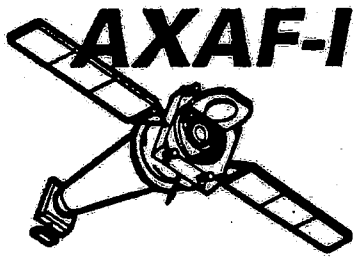
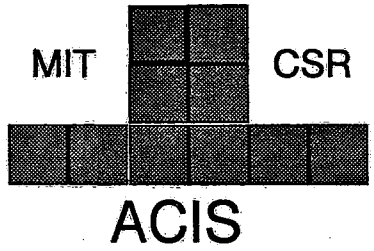
CSR

36-01104-01
September 29, 1994
NAS8-37716
DR DM07





Advanced X-ray Astrophysics Facility

AXAF - I CCD Imaging Spectrometer

ACIS Science Instrument Software Fault Tolerance and Failure Modes and Effects Analysis

Submitted to:

George C. Marshall Space Flight Center
National Aeronautics and Space Administration
Marshall Space Flight Center, AL 35812

Submitted by:

Center for Space Research
Massachusetts Institute of Technology
Cambridge, MA 02139

AXAF-I CCD Imaging Spectrometer
(ACIS)

ACIS Science Instrument Software Fault Tolerance and Failure Modes and Effects Analysis

36-01104-01

DR DM07

Contract # NAS8-37716

September 29, 1994

Submitted to:

George C. Marshall Space Flight Center
National Aeronautics and Space Administration
Marshall Space Flight Center, AL 35812

Submitted By:

Massachusetts Institute of Technology
Center for Space Research
77 Massachusetts Avenue
Cambridge, MA 02139

Approvals:

Dr. Peter Ford
Software Project Manager
Massachusetts Institute of Technology

Philip J. Gray
Project Manager
Massachusetts Institute of Technology

CSR

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CENTER FOR SPACE RESEARCH
CAMBRIDGE, MASSACHUSETTS 02139

REVISION LOG

TITLE:
ACIS Science Instrument Software Fault Tolerance and Failure Modes and Effects Analysis

DOC. NO.
36-01104-01

Revision	Date (mm/dd/yy)	ECO No.	Page(s) Affected	Reason	Approval
01	9/29/94	-	All	Initial Release for Software PDR	

Table of Contents

ACIS Science Instrument Software Fault Tolerance and Failure Modes and Effects Analysis

MIT Center for Space Research

36-01104-01

September 29, 1994

1.0 Introduction

The AXAF-I CCD Imaging Spectrometer (ACIS) Science Instrument Software is being developed by the Massachusetts Institute of Technology, Center for Space Research (MIT-CSR) as part of the ACIS Digital Processor Assembly (DPA). The DPA resides on-board the Advanced X-ray Astrophysics Facility - Imaging (AXAF-I). The DPA Science Instrument Software is responsible for acquiring and processing image data from the ACIS CCD Imaging Spectrometer and transferring the processed data to the AXAF-I Command and Telemetry Unit (CTU), which is then responsible for sending the information to the ground.

1.1 Purpose

The ACIS Science Instrument Software Fault Tolerance and Failure Modes and Effects Analysis (FT&FMEA) defines the degree of fault tolerance, effect and criticality of the instrument software, and defines the means by which the software detects and handles the defined faults. All faults analyzed in this document are identified and described in the ACIS instrument-level FMEA.

NOTE: At this time, no instrument-level failures have been documented in the instrument FMEA which affect the software. As a result, this document is currently serving only as a template. As the instrument FMEA is further refined, any identified failures which affect the software will be analyzed and incorporated into this document.

1.2 Scope

This document applies to the design of the ACIS DPA Science Instrument Software. It does not provide information for the Ground Support Software (GSS), which is maintained separately as part of the Electronic Ground Support Equipment (EGSE).

This document supplies information applicable to the software portion of SPA04, and to DM07 from MM8075.1.

By mutual agreement, MSFC Software Management and Development Requirements Manual MM8075.1 which supersedes MA-001-006-2H, forms the basis for this plan.

1.3 References

TABLE 1. Reference Documents

Part Number	Version	Title
MSFC MM 8075.1	January 22, 1991	MSFC Software Management and Development Requirements Manual
MIT-CSR 36-02402	01	ACIS SIS Preliminary Design Specification
MIT-CSR 36-01406	01	ACIS Failure Modes and Effects Analysis

2.0 Overview

The ACIS Science Instrument Software (SIS) Fault Tolerance and Failure Modes Effects Analysis (FMEA) is derived from the ACIS System Failure Modes and Effects Analysis document. The System FMEA identifies and defines each hardware failure which the software must detect and manage.

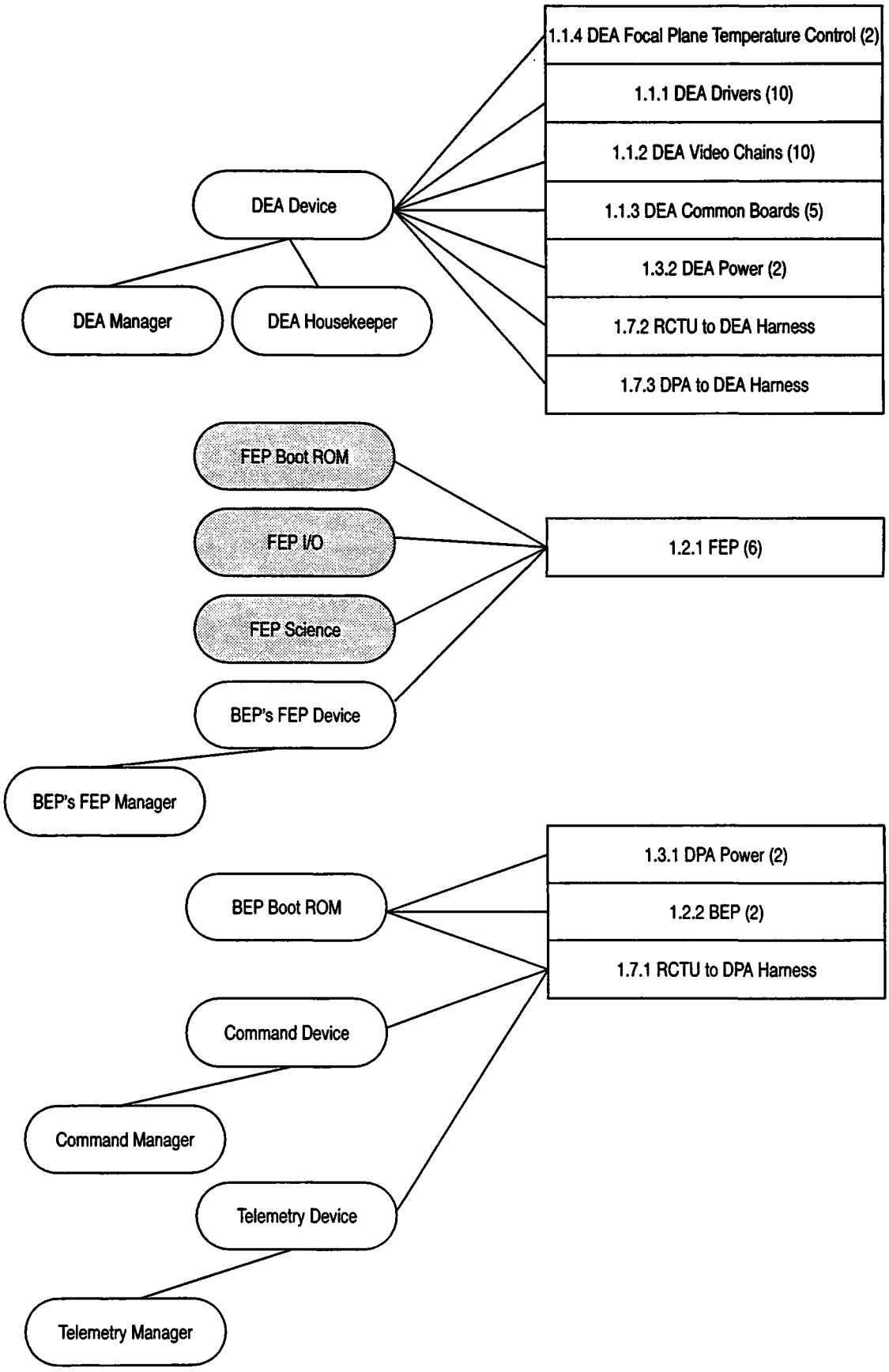
The following sections provide an overview of the software/hardware interfaces, a list of assumptions and ground rules in effect when performing the analysis, definitions of criticality levels and degrees of fault tolerance.

The remaining sections are grouped by hardware subsystem, as identified by the System FMEA. Each section contains a list of hardware failure definitions, with explanations as to how the failure is to be detected and reacted to by the software.

2.1 Hardware/Software Interface Overview

The ACIS SIS software is organized into layers. A single layer is devoted to the software hardware interfaces. Within this layer, each hardware interface, or group of related interfaces are managed by a single software unit. Figure 1 illustrates the software/hardware interfaces and assigns primary responsibility of the interface to one or more software units. The hardware elements are specified down to the level identified in the System FMEA. At this level of granularity, several software elements may be responsible for a single System-level hardware element. Hardware which does not affect a hardware/software interface is not shown. In the figure, boxes represent a hardware element as identified in the System FMEA, ovals represent a software unit, lines between a hardware element and software unit indicate a direct hardware/software interface, and lines between software units represent cases where a software unit has indirect connections to the hardware subsystem and may have fault detection/management responsibilities. Shaded ovals represent software which executes on the Front End Processors. All other indicated software executes on the Back End Processor.

FIGURE 1. Hardware/Software Interface Block Diagram



2.2 Assumptions and Ground Rules

This section lists the assumptions and ground rules in effect during this analysis.

1. The system design ensures that the software cannot damage the science instrument or crew by issuing any hardware command or by not responding in time to a hardware condition.
2. The system design ensures that the software cannot exhaust any consumable resource (such as power) by issuing any hardware command or by not responding in time to a hardware condition.
3. All analysis will performed as a result of failure conditions specified in the ACIS System FMEA. Other types of failures will not be addressed in this document.

2.3 Criticality Level Definitions

This section lists the criticality levels, as defined in MM8075.1 Section 2.2.2.7.2.c:

- Criticality 1 (C1) - Crew Safety. A failure which can result in the loss of system, system element, or flight/ground crew.
- Criticality 2 (C2) -Mission Critical. A failure which can result in the loss or suspension of mission operational capability.
- Criticality 3 (C3) - Mission Support. All other kinds of failures.

Given the assumptions listed in Section 2.2, all failures described in this document have a level of Criticality 3. At worst, any single fault specified in this document may result in the loss of part of the science data.

2.4 Fault Tolerance Level Definitions

This section lists the fault tolerance levels, as defined in MM8075.1, Section 2.2.2.7.2.d:

- F0 - No fault tolerance provided by the software.
- F1 - One level of fault tolerance provided by the software. The software element is capable of sustaining a single fault.
- FM - Multiple levels of fault tolerance provided by the software. The software element is capable of sustaining multiple faults.

3.0 DEA Subsystem

This section describes the software responsibilities concerning defined failures within the Detector Electronics Assembly.

3.1 DEA Drivers

3.1.1 <Name of Failure>

Specify name of the failure, the section number and failure id used within the instrument FMEA.

Specify the criticality of the failure and fault-tolerance implemented within the software.

3.1.1.1 Description of Failure

Describe the failure and how it affects the hardware/software interface

3.1.1.2 Affected Software Element(s)

List the affected software design elements.

3.1.1.3 Detection of Failure

Describe how the software element(s) detects the failure.

3.1.1.4 Software Response

Describe how the software indicates and responds to the failure. Provide flow-charts or psuedo-code if necessary.

3.2 DEA Video Chains

3.3 DEA Common Boards

3.4 DEA Focal Plane Temperature Controller

3.5 DEA Power

3.6 RCTU to DEA Harness

3.7 DPA to DEA Harness

4.0 DPA Subsystem

This section describes the software responsibilities concerning defined failures within the Digital Processor Assembly.

4.1 Front End Processors

4.1.1 <Name of Failure>

4.1.1.1 Description of Failure

4.1.1.2 Affected Software Element(s)

4.1.1.3 Detection of Failure

4.1.1.4 Software Response

4.1.1.5 Results

4.2 Back End Processors

4.3 DPA Power

4.4 RCTU to DPA Harness