

**Use of FPGAs in  
Critical Space Flight Applications—  
A Hard Lesson**

Wally Gibbons  
WIRE Lead Electrical Engineer  
Research Engineer  
Space Dynamics Laboratory  
Utah State University

Harry Ames  
Director, Programs Division  
Space Dynamics Laboratory  
Utah State University

## Abstract

In early March of 1999, the NASA Wide Field Infrared Explorer (WIRE) experiment was launched on a Pegasus air launch vehicle from a location in the Pacific Ocean just west of Vandenberg Air Force Base. The launch itself was successful, but a system anomaly prematurely opened the aperture cover of the telescope. This premature opening resulted in excessive venting of gaseous hydrogen from the WIRE instrument. The escaping gas increased the torque rates to the spacecraft to such an extent that the spacecraft could not control them. All the solid-hydrogen cryogen in the instrument was vented within a few hours rather than within the projected four months of nominal mission life. Days after the anomaly, the spacecraft was stabilized, and it is currently being used as an attitude control test vehicle by its builder, Goddard Space Flight Center (GSFC).

Three pyrotechnically released separation nut and bolt assemblies retained the door. The circuitry that drives these assemblies was designed, fabricated, and tested by the Utah State University Space Dynamics Laboratory (SDL). A principal element of the circuitry is the Actel 1020 field-programmable gate array (FPGA). SDL and other government subcontractors have used this device successfully in space applications over a period of years. Because of the past success with this product, SDL chose to use it to provide logic functions to control the deployment of the WIRE instrument aperture cover. The premature release of the cover has been directly traced to the use of this part in a circuit architecture for which it was not well suited. A power-up idiosyncrasy allows a period of a few milliseconds during which the part has indeterminate states on its output devices.

The Actel 1020 FPGA has seen extensive use in electronics hardware throughout the aerospace industry. The 1020 device was an integral part of the telemetry and housekeeping hardware for the SPIRIT III instrument, which was flown on the MSX (Midcourse Space Experiment) satellite. It was also used in the data compression hardware for the same sensor system. The ground station data decompression hardware, telemetry decoders, etc., also used the same 1020 device. Indeed, because of the logic density, power consumption, radiation tolerance, and performance of this part (and others like it), it has become an indispensable part of spacecraft hardware throughout the aerospace industry. Jet Propulsion Laboratory (JPL) and GSFC have both successfully built, tested, and flown hardware using Actel FPGA devices.

## WIRE Pyro Release Architecture

The WIRE cryostat has four pyrotechnic mechanisms (one on a vent, three on the cover) that need to be fired to properly configure the cryostat for operation in space at the design temperatures. Releasing the cover requires the firing of six initiators on three bolt-release mechanisms. Two initiators fire to open the cryostat secondary vent, while wax actuators are used to open the primary vent hardware. A detailed study was made of two types of firing circuitry that could accomplish the task. Energy storage was evaluated (slow-charged capacitor banks to reduce battery and power system peak loading), as was direct battery power. GSFC studied the spacecraft power system in detail because the firing of the cover imposes a load of 36 amps (typical) on the 9-amp-hour spacecraft battery and wiring harness. GSFC selected the direct-fire method, a firing system that must be integrated carefully into a satellite design to avoid ground loops and to ensure that damage to the spacecraft power system does not occur.

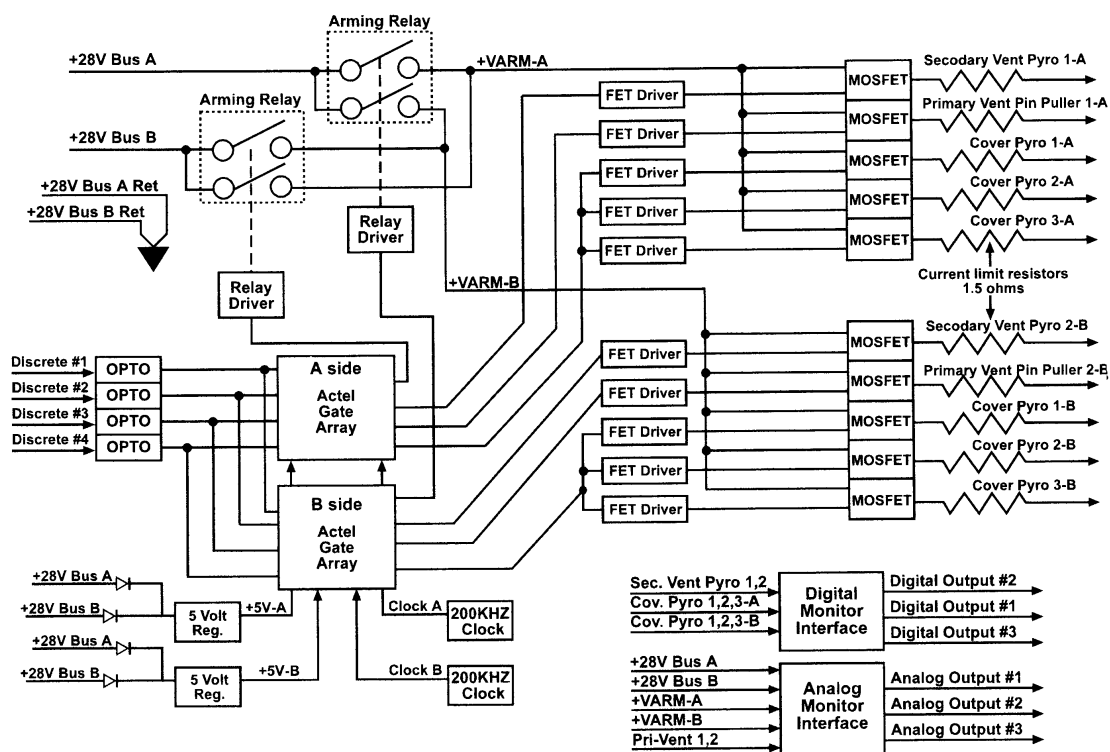
**Spacecraft System Design.** The pyrotechnic box is wired to the SPE (spacecraft power electronics) using two power source buses (A and B) and matching returns. Each is composed of three individual wires. All high-current firing pulses go through these lines. The returns tie directly to the spacecraft battery. Two low-level returns, which carry the pyro box logic and relay currents, return to the SPE through the essential bus current monitor. There is a pair of connections out of the pyro box for each initiator. The wiring harness goes to the arming connector on the spacecraft access panel and then to an interface connector near the WIE (WIRE instrument electronics) box. At this point, SDL's cryostat harness connects to the pyro harness for connection to the initiators on the cryostat itself. The returns of each initiator are wired so that during any one firing event, each initiator has an individual return wire that goes back to the spacecraft battery. No two initiators share a return when they are being fired, and no other connections are made to any pyro initiator returns. Sufficient resistance is included in series with each initiator to limit the fire pulse to 6 amps at a nominal bus voltage of 28 volts. All wiring to the initiators is composed of twisted shielded pairs, and all connectors use backshells. The wire size used was the result of trades between thermal conductivity and electrical conductivity. The mechanisms used for the primary vent, secondary vent, and cover have two initiators each (two heaters for the primary vent wax actuator), which gives the system a level of redundancy from the power bus to the mechanisms.

The command signals to the pyro box come from the SCS (spacecraft computer system) as digital-discrete commands. The command interface is optically isolated inside the pyro box. Three digital-discrete monitors (optically isolated in the SCS) and three analog voltage monitors are fed back to the SCS to monitor pyro box operation.

**Command Operations.** Three events must occur to fire any initiator in the WIRE pyro system. First, the spacecraft power electronics must be commanded to power on the pyro box buses. Second, an arm-discrete command must be sent to the pyro box. This initiates a 10-second window in which the third event must occur: a fire-discrete command must be received to fire a specific set of initiators. The resultant fire pulse is 100 milliseconds long.

The primary vent opens by means of a wax actuator mechanism. To handle that case, the 10-second armed window can be restarted if the SCS de-asserts and then re-asserts the armed-discrete command. A specific SCS software routine is started to accomplish this for the primary vent open command operation. The specific primary vent command discrete is also asserted, supplying 28 volts to the heater on the wax actuator (the 100-millisecond output enable is bypassed on the primary vent output). A temperature monitor on the actuator mechanism and a micro-switch on the vent door are monitored by the SCS so that power can be removed from the heater and the armed status can time out and stop.

**WIRE Pyro Box Design.** The pyro box was designed with the intent of maximizing the initiator fire reliability while keeping the design light weight (see Figure 1).



**Figure 1. WIRE Pyro Box Block Diagram**

The SDL team thought it necessary to use a small amount of digital timing logic to control the firing operations. Therefore, the 1020 FPGA was selected for its availability (existing stock), low power consumption, radiation tolerance (a desirable feature in a pyro-firing circuit), and flight heritage on other programs. Having the firing signals directly controlled by the SCS was considered but rejected because of operating system and software complexities—multi-tasking, interrupts, etc.—that made it difficult to ensure there would be accurate timing loops for accomplishing firing pulses and arming pulses. In hindsight, it appears that it was unrealistic to expect accurate control. There were, however, limited monitoring resources and SCS sample

rates, and therefore some monitoring circuits were desirable to ensure adequate verification of the correct operation.

In keeping with the redundant power input bus, redundant logic blocks, arming relays, and power FETs were used in the design. Relays were used for arming. The team selected non-latching relays so the system could not “hang” in a high-current state. The outputs of the arming relays were cross-strapped to allow the system to work if only one of the input power buses was functional. Two separate logic blocks, with separate power supplies and clock oscillators, were included, maximizing the odds of accomplishing the fire events.

Power FETs were used for switching the voltage to the initiators, with the logic providing the drive voltage to the FETs. The FETs were radiation hardened to  $1 \times 10^5$  rads (Si), single-event-burnout hardened, single-event gate-rupture hardened, gamma-dot (flash x-ray) hardened, neutron tolerant, and specified for repetitive avalanche operation. They were rated for a  $BV_{dss}$  of 100 volts and an  $I_d$  of 21 amperes.

The relays were rated for 25 amps continuous operation and were capable of switching transient currents of 50 amps for 5 seconds.

The discrete command inputs were glitch filtered by sampling them at a 1-millisecond rate. Two successive samples of a discrete input must match before the logic accepts it. Glitches on the discrete inputs of less than 1 millisecond were therefore ignored.

The monitor portion of the design is intended to show that the pyro box has received input power and that the relays have closed, thus creating the armed condition. This was accomplished by using simple voltage dividers with the outputs fed back to the SCS for monitoring by means of two of the analog monitors. The third analog monitor monitors the primary vent output and asserts when either of the primary vent actuator outputs is active. All pyro box actuator outputs are monitored by a simple threshold detector that switches if any output exceeded approximately 13 volts for a period of time longer than ~500 microseconds. Because the primary vent heater is on for a time period of one to two minutes, the 5-second sample rate of the SCS is adequate to reliably capture the monitor status. This is not true for the secondary vent or cover fire pulses. They are of relatively short duration and probably would be missed by the SCS monitor electronics. Therefore, for the secondary vent, the threshold detector output was latched in logic and could only be cleared by power cycling the pyro box. This monitor asserts if either of the secondary vent outputs asserts. For the cover, slightly more logic was used, but the latching function was retained. To assert the cover monitor, the three cover initiator outputs must assert. They can be either A or B, but three must assert. Each Actel has a separate cover monitor output that is fed to the SCS.

### **WIRE Pyro Box Hardware Testing**

The pyro box was subjected to the standard electronics hardware tests, which included vibration in three axes, thermal-vacuum temperature cycling, and EMC/EMI testing. These tests are well documented and are typical of the kinds of testing space-level hardware undergoes for space

qualification. These tests will not be discussed in great detail here other than to note that at no time were spurious transient outputs ever noted.

Transient output spikes were anticipated, and, in fact, a transient output pulse was found during engineering tests. When the arm command was sent and the arming relays closed, it was found that the intrinsic capacitance in the FETs (~300 pf each) would charge through the pyro outputs. This current spike never exceeded one ampere (the specified “must not fire” threshold for the initiators), and was of very short duration. Still, its existence was considered undesirable and was brought to GSFC’s attention. GSFC, too, had seen this occur in its pyro electronics designs, and the cure it applied was to put a resistor across the arming relay to pre-charge the FET capacitance prior to the arming relay closure. Therefore, a 15K resistance was wired across the arming relay contacts on both the A- and B-side arming relays to accomplish the pre-charge. The post-modification current spike was captured and found to be at the 6-milliamp level.

An initiator/pyro box/harness test was also conducted. A set of initiators was connected to the flight pyro box with SDL’s portion of the flight harness (and a test version of GSFC’s portion of the harness), and a test fire was carried out. Again, the operation took place as expected: no spurious initiator firing was noted. The current pulses were recorded to validate the design, which indicated the firing current level attained was as expected. The reasons why this live-fire test did not reveal the anomaly are twofold. First, the test setup had been subjected to a power on and arming test without using initiators to verify the power and pyro box static-current levels. Second, a lab supply was used for the test. Even had test timing been long enough to allow the Actel to discharge completely, the glitch would still have not occurred because of the risetime of the bench supply. Further details of this behavior are detailed next.

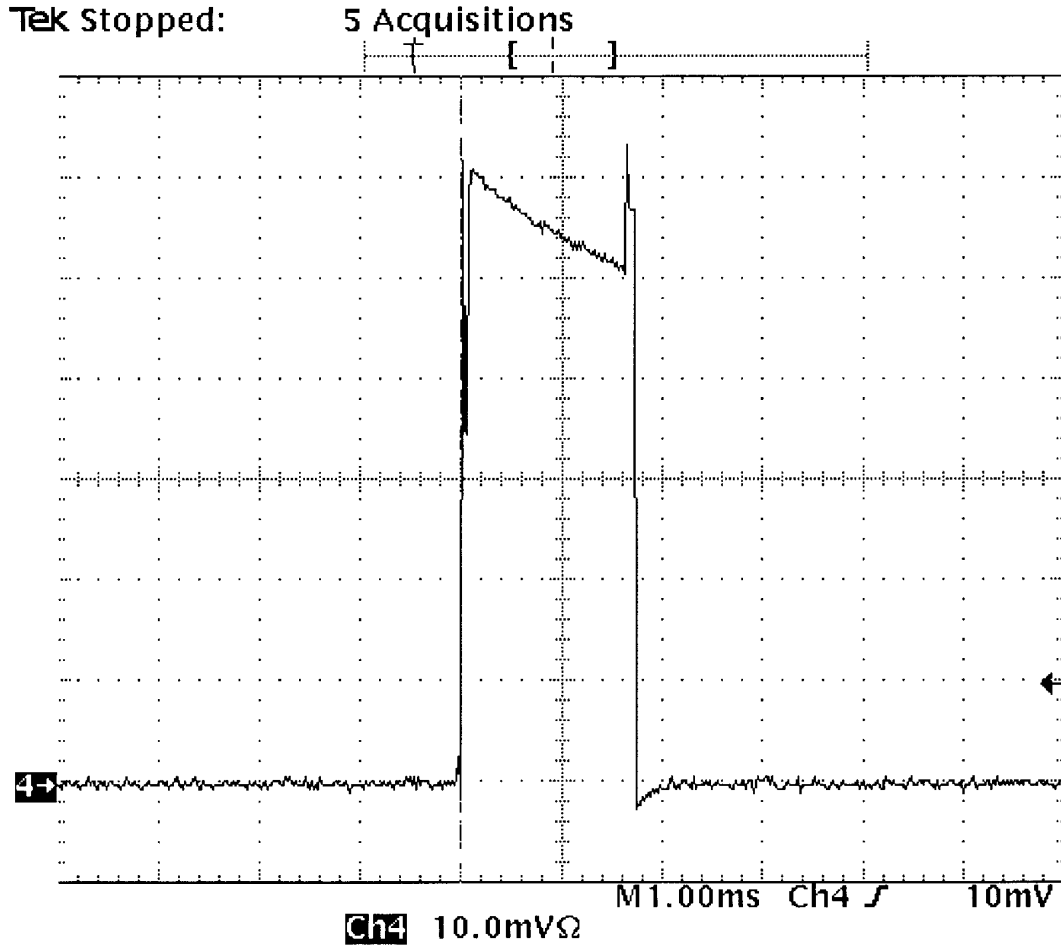
### **Pyro Box Anomaly Description**

From a timeline compiled by GSFC that covers the post-separation events through the start of spacecraft tumbling, it is fairly apparent that the cover was released from the WIRE cryostat when the pyro box was first powered on via its A-side power input.<sup>1</sup> Discussions with Richard Katz of GSFC alerted the lead author to a phenomenon exhibited by Actel gate arrays. Specifically, these integrated circuits have a built-in charge pump or DC-to-DC converter that, as the part is powering up, disconnects all the device programming circuits from the functional logic cells. During this interval, the part is completely undefined; indeed, pins that are programmed as inputs can be outputs, and output pins can (and usually do) assert. In the WIRE pyro box, this condition exists for approximately 14 milliseconds as the +5 volt supply is powering up. During this time, all outputs are asserted. This causes the arming relay to begin to close and enables all output FETs. The measured close time on the relay is 10 milliseconds. The arming relay contacts close, the FET outputs are enabled, and all initiator outputs are fired. Approximately 1.5 to 2 milliseconds later, the Actel is now operational, and the outputs assume their power-up state. The damage, however, has been done. What is interesting about this behavior is its transitory nature. The Actel will not do this again unless it is allowed to sit unpowered for at least 1.5 to 2 hours (ETU box testing result). Had this transient fire pulse been

---

<sup>1</sup> “Table 1,” *WIRE Mishap Investigation Board Report, vol. 1*, June 8, 1999, p. 17.

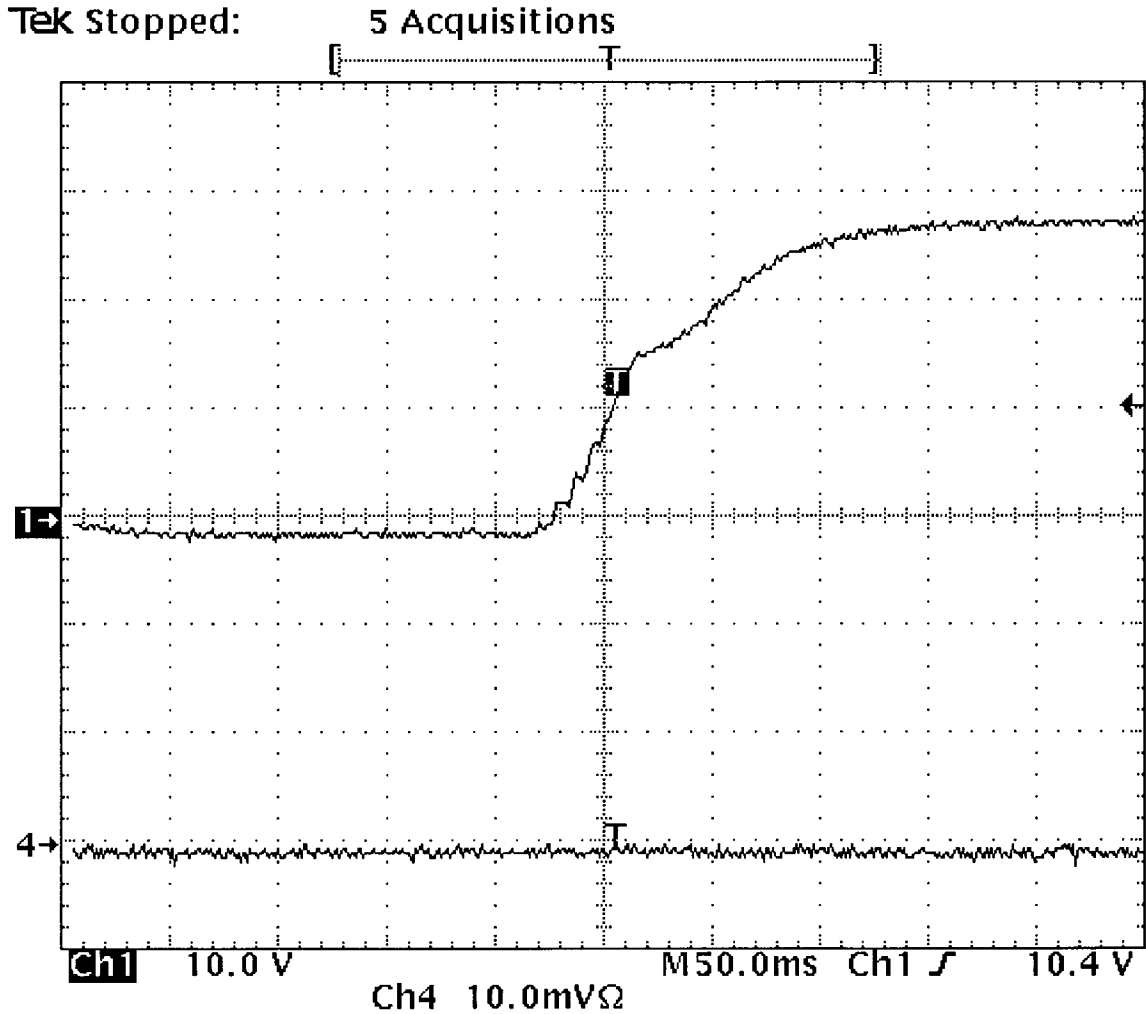
noticed and the box powered up in an attempt to repeat the event, the event would not have occurred until the discharge time of the Actel had been allowed to elapse. One of the pyro box output transient fire pulses is shown in Figure 2.



**Figure 2. Vertical Scale–1 Amp/Div, 1 Ω Load**

This spurious output pulse was never seen in testing because a power supply was used to power the hardware for testing and merely turned it on to power the system. The risetime of the 35-amp Hewlett Packard power supply is ~125 milliseconds (Figure 3). Thus, the Actel was outputting spurious signals, but the reduced power supply voltage present during the first 15 milliseconds slowed the arming relay’s attempt to close, and, in fact, it never did close.

The glitch was never seen during spacecraft hardware testing nor was it recognized for what it was because the GSFC pyro test box is *very* sensitive to spurious triggers. When it does see a trigger (such as the spurious output), it waits 23 milliseconds before applying a load to the pyro box. GSFC included the load delay to avoid stressing the relay contacts in their pyro circuits so that closing the contacts would initiate current flow. The delay avoids this by allowing the



**Figure 3. +28 Volt Power Supply Risetime**

contacts to close prior to load application. This is not a realistic test because this is not how the relays operate when actually used. The test fixture would reliably trigger every time the pyro circuits were powered up because the threshold for triggering is approximately 0.6 volts for a duration greater than 500 nanoseconds. The SMEX team had seen such spurious triggers on this pyro test hardware during the testing of two previous missions and (incorrectly) assumed the triggers SDL had seen had the same cause. Having no knowledge that something else might have happened, the team disregarded them. Thus, during spacecraft testing of the pyro electronics, no indication of trouble was ever seen because no load existed on the pyro box outputs during the transient fire pulse. The glitch disappeared long before the 23-millisecond delay; therefore, no current was drawn from the spacecraft power system, and nothing showed on the strip chart recorder monitoring the spacecraft power electronics.

On orbit, the pyro electronics were switched on, and because the Actel had been unpowered for weeks, it was ready to output a spurious pulse. The pyro electronics output a pulse of approximately 1.5 milliseconds, and all initiators fired.

## Critical Function Architectures—How to Improve Them

In hindsight, it appears some unnecessary complexity was built into the pyro box design, suggesting simplicity should always be a goal. Always make an analysis of the trades (risks) in the system architecture. This analysis should consider logic families and design architectures and should address the question of whether logic designs are even required to accomplish the task. The fundamental baseline purpose in a pyro initiator firing is to run current through a loop. Is a complex logic design necessary to accomplish this? What sorts of monitors are necessary? In WIRE's case, only four discrete commands were available from the spacecraft computer and one switched, redundant power bus. At the design phase of the program, it was thought necessary to use logic to translate the discrete logic signal *edges* to fire the control signals. In reality, these discrete outputs could have controlled relays that would directly fire the initiators, thus accomplishing the same task using the spacecraft computer software timing loops to control firing timing. A variation in any timing loop of 100 milliseconds does not pose a problem, though the possibility of software crashes causing spurious pyro firings becomes a factor in the system design. Again, this means an analysis of the spacecraft as a system is necessary; the *simplest* solution that meets the system requirements is likely to be the best one.

Another system flaw in the WIRE pyro box design stems from a subtle violation of the safety-induced “three-inhibits rule” for pyro-firing circuits. WIRE indeed had three inhibits. One was a spacecraft power-switching relay; the second was a pyro box arming relay. And the third was a firing FET transistor. Two of the three inhibits (the arming relay and the FET) were controlled by one integrated circuit, in effect making them only one-inhibit deep if that one integrated circuit had a design flaw. In essence, this was a design architecture that allowed the Actel behavior to bypass two inhibits. Power should be supplied to pyro-firing logic using a different circuit than the power used to fire the initiators. This would allow any logic power-up transient behavior to occur without a possibility of spurious fire events.

### System Test Methodologies

One difficulty in finding a problem like the one that occurred on the WIRE spacecraft is that testing done at the hardware box level could not produce the transient. It is important to make sure any spacecraft hardware is *tested the way it is going to be used!* Hardware test timelines should be run that duplicate those that will be used on orbit; hardware should be used that simulates, to the greatest extent possible, the hardware on the spacecraft. This testing should be done as early as is practical. A pyro-firing system test should be done as a live initiator test.

With the advent of affordable computers and their accompanying data acquisition hardware, a fairly rigorous testing setup could be put in place to monitor a pyro-firing system. A PC-based system, coupled with interface hardware that the pyro hardware identifies as an initiator, could be connected to a spacecraft electronics system and left running during all spacecraft testing. Fairly simple software could monitor all initiator outputs for glitches, intended firing events, etc., and capture the data for analysis. Software control parameters could be set up for signal amplitude, duration, and the like that would start a data acquisition sequence. Audible alarms could be triggered to indicate that some transient has occurred. This could also be used to verify

intended fire sequences. Fuses could be used as a part of this test setup, although it is worthy of note that the transient that crippled the WIRE cryostat would *not* blow a 250-mA fuse connected to the pyro box hardware instead of an initiator.

Always perform specific test procedures that will simulate the various potential problems that can occur in pyro-firing systems. One of the known failure modes of a firing initiator is a short-to-case. Learn what the actual effects are on a pyro-firing electronics system if this occurs. Blowing actual fuses with a fire pulse is another way of simulating the sort of current transient that may occur when an initiator opens during firing. Live-fire tests, with actual initiators, are mandatory and should be done with timing parameters simulating on-orbit timing scenarios. If the pyro electronics are going to be off for a week prior to on-orbit activation, simulate that on the ground. This way, time-dependent design flaws can be exposed in a system that may not reveal themselves under more routine cyclical testing.

### **Program Design View Consideration**

The key word in design reviews is “experience.” A robust design review process should specifically target design details that are not presented during the normal critical design review (CDR) or detailed technical review (DTR). Both these reviews are valuable from a systems point of view but can be found lacking in unearthing specific design flaws. Peer review is a good attempt at addressing this issue, but for it to be meaningful, the peers must have a knowledge base applicable to the design being reviewed.

For example: the transitory power-up behavior of the Actel FPGA was not known by any design engineers who worked with the SDL team. An informal poll was taken at SDL to ask if the engineers knew about the behavior exhibited by the Actel 1020. None had heard of it. When the local field application engineer for Actel was briefed, he said he was unaware that the 1020 FPGAs exhibited that behavior, although he did know that the 1280 series parts did. Thus, a peer review of the WIRE pyro design by engineers at SDL would not have been effective in spotting this design flaw. Had a detailed peer review been held with other programmable logic array (PLA) experts in attendance, the outcome may have been entirely different. There are experts in the industry with good review capabilities, and this is a knowledge base worthy of tapping into.

During the review board’s investigation of the WIRE failure, they addressed the methods used to inform designers of this sort of design information. They discussed GIDEP alerts, but because the Actel 1020 parts were not defective, their problem is not the kind that GIDEP was set up to handle. Perhaps what is needed is an information hotline, set up on an industry-wide lessons learned web page. Katz of GSFC has developed an informal web page where he posts such information. Manufacturer web pages can be a resource, too, but the wide variation in web page content and ease of use can make this a frustrating and ineffective tool for the design engineer. Nevertheless, with the proliferation of the world-wide web, a mechanism exists, but the question remains, how to let people know about such resources?

Manufacturer data sheets could be improved in content. No mention is made in the Actual 1020 data sheets about this power-up phenomenon. Such data *are* in the data book; they are also on Actel’s web page in an application note titled, “A Power-On Reset (POR) Circuit for Actel

Devices.”<sup>2</sup> This information about power-up behavior should be on the data sheet of every part that exhibits this behavior. Engineers do review data sheets, but most do not have the time to do extensive searches of web pages or application notes whose titles do not reflect their real content. Finding relevant information about WIRE PLA is a clear example. The pyro box designer was not looking for a reset circuit because he already used a reliable and much-tested one. Therefore, Actel’s application note seemed irrelevant, and he had no reason to browse Actel’s entire web site. Engineers need clues about what information exists and where it is.

An aerospace company quality assurance representative spoke with the designer shortly after the WIRE failure review board report was issued. The responsibility of the division he represents is to watch for such information, reports, etc., and to formalize the process by sending out copies of papers and reports to its engineers, who are then mandated to verify they have received the information. This process is perhaps a bit extreme, but the company’s intent is to provide a mechanism for spreading crucial design information to the institution’s engineering teams.

This MAPLD conference (and indeed this paper) is another step in trying to provide an information base to help ensure that the widest number of people gain an understanding of the behavior of these logic integrated circuits, and not just for the Actel device. As demands for data compression, advanced data systems, and complex attitude-control functions increase and match the ability of silicon producers to provide hardware, the need for an experienced base of reviewers likewise increases.

Both authors would like to thank Gina Wickwar, SDL senior technical editor, for her contributions to this paper.

---

<sup>2</sup> “A Power On Reset (POR) Circuit for Actel Devices,” *Actel FPGA Data Book & Guide Design—1996*. Sunnyvale, CA: Actel Corporation, 1996, pp. 4-127 – 4-128.