prototype systems and thoroughly test freshly manufactured systems, ensuring that they contain no hidden flaws. Gigascale levels of integration make vast quantities of transistors available to designers so they can dedicate enough circuitry to test and maintenance functions. Built-in-test circuits will help functioning systems diagnose and perhaps even repair themselves before critical failures occur.

Finally, advanced packaging technologies such as SMT and TAB will help you create the very compact, lightweight systems that many future applications will require. These improved technologies will also boost intrinsic system reliability by reducing the number of interconnections in a typical system and increasing the reliability of the remaining connections.

Whether they're destined for space or for terrestrial applications, electronic systems of the 1990s will be more reliable than today's designs. Many of your customers already perceive reliability as a key differentiating factor when making purchase decisions, and that attitude will become more prevalent in the future. In fact, applications involving life-or-death situations—and applications where errors are extremely costly—absolutely require highly reliable, fault-tolerant designs. In any case, reliability will be a big selling point for almost any type of system in the next decade. The companies that recognize and act promptly to satisfy these needs will become the leading system designers of the 1990s. **EDN**

References

1. Carassa, F, Broglio, L, et al, *Quest for Space*, Crescent Books, New York, 1986.
2. Dawes, W R Jr, *IEEE Nuclear and Space Radiation Effects Conference Short Course*, July 27, 1987.
3. Stine, Harry G and Wilfred C Smith, "Laughing all the way to orbit," *Analog*, February, 1988, pg 68.

Article Interest Quotient (Circle One)
High 497 Medium 498 Low 499