DETECTOR CONTROL ELECTRONICS (DCE) FLIGHT SOFTWARE REQUIREMENTS DOCUMENT

for the

COSMIC ORIGINS SPECTROGRAPH

(COS)

Contract No NAS5-98043
CDRL No. DM-03

Prepared for:

Goddard Space Flight Center
Greenbelt, MD

Prepared by:

Experimental Astrophysics Laboratory, Space Sciences Laboratory
University of California, Berkeley

COS-UCB-004

August 26, 1999

Prepared By:	Reviewed By:
Mr. Daniel Blackman FUV Detector Software Lead	Mr. Geoff Gaines FUV Detector Systems Engineer
	Dr. Derek Buzasi FUV Detector Scientist
	Mr. Grant Blue BATC COS Software Manager

Approved By:

Dr. Oswald Siegmund, University of California, Berkeley Detector Principal Investigator	Date
Dr. James Green, University of Colorado, Boulder HST-COS Principal Investigator	Date
Dr. Kenneth Brownsberger, University of Colorado, Boulder HST-COS Software Scientist	Date

TABLE OF CONTENTS

TABLE OF FIGURES

1 SCOPE

1.1 IDENTIFICATION

This DCE FSW Requirements Document (COS-UCB-004) is the top-level specification that establishes the requirements governing the development of the FUV Detector Control Electronics Flight Software (DCE FSW) Computer Software Configuration Item (CSCI) for the Cosmic Origins Spectrograph (COS) instrument. The developer of the FUV Detector Subsystem is the Experimental Astrophysics Group (EAG) at the Space Science Laboratory, University of California, Berkeley.

This document is prepared in accordance with the requirements of a subcontract. This document satisfies the subcontract requirements for Flight Software Documents, DCE FSW Computer Software Configuration Item (CSCI). It is written using an example document provided by BATC as a guide.

1.2 DOCUMENT OVERVIEW

This DCE FSW Requirements Document defines the requirements that have been allocated to the COS DCE FSW. The organization of this document is outlined below in a description of the contents of each of the ensuing sections.

Section 1 defines the scope of this document and introduces the DCE FSW.
Section 2 lists documents that have been directly or indirectly referenced by this document.
Section 3 contains a glossary of document acronyms.
Section 4 presents a top-level functional, performance and interface overview for the DCE FSW.
Section 5 describes the detailed requirements for each of the DCE FSW components.
Section 6 describes the FUV Detector Control Electronics hardware and software environments.

1.3 COS FLIGHT SOFTWARE OVERVIEW

Within the FUV Detector Subsystem, the DCE FSW provides the FUV detector with the computational, interface, and memory resources necessary for performing overall FUV detector control tasks. Commands are accepted and processed by the DCE FSW. The DCE FSW outputs engineering telemetry data (housekeeping). Note that while the DCE FSW controls hardware that generates Science Data, the DCE FSW sees only counts and not location information for each photon event. Science Data does not pass through the DCE FSW, but is output directly in FUV detector hardware.

The DCE FSW is the brain of the FUV Detector Subsystem, with an internal interface to the TDC, HVPS, and LVPS, known collectively as the Electronics Interface. The FUV Detector Subsystem includes a number of temperature, voltage, current, and other sensors that are converted to a digital format and reported by the DCE FSW in regular housekeeping updates. The DCE FSW will implement a command interface for the MEB, permitting direct control of the FUV detector. The DCE FSW will also perform checking of some limits and other self-tests.

1.4 RELATIONSHIP TO OTHER DOCUMENTS

This COS DCE FSW Requirements Document establishes the CSCI requirements that will be used to verify the functionality of the COS DCE FSW. Software requirements herein were derived from existing FUSE software and modified to support an interface with the MEB. Requirements traceability will be documented in matrix format in the Software Test Plan. Many details of FUV detector operations are described in the ICD and the Software User's Guide. The organization of the Command and Housekeeping interface to the MEB is described in detail in the FUV detector ICD.

2 APPLICABLE DOCUMENTS

The following documentation relates to the DCE FSW requirements as listed in this document. These documents provide additional details concerning the design and implementation of features required of the DCE FSW.

2.1 COS RELATED DOCUMENTATION

Interface Control Document, FUV Detector Subsystem, COS-UCB-001
Configuration Management Document, FUV Detector Subsystem, COS-UCB-003
FUV Detector Software Configuration Management Plan, COS-UCB-005
Appendix to Software User's Guide, BATC
FUV Detector Software Test Plan, COS-UCB-008
FUV Detector Software Test Procedures
COS Control Section Flight Software Requirements Document

3 LIST OF ACRONYMS AND ABBREVIATIONS

Aux	Auxiliary Power
COS	Cosmic Origins Spectrograph
BATC	Ball Aerospace & Technologies Corp.
CRC	Cyclic Redundancy Check
CSC	Computer Software Component
CSCI	Computer Software Configuration Item
DCE	FUV Detector Control Electronics
EAG	Experimental Astrophysics Group, Space Sciences Laboratory, UC Berkeley
FSW	Flight software
FUSE	Far Ultraviolet Spectrographic Explorer
FUV	Far Ultraviolet
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HST	Hubble Space Telescope
HV	High Voltage
HVPS	High Voltage Power Supply
Hz	Hertz, cycles per second
ICD	Interface Control Document
ICE	In-Circuit Emulator
I/O	Input/Output
I&T	Integration & Test
LVPS	Low Voltage Power Supply
MEB	Main Electronics Box
NASA	National Aeronautics and Space Administration
PROM	Programmable Read-Only Memory
PHD	Pulse Height Distribution
RAM	Random Access Memory
ROM	Read-Only Memory
SEU	Single Event Upset
SRD	Software Requirements Document
TDC	Time-to-Digital Converter
UCB	University of California, Berkeley

4 DCE FLIGHT SOFTWARE OPERATIONAL OVERVIEW

This section provides an operational overview of each of the functional, performance, and interface requirements that have been allocated to the FUV Detector Control Electronics (DCE) Flight Software (FSW) for the FUV Detector Subsystem. The top level DCE FSW overview presented in this DCE FSW Flight Software Requirements Document are repeated in this section of this document to provide a continuity to the CSCI level. The CSCI level testable requirements for the DCE FSW are presented in Section 5 of this Software Requirements Document (SRD).

The FUV Detector Control Electronics is the main control and coordination center for the FUV Detector Subsystem. The flight software being developed by EAG for the COS program will reside in the FUV Detector Control Electronics (DCE). The DCE FSW provides the major command and housekeeping functions for FUV Detector subsystem.

The FUV Detector Control Electronics CSCI will accept and validate incoming command packets, command and coordinate the configuration of the FUV detector door, HVPS and TDC for an observation, collect and format Housekeeping data packets, and perform internal limit checking of critical detector parameters. FUV Detector configuration and observation will be driven by the execution of commands from the MEB, initiated and controlled through command packets accepted by the FUV Detector Control Electronics. No Science Data processing tasks are required within the DCE FSW. Engineering telemetry collected by the DCE FSW is formatted for output to the MEB via the Housekeeping interface.

4.1 DCE FSW FUNCTIONAL OVERVIEW

For the DCE FSW to perform the top-level functions allocated to it, it must provide the following capabilities:

1) Initialize DCE and FUV detector electronics.
2) Receive and process command packets and upload data.
3) Configure the FUV detectors and control the FUV detector electronics, including the ramping of HV.
4) Control FUV Detector Subsystem door.
5) Gather and output housekeeping data.
6) Monitor FUV detector protection parameters and maintain the detector in a protected configuration.
7) Perform self-tests.

4.1.1 INITIALIZE DCE AND DETECTOR ELECTRONICS

The DCE FSW will implement an initialization scheme that ensures operation to a known state, while making engineering data available even after an unexpected reset. Information left over in memory after an unexpected event can be very helpful in reconstructing and understanding the event.

On initialization the DCE FSW determines whether it is starting from power-on or from a watchdog reset. In the case of a power-on reset, the DCE makes no assumptions about the state of the FUV detector and sets all controls to a default, inactive state. Memory used for operations, including housekeeping and command channel buffers, code memory, and variables, is initialized to start-up values. Some regions of memory may be left untouched at power-on reset. The power-on reset self-test requires 10 seconds, while the watchdog is being tested. The DCE remains in the boot state, accepting commands and sending housekeeping responses, while executing out of PROM.

In contrast, a watchdog reset will immediately restore control to the boot state FSW executing out of PROM.

Initialization steps include: resetting stack pointer, initializing timers and communications hardware, possibly setting HV to the HV_OFF state; testing for power-on reset; wiggling a reset signal to various detector components; initializing background tasks such as CRC checking on memory regions and HV overcurrent protection; and finally passing control to a boot state main loop that performs command handling and housekeeping response tasks.

4.1.2 COMMAND RECEPTION AND PROCESSING

Activities performed by the FUV Detector Subsystem in support of science observations and detector maintenance tasks are initiated and controlled through the use of command information sent to the DCE FSW from the MEB. The DCE FSW within the FUV Detector Subsystem provides the ability to accept the incoming command packet and perform the required actions indicated by the command opcode. The DCE FSW will implement a commanding structure, which will allow the FUV detector to be commanded at a low level, executing a single function per command packet from the MEB.

4.1.3 OPERATIONAL CONTROL AND COORDINATION

The DCE FSW will operate the FUV detector in two software states: the boot state and the operate state. The boot state will execute a self-test and remain in boot state. Boot state FSW will execute from PROM, and may be designed to avoid dependence on a single external RAM.

In boot state, the DCE FSW will receive commands, but execute only those designated as boot-state commands; and in any case, the DCE FSW will respond with at least one housekeeping packet.

Among the commands supported while in boot state, one command will transfer control to the operate state.

4.1.3.1 Boot State Flight Software

When power is applied to the main electronics of the FUV Detector Subsystem, the FUV Detector Control Electronics embedded processor will begin execution of the boot state flight software. The primary purpose of the boot state software is to perform power-on initialization, to copy the operate state software located in PROM into Random Access Memory (RAM) and then, on command, transfer control to the operate image in RAM. The flight software necessary to perform the boot state software functions will reside in a radiation hardened PROM non-volatile memory area. The functions of the boot state software are:

1) Perform initialization functions, including reset tests and memory initialization.
2) Transfer the code from the PROM into the RAM.
3) Begin execution of the operate state software.
4) Support upload of code to overwrite the default operate code.

4.1.3.2 Operate State Flight Software

After all of the boot state operations are completed, code execution transfers into the operate state. The operate state software performs all FUV detector sensing, control, calibrations and diagnostics. The operate state software must be able to:

1) Configure and operate detectors, including door, HV, and TDC.
2) Collect detector state, memory download, memory upload and diagnostic information.
3) Monitor engineering data for limit checking, perform autonomous shutdown on overlimit.
4) Output engineering housekeeping packets to the MEB.
5) Accept command packets from the MEB

4.1.4 DOOR CONFIGURATION

Reliable and protected configuration of the FUV detector door is a critical factor in supporting the capability of the detector to meet its scientific performance requirements. **Opening the door in air will severely degrade the performance of the FUV detector**. The door must be open for the FUV detector to perform useful science. The DCE FSW will perform the functions necessary to open the door via support electronics:

Specifically, the door will have interlocks to prevent inadvertent powering of the door motor or actuators. Some of these interlocks may be in hardware. At least two separate command packets are required to move the door. A door-stop command, timeout, or DCE reset will stop the door motion by reverting to the reset state: door and actuator power off, door commands disabled.

Additional protection for the door includes an approximately 3-4 minute timeout (exact value TBD), which triggers the door-stop function. The door has a latch used as part of a redundant door opening mechanism. The latch has a sensor that must be monitored by the DCE: when the latch state changes, the door-stop function will be called. The DCE also monitors the Aux current sensor, which indicates the current draw by the door motor and is monitored on a per-second basis. If the Aux current sensor value exceeds a settable current-limit, the stop-door function will be called.

4.1.5 HOUSEKEEPING DATA COLLECTION AND PROCESSING

Insight into the operations and performance of the FUV Detector Subsystem is obtained through the housekeeping data streams. The DCE FSW provides the ability to collect, format, and output the engineering data necessary to achieve the scientific objectives of the FUV Detector Subsystem and to maintain the health and protection of the detector. Detailed requirements for Housekeeping are laid out in section 5.2.3, Command Response.

4.1.5.1 Housekeeping (Engineering Telemetry)

The main insight into the operations of the FUV Detector Subsystem will come through the Housekeeping data. To gain the required visibility into the detector operations, all key detector parameters will be identified and placed into the Housekeeping data stream to the MEB. A detailed description of the Housekeeping data format will be documented in the ICD.

In general, a housekeeping packet includes: echoes for all commanded settings; monitors for various temperature, voltage, current, and other sensors; command packet counters and photon event counters; pulse-height histogram data; self-test and diagnostic information; an array of status flags. Memory download packets will be sent in response to a download command only, after which the regular housekeeping packet will be sent.

4.1.5.2 Science Data

The DCE FSW does not directly control the rate or format of Science Data flowing to the MEB. A detailed description of the science telemetry format is documented in the ICD.

The DCE FSW will have access only to photon event counters and pulse height histogram data. No information about the timing, location or pulse height of individual photon events will be available to the DCE FSW. This SRD levies no requirements upon the Science Data interface to the MEB.

4.1.6 DETECTOR MONITORING, MAINTENANCE & PROTECTION

The DCE FSW will be capable of collecting and monitoring key Housekeeping data items for each of the identified critical FUV detector components. Key detector parameters will be monitored at a rate that is sufficient to allow DCE FSW to be capable of performing predetermined corrective actions when a protection violation is discovered.

Most engineering telemetry are simply reported in housekeeping. Some engineering telemetry are deemed especially important, like HV, and are checked often; others, like door current, are checked every second in support of door operations. These engineering telemetry are subject to current level over-limit checking. The actual engineering telemetry and levels selected for checking will be designated during detector development.

NOTE: References to protection (as a synonym for “safety”) throughout this document refer to steps taken to prevent degraded detector performance.

4.1.7 SELF-TESTS

The FUV Detector Control Electronics FSW will perform certain self-tests at initialization and during operations. The DCE FSW will report unusual or unexpected events as diagnostic messages. Beyond simple sanity checks in the software design, the DCE FSW will be actively looking for problems such as SEUs in memory or other hardware failures. Active protections include count-rate limit checking and current limit checking. The DCE also performs continuous computation of CRC values for various regions of DCE memory.

4.2 DCE FSW PERFORMANCE OVERVIEW

The DCE FSW will meet the following performance constraints in order to support the operational and performance requirements of the FUV Detector Subsystem.

4.2.1 COMMAND AND HOUSEKEEPING PERFORMANCE

The DCE FSW will support the following performance constraints:

1) The DCE FSW will be capable of processing command packet data from the MEB at least 1 command packet per second. The DCE FSW may process command packets faster, but all command execution and housekeeping packet traffic must complete within one second of receipt of the command packet.

2) The DCE FSW will protect the FUV detector when it has not received a valid command opcode in the last ten seconds.

3) A command packet may be preceded by up to 512 long words of upload data. A command packet consists of long words that may be sent in any order, provided that the command packet long word containing the command opcode is transmitted last.

4) Engineering telemetry data will be output to the MEB interface by the DCE FSW at the rate of up to 512 Housekeeping long words in each command response.

5) Housekeeping channel may also include 512 Memory Download long words transmitted in response to a Memory Download command.

Please refer to the ICD for details concerning communications contents and format. Exact message timing requirements are better described in the ICD section 8.5 Packet Protocols.

4.2.2 ERROR DETECTION

The DCE FSW may detect errors. Among the kinds of errors that may be reported: damaged or otherwise incorrect commands, interlock not set to allow command, some memory region experiences a changed CRC caused by SEU, watchdog timer in 8051 triggered, and some protection limits that trigger HV and door shutoffs.

4.3 DCE FLIGHT SOFTWARE INTERFACE OVERVIEW

The DCE FSW will interface with the detector sensors, the detector door electronics, the detector electronics and the MEB command and housekeeping interfaces. The primary interface requirements supported by the DCE FSW include:

4.3.1 ELECTRONICS INTERFACE

The DCE FSW controls and coordinates the DCE activities by interfacing with the various detector components through the electronics associated with the components. The Electronics Interface connecting the DCE to the TDC, HVPS, LVPS and door is memory-mapped in hardware. DCE Board C also converts all sensor signals, such as temperatures, to digital values. The DCE hardware interfaces to the TDC (digitizer), HVPS and LVPS. The LVPS includes control and sensors for the door.

4.3.2 MEB INTERFACE

Operations of the FUV Detector Subsystem are controlled by the MEB. The DCE FSW provides command and housekeeping processing that is mediated by the MEB with respect to HST. The MEB must verify correct housekeeping responses to commands and report information about the DCE behavior in accordance with HST's constraints.

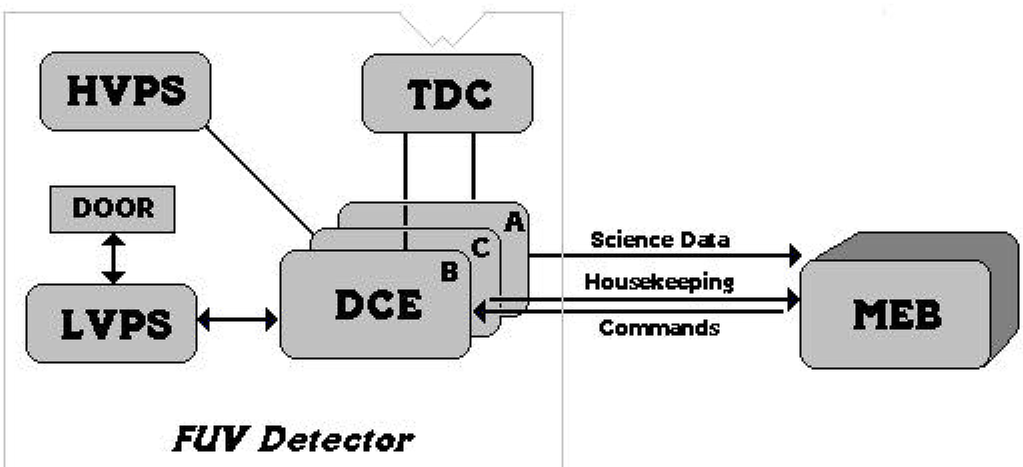

Figure 4-1 FUV Detector Block Diagram

Figure 4-1 above shows that the DCE interfaces with several internal components, and one external host.

5 DCE FSW DETAILED REQUIREMENTS

The DCE FSW is composed of two related software constructs known as the "boot image" and the "operate image". The "boot image" is burned into PROM, and contains initialization code plus "operate image" data that must be relocated to RAM. At power-up or any reset, the "boot image" code executes a self-test and initialization. After initialization, the DCE FSW starts execution of the "operate image" code in RAM. The requirements allocated to the DCE FSW Computer Software Configuration Item (CSCI) are grouped as follows:

1) Detector initialization
2) Command Reception and Processing
3) Detector Operations and Protection
4) Door Control and Protection
5) Memory Management

5.1 DCE FSW Initialization

This section discusses the requirements related to the maintenance, support and general operation of the COS FUV detector. At power-up initialization, the DCE FSW must reset memory to a known state; however, during any other system reset the memory should be preserved so that evidence of activity prior to the reset may be analyzed to determine the cause of the reset. The initialization function therefore forces the DCE into a known state while providing error-detection information in the housekeeping data stream.

5.1.1 DETECTOR INITIALIZATION

FUV detector initialization consists of the steps the DCE FSW must go through to properly setup its operating environment. Initialization steps include configuring the various pieces of DCE hardware, initializing global memory areas and starting execution of the various tasks in the system. This section covers the DCE FSW requirements that deal with resetting the system and causing the DCE FSW to re-initialize.

5.1.1.1 Requirement: Initialize to Boot State After Reset

The DCE FSW shall perform the necessary steps to initialize the DCE FSW to boot state after any reset event.

Comments: Resets are of two kinds: Power-on and watchdog. A watchdog reset is any reset from any source, other than power-on. The power-on reset activity will include the initialization of the interrupt controllers, interval timers and watchdog controller, and initialization of the command and housekeeping memory. In contrast, the watchdog reset immediately restores control to boot state.

5.1.1.2 Requirement: Distinguish Between Power-up and Watchdog Resets

The DCE FSW shall indicate the cause of the reset to the MEB upon recovery from the hardware/software reset.

Comments: The DCE FSW will distinguish between Power-up and any other reset. It may not be possible to determine the exact source of a reset, but it is important to know whether the DCE memory contains further evidence of activity prior to a just-occurred reset.

5.1.1.3 Requirement: Commands To Reboot DCE FSW

The DCE FSW shall process a command to reboot the DCE FSW.

Comments: This software-reset command will be provided in case a software reboot is needed or desired. The software reset command will cause a watchdog reset causing the boot code to start executing.

5.1.1.4 Requirement: Memory Initialization On Power-Up Only

On power-up only, the DCE FSW shall initialize memory to a known state. All variables, housekeeping, any other memory items without another specified default state shall be initialized to zero.

Comments: Ensure that otherwise uninitialized variables are set to zero just once at power-up, and never again, thus preserving state information after FSW reset.

5.1.1.5 Requirement: Code In PROM (Non-Volatile Memory)

The DCE FSW shall reside in non-volatile memory.

Comments: The DCE FSW must be contained in a protected environment such that it is not lost when the FUV Detector Control Electronics hardware is powered down. The boot code and the operate code will be stored in PROM.

5.1.2 ERROR DETECTION

The ability to log the errors is important in troubleshooting problems and fixing them. The following are the requirements associated with the DCE FSW 's ability to recognize and process errors in the system

5.1.2.1 Requirement: Watchdog

The Watchdog shall reset the DCE FSW if not serviced. The DCE FSW shall be designed such that only valid command packets from the MEB will feed the watchdog and prevent an autonomous reset.

Comments: Watchdog resets will be enabled only after the first command packet after any reset, thereby preventing continuous resets when the MEB is offline. Once the watchdog is enabled, the DCE will expect a valid command opcode from the MEB within ten seconds. The Watchdog, if not serviced within 10 seconds, initiates the autonomous reset.

5.1.2.2 Requirement: Command to Disable/Enable Watchdog

The DCE FSW shall accept a command packet to disable and enable the watchdog function.

Comments: The watchdog will be entirely disabled in hardware on command. When enabled, the DCE FSW will feed the watchdog only when an op-code is received on the command channel.

5.1.2.3 Requirement: Capability To Log Diagnostics

The DCE FSW shall provide the capability to log diagnostics during execution of the flight software.

Comments: The DCE FSW will log the system errors encountered during execution to an error log. The diagnostic list reports the latest diagnostic at the top of a list of accumulated diagnostic reports. Up to 32 diagnostics can be reported in any housekeeping packet.

5.1.2.4 Requirement: HST Error Logging

The DCE FSW shall provide the capability to log errors detected during execution of the flight software.

Comments: The DCE FSW will log the errors encountered during execution to an error log that will be included in the housekeeping packet. Errors are defined as all unexpected conditions.

5.1.2.5 Requirement: HST Error Format

The DCE FSW error reporting shall consist of an error identification and up to 16-bits of supporting data, if applicable, for each error encountered.

Comments: The format of the error reporting will be defined in the COS FUV Detector ICD. The errors will be reported in the order received since the last housekeeping packet. Up to four HST Error reports will be available in a housekeeping packet; if more than four HST Error reports occur, then the fact is indicated by the presence of a fifth Error report in the housekeeping packet. The five Error reports are reset to zero after every housekeeping packet is sent.

5.2 Command Reception And Processing

The DCE FSW must provide a method for the successful and timely reception and interpretation of command packets from the MEB. The DCE FSW is required to properly accept and process command packets and uploaded data from the MEB, which is the method by which the FUV detector hardware and software components can be commanded and controlled.

5.2.1 COMMAND RECEPTION

The following are the requirements concerning the ability of the DCE FSW to provide for the successful and timely reception of command packets from the MEB.

5.2.1.1 Requirement: Error-Detecting Command Format

The DCE FSW shall have an error-detecting format imposed on the design of the command packet buffer.

Comments: Catch command errors of incorrect format, such as data error and computer or human error. Valid, executable command packets must be passed with some redundant information that is checked for correctness before the command is executed. Only command packets having a valid format may be executed. All command packets having a validated format may be executed.

5.2.2 COMMAND RATE

Command packets are expected from the MEB on a regular basis. The DCE FSW must meet the following command performance requirements:

5.2.2.1 Requirement: Command Rate: One Per Second

The DCE FSW shall accept a command packet from the MEB at least once per second.

Comments: The DCE FSW will not depend on the MEB to send commands at any particular frequency, but must be able to handle an incoming command packet at least once per second.

5.2.3 COMMAND RESPONSE

Insight into the operations and performance of the FUV Detector Subsystem is obtained through the Housekeeping stream. The DCE FSW provides the ability to collect, format and output the engineering data necessary to achieve the scientific objectives of the FUV Detector Subsystem and to maintain the health and protection of the detector.

The DCE FSW will report Housekeeping data, monitor limits at the Electronics interface, and record diagnostic messages when self-tests indicate an unusual event in the DCE FSW.
The main insight into the operations of the FUV Detector Subsystem will come through the Housekeeping data stream. To gain the required visibility into the detector operations, all key detector parameters will be identified and placed into the Housekeeping data stream.

Every command, valid or not, will elicit a response from the DCE. If the command is invalid and not executed, the DCE FSW must report the attempt in Housekeeping. The command response may be interpreted as readiness for a new command packet at the DCE. A housekeeping packet contains enough information to determine whether the command packet was executed properly. The DCE FSW must meet the following command performance requirements:

5.2.3.1 Requirement: Housekeeping Response Within One Second

The DCE FSW shall respond to a command op-code within one second of receipt by sending a Housekeeping packet response to the MEB.

Comments: The DCE FSW only and always responds to the MEB with a Housekeeping packet. No command will take more than a second to execute. The command, generated by the MEB, will cause the DCE FSW to write the Housekeeping data message to the MEB.

5.2.3.2 Requirement: Echoes For Command Opcode And Parameters

The DCE FSW shall include in its Housekeeping packet the most recent command op-code, serial number, and parameters.

Comments: Users can verify that the command was properly executed. A command packet is composed of a command op-code, serial number, and parameters.

5.2.3.3 Requirement: Counters For All Commands

The DCE FSW shall report in housekeeping counters for all command packets.

Comments: Counters include those for commands received and commands executed. NOP commands are not counted as received or executed. There is also a packet counter that is incremented on receipt of any command op-code. Counters are helpful in verifying that all scripted commands were executed, and in detecting unexpected commanding from any source.

5.2.3.4 Requirement: PHD Handling

The DCE FSW shall place Pulse Height Distribution data into the Housekeeping data stream output to the MEB interface.

Comments: PHD data is two 128-bin word-sized histograms accumulated by the FUV digitizer electronics. The PHD bins are cleared every second, after the contents are copied to Housekeeping. Every housekeeping packet contains PHD data accumulated since the previous packet.

5.2.4 SPECIAL COMMANDS

5.2.4.1 Requirement: Command to Jump Anywhere in Code

The DCE FSW shall accept a command packet to jump to any executable code address.

Comments: This is also known as a GOTO command, and is used to start execution of uploaded code.

5.3 Detector Operations And Protection

The FUV Detector Subsystem operates two detectors named A and B. To support the goal of maintaining optimum detector performance over the life of the instrument, the DCE FSW will provide the ability to configure each detector along with its associated detector interface electronics based on user commanded configuration information. The DCE FSW provides the capability to set each of the detectors and their associated interfaces to the proper configuration.

5.3.1 DETECTOR OPERATIONS

To aid in maintaining optimum FUV detector performance over the life of the instrument, the DCE FSW will provide the ability to issue instructions to select detector gains, offsets, biases, clock voltages, and any other variable detector parameters.

5.3.1.1 Requirement: HV Ramping Function

The DCE FSW shall provide the capability to control HV with an autonomous ramping function with command parameters that control the rate of HV ramping.

Comments: Ramping schemes are configurable over a range of ramping rates and the FSW will provide the capability to modify any default settings. Ramp command parameters include destination HV setting, and the time in which to achieve the HV setting (ramp rate). The DCE FSW will accept a command packet to disable HV Ramping. . A complete scenario for ramping HV may be found in the User's Guide.

It is understood that the DCE ramping function may have parameters, such as the step size of the step function that will not be commandable. If experience with the COS FUV detector requires a different ramping procedure than can be supported by the HV ramping function implemented in the DCE FSW, changes to the DCE FSW, CS FSW, commanding procedures or some combination of the three will be required.

5.3.1.2 Requirement: Commands To Set Detector Digitizer Gains And Offsets

The DCE FSW shall process commands to set FUV detector gains, offsets, and other digitizer parameters as required by detector hardware.

Comments: The DCE FSW must setup the digitizers on command. The full set of digitizer settings is TBD, so this requirement is intended to cover the full set of controls to the FUV detector electronics, excluding the door.

.

5.3.1.3 Requirement: Commands To Control High Voltage

The DCE FSW shall accept commands to turn on and ramp and set HV.

Comments: An interlock scheme is required to prevent accidental increase of HV, while allowing HV to be turned down or off with a single command packet.

5.3.2 DETECTOR PROTECTION

The DCE FSW provides for global bright-object protection and overcurrent protection. These capabilities can be enabled or disabled by commanding from the MEB to the DCE FSW. Thresholds can be commanded from the MEB to the DCE FSW. If this level of protection is enabled and the threshold is exceeded, the detector HV will be turned off by the DCE FSW. The DCE FSW will also set the appropriate status bit to indicate that the detector HV has been turned off.

The DCE FSW does not perform Local Rate Monitoring.

5.3.2.1 Requirement: Commands To Enable/Disable Global Rate Monitoring

The DCE FSW shall accept a command to enable/disable detector bright-object Global Rate Monitoring.

Comments: This command may be constructed by setting a command parameter to zero to disable, or any other value to enable Global Rate Monitoring. The command parameter specifies the integration time applied to Global Rate Monitoring: if the time is 0, the function is disabled; otherwise integration time is the interval over which we are checking for a level of excess counts. Global Rate Monitoring is also known as Count Rate Protection (CRP).

5.3.2.2 Requirement: Commands To Set Global Rate Monitoring Parameters

The DCE FSW shall accept commands to set threshold limits for detector bright-object Global Rate Monitoring.

Comments: Global Rate Monitoring parameters include integration time, count level (together they define the rate). The over-limit response is to lower the HV setting to a preset level, which is also a settable parameter to Global Rate Monitoring. There is also an optional recovery timer, disabled by default, that will autonomously restore HV after a set delay.

5.3.2.3 Requirement: HV Current Over-Limit Checking

The DCE FSW shall turn off High Voltage when a preset current level is exceeded.

Comments: The requirement is to catch persistent spikes that might be damaging the FUV detectors. The DCE FSW must turn off the High Voltage when a current level has exceeded its threshold during the routine monitoring of the HV and Aux current levels

5.3.2.4 Requirement: HV Interlocks

The DCE FSW shall require two separate commands to activate functions that turn on or increase power to the HV components of the FUV detector.

Comments: This scheme ensures that turning up HV is not an accident. At minimum, two separate commands are required to increase HV at the detector. Command interlock is not required to turn down or off HV.

5.3.2.5 Requirement: Take Appropriate Protection Measures If Limit Exceeded

The DCE FSW shall take appropriate protection measures if the limit conditions for any designated items are exceeded more than the specified allowable number of consecutive times.

Comments: Each item to be limit checked will have stored, along with its high and low limits, the maximum number of consecutive times the item's value may go out of the limits boundaries before an error is reported. Appropriate measures may include powering off HV or Aux. The DCE FSW will always issue a diagnostic report warning of action taken.

5.3.2.6 Requirement: Command Enable Or Disable Limit Checking

The DCE FSW shall accept commands to enable or disable the Housekeeping data limit checking function.

Comments: Default configuration will be to have limit checking enabled. DCE may command limit checking of monitors enabled or disabled. Limit checking applies only to current and Aux current samples.

5.4 Door Control And Protection

In support of maintaining the highest level of door protection possible, the MEB will command the movement of the door using a sequence of independent command packets. The DCE FSW will provide the capability to command the configuration of the door and provide Housekeeping information adequate to determine the position of the door and the state of its associated electronics.

5.4.1 DOOR CONTROL

The DCE FSW must enable door commands, select door direction, and power the door on command. No action is required to stop the door. If the door should fail to open, the actuators may be used as an auxiliary means to open the door. Once the actuators have popped the door latch, it may be reset by driving the door motor. The door has an endswitch override capability to support the relatching of a door opened with actuators. The DCE FSW must meet the following command performance requirements:

5.4.1.1 Requirement: Door Direction
The DCE FSW shall accept a command to select the door direction.

Comments: Choices are Open, Close, and Protect ("safe," as referred-to in the ICD). Door direction is initialized to Protect ("Safe") and must be selected as Open or Close. Door endswitches prevent the door from driving against its endstop. Endswitches may be overridden, allowing door to drive without regard to endswitches.

5.4.1.2 Requirement: Door Power
The DCE FSW shall accept a command to turn on and off door power.

Comments: Door power can only be turned on by command. Door power may start door motion, assuming those prior commands for enabling and selecting the door direction have been processed.

5.4.1.3 Requirement: Actuator Power
The DCE FSW shall accept a command to turn on auxiliary actuators to force the door open.

Comments: Actuators are the last-ditch method of opening the door and should be done only if the door motor fails to open the door.

5.4.1.4 Requirement: Door Override
The DCE FSW shall accept a command to override door endswitches.

Comments: This command allows the door motor drive to be forced against the actuator latch, allowing the door to be relinked to its drive.

5.4.1.5 Requirement: Settable Door Current Limit
The DCE FSW shall accept a command to set door current (AuxI) limit.

Comments: The default current limit will be set low enough to prevent unplanned door operation. When the limit is exceeded, the DCE FSW will turn off Aux power.

5.4.2 DOOR PROTECTION

Moving the door has the potential to severely degrade the FUV detector, so door commands are subject to interlocks and special restrictions. The door actuator is a backup means to open the door in case the door motor fails. The actuator disconnects the door linkage and allows the door to open with a preloaded spring. There is a latch sensor that detects the state of the door linkage. The DCE FSW must meet the following command performance requirements:

5.4.2.1 Requirement: Door Timeout
The DCE FSW shall reset door power and disable door commands after an interval without door commands.

Comments: This is a means of triggering the door-stop function that functions as a backup to detector door endswitches. The door timeout will stop the door and turn off the door enable flag to prevent subsequent door commands from affecting the door. Stopping the door includes removing power to both door motor and actuators. Door motion takes up to four minutes and is the chosen door timeout value.

5.4.2.2 Requirement: Door Enable
The DCE FSW shall not process a door command unless preceded by a door enable command.

Comments: We are attempting to prevent spurious door commands from inadvertently turning on the door. When executing other door commands, the door commands must be recently enabled. The door enable times out with the door timeout, and prevents any additional door commands from executing.

5.4.2.3 Requirement: Aux Current Checking During Door Motion

The DCE FSW shall monitor AuxI current while the door is opening, and shut off power and enable to the door if the AuxI current monitor exceeds the settable limit specified in section 5.4.1.5 above.

Comments: If a door endswitch fails to stop the door at the end of its travel, or if the door motor is otherwise unable to move the door, the first clue will show up in the AuxI monitor. If an overcurrent is detected while moving the door, then the DCE FSW will power off the door motors.

5.4.2.4 Requirement: Latch Checking

The DCE FSW shall perform latch checking to turn off door motion and actuators in the event of a change of state in the latch position.

Comments: This is actually a design detail that separates other door functions from the detection of an event that will in any case stop the door. If the latch opens, it probably means the actuators have performed their function, so the actuators are turned off. If the latch closes, we are probably recovering from an actuator opening by driving the door motor, so the DCE FSW will shut off the door motor and reset the override control. A complete scenario for operating the door may be found in the User's Guide.

5.5 Memory Management

This section addresses the requirements related to the management of the memory and information within the DCE FSW. The management of memory refers to the ability of the DCE FSW to accept data loads from the MEB and place the data into memory, to download memory to the MEB, to verify correct memory transfers, to detect SEUs in memory, and to provide HST memory monitors.

5.5.1 MEMORY UPLOADING

In order for updates to be made to the DCE memory, there must be a method for uploading new data values and code segments into DCE memory through the MEB. The DCE FSW will be able to take uplinked data values and load them into specified areas of memory. In addition, the FSW will provide the capability to copy various areas of memory to other areas of memory. This will allow an operate image to be copied to RAM so that it can be executed. The following are the requirements associated with memory loading and copying within the DCE.

5.5.1.1 Requirement: Process Memory Copy Commands

The DCE FSW shall accept a command to upload data into DCE memory, that is to copy data from DCE data transfer memory area to a specified address in the DCE's main memory.

Comments: The DCE will support the capability of uploading code and data. Transferred data may to be verified for correctness (see 5.5.1.3). Uploads failing the CRC-check will not be loaded into memory as commanded, unless the CRC-checking requirement has been disabled (5.5.1.4).

5.5.1.2 Requirement: Capability To Upload Data

The DCE FSW shall provide the capability to upload code and data by receiving upload and storing the data in a transfer memory pending receipt of the command described in 5.5.1.1 above.

Comments: The flight software will allow data coming from the MEB to be loaded into a small section of data transfer memory only. Once there, the data can be transferred to other areas of memory. Data may be executable code when loaded to the appropriate memory locations.

5.5.1.3 Requirement: Check Upload Integrity

The DCE FSW shall provide the capability to verify that code and data to be moved into RAM is correct.

Comments: A CRC check of data to be transferred is sufficient to ensure that no bit-errors have been introduced during transmission.

5.5.1.4 Requirement: Command To Disable/Enable CRC Checking On Upload

The DCE FSW shall accept a command to disable or enable CRC checking on upload data.

Comments: The DCE FSW will by default ignore an upload command if the CRC calculated on the upload data does not match that CRC specified as a parameter to the upload command. This requirement ensures that the MEB can upload unverified data to the DCE memory.

5.5.2 Memory Downloads

The DCE FSW will provide the ability to download memory data. The same command may be used to specify the memory region to be downloaded, compute the CRC of the region, and transmit the data over the Housekeeping channel. The following are the DCE FSW requirements associated with the downloading of data:

5.5.2.1 Requirement: Process Memory Download Commands

The DCE FSW shall process Memory Downloading commands.

Comments: The DCE FSW will compute a CRC on the region to be downloaded and includes the computed value in Housekeeping.

5.5.2.2 Requirement: Download Data Timing

The DCE FSW shall transmit the selected download data.

Comments: Download data can be transmitted as soon as processed. The data is transmitted over the Housekeeping channel on receipt of the download command and before the usual housekeeping response to a command. See the ICD for detailed timing information.

5.5.3 Error Detection

5.5.3.1 Requirement: CRC Background Checking On Memory Regions

Changes to code space shall be detected by the DCE FSW.

Comments: The DCE FSW can detect SEUs and other activity in code memory. The preferred method involves computing a CRC value. If the computed CRC differs from previously computed values, some location in that region has changed, and the fact will be reported as a diagnostic message. The following regions must be CRC-checked:

- RAM: Code memory
- PROM memory

5.5.4 Memory Monitors

5.5.4.1 Requirement: HST Memory Monitors in Housekeeping

The DCE FSW shall support 8 HST memory monitors in the housekeeping packet.

Comments: HST memory monitors consist of housekeeping long words that report the contents of memory locations within DCE memory. HST memory monitors allow the contents of any readable location in DCE memory to be continually sent out in housekeeping packets. The reports are automatically updated with each housekeeping packet. Housekeeping packets must also include the list of memory addresses and indicators of the type of memory specified. Exactly 8 memory monitors are required. Memory monitors point to 8-bit values.

5.5.4.2 Requirement: HST Memory Monitor Commanding

The DCE FSW shall accept commands to allow assignment of addresses to memory monitors.

Comments: Memory monitor commands are used to change the addresses assigned to the memory monitors. Command parameters include a memory monitor index (0..7), the address of the memory to be monitored, and a memory type, one of: internal data, external data, or external code. The three memory types reflect 8051 architecture.

6 HARDWARE AND SOFTWARE ENVIRONMENTS

The following sections summarize the hardware and software environments in which the DCE FSW will reside and operate. Also listed are software tools that are part of the development environment.

6.1 HARDWARE ENVIRONMENT

The following hardware items are the major hardware components that together form the hardware environment in which the DCE FSW will reside:

ITEM	DESCRIPTION	COMMENTS
Microprocessor	UT69RH051 (rad-hard 8051FX)	16 MHz
PROM	16 Kbytes	Boot code and operational code image
RAM	32 Kbytes	Operational code image and data
Low RAM	16 Kbytes	Command and Housekeeping data, including data transfer areas; may contain interrupt service code

6.2 SOFTWARE ENVIRONMENT

The following software items are the software packages that together form the software environment in which the DCE FSW will be developed and reside:

ITEM	DESCRIPTION	COMMENTS
Configuration Manager	Pkzip	Every tested version saved
8051 Assembler	Archimedes A51	Archimedes
Linker	Archimedes L51	Archimedes
Object-to-Hex	Archimedes OH51	Archimedes
In-Circuit Emulator	High-Tex ICE	High-Tex
Hex2cmd	Creates upload script	EAG
Hexmv	Moves load addresses to PROM space	Required for creating PROM burnable code images.