Flight Note

FLIGHT NOTE NO.	#394
SUBJECT	DPA-A Turn Off Anomaly Report
DATE	09-18-01
REVISION	1.2
AUTHOR	Jeff Shirer

<u>Summary</u>

On October 26, 2000, the primary ACIS Digital Processing Assembly (DPA-A) unexpectedly powered off between science observations and not during a real-time communications pass. After development of a fault tree and exoneration of ground based causes, the focus was on a Single Event Upset (SEU) to either the Science Instrument Remote Command and Telemetry Unit (SI-RCTU) or the ACIS Power Supply and Mechanisms Controller (PSMC). A detailed study did not uncover a credible cause within the SI-RCTU. The PSMC does have credible failure modes due to a single SEU. By the process of elimination, an SEU to a PSMC electrical component is considered to be the most likely cause of the DPA-A turn off. This problem has not reoccurred.

<u>Background</u>

The ACIS DPA receives X-ray event data from the CCDs through the Digital Electronics Assembly (DEA). **Figure 1** shows the flow of information within the ACIS instrument. The DPA extracts valid X-ray events and readies the data for insertion into the telemetry stream. The DPA also controls ACIS operation by processing instrument software commands. The DPA was supplied by MIT.

The ACIS PSMC performs several functions. It supplies power to the DEAs and DPAs and it controls the ACIS door and valves. As shown in **Figure 2**, high level pulses from the SI-RCTU are used to control the 5 Volt power supplied to the DPAs. As shown in **Figure 3**, the high level pulse is used to trigger a signal in an opto-isolator. The output signal from the opto-isolator is then used to set or reset the state of a solid state flip-flop, which ultimately controls the on/off state of the DPA power supply. A flip-flop is a two state logic circuit which stores one bit at a time, either a one or a zero.

The PSMC receives commands from and provides telemetry to the SI-RCTU. Chandra's RCTUs provide command output and telemetry data acquisition to and from the "user" units. In this case, the "user" is the ACIS instrument. The SI-RCTU is used to issue high level pulse, latching relay, and serial digital commands to the user. The commands to turn the DPA on and off are high level pulses, which are momentary voltage states provided to the user equipment. High level pulses are 20 - 28 V in magnitude and 33.5 - 40 msec in duration. In this case, the pulses are provided to the PSMC opto-isolator. ACIS is unique in its use of opto-isolators as the high level pulse interface with the RCTU. User equipment typically has a relay as the interface to the RCTU.

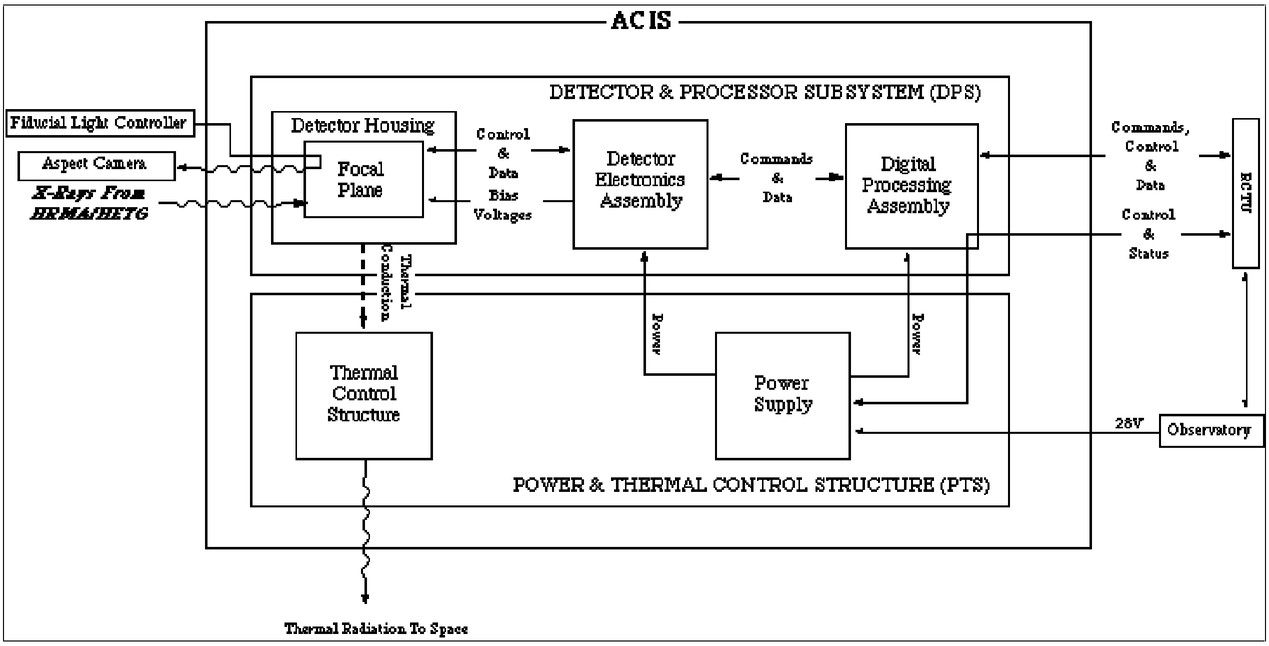


Figure 1 - ACIS Block Diagram (From Ref [1])

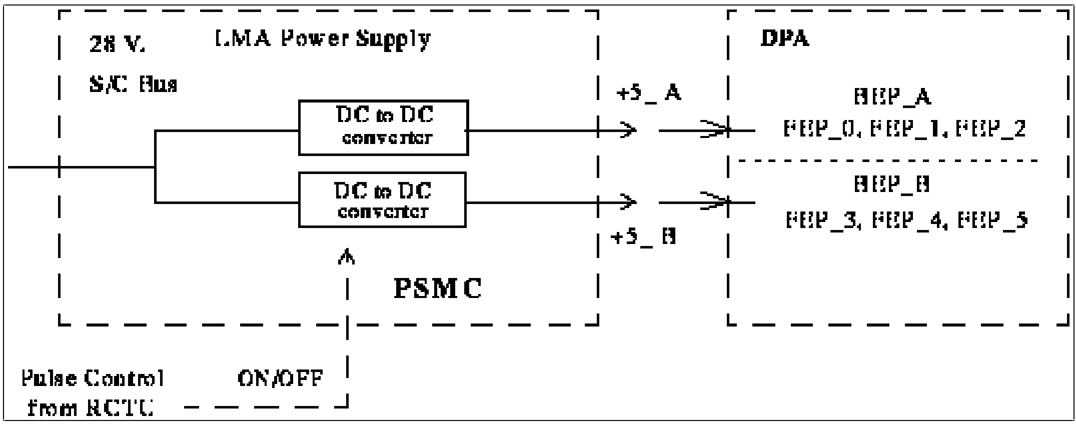


Figure 2 - PSMC Interfaces (From Ref [2})

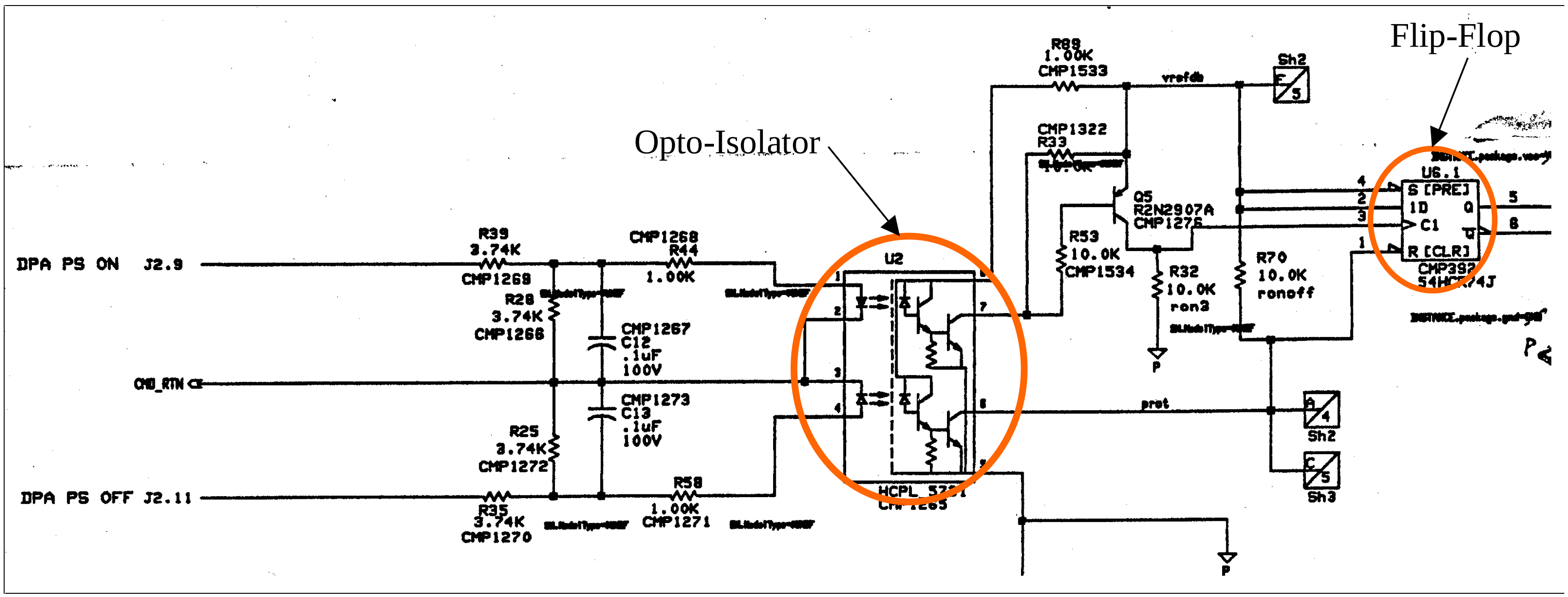


Figure 3 - PSMC Components

Timeline

Table 1 has the timeline of the events surrounding the anomaly. At the time of the anomaly, the OCC was not in communication with Chandra. The problem was not discovered until the scheduled pass with DSS-66 (Madrid). Fortunately, the pass occurred on the day shift. The on-duty SOT representative noticed that DPA-A was off in a scan of real-time telemetry. At the same time, the Greta limit exception monitor displayed the unexpected state of the DPA-A on/off status. The Command Controller noted the limit exception and notified the spacecraft Systems Engineer.

The OC scheduled extra communications time on DSS-27 (Goldstone). Telemetry dropouts plagued the early portion of the pass. Later in the pass, the SOT was able to restore ACIS to an operational state and continue the observing schedule, which was still running in the OBC. Science data loss due to the anomaly was just over six hours. This was minimized by the closeness of the anomaly to the scheduled pass on DSS-66, the presence of a SOT representative during the day shift, the quick detection by the SOT and CC, the availability of extra comm time on DSS-27, and the rapid response of the SOT.

Table 1 - Event Timeline

Time (GMT)	Event
2000:300:15:28	Start maneuver to OBSID #979
: 15:41:52	DPA-A turns off
: 15:46	End maneuver to OBSID #979
: 17:40	AOS on DSS-66. SOT, CC discover anomaly
: 19:15	DPA-A commanded back on
: 19:40	LOS on DSS-66
: 20:30	Good telemetry on DSS-27
: 20:50	Execute SOP 61010 - Load and Start DEA Run
: 21:09	Execute SOP 61083 - ACIS Standard Patches
: 21:20	Execute CAP #548 - Reset ACIS Focal Plane to -121°C
: 21:45	Execute #574 - Start ACIS-I Array Science Run

At the time of the anomaly, a typical observing schedule was running onboard. The spacecraft was maneuvering from observation #1032 to an attitude for observation #979. The maneuver completed normally, and the load continued to execute after the anomaly. The spacecraft was on the ascending leg of the orbit, well out of the radiation zone at an altitude of 121,972 km. The ambient radiation was relatively low in both high energy and low energy regimes.

Figure 4 shows the DPA-A voltage, current, and on/off indication telemetry for the day of the anomaly. The upper plot shows both the voltage (msid 1DPPOAVO) and current (msid 1DPICACU) dropping directly to 0 from their normal values. The upper plot also shows that the current did not return to the normal operational level until the ACIS-I science run was started at 21:45, as expected. The lower plot shows that the DPA on/off status (msid 1DPPSA) goes to the "OFF" state at the same time as the voltage and current drop-off. In summary, the DPA-A turn off appeared to be a "nominal" turn off. The DPA-A acted just as it would if it received the DPA-A turn off command from the ground.

<u>Fault Tree</u>

The fault tree developed for this anomaly is shown in **Figure 5**. The fault tree approach is used to ensure that all possible causes of the anomaly are listed and addressed. Criteria for exonerating each possible cause are developed. Below, each box on the fault tree is addressed.

1.0 Commanded Turn Off - This branch lists possible causes of the DPA-A power off command being issued to the PSMC.

> **1.1 Ground Command -** This branch represents the case of a real-time DPA-A power off commands being issued to the spacecraft. This case is considered to be <u>**non-credible**</u> because:
>
> The spacecraft was not in contact with a ground station at the time of the anomaly. A snapshot of the command lock telemetry in **Figure 6** shows that the receivers were not locked onto an uplink carrier (msid CRXACL=CRXBCL="NLCK").
>
> The CTU command counter did not increment. A plot of the CTU command counter and command reject counter in **Figure 7** shows that no commands were received by the CTU at the time of the anomaly.

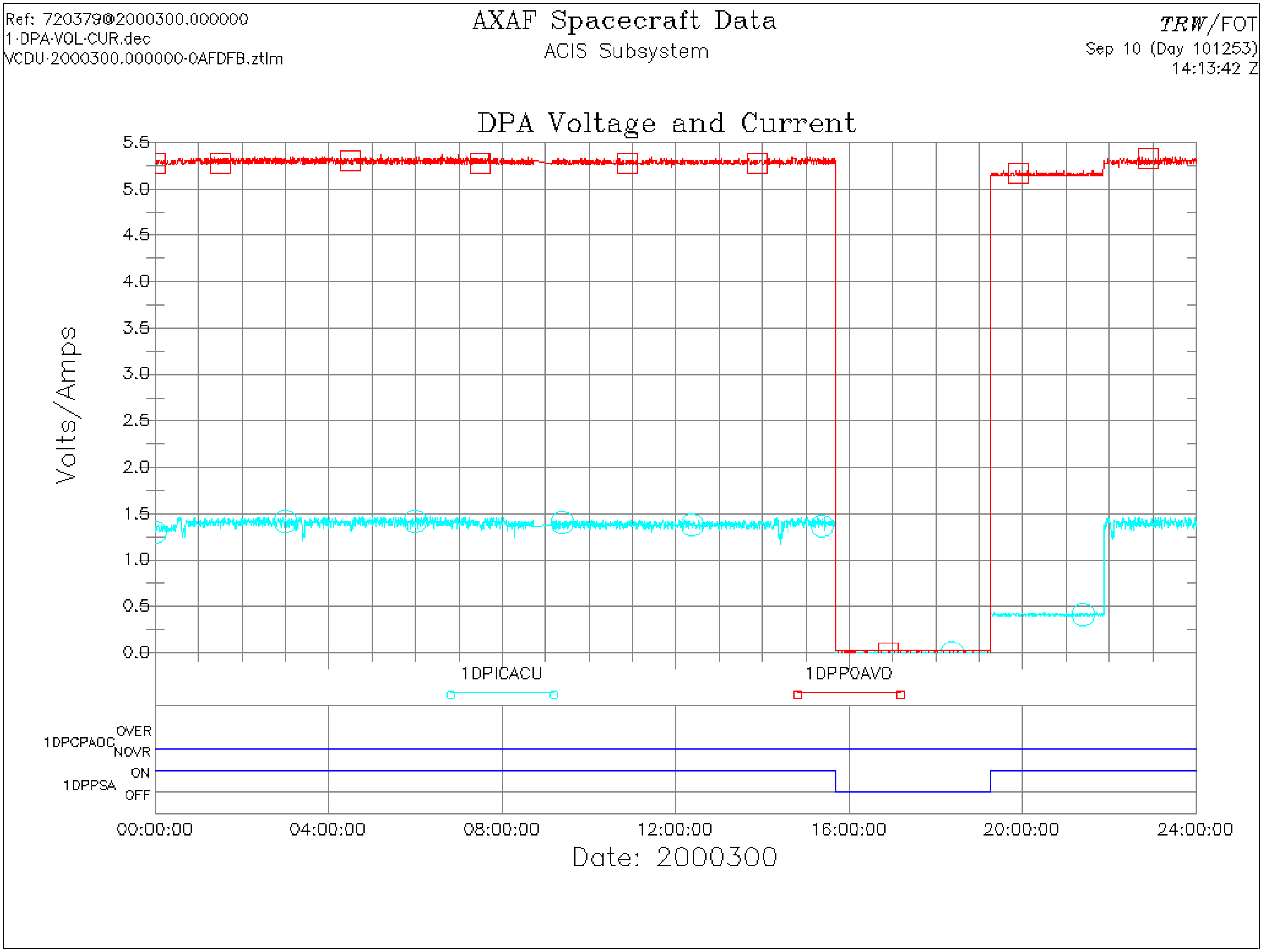


Figure 4 - DPA-A Voltage and Current

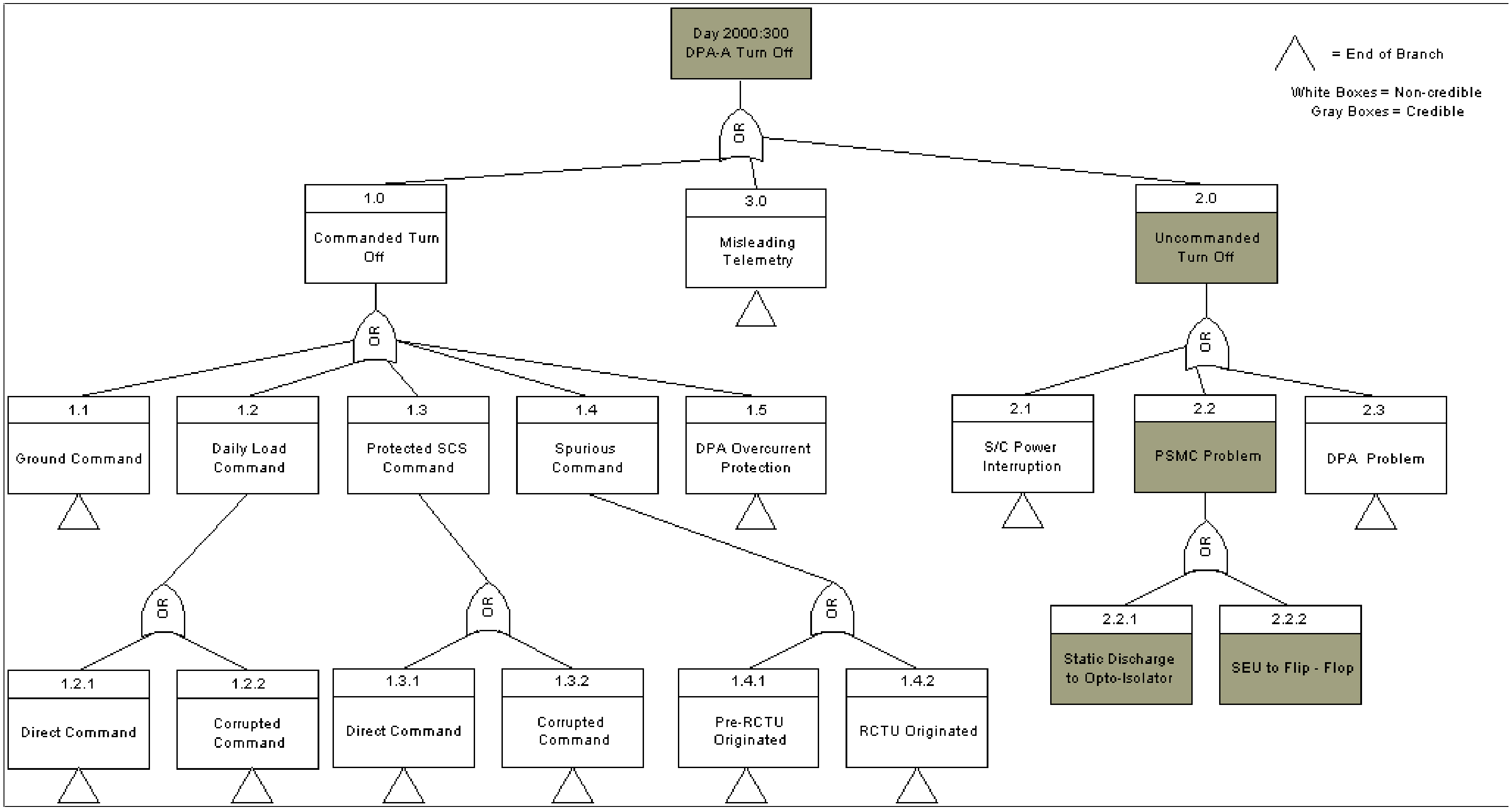


Figure 5 - Fault Tree

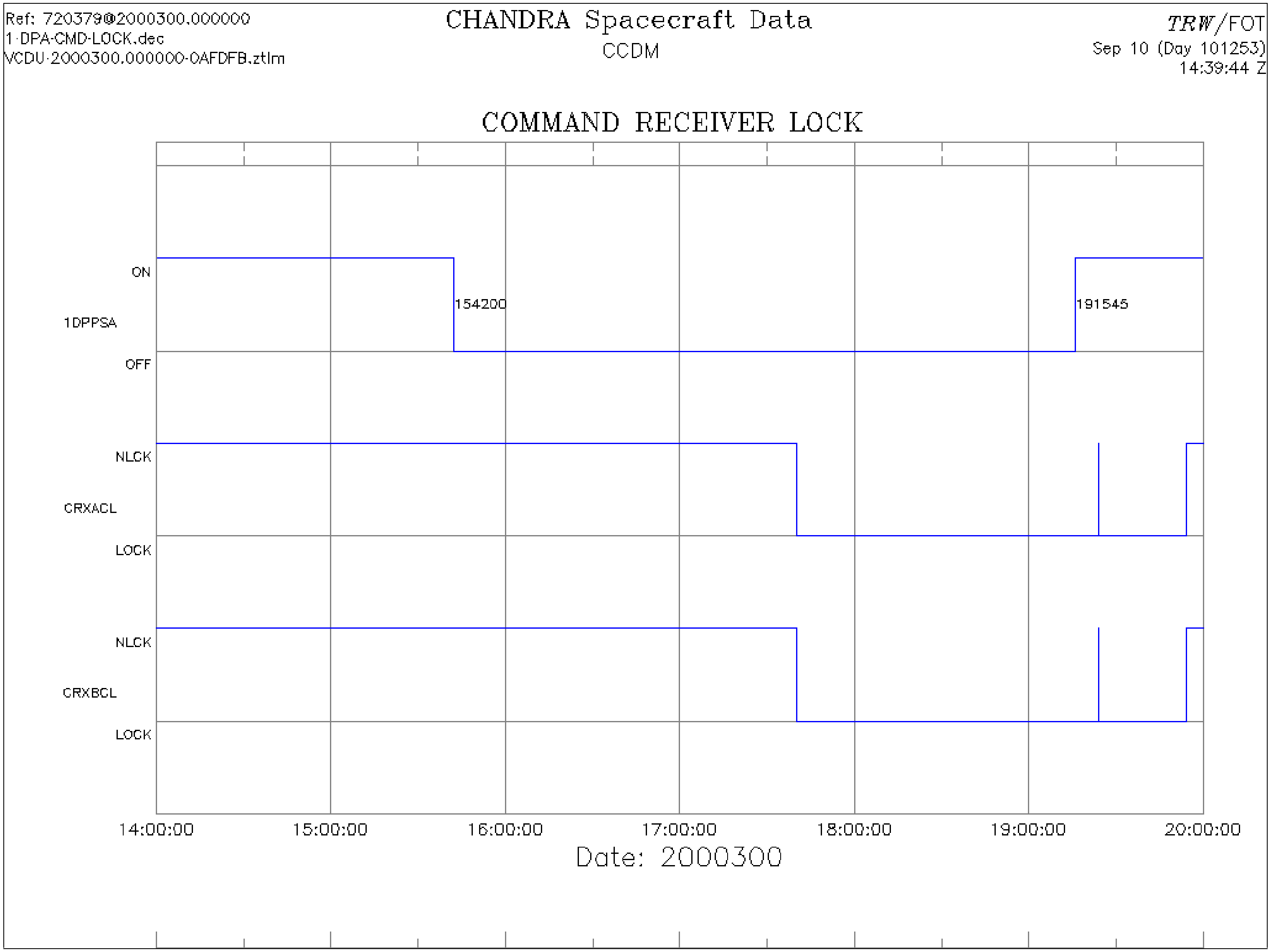


Figure 6 - Command Receiver Lock

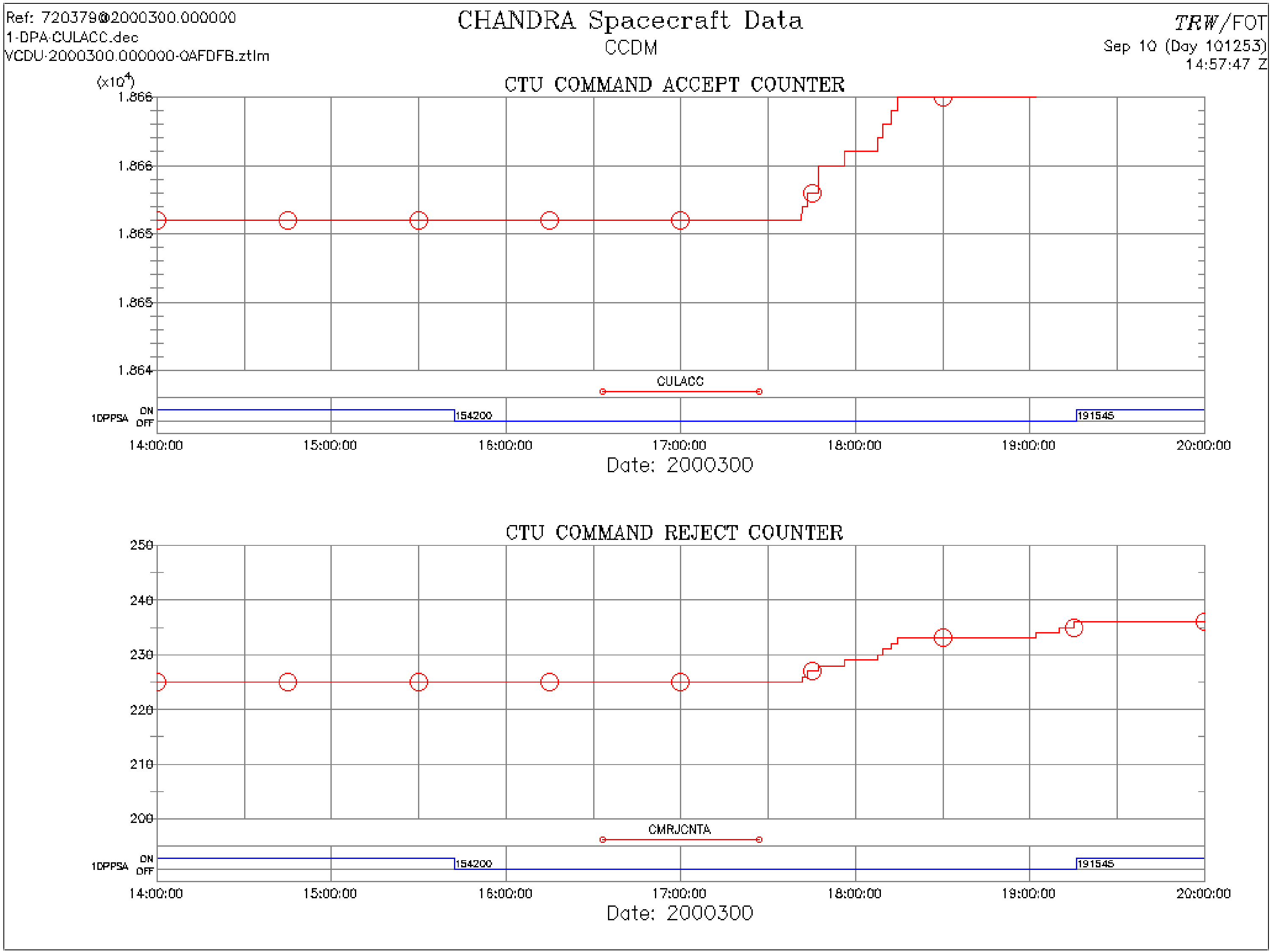


Figure 7 - CTU Command Accept and Reject Counters

1.2 Daily Load Command - This branch lists possibilities for the DPA-A off command to have come from the daily load running on-board at the time.

1.2.1 Direct Command - This branch represents the case that the DPA-A off command was actually included in the daily load running on-board. This case is **non-credible** because:

Review of the daily load shows that the command to turn off DPA-A (1DPPSAOF) was not included. **Table 2** is a listing of the commands in the daily load near the time of the anomaly. There were no commands issued from the daily load for more than 10 minutes before the anomaly.

Table 2 - Daily Load Commands Surrounding the DPA-A Anomaly

Time (GMT)	Command	Description
2000:300:15:28:20	AOMANUVR	Start maneuver to OBSID #979
2000:300:15:28:21	AOACRSTE	Enable ACA Auto-Restart
2000:300:15:28:21	COACTSX	Activate SCS #38 - Idle ACA Windows
2000:300:15:28:19	AOMANUVR	Start maneuver to OBSID #979
2000:300:15:31:09	COAOSQID	Set OBSID to 979
2000:300:15:41:52		DPA-A turns off
2000:300:15:46:21	AOFIDP	Select Fiducial Lights for OBSID #979

1.2.2 Corrupted Command - This branch represents the case that the DPA-A off command was not included in the daily load running on-board, but that another command from the daily load was somehow corrupted into the DPA-A turn-off command. This case is **non-credible** because:

Referring again to **Table 2**, there were no commands issued from the daily load for more than 10 minutes before the anomaly. A corrupted command would not be delayed to be executed later. The commands are issued within a minor frame (128 ms) of their scheduled time.

Furthermore, if a command had been corrupted into the DPA-A turn off command, it would have been issued to the SI-RCTU. However, the SI-RCTU command accept counter did not increase at the time of the anomaly, as shown in **Figure 8**. The increments in the SI-RCTU command counter near the time of the anomaly are accounted for with commands from the daily load.

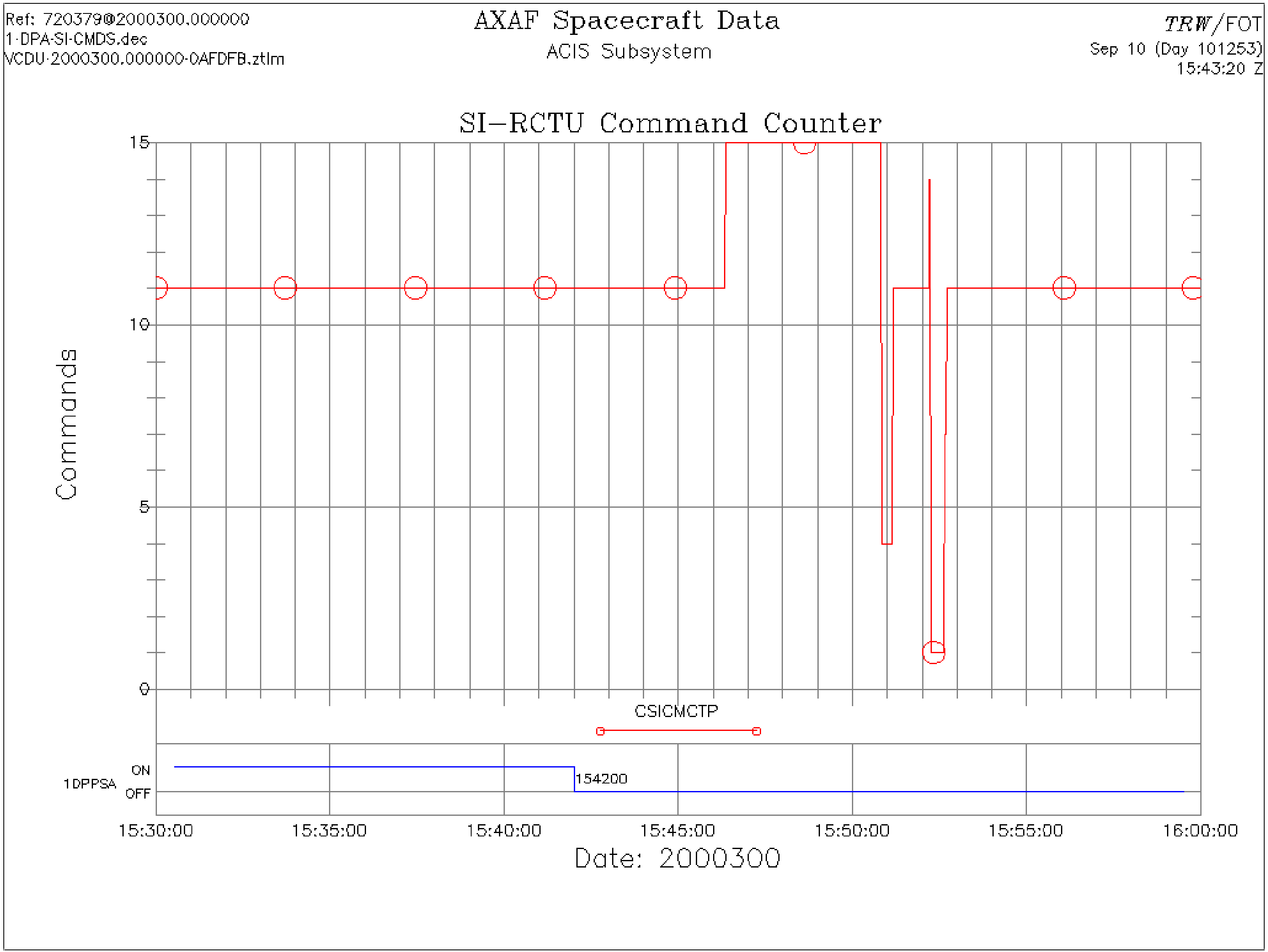


Figure 8 - SI-RCTU Command Accept Counter

It should be noted that the OBC is constantly sending NO-OP commands to the SI-RCTU as part of the command wrap monitor function. The command wrap monitor is disabled when command lock with the ground is detected. The command wrap monitor sends out 1 NO-OP every minor frame or 32 NO-Ops approximately every 8 seconds. Also, the 4 bit (0-15) SI-RCTU command accept counter is inserted into the telemetry stream every 8 seconds. This means that if no other commands besides the NO-Ops are issued to the SI-RCTU, the command accept counter appears to remain constant. The counter rolls over to its previous value every 4 seconds due to the NO-Ops.

1.3 Protected SCS or FSW Command - This branch lists possibilities for the DPA-A off command to have come from a Protected SCS, which reside in checksummed OBC memory in slots 0 - 127 or from the flight software.

1.3.1 Direct Command - This branch represents the case that the DPA-A off command was issued from an protected SCS. This case is **non-credible** because:

Review of all protected SCSs and the flight software showed that the DPA-A off command is not present. Furthermore, the SI-RCTU command counter did not increment at the time of the anomaly, as shown in **Figure 8**.

1.3.2 Corrupted Command - This branch represents the case that the DPA-A off command was created by the corruption of a command from a protected SCS or the flight software. This case is **non-credible** because:

The SI-RCTU command counter showed that no commands were received at the time of the anomaly.

1.4 Spurious Command - This branch lists possibilities for the DPA-A off command to have come from a source other than the ground or the OBC.

1.4.1 Pre-RCTU originated - This branch represents the case that the DPA-A off command was issued to the SI-RCTU from a source other than the ground or the OBC. This case is **non-credible** because:

There were no unexpected commands received by the SI-RCTU. The SI-RCTU command counter did not increment at the time of the anomaly. Furthermore, the OBC would detect such spurious commands via the SI-RCTU command wrap monitor. If the SI-RCTU received a command not generated by the OBC, the command wrap monitor would have tripped, causing a swap to the redundant SI-RCTU and safing of the science instruments. Before launch, the three spurious command events resulted in increments of an RCTU command counter (Ref [3]).

1.4.2 RCTU originated - This branch represents the case that the RCTU produced the DPA-A off command by corrupting an incoming command. This possibility was investigated by the RCTU vendor, BF Goodrich, and the report is in **Appendix A**. This case is **non-credible** because:

The only commands being received at the time of the anomaly were NO-OP commands issued by the OBC as part of the command wrap monitor. For the NO-OP command to be corrupted into the DPA-A off command, three bit flips would have to occur in exactly the right locations. The report shows that although the possibility exists for SEUs in the RCTU, the likelihood of even a single bit flip is extremely low.

1.5 DPA Current Limit Monitor - The DPA has built-in overcurrent protection. If an current above the threshold is reached, the DPA will be turned off. This case is **non-credible** because:

ACIS telemetry contains an indicator of the running state of the overcurrent protection monitor as well as a flag which will be set if the overcurrent protection monitor is tripped. Neither of these telemetry values indicated an overcurrent situation. Furthermore, the DPA current telemetry was well behaved before the anomaly, as shown in **Figure 4**. The state of the overcurrent protection monitor is also shown the lower portion of **Figure 4 (**msid 1DPCPAOC) .

2.0 Uncommanded Turn Off - This branch represents cases where the DPA-A turned off for any reason other than being commanded off from any source.

2.1 Spacecraft Power Interruption - This branch represents the possibility of the spacecraft not providing power to the DPA correctly. This case is **non-credible** because:

Telemetry shows that spacecraft power was constantly provided to the DPA power supply in the PSMC. Power from the spacecraft bus, at a nominal 28 volts, is gated and regulated to a 5 volt signal in the PSMC (see **Figure 2**). The PSMC then provides the 5 volt power to the DPA. As shown in **Figure 9,** the power supplied to the PSMC by the spacecraft was not interrupted and the 28 volt bus had power before, during, and after the DPA-A turned off.

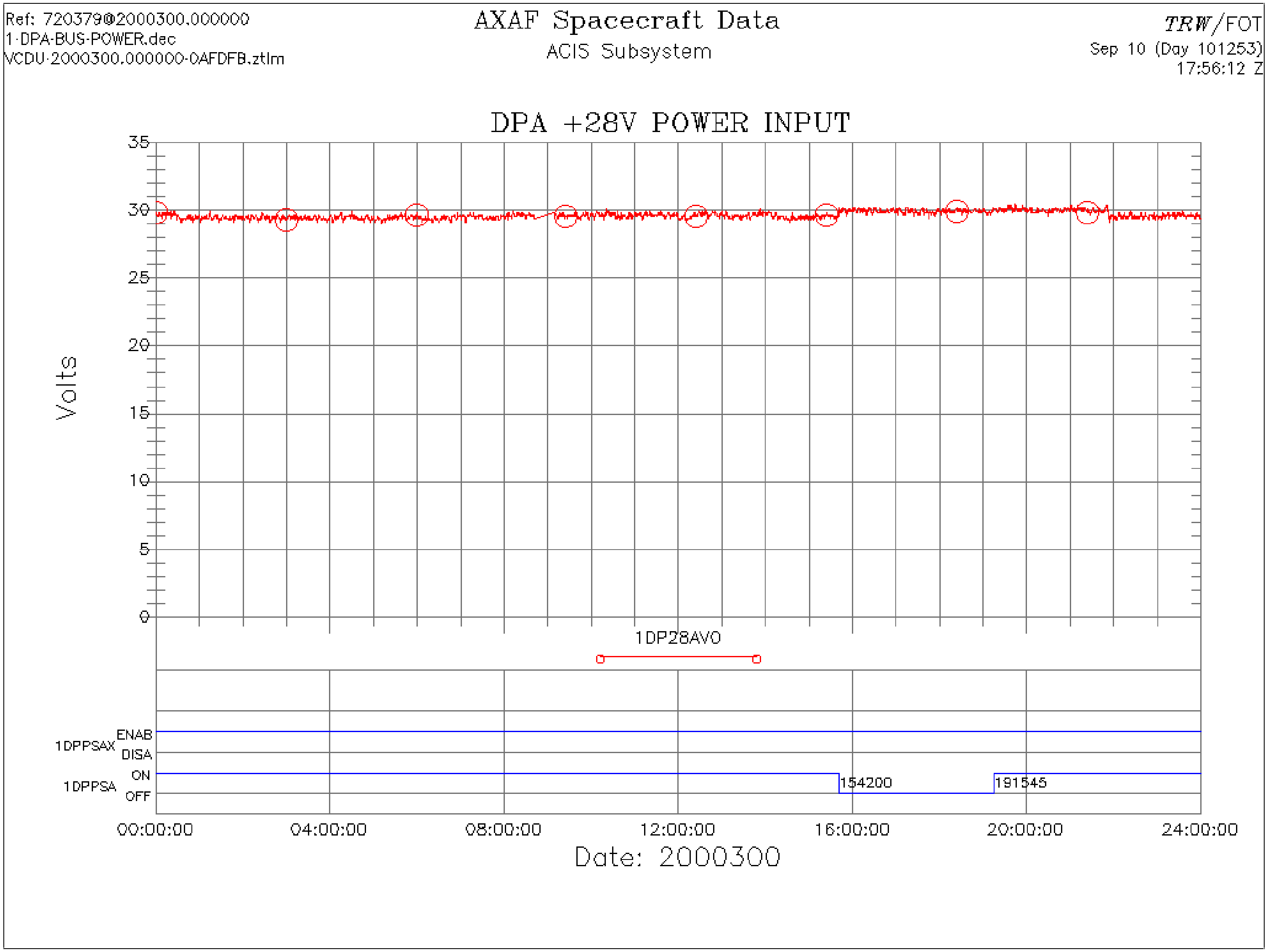


Figure 9 - Power Supply to PSMC

2.2 PSMC Problem - This branch represents the case that a problem internal to the PSMC caused the DPA-A to be turned off. As mentioned earlier, the PSMC switches power to the DPA with an opto-isolator and a flip-flop.

2.2.1 Static Discharge to the Opto-Isolator - Exposure to high energy electrons can result in significant spacecraft charging effects. Potential differences between spacecraft surfaces or between spacecraft surfaces and spacecraft ground can cause an electrostatic discharge (ESD) to occur. The transient generated by this discharge can couple into the spacecraft electronics and cause unwanted effects. This case hypothesizes that an ESD created a transient signal on the same input that would be created by a DPA-A off high level pulse command. This would trigger the opto-isolator which would send a signal to the flip-flop, turning the DPA-A off. This case is **credible** because:

It is essentially impossible to prove that this did or did not occur. However, the ACIS team believes that the PSMC is qualified to handle ESDs of the expected magnitude for our orbit. Furthermore, there have been no other ESD effects observed for the entire mission.

2.2.2 SEU to the Opto-Isolator - Energetic particles, such as cosmic rays, can produce spurious signals in electrical components. A common effect is a bit-flip, which is a reversal in the state of the silicon transistors in a flip-flop. **Figure 10** shows how an energetic particle can produce charges in silicon, leading to an electrical charge which can replicate the application of a normal signal to a transistor. This case hypothesizes that an energetic particle created a transient signal which changed the state of the PSMC DPA-A power supply flip-flop, thus turning off DPA-A. This case is **credible** because:

It is essentially impossible to prove that this did or did not occur. The susceptibility of the PSMC flip-flops to energetic particles is not known from ground testing. However, using the rate of observed bit flips in bulk ACIS memory, the probability of a bit flip in a single memory element is very small.

2.3 DPA Problem - This branch represents the case that a problem internal to the DPA caused the DPA-A to be turned off. This case is **non-credible** because:

Telemetry from the PSMC indicated that the power had been removed from the DPA in the PSMC. There were no indications of an internal failure in DPA-A either before or after the anomaly.

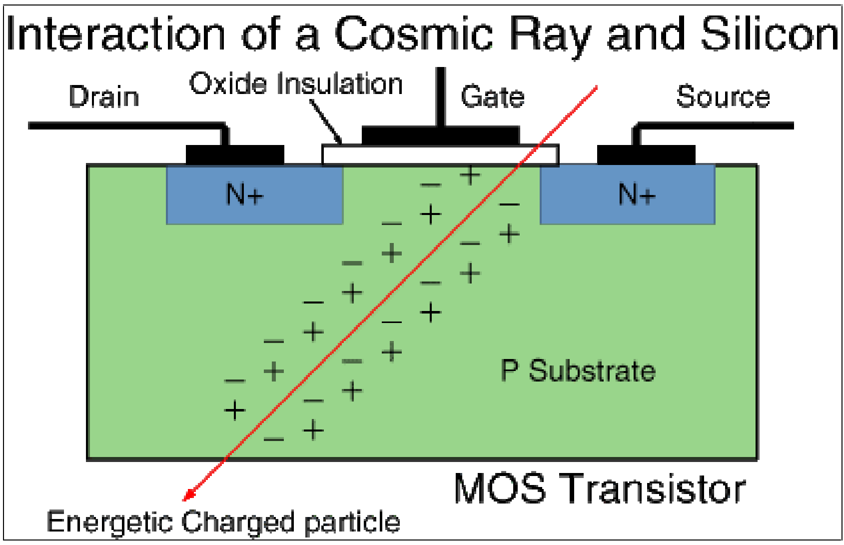


Figure 10 - SEU Effects on Electronics (from Ref [4])

3.0 Misleading Telemetry - This branch represents the case that the DPA was not actually off, but telemetry showed that it was. This case is **non-credible** because:

Both analog and bilevel telemetry showed that DPA-A was powered off. For example, **Figure 4** shows that the DPA-A voltage and current dropped out at the same time as the on/off status showed that the DPA-A was off.

Conclusion

The analysis conclusively showed that the DPA-A was not turned off by a command from any source. This includes commands from the ground, the daily load, the flight software, a spurious command from any source, and the DPA overcurrent protection. Furthermore, it was shown that the anomaly was not caused by an interrupt in the spacecraft power supply or by an internal DPA problem.

It was by process of elimination that the focus of the analysis turned to the PSMC. Both an ESD to the Opto-Isolator and SEU to the flip-flop within the PSMC DPA power supply are considered to be credible causes of the anomaly. An SEU to the flip-flop is the more likely cause. There is supporting data to show that the PSMC would be resistant to ESD, but there is no data for the susceptibility of the flip-flop to SEUs.

The problem has not reoccurred, and there are no recommended changes for mission operations. A reoccurrence of the anomaly should be caught by the normal FOT State of Health checks of the Limit Exception Monitor. Since the DPA was powered up with no problems after this anomaly, the only mission impact of a reoccurrence is loss of science.

References

1. " ACIS FOCAL PLANE INSTRUMENT FOR THE AXAF-I SPACECRAFT", E. A. Boughan, J. P. Doty, R. F. Foster, N. Tice, http://acis.mit.edu/acis/eb-paper/main.html.
2. " DPA Hardware Specification & System Description", http://acis.mit.edu/axaf/dpa/dpaspecC.html
3. "AXAF Noncompliance Report IOC", AXAF.98.332.050, Oct. 4, 1998, M. Roderick
4. "Single Event Effects Primer", The Aerospace Corporation, http://www.aero.org/seet/primer/index.html

Appendix A - BF Goodrich RCTU SEU Study

RCTU SEU Study Synopsis

1.0 Introduction

The goal of this study was to identify if a mechanism exists whereby the ACIS DPA-OFF high level discrete command could have inadvertently been issued by the science instrument (SI) RCTU. The DPA OFF anomaly occurred on the Chandra X-ray Observatory in October of 2000. The AXAF RCTU SEU Special Study was performed to the rules provided by TRW on the AXAF program. SEU study results were submitted by BFGoodrich (Gulton) beginning in the fourth quarter of 1995. The SEU Study was geared to looking at flip/flop upsets caused by high-energy particles. This present study has found two subtle problems where an SEU can cause a valid command to be corrupted. The mechanisms and timing are discussed. An estimate of the mean time to upset is calculated and indicates a rate of upset in both cases that is extremely small.

2.0 RCTU Topography

The RCTU contains the following FPGAs:

AI300 – RCTU Telemetry Slave Logic
AI301 – RCTU Matrix Control
AI302 – RCTU Command Validation
AI303 – RCTU Command Execution
AI304 – Data Bus Slave Logic
AI308 – Serial Digital Telemetry
AI312 – Serial Digital Command

The AI300 and AI308 were not included in this summary since they are telemetry system FPGAs. The AI301 Matrix Control and the AI312 Serial Digital Command FPGAs contain no flip/flops and therefore have no entries in the summary table.

The following table represents a summary of the information contained in the SEU Study that is pertinent to RCTU command outputs.

3.0 FPGA	**3.1**	**Effect of Upset**	**Can Errant CMD be Issued?**
4.0 AI302	60	Good Command is Aborted	No
5.0	6	Benign Upset	No
	4	Shortening/lengthening of reset pulse by 1.953 usecs	No
	4	Issue a reset, will abort a command if one is in progress	No
	4	Can cause a status bit to be invalid	No
	2	Affects a test output	No
	80	Total AI302 Flip/Flops	

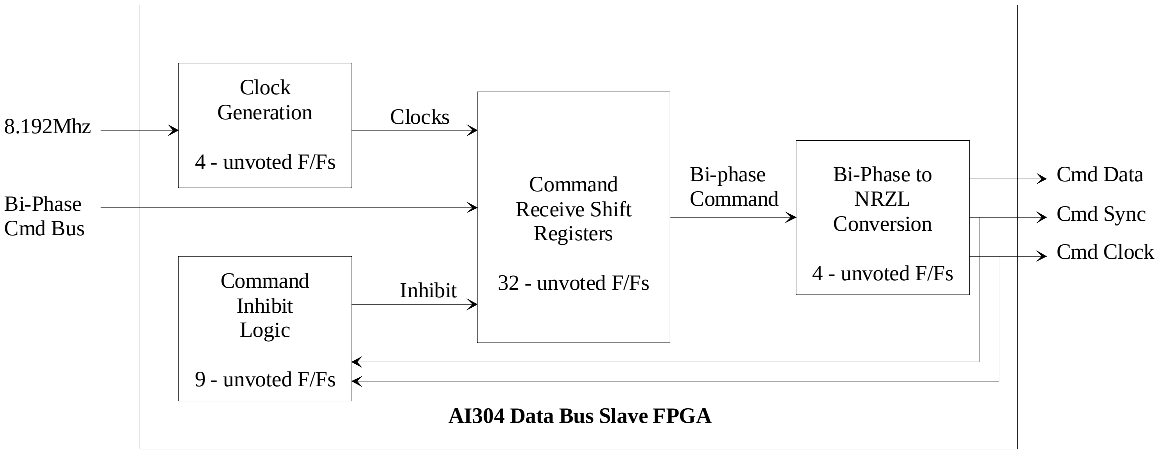
6.0 AI303	21	Benign Upset	No
	19	Good Command is Aborted	No
	13	Shorten/lengthen a LLD or HLD command	No
	10	Shorten/lengthen watchdog timer cycle	No
	4	Command execution counter can be altered	No
	3	Duplicate HLD or LLD can be issued	No
	2	Shorten/lengthen WDT and effect back-to-back HLD commands	No
	1	Shorten/lengthen WDT and effect an executing HLD and delete pending HLD or LLD commands	No
	1	Good command is cut short	No
	74	Total AI303 Flip/Flops	
7.0 AI304	78	Benign Upset	No
	10	Good command is aborted	No
	11	Double bit error is set in status word	No
	14	Tlm reply can be corrupted, rejected or lost	No
	23	Tlm request can be corrupted, rejected or lost	No
	27	Incorrect Tlm request can be issued	No
	163	Total AI304 Flip/Flops	

8.0 Description of the Sensitive Circuits (FPGAs)

The flow of commands through the RCTU involves some interface electronics, which are not diagrammed here. The entire command word is covered by a polynomial CRC (cyclic redundancy check) and a single event upset in any of these circuits would result in a bad check sum thereby rejecting the command.

9.0 AI304 Data Bus Slave FPGA

The commands are received from the Command Bus by the RCTU and are routed to the AI304 Data Bus Slave FPGA. This FPGA converts the bus signals to standard NRZL format and simply passes the command on serially with its corresponding clock and sync signals. No redundant voting of the storage elements is performed in the AI304 since the command is still protected by the polynomial and the polynomial is passed intact to the AI302 Command Validation FPGA. The Command Bus data is received into shift registers which attempt to locate a valid sync code and clock (bi-phase data has the clock encoded with the data as one signal). If a valid sync code is detected the FPGA converts the bi-phase information into separate command Data, Clock and Sync output signals that are provided to the AI302 FPGA. The generation of false or spurious commands is inhibited when a valid sync code has not been received from the Command Bus.



10.0 AI302 Command Validation FPGA

The Command Validation FPGA checks commands serially, as they are received, for:

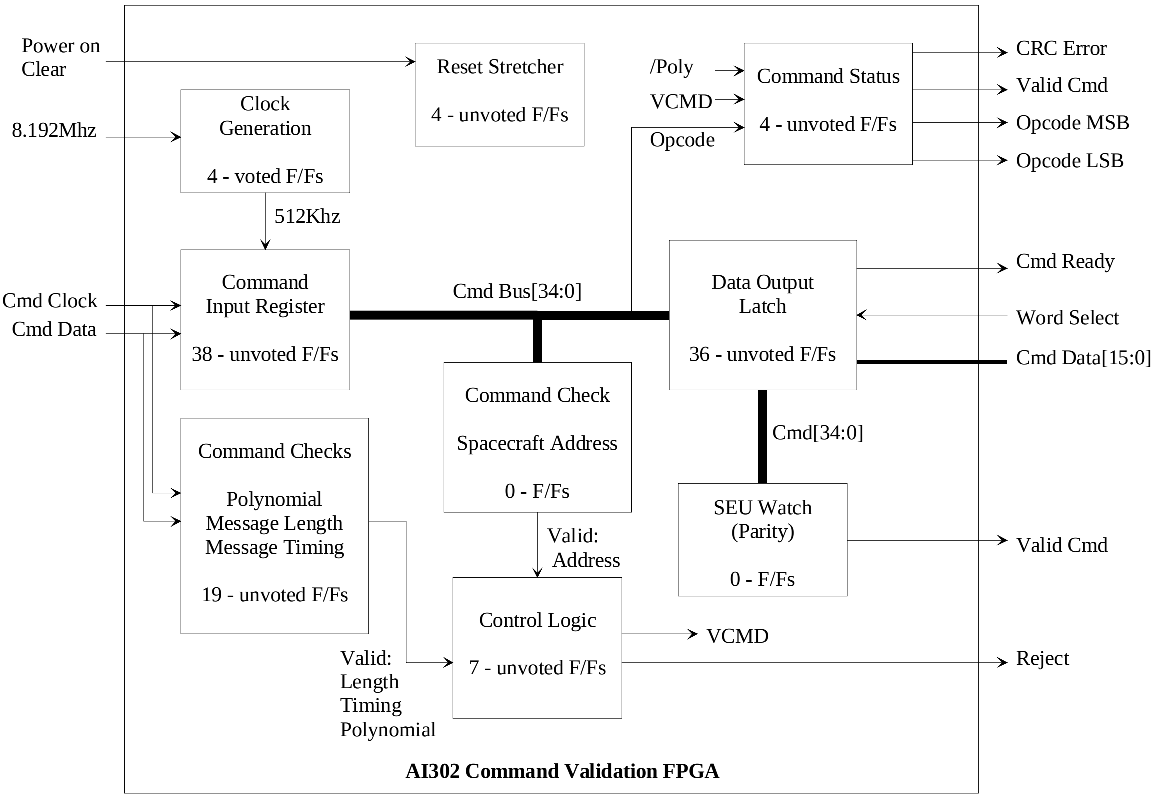
1) Message Length – verifies the bit length of the command message
2) Message Timing – verifies the regularity of command clocks
3) Polynomial validity – verifies the correctness of the polynomial

The Command Validation FPGA checks commands in parallel, after they are latched, for:

1) Spacecraft Address

The control logic in the Command Validation FPGA immediately rejects any command that does not pass all of the command validation criteria. The Command Validation FPGA signals that it has a valid command by activating the Cmd Ready signal to the AI303 Command Execution FPGA. The Command Execution FPGA takes the command data on a 16-bit bus using the Word Select signal. When Word Select toggles, the Command Validation FPGA clears the command buffer by setting all of the storage elements to a logic 1. This bit pattern is an invalid command that has the data type of a reserved (NOP) command. The Cmd Ready and Valid Cmd signals are both deactivated until a new, valid command is received.

While the command is stored in the Command Validation FPGA, awaiting transfer to the Command Execution FPGA, it is protected by a single parity bit called “Valid Cmd”. If an SEU upsets a bit in the command holding register this signal will indicate to the Command Execution FPGA that the command is no longer valid. While no command is stored in the Command Validation FPGA the command data register is set to all “1”s. An all “1”s pattern in the command holding register yields a VCMD of “0” or invalid. If an SEU upsets a bit in this register when no command is stored this signal will indicate to the Command Execution FPGA that the command is valid but the CMD RDY signal will not be present and no command will be issued.

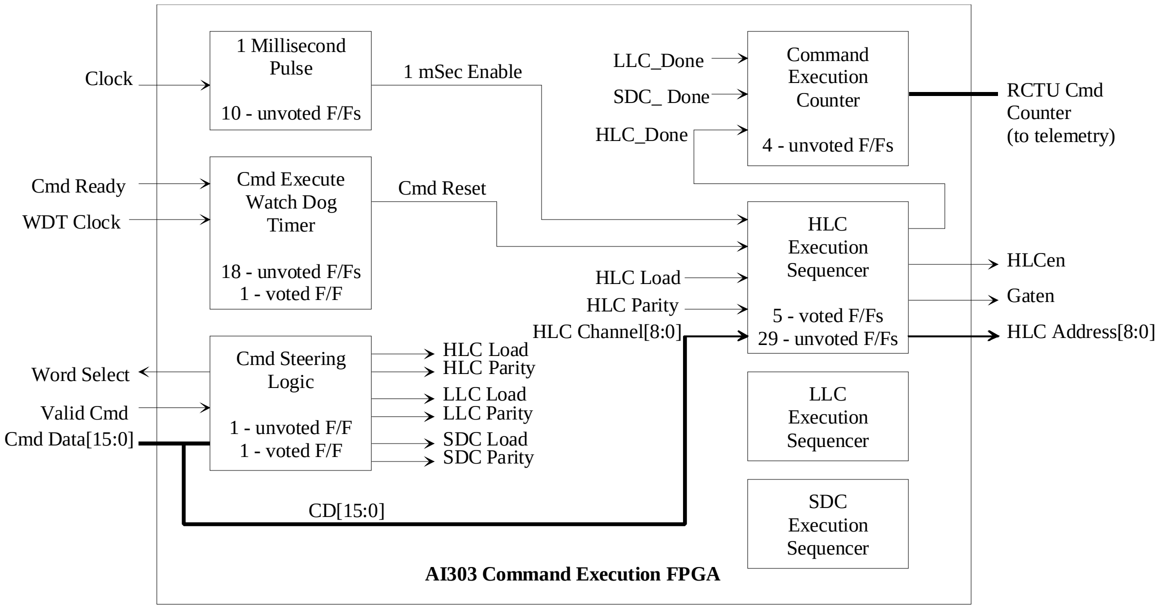


In the AI302 voting is only used in the clock generation circuit. This divide by 16 circuit produces the 512K system clock used by the command system. This must be done in order to provide a clock with unvarying characteristics. The remainder of the AI302 is unvoted for a few reasons. The command data itself is protected by a polynomial and/or parity inside the Command Validation FPGA and therefore is protected from a single event upset. The goal of the addition of SEU protection to the FPGAs was to prevent bad commands from being issued. If any of the command check circuits were upset they would indicate that a bad command was received and not vice versa, except for the newly discovered problems discussed later. The RCTU command system FPGAs were nearly fully utilized which means that few or no free modules were available with which to add substantial majority voting. Other, less module hungry design techniques were used to enhance the protection such as setting the command storage latch to all “1”s when a valid command is not being held. This bit pattern represents a no-op command that has bad parity. If the control logic is upset and initiates a command from this buffer the command will be rejected. These approaches were used instead of majority voting the control logic due to the high utilization of modules within the FPGA.

11.0 AI303 Command Execution FPGA

The Command Execution FPGA awaits commands from the Command Validation FPGA. It decodes the “data type” field from the incoming command and if the command is valid generates a load pulse that is gated with the data type (HLC, LLC, SDC) and the “Valid Cmd” signal. This load pulse causes command data to be loaded to the buffers for the HLC, LLC or SDC command sequencers. This load pulse also generates a new parity bit corresponding to the type of data being loaded. If during the execution of any of these commands an upset occurs in the data, either the HLC or LLC channel or the SDC channel or data, the command is immediately discontinued. A 1 millisecond enable is generated and provided to the execution sequencers in order that they time their command execution (i.e. a HLC is 40 milliseconds in length). When a new command is received the command execution watchdog timer is reset. This provides an approximate 100-millisecond window in which commands can be issued. The watchdog timer allows for two back-to-back high level commands to be buffered and executed before it expires. When the watchdog timer expires it generates a reset pulse and causes all of the command execution sequencers (HLC, LLC, and SDC) to be reset. When no commands are received the watchdog timer continues to reset the sequencers approximately every 100 milliseconds. The execution sequencers are held in reset when no command has been loaded preventing spurious commands from being issued from these circuits due to SEUs.

When the high-level command execution sequencer receives a new command it stores the command in a buffer composed of latches. This buffer holds the command data until the HLC execute register is empty, at which time the buffer contents, including the parity bit, are copied to the execute register. After the command is loaded into the execute register the HLC sequencer begins execution. The HLC execution counter starts to down count the period of the high-level command and asserts both the HLCEN and Gaten signals. The HLCEN signal provides the PWRON signal on the HLC output driver card. The Gaten signal is provided to the external circuitry and becomes GATON. GATON signals the RCTU power supply to enable the HLC power output through its fold-back current limiter to the selected HLC output channel. Both Gaten and HLCEN must be active to fire a high-level command output. When the command execution is finished, the sequencer issues a “HLC_DONE” signal to the command execution counter. This four-bit counter is provided to telemetry and gives a record of commands that have been executed. However, if the command parity becomes bad during execution of the command the “HLC_DONE” signal is not issued and the (partial) command execution is not counted. The HLCen and HLC Address are provided to the AI301 Matrix Control FPGA which decodes, selects and enables the high-level command. The AI301 does not contain any storage elements (latches or flip/flops) and as such was not part of the SEU Study.



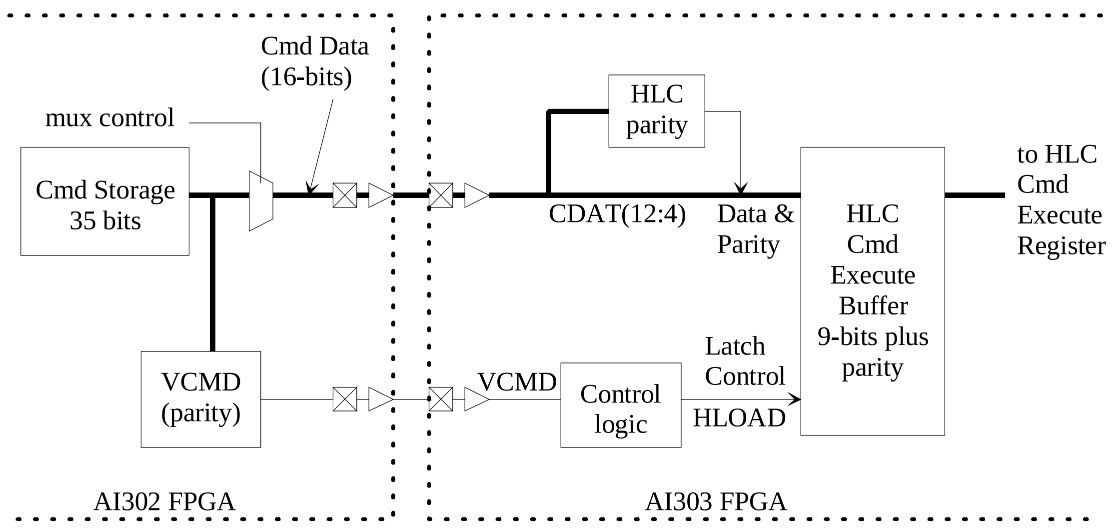
Once again majority voting was used judiciously in the Command Execution FPGA because it had a very high module utilization. Only those circuits that were thought to absolutely require voting were voted. A new parity was generated for each command type and a single parity bit was stored with each command data word for protection of commands through execution. Other check and balances were used to protect inadvertent commanding such as holding the execution sequencers in reset when a valid command is not present. A watchdog timer was used to periodically reset the command circuits to prevent the accumulation of errors in the command data and control logic storage elements.

Discovery of Two Potential SEU Effects
Two potential SEU effects were discovered during the course of this study. Either can potentially cause a number of problems with a very low probability of occurrence.

12.0 Potential SEU Effect 1

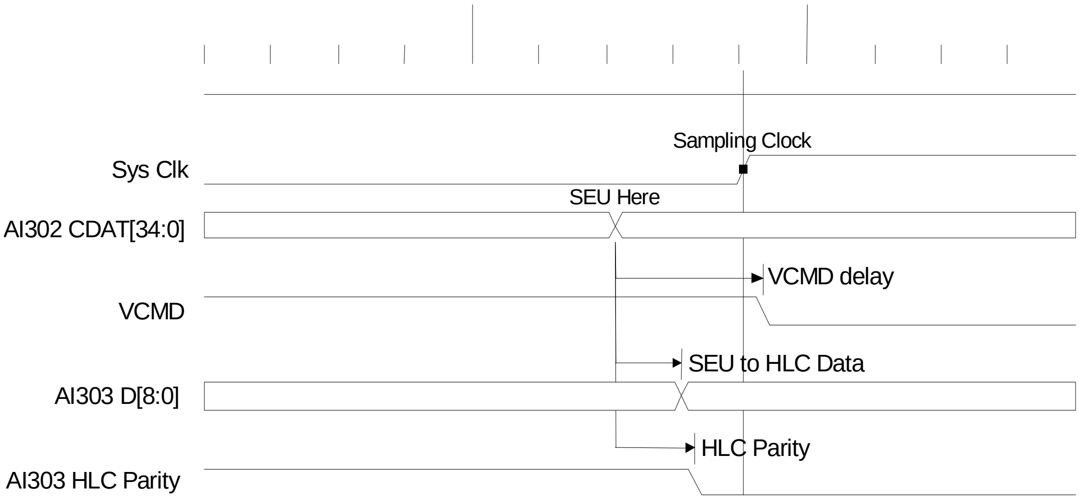
The first potential effect is fairly subtle. The block diagram of a command passing from the AI302 to the AI303 FPGA shows the CDAT (command data) and the VCMD signal. While a command is stored in the AI302 output storage register the VCMD signal is generated and represents parity over the entire 35 bits of the command. VCMD passes along with the CDAT (command data) to be stored in the AI303 FPGA. VCMD is an input that in part controls the latching of the command data in the AI303. If VCMD is valid (logic 1) the command is considered to be valid and the loading of the AI303 command data latch begins. At the same time the data is stored in the AI303 FPGA, a new parity bit is generated and stored (in the AI303). This new parity bit is only associated with the bits relevant to the particular command. For example, a high level discrete command has only 9-bits that describe the desired channel to be issued and the new parity is generated from only these 9-bits.

When a new command is received by the RCTU and is validated, VCMD changes to a logic "1" indicating that the command is good. This starts the process of loading the command to the AI303 execution buffer and ultimately the execution register. If a single event upset occurs in the AI302 command storage register, the change in the data will propagate over to the storage latch in the AI303. The VCMD is the output of a parity circuit and is generated from the data in the AI302 register. As such, the change in VCMD lags the data by the delay through the parity circuit until it reaches the gate control (called HLOAD) for the latch storing the command data. This means that once the transfer has started, if an SEU occurs on the data, the data will change before the VCMD can change. This opens a small window where the command data has been upset (and is incorrect) and yet the VCMD signal still indicates that the command is good. In order to store command data that has been upset HLOAD must be present at the data latch in the AI303 when the next operating clock arrives. Otherwise, the command is not considered as having been loaded.



AI302 to AI303 Command Transfer

The following timing diagram illustrates the relative timing of the operating clock (SysClk), the source command data (CDAT[34:0]), the received command data (D[8:0]), VCMD and HLC Parity.



RCTU Command Upset Relationships

As shown in the timing diagram, a well placed SEU in the data can cause the AI302 FPGA to send over corrupted data with an indication that the data is valid (VCMD) to the AI303.

Timing analysis indicates that the potential upset window, in the typical timing case, is as follows for the HLC command data (of the 16 bits of CDAT only CDAT4 through CDAT12 are used for HLC commands):

HLC Channel Data Upset Susceptability Window (ns)	
CDAT4	43.1
CDAT5	41.4
CDAT6	30.8
CDAT7	39.1
CDAT8	44.2
CDAT9	44.1
CDAT10	47.9
CDAT11	43.5
CDAT12	63.3

For each CDAT, data was generated by the Actel timing Analyzer and shows that windows of from 30.8 to 63.3 nanoseconds exist in the typical case (all circuits at 25°C, 5 volts, and typical process) for the command data bits being transferred from the AI302 to the AI303. This means a window of time exists for each command sent to an RCTU where:

1) If one of a set of specific bits in the command register in the AI302 is hit,
2) With enough energy to flip a command bit,
3) During a specific portion (window) of the single clock cycle,
4) When the command is being transferred from the AI302 to the AI303 FPGA,

The command will be corrupted. The new command will be the same as the original command except for the state of one bit of the command.

This problem also affects serial digital commands and low level discretes. Timing for low level discrete commands is shown in the following table. The timing was not generated for the SDC circuits.

LLC Channel Data Upset Susceptability Window (ns)	
CDAT4	46.4
CDAT5	44.4
CDAT6	33.8
CDAT7	44.1
CDAT8	46.1
CDAT9	46.9
CDAT10	51.7
CDAT11	47.8

Another effect of this upset is that the command bits used to describe the type of command, known as the "data type" field, are a part of the data that can be upset. Potentially this means that a high-level command, data type "00", can be changed into a low-level command, data type "01", or a serial-digital command, data type "10", or vice versa. It also means that a reserved command, data type "11", can be changed into a low-level command or a serial-digital command or vice versa.

Upset Susceptability Window (ns) changing command type			
Data Bit	LLC or SDC to HLC	HLC or Reserved to LLC	HLC or Reserved to SDC
CDAT0	51.8	53.8	51.8
CDAT1	45.9	46.0	46.0

While this upset can occur the expected rate is extremely small. After analyzing for upsets in low level and high level command data as well as upsets in the data type field the following is a summary of the results. Note that these numbers are based on the maximum number of commands per second that the system can provide (2844/sec). The upset rates will reduce linearly with reductions in the command rate.

Mean Time Between Upsets

For command data and data type upsets

From the AXAF Radiation Analyses (BFG):

A1020	Cosmic Ray (upsets / sec)	Solar Flare (upsets/sec)
Bistable Element	8.64E-12	1.10E-06

Rates for SEUs that cause HLC command channel data bits to be corrupted.

High Level Command Data	**Particle Environment**		
Mean Time Between Upsets	Cosmic Ray	Solar Flare	
Bistable Element	8.64E-12	1.10E-06	Upsets / sec
Average commands issued/sec	2844	2844	Cmds / sec
Average upset window	44.2	44.2	nanoseconds
Duty Cycle	0.000125705	0.000125705	%
Number of bits	9	9	
Upset rates	9.77E-15	1.24E-09	Upsets / sec
MTBU	>>1000 yrs	25 yrs	

Rates for SEUs that cause LLC command channel data bits to be corrupted.

Low Level Command Data	Particle Environment		
Mean Time Between Upsets	Cosmic Ray	Solar Flare	
Bistable Element	8.64E-12	1.10E-06	Upsets / sec
Average commands issued/sec	2844	2844	Cmds / sec
Average upset window	45.2	45.2	nanoseconds
Duty Cycle	0.000128549	0.000128549	%
Number of bits	8	8	
Upset rates	8.89E-15	1.13E-09	Upsets / sec
MTBU	>>1000 yrs	28 yrs	

Rates for SEUs that cause LLC or SDC commands to be changed to HLC commands (data type bits are corrupted).

Change to HLC

Command Data Type Bits	Particle Environment		
Mean Time Between Upsets	Cosmic Ray	Solar Flare	
Bistable Element	8.64E-12	1.10E-06	Upsets / sec
Average commands issued/sec	2844	2844	Cmds / sec
Average upset window	48.9	48.9	nanoseconds
Duty Cycle	0.000139072	0.000139072	%
Number of bits	2	2	
Upset rates	2.40E-15	3.06E-10	Upsets / sec
MTBU	>>1000 yrs	104 yrs	

Rates for SEUs that cause HLC or reserved commands (NOPs) to be changed to LLC commands (data type bits are corrupted).

Change to LLC

Command Data Type Bits	Particle Environment		
Mean Time Between Upsets	Cosmic Ray	Solar Flare	
Bistable Element	8.64E-12	1.10E-06	Upsets / sec
Average commands issued/sec	2844	2844	Cmds / sec
Average upset window	49.9	49.9	nanoseconds
Duty Cycle	0.000141916	0.000141916	%
Number of bits	2	2	
Upset rates	2.45E-15	3.12E-10	Upsets / sec
MTBU	>>1000 yrs	101 yrs	

Rates for SEUs that cause HLC or reserved commands (NOPs) to be changed to SDC commands (data type bits are corrupted).

Change to SDC

Command Data Type Bits	Particle Environment		
Mean Time Between Upsets	Cosmic Ray	Solar Flare	
Bistable Element	8.64E-12	1.10E-06	Upsets / sec
Average commands issued/sec	2844	2844	Cmds / sec
Average upset window	48.9	48.9	nanoseconds
Duty Cycle	0.000139072	0.000139072	%
Number of bits	2	2	
Upset rates	2.40E-15	3.06E-10	Upsets / sec
MTBU	>>1000 yrs	104 yrs	

This upset mechanism does not explain the ACIS DPA-OFF anomaly of October 2000. The only reported command being sent to the RCTU at the time of the anomaly was a No-op (reserved) command with a bit pattern of:

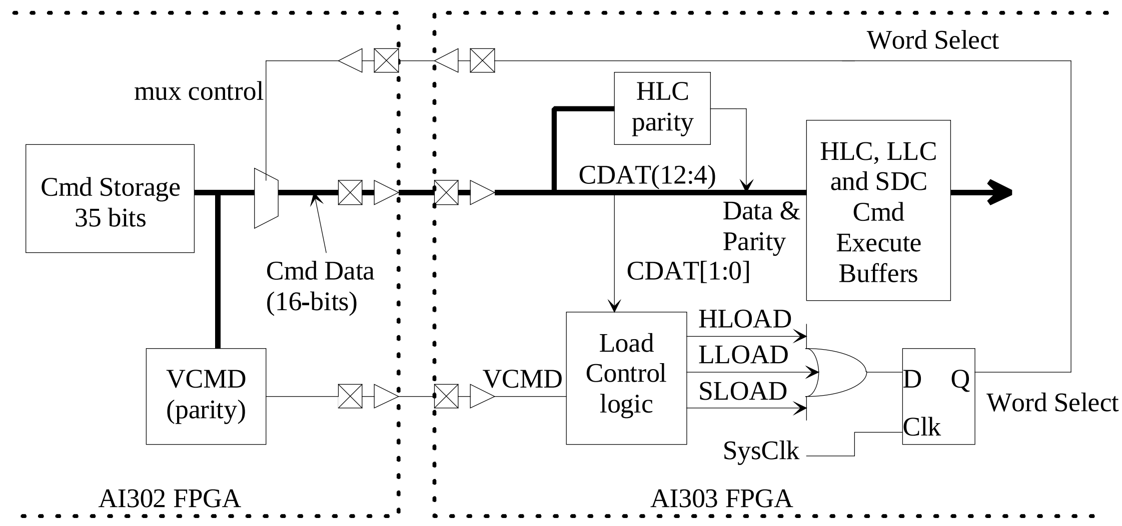
	MSB	7	6	5	4	3	2	LSB
Reserved Cmd	0000	0110	0110	0000	0000	0000	0000	0000
HLC Channel 7	0000	0110	0000	0000	0000	0000	0000	0111

For this command to be changed to HLC channel 7, five bit upsets would have to had occurred, 2 bits in nibble 6, from 1 to 0, and 3 bits in the LSB nibble, from 0 to 1.

Potential SEU Effect 2

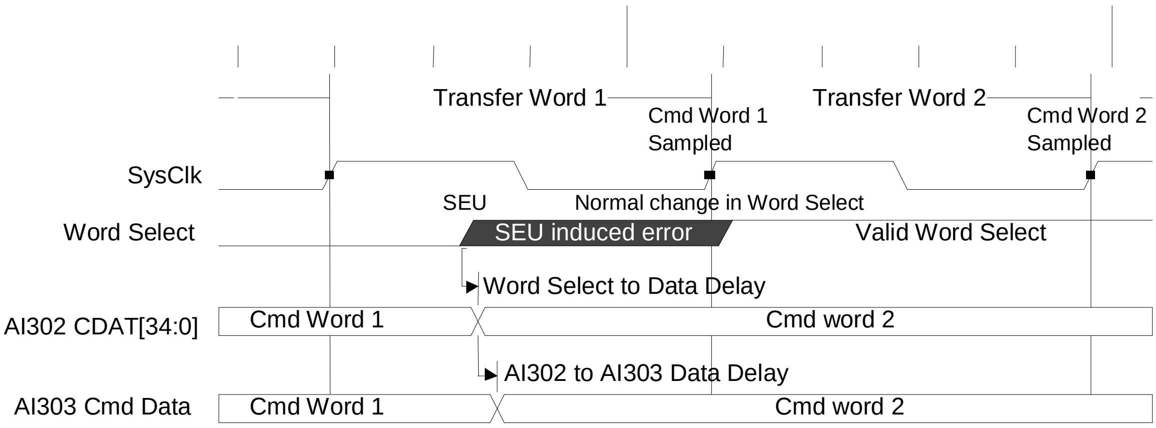
Command data is transferred from the AI302 Command Validation FPGA to the AI303 Command Execution FPGA on a multiplexed, 16-bit bus. This multiplexing of the command word between FPGAs was necessary because there were not enough pins on the A1020 device to bring the command word, all at once, over one bus. The command channel information, which is contained in the lower half of the command word, is transferred over first. For high level and low level commands a subset of these 16 bits is all that is necessary to issue the commands. For serial digital commands the first 16 bits contains the channel and the lower 2 bits of the data word which contains the command type. The upper part of the serial digital command word contains the 16-bit serial digital data word and is transferred in a second transfer. The AI303 receives the first 16 bits from the AI302 FPGA and it then sets the Word Select signal to signify to the AI302 FPGA that it has completed the transfer of data. If the command is a low level or high level command the AI303 FPGA prepares to execute the command and ignores any further CDAT data (the second 16-bit word) because it is not needed. If the command is a serial digital command the AI303 latches the SDC channel information (5 bits) from the first 16-bit transfer and then sets the Word Select signal. This once again tells the AI302 that the transfer is complete and the AI302 changes the data to the second 16-bit part of the command word. In this case, the second word contains the 16-bit data field of the serial digital command. This is latched by the AI303 and then it begins to issue the command.

The storage element that generates the Word Select signal is an unvoted flip/flop. If the Word Select flip/flop is upset during the clock cycle (512Khz clock) associated with the transfer of the first command word, the AI302 output multiplexer will switch to the second command word which is the field normally associated with a serial digital command data word. The bits in this field of the command will then be used to determine what type of command and which channel to execute (not the intended command). For bit patterns that are interpreted as high level or low level commands the second word will not be transferred or used. For bit patterns that are interpreted as serial digital commands the channel information will be incorrectly selected as with high and low level commands. The second word transfer will occur. This will simply be the same word transferred again. The serial command data will be correct but will potentially be sent to the wrong channel address.



Word Select Upset

The following timing diagram shows that an asynchronous change in Word Select, caused by an SEU, will cause command data word 2 to be latched for both of the word 1 and word 2 samples.



Word Select Upset Timing

For this anomaly to inadvertently cause the ACIS DPA-OFF command to be issued the command received would have had to be the following 32-bit command in TRW's database format:

MSB	7	6	5	4	3	2	LSB
0000	0110	011x	xx00	0000	111x	x00x	xxxx

Note that bits 5,6 and 12-17 must be 0 and bits 9-11 must be 1. The "x" bits could be either 0 or 1. This command would cause HLC channel 7 to be issued. The only reported command being sent to the RCTU at the time of the anomaly was a No-op (reserved) command with a bit pattern of:

MSB	7	6	5	4	3	2	LSB
0000	0110	0110	0000	0000	0000	0000	0000

Had this anomaly occurred during the execution of this command the resulting command would have been a High Level Discrete command to channel 0.

Conclusions

This RCTU command study found two mechanisms where commands are susceptible to single event upsets. Both problems can cause valid RCTU commands to be corrupted and issued. However, both problems exhibit such a small window of opportunity for an SEU to effect the circuits involved that the mean time between upset, for the cosmic ray background flux environment, is estimated to be greater than 1,000,000 years. These command changes can occur after the RCTU has been selected and enters the process of decoding the command. As such the command will always go to the intended RCTU. Also, no effects were found that could explain the Chandra ACIS DPA-OFF command anomaly of October 2000.