Small Explorer

WIRE

Failure Investigation

Report

May 27, 1999.

Prepared by: Richard B.Katz
NASA Goddard Space Flight Center
Microelectronics and Signal Processing Branch

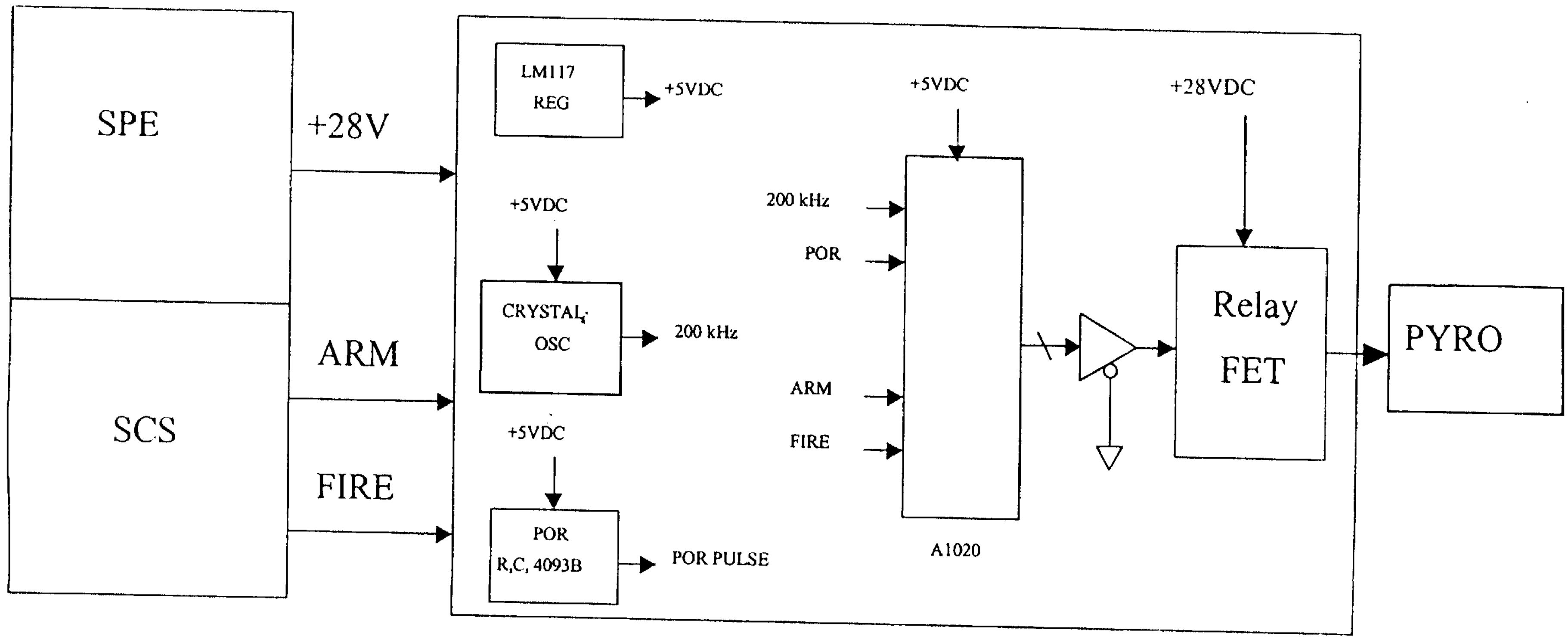


Figure 2-1 Overview of the Pyro Box and key interfaces. The Spacecraft Power Electronics (SPE) provides power via relays; the Pyro Box is launched powered off. The Spacecraft Computer System (SCS) provides two command signals for firing the cover pyrotechnic devices, called "ARM" and "FIRE" in this drawing. The pyrotechnic devices are fired when both the arming relay is closed and the FET is turned on. The pyrotechnic device will fire in approximately 1 msec with 5 amperes of current. The LM117 provides +5V regulation for local logic while the A1020 Field Programmable Gate Array (FPGA) provides logic functions.

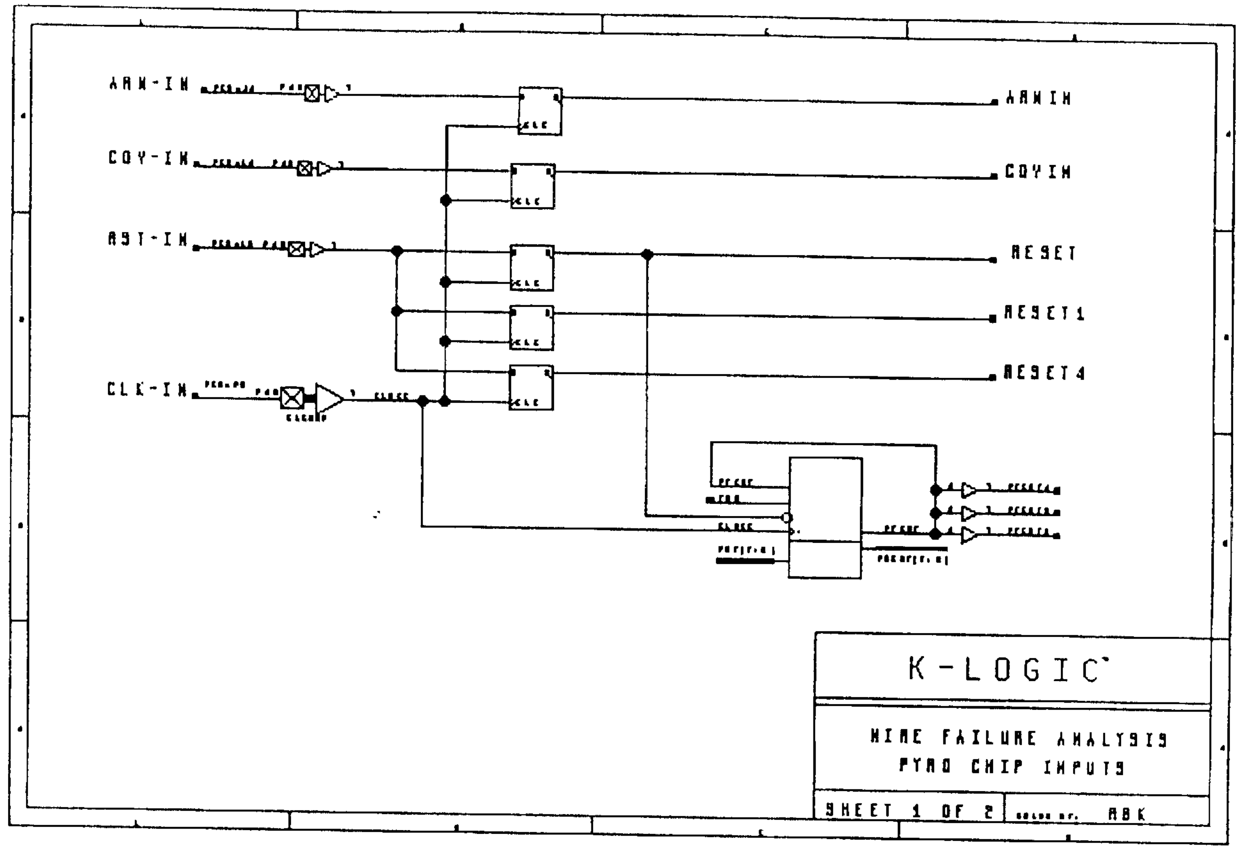


Figure 3-1 Schematic diagram of the A1020 FPGA inputs. Inputs to the device on the left side of the drawing are all synchronized by a rising edge of the clock oscillator. RESET, RESET1, and RESET4 are active low output signals on the right side of the drawing. Ideally, all three RESET signals will be driven to the low state on power-up but are not initialized since the clock oscillator is slow starting. Any one of the three RESET signals would prevent the cover pyrotechnic devices from firing.

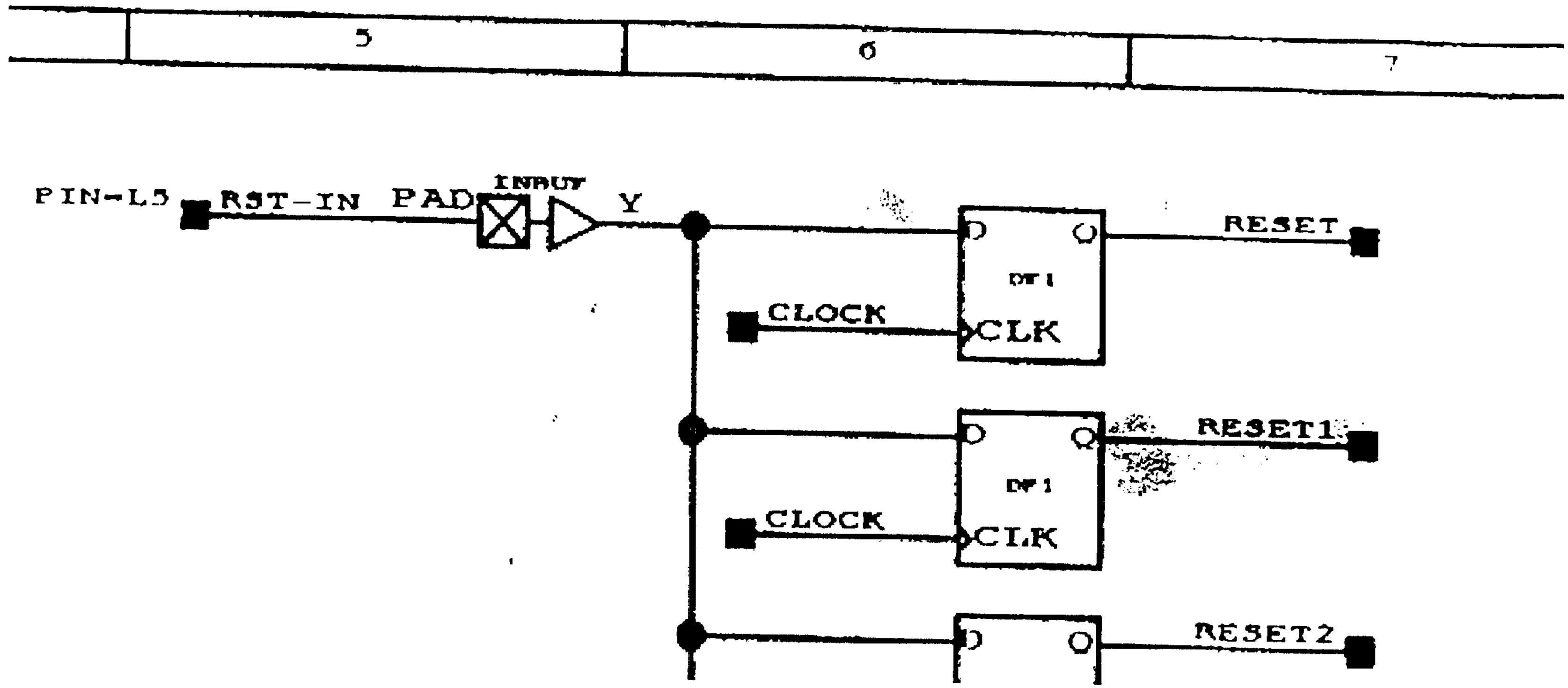


Figure 3-2 Three critical FPGA reset signals shown in detail. Each DF1 flip-flop stores one bit of data. Data is sampled at the D input of the flip-flop at the rising edge of the clock and then transferred to the output, Q. The data can only change at the rising edge of a clock.

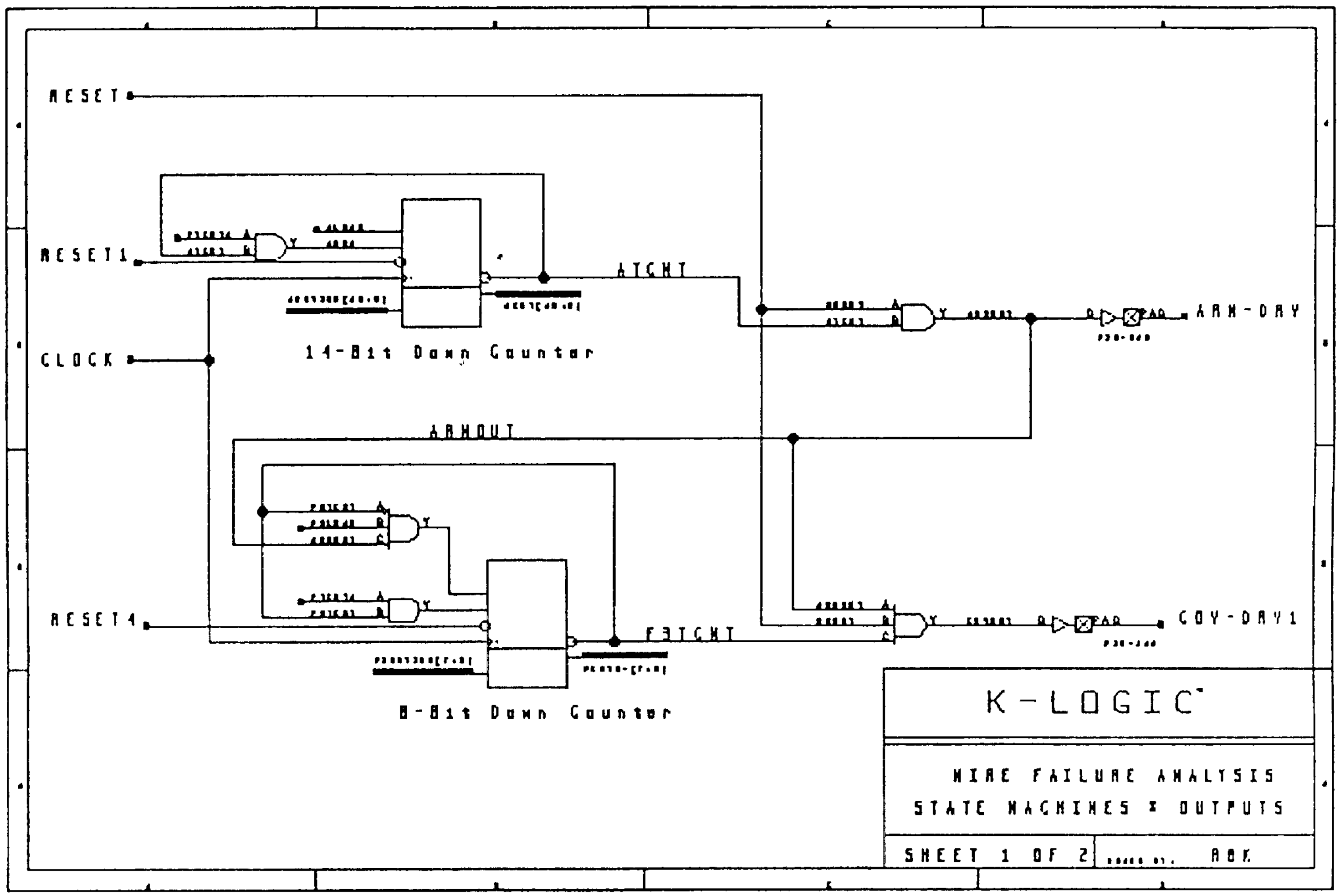


Figure 3-3 State machines for firing the cover pyrotechnic devices. The critical signals for the power-on state of the state machines are shown on the left, RESET, RESET1, RESET4, and CLOCK. The two outputs on the right control the arming relay and the FET, which switch power to the pyrotechnic devices. Each output is ANDed with RESET and a state machine terminal count. Additionally, the COV-DRV1 signal is ANDed with the arming signal.

4. 200 kHz Oscillator

4.1 Oscillator Overview

The Pyro box uses a 200 kHz crystal clock oscillator. This device is made by Vectron and the parts list (P0831-1 Rev A) calls out part number "CO-422A-2S at 200." Decoding the part number we see that the oscillator has the following characteristics:

- CMOS Outputs
- 200 kHz Frequency
- 14-Pin Dual Inline Package (DIP)
- Accuracy of ±50 ppm
- Temperature Stability of ±50 ppm
- Screening Class S
- Symmetry of 55/45 to 45/55
- Startup Time is Not Specified on the Supplied Data Sheet.

4.2 General Crystal Oscillator Startup Characteristics

It is known that crystal oscillators do not start immediately with the application of power. From Horowitz and Hill's The Art of Electronics, 2nd Edition:

> ... However, because of its high-resonant Q, a crystal oscillator cannot start up instantaneously, and an oscillator in the megahertz range typically takes 5-20 ms to start up; a 32 kHz oscillator can take up to a *second* ($Q = 10^5$). ...

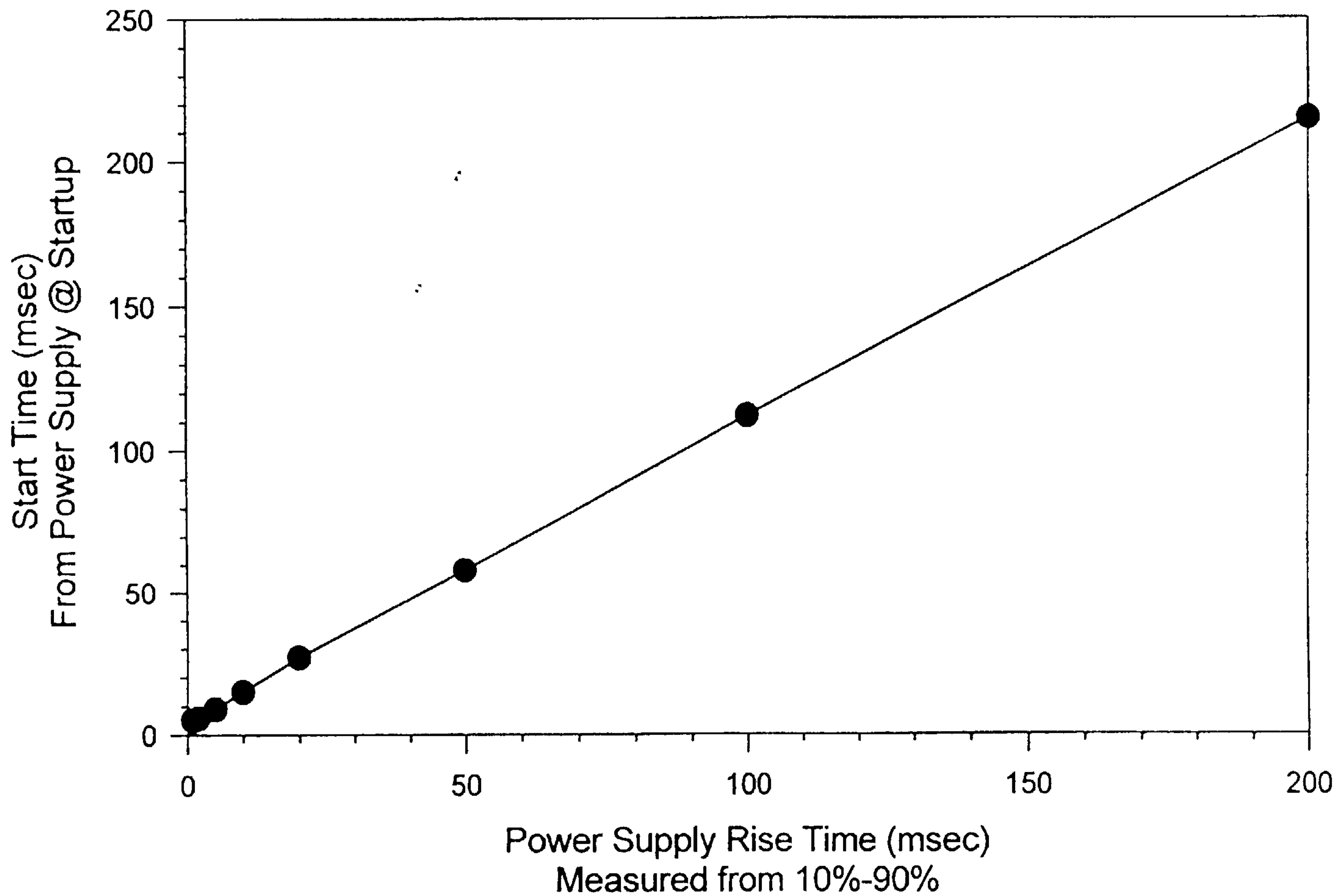


Figure 4-3 Summary of start time characteristics of a flight spare oscillator at 10 ℃. Start time is a linear function of power supply rise time using a ramp generator as the power supply.

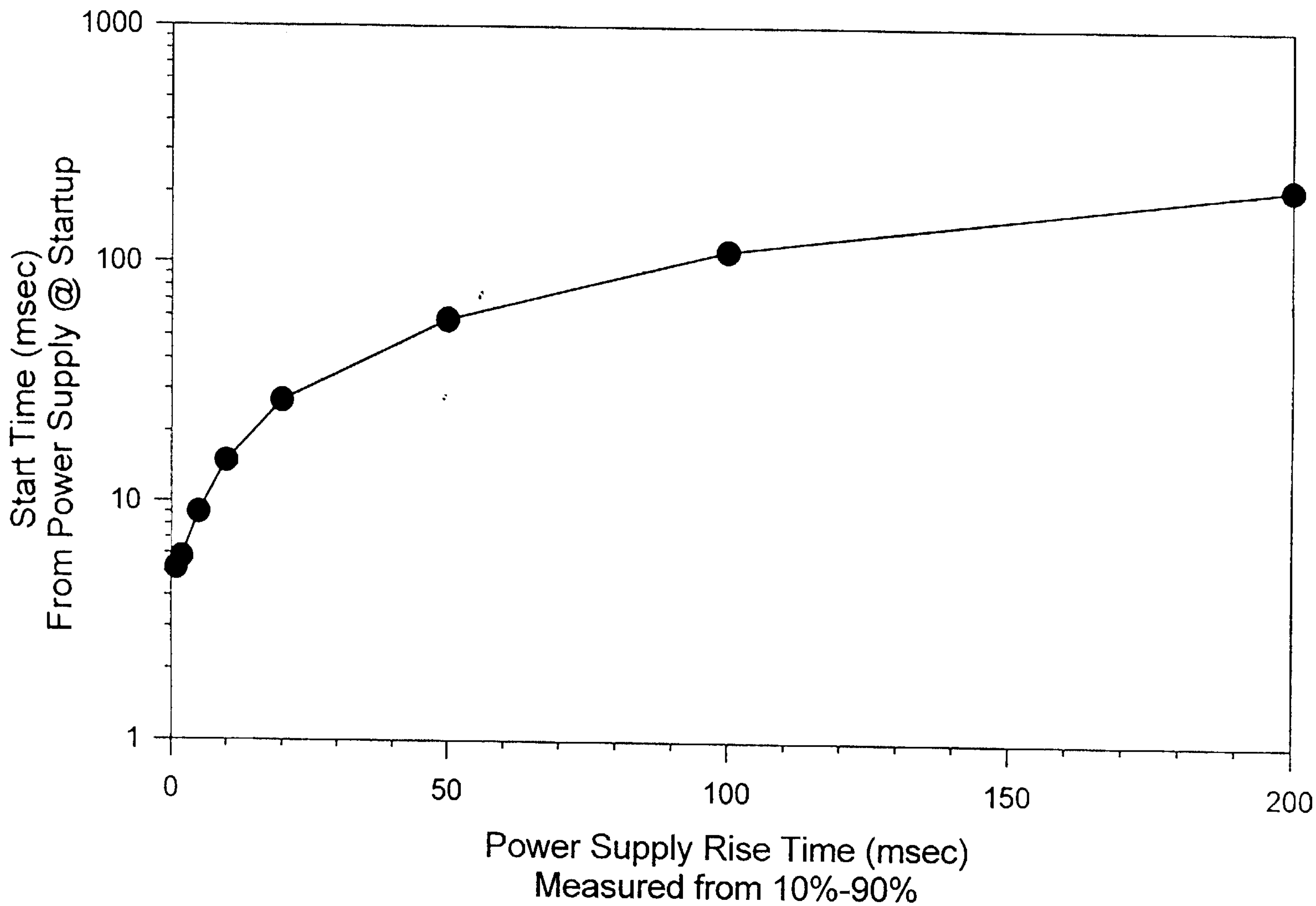
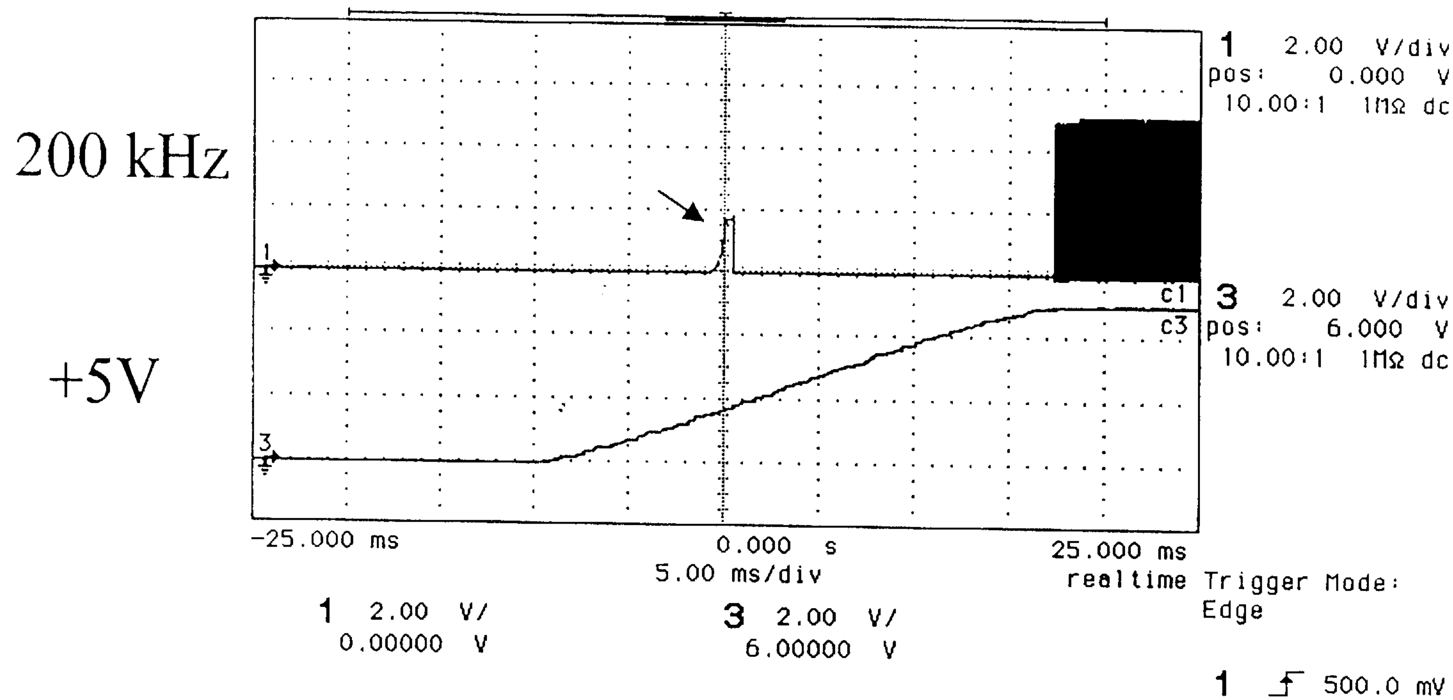


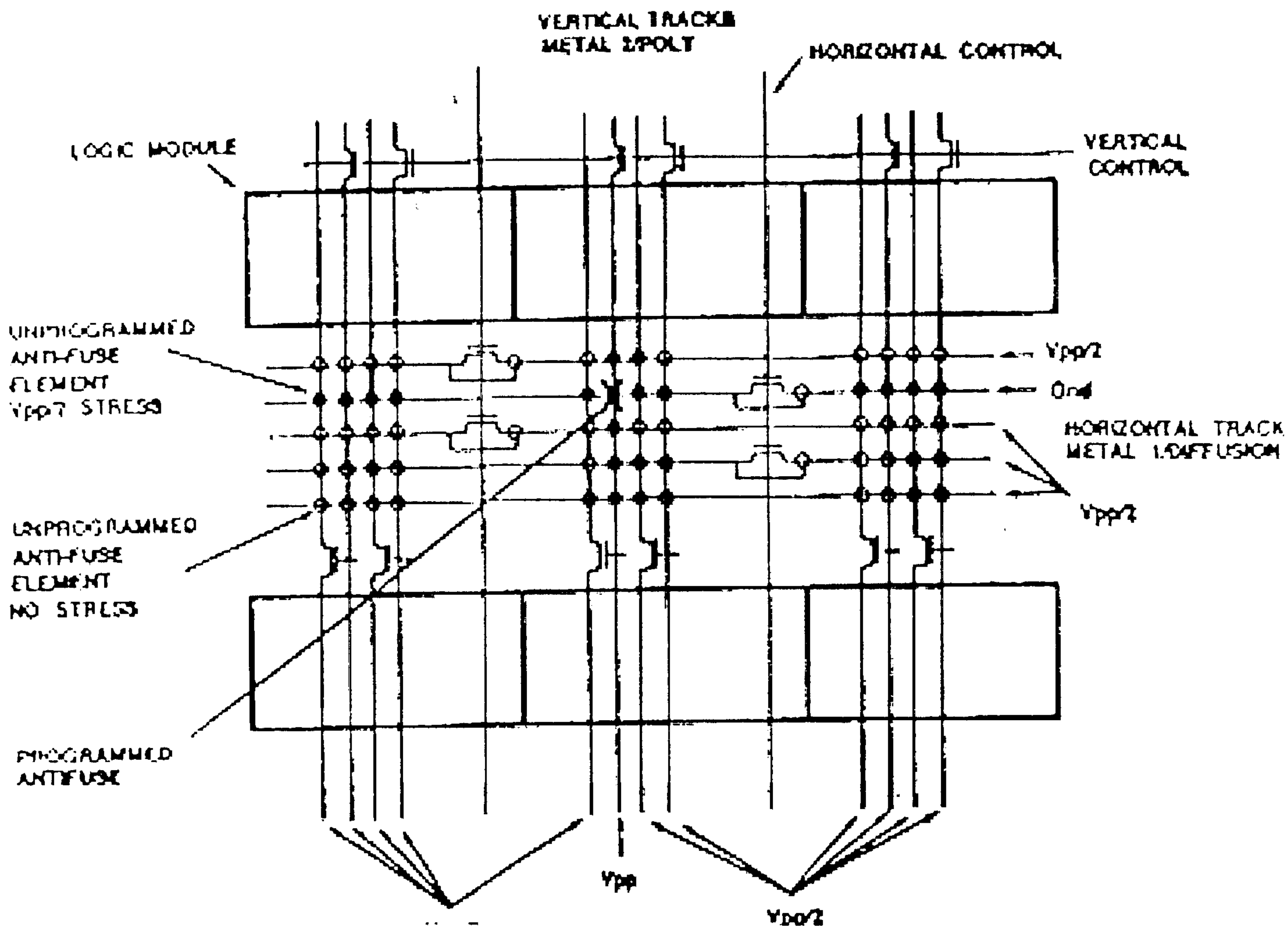
Figure 4-4 Summary of start time characteristics of a flight spare oscillator at 10℃. A logarithmic scale is used for the Y-Axis to facilitate reading of actual values for relatively small rise times.



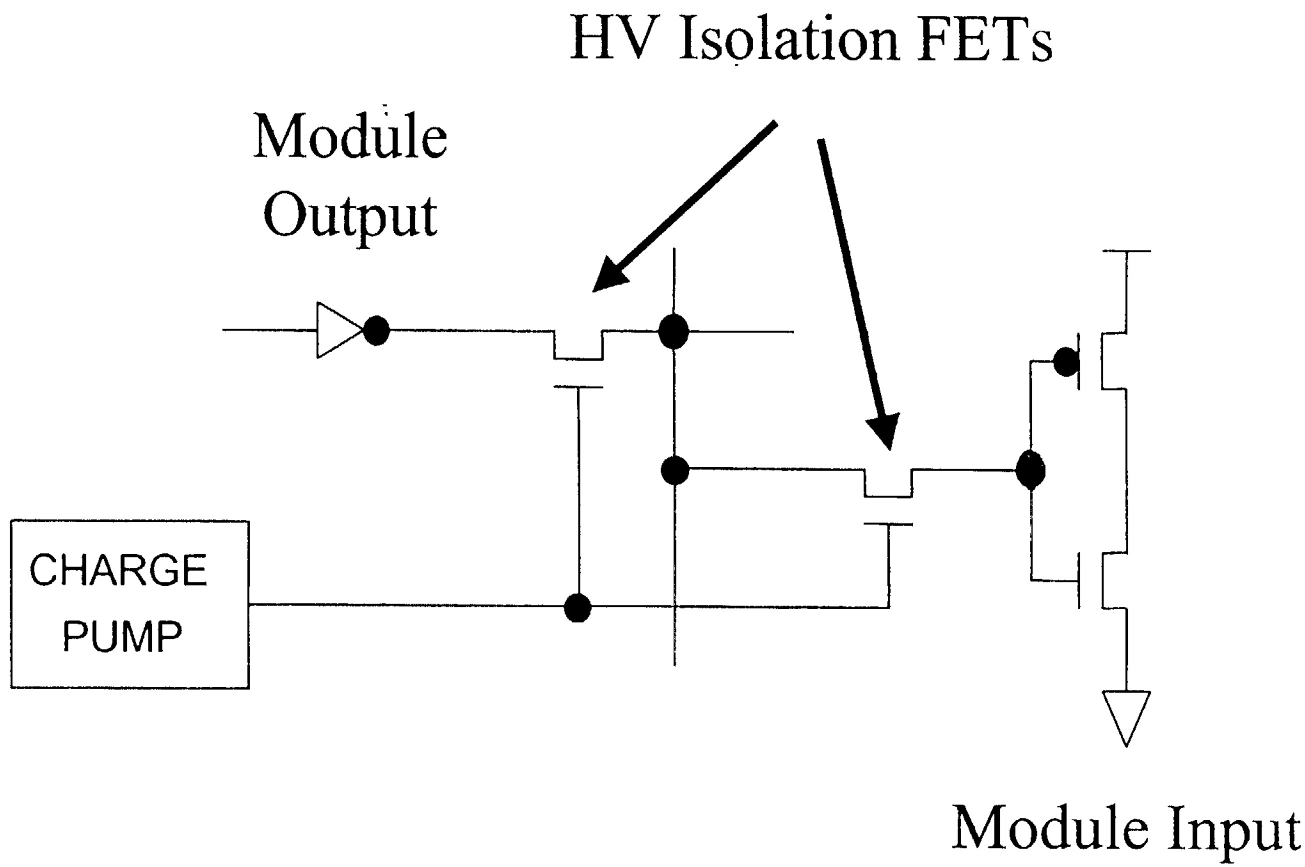
5 msec/div; $t_r = 20$ msec; $t_{start} = 14$ (27) msec

Flight Spare oscillator Testing at 10°C

Antifuse Programming



Charge Pump And Isolation FETs



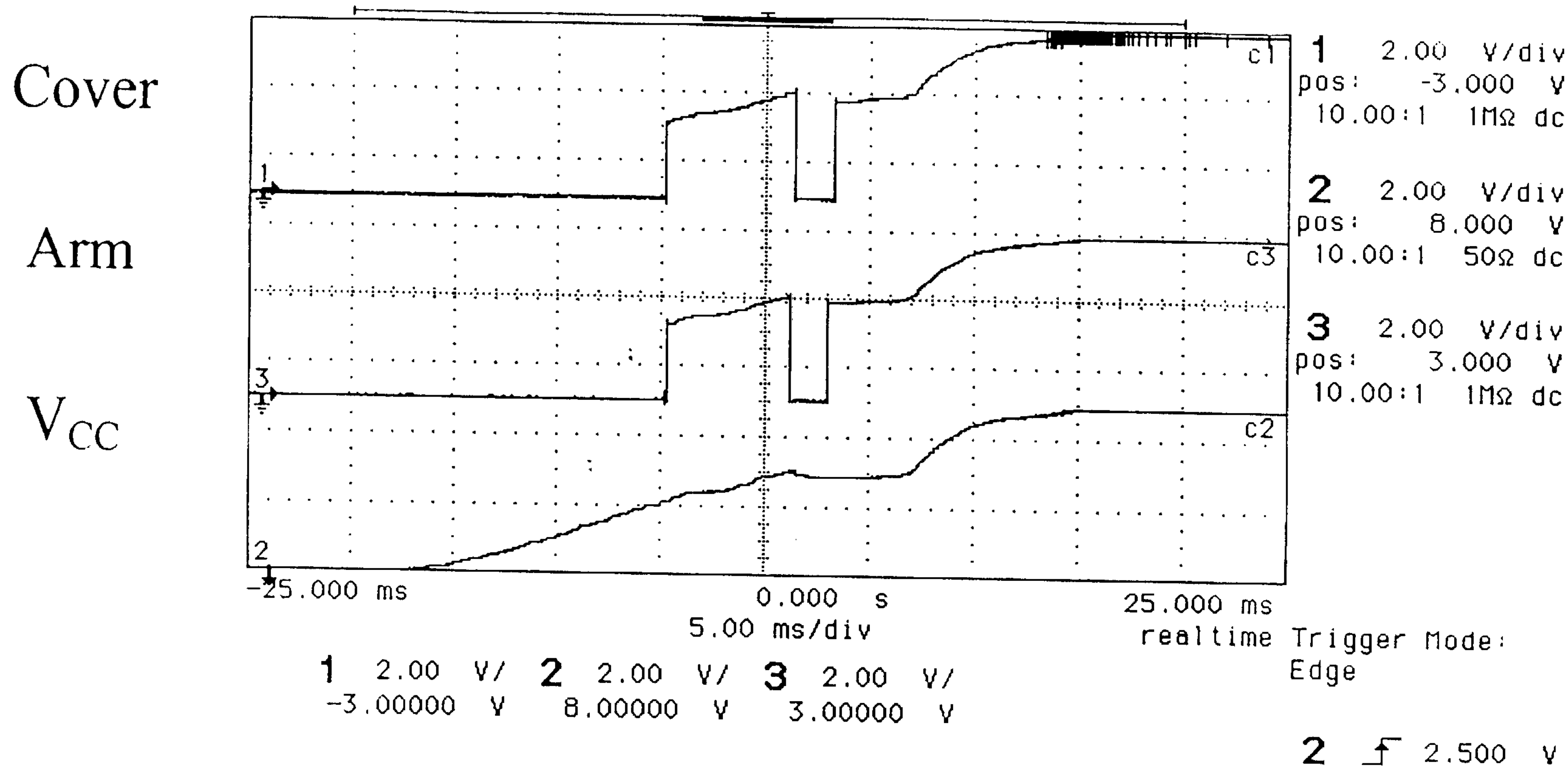


Figure 6-2 Startup characteristics of flight spare S/N 001 A1020 with a power supply rise time of 20 msec (10% to 90%) after being powered off for 24 hours. The flight unit had a power supply rise time of approximately 30 msec. Horizontal scale is 5 msec per division. Both the COVER and ARM outputs "glitched" and latched in the high state under these conditions, showing that this failure mechanism could be replicated in hardware. Flight spare S/N 002 A1020 performed similarly.

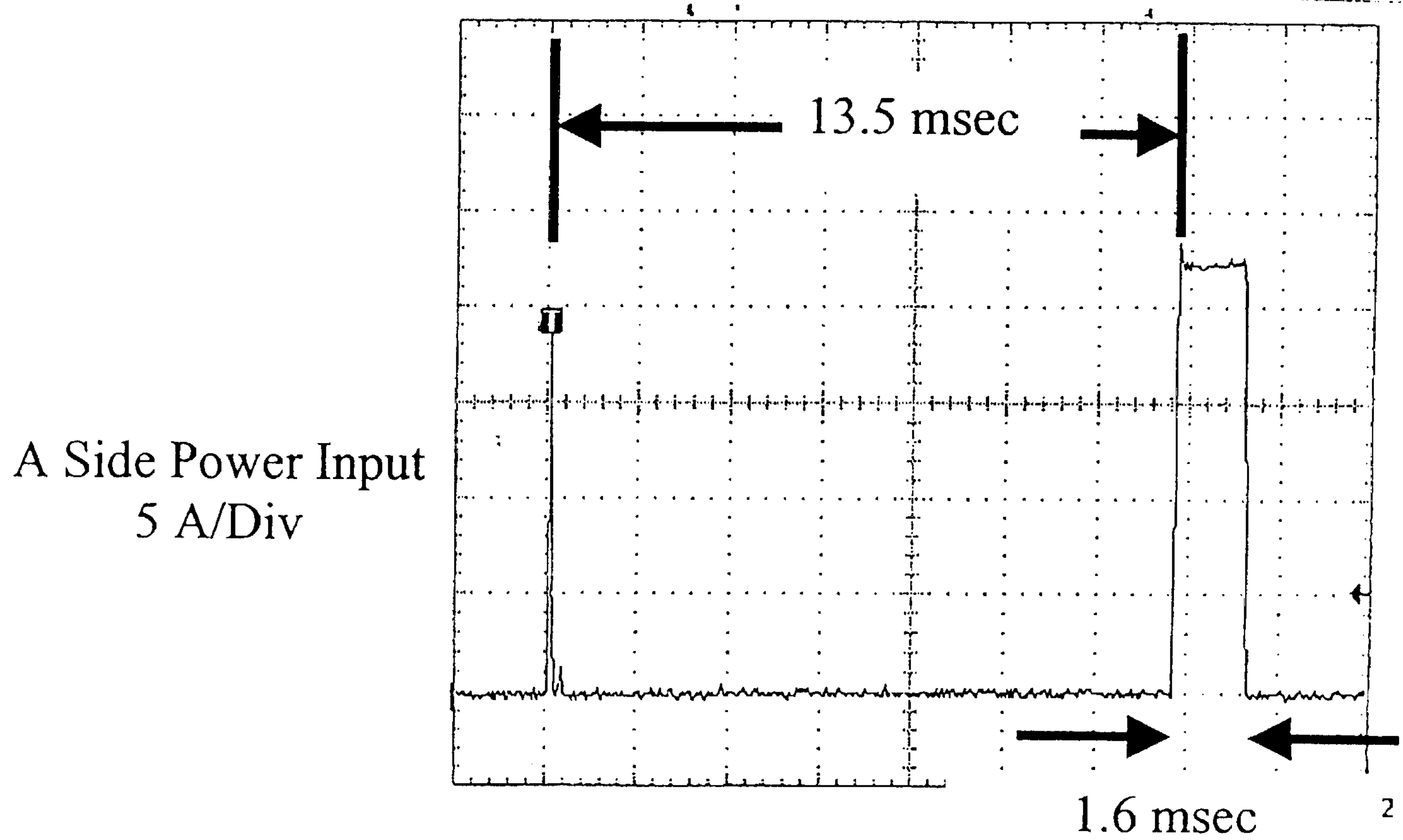
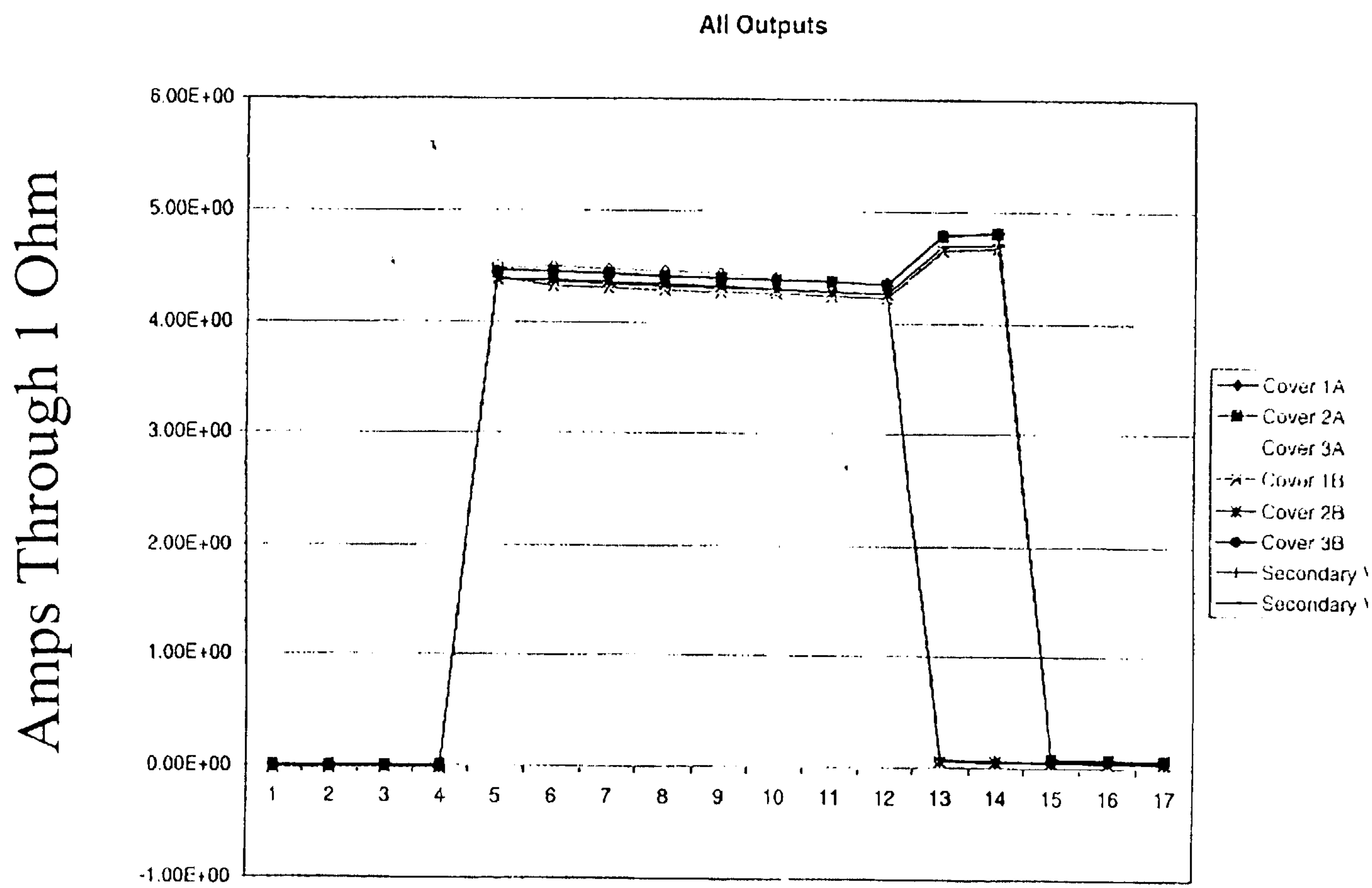


Figure 6-3 Input current of the Pyro Box Engineering Test Unit during a "cold start" where the device has been powered off for a significant amount of time. Horizontal scale is 2 msec per division. The first current spike is the box' startup current. The spike after 13.5 msec represents the pyrotechnic outputs driving a load. The second spike would not appear after 1 hour of powered off time but would appear after 1.5 hours of powered off time, showing that the memory effect was present in the failure of the ETU. The output current spike is approximately 0.8 x 2 msec = 1.6 msec. At the programmed current levels, the NSI-1 initiator will fire in approximately 1 msec.

ETU Outputs During Transient



Hor: 200 µsec/div

Courtesy of SDL

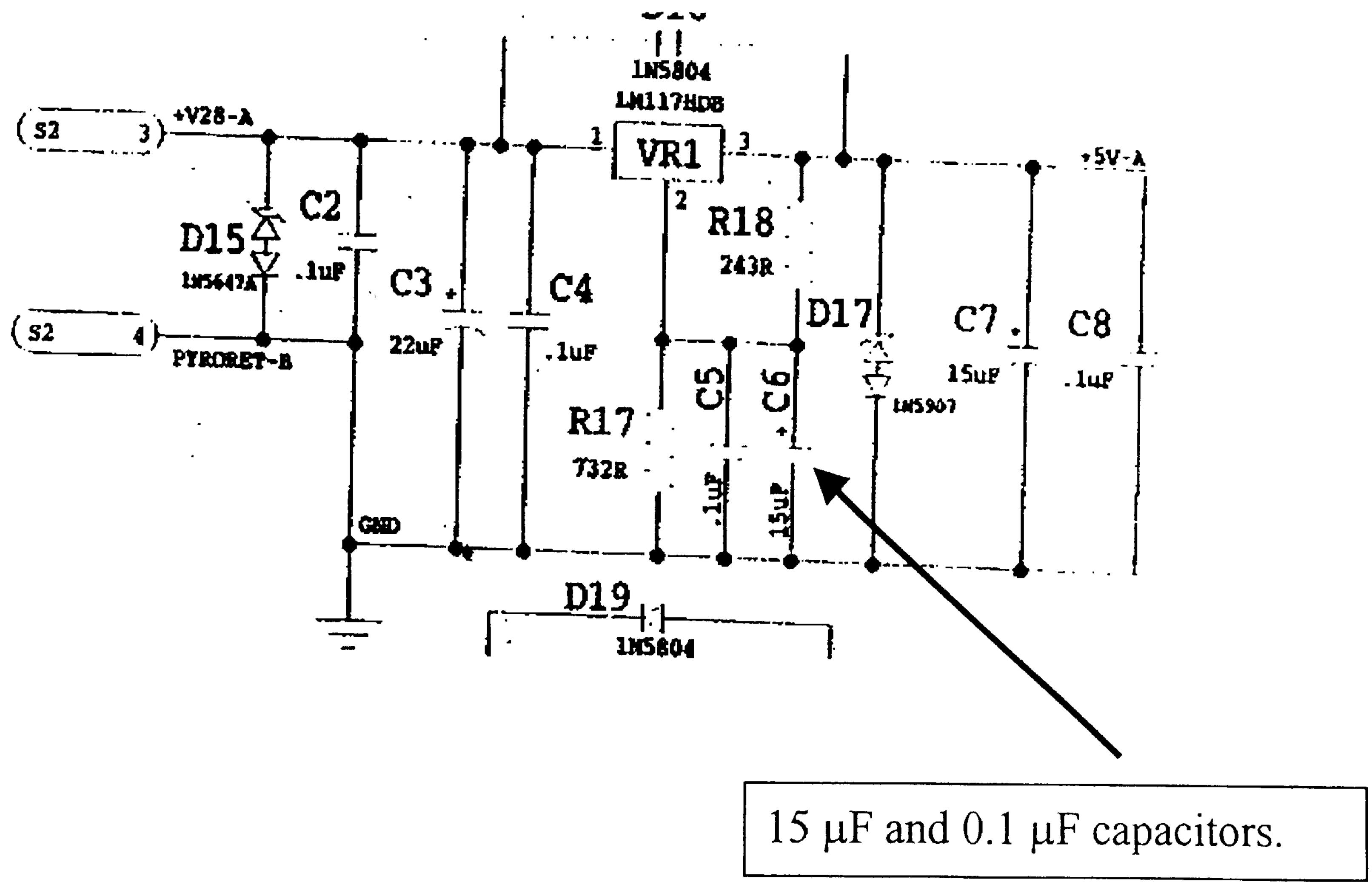


Figure 5-1 Schematic of the Pyro Box voltage regulator. This circuit uses the LM117H 3-terminal adjustable regulator. The adjustment terminal is bypassed to ground, which improves ripple rejection. It also has the effect of slowing the rise time of the output.

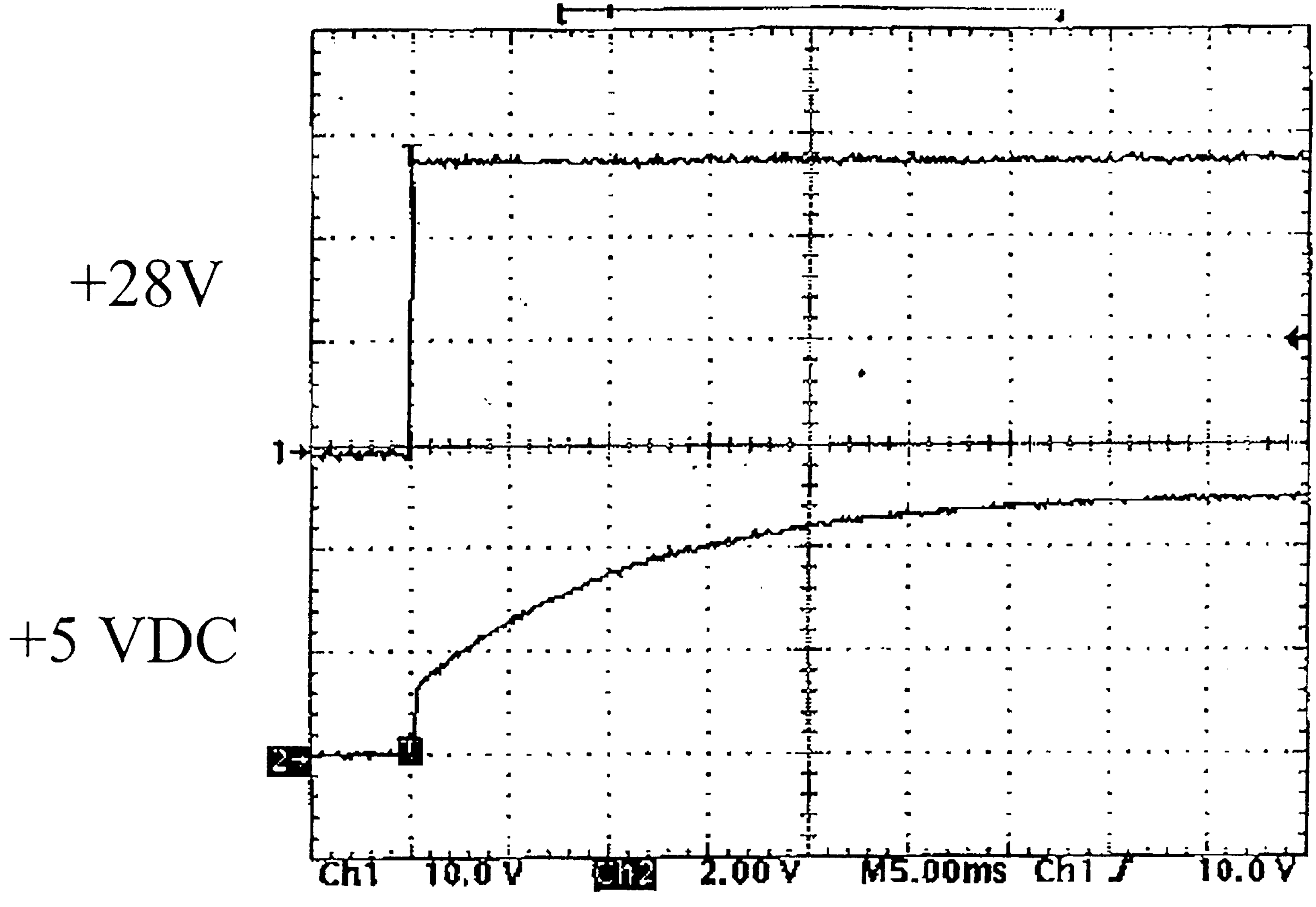
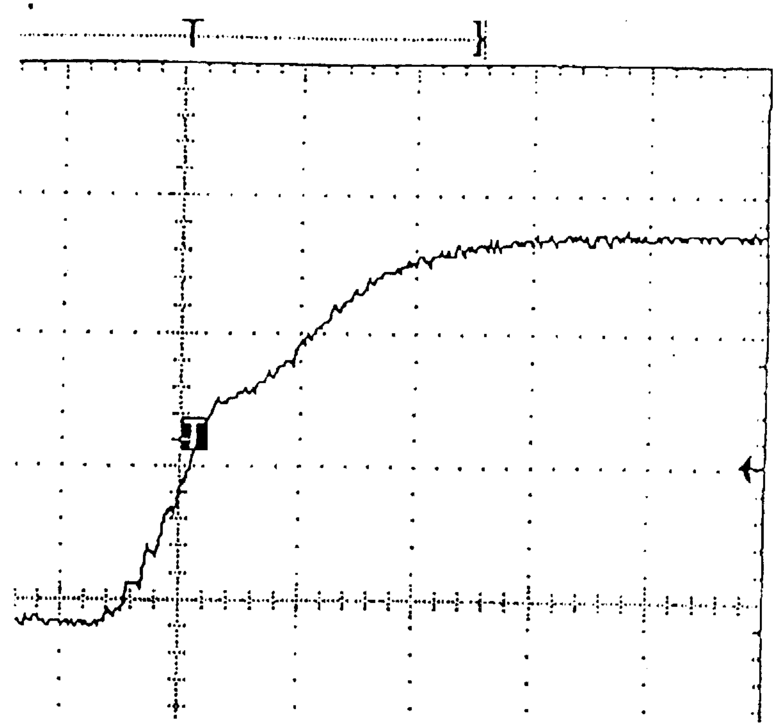


Figure 5-2 Output of the LM117H adjustable regulator on the Pyro Box Engineering Test Unit. Horizontal scale is 5 msec per division. The +5VDC voltage quickly rises to approximately 1.5 VDC then rises with a RC time constant to 5 volts. This supply takes approximately 30 msec to reach 5 volts.

+28V Bench Power
Supply
Instrument Level
Testing



50 msec / Division

Figure 7-5 Rise time characteristics of the +28 VDC power supply used for instrument level tests. The flight system's power electronics switched power to the Pyro Box with a relay, resulting in a very fast rise time. The slow rise time used in test allowed the logic to stabilize before the relay contacts could close, resulting in a false-positive test.

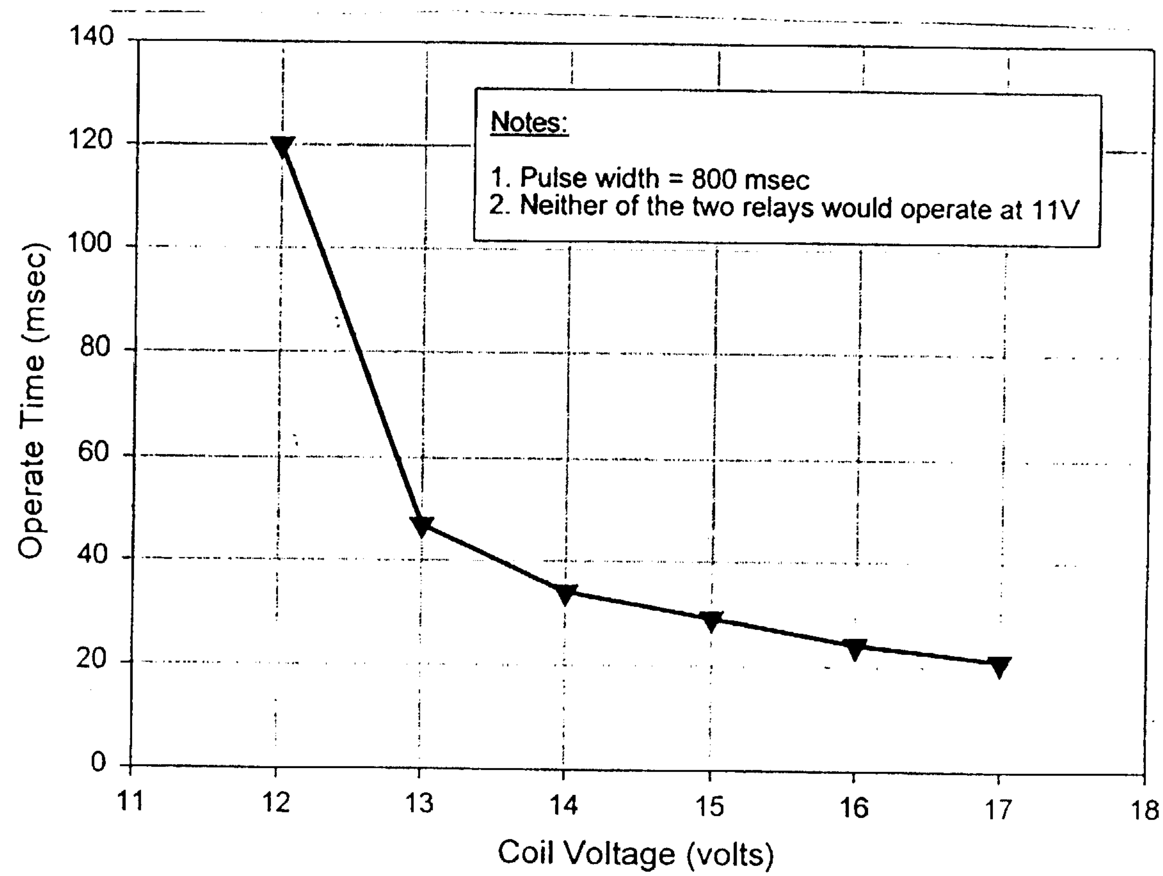


Figure 7-6. Flight spare relay operating time as a function of voltage. The relays would not close with a coil voltage of 11 VDC, giving the +5V logic circuitry time to stabilize with the slow rise time power supply used in instrument level pyrotechnic device testing.

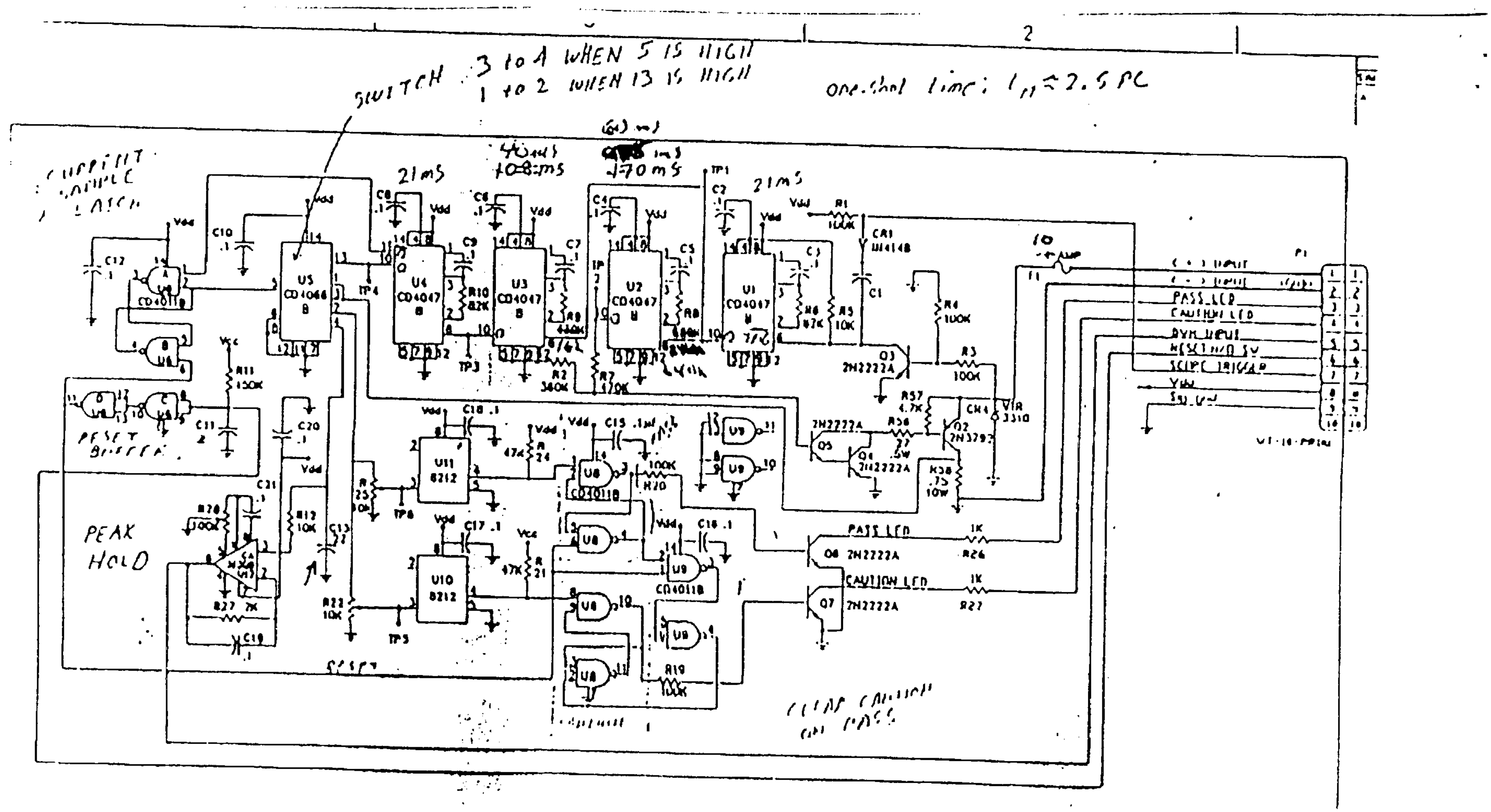
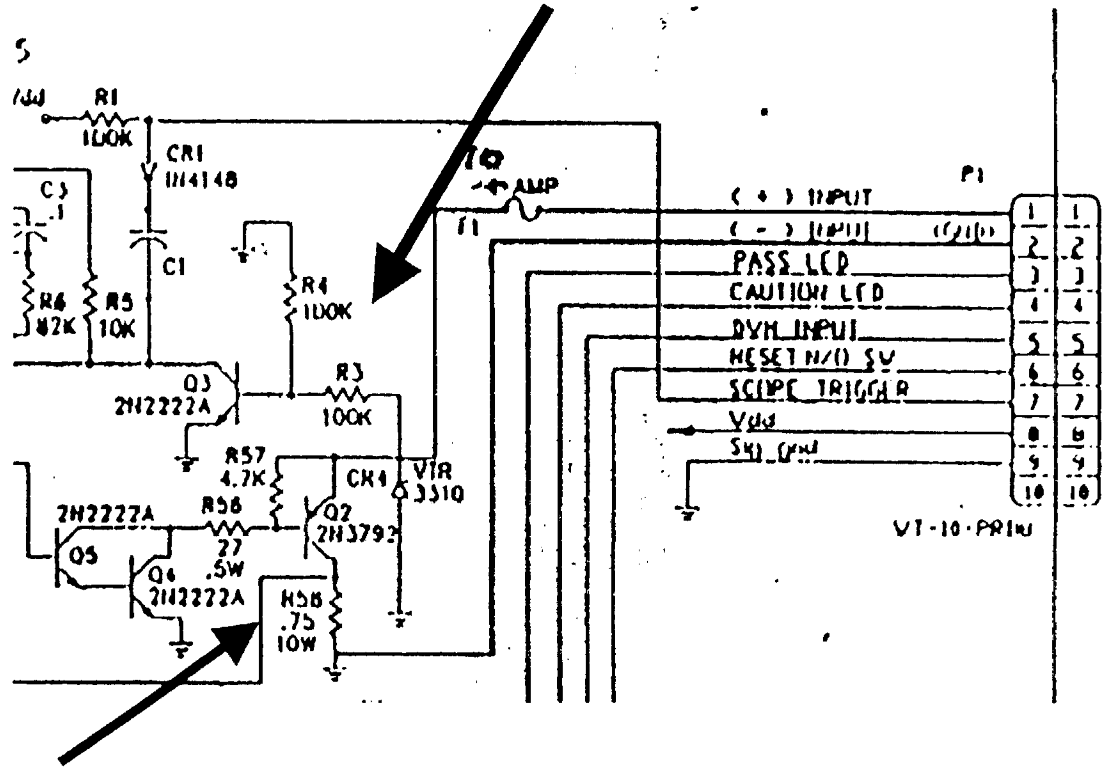


Figure 7-2. Schematic diagram of one of 10 identical circuit boards that comprise the EED Simulator electronics. Delays and windows are formed by the use of CD4047 "one-shots."

Easy To “Trip”



Low-Impedance Switched In After Delay

Figure 7-3. Close-up of the input section of the EED Simulator. The device is easily triggered and has high-impedance inputs. After a delay of over 20 msec, a load of approximately 1 Ω is switched in for approximately 60 msec. Nominal firing pulse width for WIRE was 100 msec.

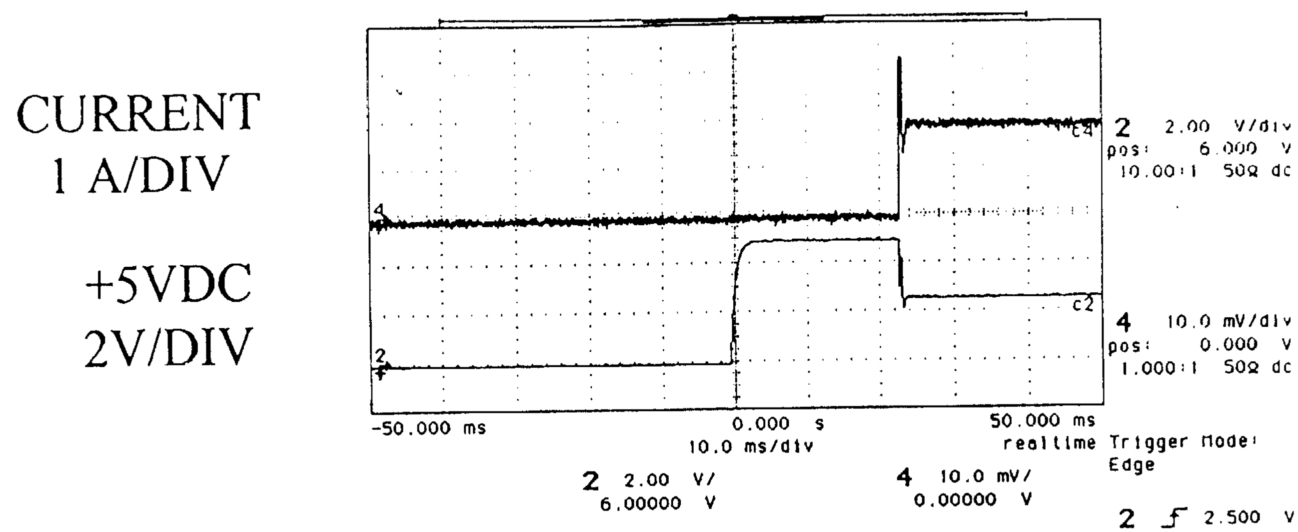


Figure 7-4. Laboratory test of the EED simulator. A power supply with a rise time of 1 msec and current limited to 2 amps was applied to the EED simulator. Initially high impedance, the EED simulator applies a load approximately 23 msec after the leading edge of the firing pulse. Horizontal scale is 10 msec per division.

Design/Analysis Summary (Key Items)

- Outputs of A1020 FPGA should have been *blocked* until circuitry is stable.
- Critical flip-flops should have been asynchronously cleared and synchronously released.
- Turn-on Characteristics of all components should have been accounted for in the design.

23

Available Documentation

http://rk.gsfc.nasa.gov/richcontent/Reports/wiremishap.htm

WIRE Main Report

http://rk.gsfc.nasa.gov/richcontent/Reports/WIRE_Report.PDF

Appendix F

http://rk.gsfc.nasa.gov/maplug/Notices/NASA_Advisory_046_ActelStartup.pdf

NASA Parts Advisory

http://rk.gsfc.nasa.gov/richcontent/General_Application_Notes/StartupNote.pdf

Startup Application Note

http://rk.gsfc.nasa.gov

Programmable Technologies Web Site

Board Charter

- Established to determine actual or probable cause of WIRE mission failure in terms of:
  1) root cause
  2) contributing causes(s)
  3) potential cause(s)
  4) pertinent observations, if desired
- Develop recommendations for preventative or other appropriate actions
- Conduct activities per NPD 8621.1(draft)
- Final report requested June 1, 1999

Board Investigation Roadmap

- Early Clues
  - Change in spacecraft body attitude control rates encountered during early spacecraft operations
  - NORAD tracking of 3 separate objects: launch vehicle, spacecraft, and cover
  - Image data from the instrument focal plane after turning on the WIRE Instrument Electronics, but prior to planned cover deployment

Board Investigation Roadmap (cont.)

Confirmation of Early Cover Deployment:

- Spacecraft attitude control and dynamics appear to be nominal prior to opening the secondary hydrogen vent.
- Spacecraft dynamics initially appear to be nominal at the opening of the secondary hydrogen vent.
- Spacecraft dynamics after the initial venting at the opening of the secondary hydrogen vent are ***not*** nominal and are consistent with a continued venting of the hydrogen at a rate lower than the initial vent rate.

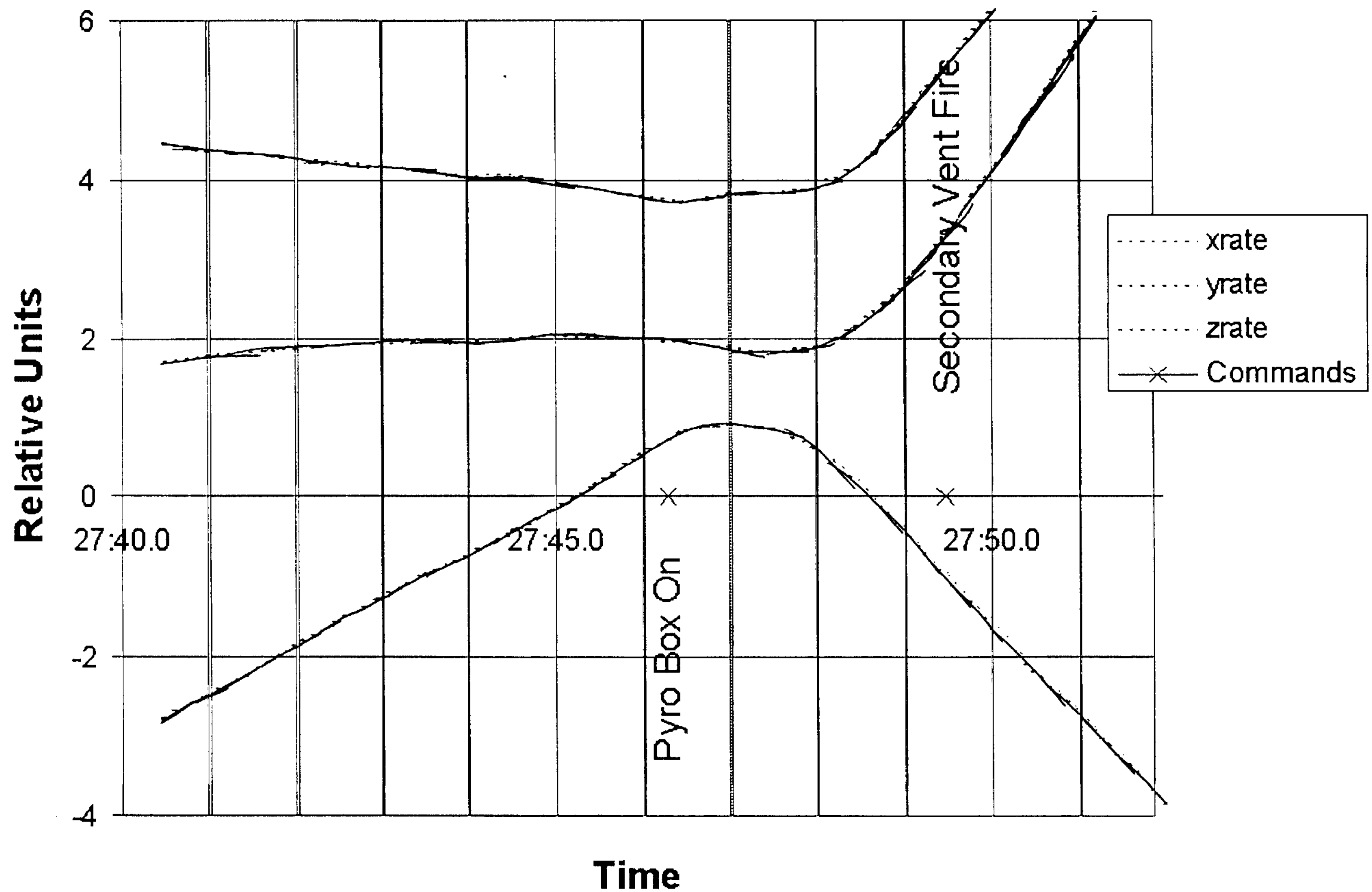
Board Investigation Roadmap (cont.)

Confirmation of Early Cover Deployment (cont.):

- The continued venting of hydrogen resulted in a torque being applied to the spacecraft that was about twice as large as the counter torque that the Magnetorquers could apply. The result was that the spacecraft continued to spin-up even though the attitude control system was performing properly.

- The continued venting of the hydrogen at a rate that would overcome the Magnetorquers capability is consistent with that which would result from the heat load applied to the spacecraft cryogen system if the telescope cover came off at roughly the same time as the secondary hydrogen vent opening.

WIRE First Pass Telemetry



Significant Contributing Cause

- Failure to identify, understand, and correct the electronic design of the pyro electronics box
  - Design errors not identified
  - Peer review, or other system reviews of the pyro electronics box were not conducted

"*It is the Mishap Board's assessment that a Peer Review by knowledgeable persons regarding pyro circuit design would have identified the turn-on characteristics of the pyro electronics box that led to failure.*"

Contributing Causes

- Spacecraft system test program did not uncover the design failure mode
- The instrument and the pyro electronics box test programs did not uncover the design failure mode
- Lack of documentation for the Actel A1020 power-up transient characteristics in the device data sheet
- Lack of documentation for the Vectron 200kHz oscillator's start time in the device data sheet
- No system level end-to-end test with live pyrotechnic devices in an as flown configuration, coupled with low fidelity simulators

Lessons Learned

1) Perform electronics power-on characterization tests, particularly for applications involving irreversible events. In some applications, power turn-off characterization may also be important and should be considered.

Recommendations:

- Independent separate pyro inhibits for mission critical events, each pyro event should require two separate actions
- Test for correct functional behavior *and* test for anomalous behavior, especially during initial turn-on and power on reset conditions

Lessons Learned

2) Detailed independent technical peer reviews are essential. Peer reviews should be done to assess the integrity of system design, including and evaluation of system/mission consequences of the detailed design and implementation.

Recommendations:

- Peer reviews should be required by Project Management
- Peer reviews should consider the heritage capability and limitations of support equipment for test of flight design
- Review should consistently penetrate system and sub-system functional design and implementation to expose risk. Cognizant systems person from each project element should review other elements' test programs and simulators for fidelity

Lessons Learned

3) The design configuration and location/mounting of external vent hardware should consider the possibility of a worst-case venting scenario to prevent mission loss or major degradation.

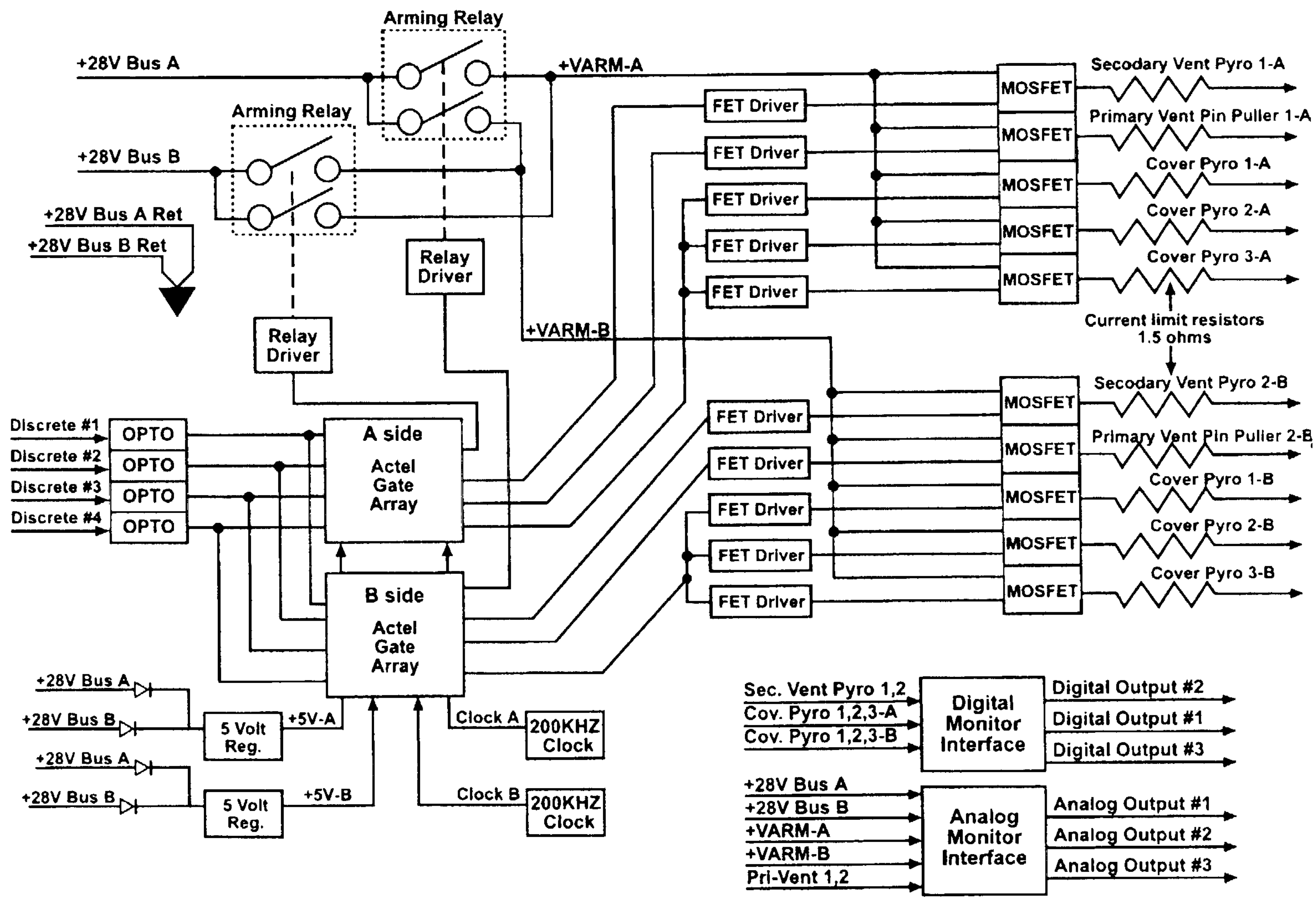
Recommendations:

- Engineering teams should consistently evaluate functional designs and implementation to expose risk areas, particularly where multiple/complex interfaces exist.

Why Did WIRE Use Logic at All?

- Limited spacecraft computer commanding resources
  - Four discrete outputs; enough but . . .
    - Software timing not compatible with operating system
  - Three digital, three analog monitors
    - Monitor sample rates not adequate to monitor fire pulses
    - Some "interpretation" required

Wire pyro box block diagram



Why Problem was Missed

- Engineering test—lab supply, slow rise time
- Acceptance test —same lab supply
- Live fire —same lab supply
- Integration test—With no other clues to the problem, pyro test fixture readouts misinterpreted; no PFR generated

System Test Methodologies

- **<u>TEST IT THE WAY IT WILL BE USED!!!!!</u>**
  - Major flaw in WIRE pyro box testing
  - Should have used relay power switching
- Test with typical-use timelines
  - Avoids missing time-related faults such as Actel "discharge" time
- Constant monitoring of critical systems

Programmatic Considerations

- In addition to QA review, have experienced engineers review parts lists, i.e., people who have used the parts
- Have peer reviews with attendees from other institutions; try to expand the experience base
- Force a re-think! Always write the PFR!

Engineering Considerations

- Review manufacturer application notes
- Review “resource” WEB pages such as Rich Katz’s
- “Lessons learned” database
- Support conferences such as MAPLD!