

520-CD-001-002

EOSDIS Core System Project

Software Critical Items List for the ECS Project

Final

March 1995

Hughes Applied Information Systems
Landover, Maryland

Software Critical Items List for the ECS Project

Final

March 1995

Prepared Under Contract NAS5-60000
CDRL Item 093

SUBMITTED BY

<u>Peter G. O'Neill /s/ for</u>	<u>3/17/95</u>
Marshall A. Caplan, Project Manager	Date
EOSDIS Core System Project	

Hughes Applied Information Systems
Landover, Maryland

520-CD-001-002

This page intentionally left blank.

Preface

This document is a formal contract deliverable with an approval code 2. As such, it does not require formal Government approval, however, the Government reserves the right to request changes within 45 days of the initial submittal or any subsequent revision. Changes to this document shall be made by document change notice (DCN) or by complete revision.

Once approved, this document shall be under ECS Project Configuration Control. Any questions should be addressed to:

Data Management Office
The ECS Project Office
Hughes Applied Information Systems
1616 McCormick Dr.
Landover, MD 20785

This page intentionally left blank.

Abstract

This document identifies those Computer Program Configuration Items (CPCIs) that have a "critical" command, control, or data receiving/storage function. A Critical Software Item is by definition a software system/subsystem where "there is the risk of a malfunction resulting in damage to or loss of the flight hardware or the mission, including inability to produce or irretrievable loss of Essential Data Products." The ECS will control a constellation of flight hardware and will receive an unprecedented amount of data. This document presents a high level analysis of this system specifically produced to isolate the software components in the critical data paths to and from the flight hardware, and the storage of essential data products.

The goal of the analysis this document presents is to produce a system that protects the large investment in resources made in this system.

Keywords: Software Critical Item List

This page intentionally left blank.

Change Information Page

List of Effective Pages			
Page Number		Issue	
Title			Final
iii through xii			Final
1-1 and 1-2			Final
2-1 and 2-2			Final
3-1 through 3-4			Final
4-1 through 4-18			Final
5-1 through 5-4			Final
AB-1 through AB-4			Final
GL-1 and GL-2			Final
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
520-CD-001-001	Review Copy	February 1995	
520-CD-001-002	Final	March 1995	

This page intentionally left blank.

Contents

Preface

Abstract

1. Introduction

1.1	Identification	1-1
1.2	Scope	1-1
1.3	Purpose	1-1
1.4	Status and Schedule	1-1
1.5	Organization of this Document	1-2

2. Related Documents

2.1	Parent Documents	2-1
2.2	Referenced Documents	2-1

3. ECS Critical Items Overview

3.1	Critical Data Flows in ECS	3-1
3.1.1	Up Link Critical Data Flows	3-1
3.1.2	Down Link Critical Data Flows	3-3
3.2	ECS Segments that Contain Critical Software Items	3-3
3.2.1	FOS	3-3
3.2.2	SDPS	3-3
3.2.3	CSMS	3-3

4. Flight Operations Segment (FOS)

4.1	FOS Overview.....	4-1
4.2	FOS Subsystems	4-3
4.3	FOS Real Time Phase	4-5
4.3.1	Pre-Contact Scenario.....	4-6
4.3.2	Contact Scenarios.....	4-9
4.3.3	Post Contact Scenario	4-17

5. Software Hazard Analysis

5.1	Hazard Mitigation Through Design	5-1
5.2	Hazard Mitigation Through Testing	5-2
5.2.1	Verification Levels and Responsibilities	5-2
5.2.2	Build/Thread Approach to Testing	5-2
5.3	Hazard Mitigation Through Maintenance and Operations	5-3

Figures

3-1.	Uplink Critical Data Path.....	3-2
3-2.	Down Link Critical Data Path.....	3-4
4-1.	FOS Conceptual Architecture	4-2
4-2.	FOS Software Architecture	4-4
4-3.	FOS Scenario Phase Mapping.....	4-6
4-4.	Pre-Contact Scenarios	4-7
4-5.	Contact SC TLM Scenarios	4-11
4-6.	Contact SC CMD Scenarios.....	4-13
4-7.	Contact Ground TLM Scenarios	4-16
4-8.	Post-Contact Scenarios	4-18

Tables

4-1.	Threads & Components for Box 1	4-8
4-2.	Threads & Components for Box 2	4-8
4-3.	Threads & Components for Box 3	4-9
4-4.	Threads & Components for Box 4	4-10
4-5.	Threads & Components for Box 5	4-12
4-6.	Threads & Components for Box 6	4-12
4-7.	Threads & Components for Box 7	4-12
4-8.	Threads & Components for Box 8	4-14
4-9.	Threads & Components for Box 9	4-14
4-10.	Threads & Components for Box 10	4-14
4-11.	Threads & Components for Box 11	4-15
4-12.	Threads & Components for Box 12	4-15
4-13.	Threads & Components for Box 13	4-15
5-1.	Design Mapping	5-1

Abbreviations and Acronyms

Glossary

This page intentionally left blank.

1. Introduction

1.1 Identification

This Software Critical Items List, Contract Data Requirement List (CDRL) Item 093, whose requirements are specified in Data Item Description (DID) 520/PA2, is a required deliverable under the Earth Observing system (EOS) Data and Information System (EOSDIS) Core System (ECS) Contract (NAS5-60000).

1.2 Scope

This document reflects the Technical Baseline submitted via correspondence no. ECS 194-00343.

1.3 Purpose

The purpose of this document is to identify those Computer Program Configuration Items that have a "critical" command, control, or data receiving/storage function, as specified in the Contract Data Requirements Document DID 520/PA2 .

A Critical Software Item is by definition (Reference 420-05-03 EOS Performance Assurance Requirements for the EOSDIS CORE System paragraph 6.4) a software system/subsystem where "there is the risk of a malfunction resulting in damage to or loss of the flight hardware or the mission, including inability to produce or irretrievable loss of Essential Data Products". The ECS will control a constellation of flight hardware and will receive an unprecedented amount of data. This document will present a high level analysis of this system specifically to isolate the software components in the critical data paths to and from the flight hardware and storage of the essential data products.

The goal of the analysis this document presents is to produce a system that protects the large investment in resources made in this system.

1.4 Status and Schedule

This submittal of DID 520/PA2 meets the milestone specified in the CDRL of contract NAS5-60000.

1.5 Organization of this Document

This paper is organized as follows:

Section 1 Introduction

Section 2 Related Documents

Section 3 ECS Critical Items Overview - A high level description of ECS and its context with the rationale for identifying the segments that contain critical software items.

Section 4 FOS - A detailed examination of FOS and its subsystems, with real time scenarios used to identify the critical CSCIs.

Section 5 Software Hazard Analysis - A overview of the hazards that critical CSCIs present and the steps necessary to mitigate these risks.

Abbreviations and Acronyms

Glossary

2. Related Documents

2.1 Parent Documents

The following documents are the parents from which this document's scope and content are derived:

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-03	Goddard Space Flight Center, EOSDIS Core System (ECS) Contract Data Requirements Document

2.2 Referenced Documents

The following documents are referenced herein and are directly applicable to this document. In the event of conflict between any of these documents and this document, the referenced document shall take precedence.

194-207-SE1-001	System Design Specification for the ECS Project
304-CD-001-002	Flight Operations Segment (FOS) Requirements Specification for the ECS Project, Volume 1: General Requirements, Final
305-CD-001-002 & 311-CD-001-002	Flight Operations Segment (FOS) Design Specification and FOS Database Design and Database Schema Specifications, Final
305-CD-003-002	Communications and System Management (CSMS) Design Specification for the ECS Project, Final
705-CD-001-001	FOS Preliminary Design Review Vu-graphs <ul style="list-style-type: none">• FOS PDR Overview, Cal Moore, December 13,1994• FOS Software Architecture, Jeff Cox, December 13,1994• FOS Failure Recovery, Andy Miller, December 13,1994• Real-Time Scenario, Carrie Williams, Ken Fregeolle, Tim Holtz, Dave Peters, December 14,1994
420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
560-EDOS-0502.0001	Goddard Space Flight Center, Earth Observing System (EOS) Data and Operations System (EDOS) Operations Support Plan

This page intentionally left blank.

3. ECS Critical Items Overview

3.1 Critical Data Flows in ECS

A critical data path is the string of functions that includes all Critical Items. ECS is a critical component of EOSDIS on the up link (the data flows to the flight hardware) path because commands to the flight hardware originate and/or pass through ECS. ECS is also a critical component on the down link (the data flows from the flight hardware) because it is responsible for the permanent capture of the returned data and telemetry.

The following two subsections present diagrams based on the conceptual architecture presented in Section 3.2 of Reference 194-207-SE1-001 “System Design Specification for the ECS Project”.

3.1.1 Up Link Critical Data Flows

The up link path originates with human initiation and terminates at the flight hardware. Figure 3.2 highlights the Up Link Critical data flows. ECS’s Flight Operations Segment (FOS) manages and controls the EOS spacecraft and instruments. The FOS is responsible for mission planning, scheduling, control, monitoring, and analysis in support of mission operations for U.S. EOS spacecraft and instruments. The FOS also provides at the investigator’s sites ECS software (the Instrument Support Terminal (IST) tool kit) to connect a Principal Investigator (PI) or Team Leader (TL) facility to the FOS in remote support of instrument control and monitoring. PI/TL facilities are outside the FOS, but connected to it by way of the EOSDIS Science Network (ESN). The Flight FOS focuses on the command and control of the flight segment of EOS and the interaction it has with the ground operations of the ECS. The FOS’s functions and requirements are described in more detail in Reference 304-CD-001-001 “FOS Segment Requirement Specification”.

ECS’s Flight Operations Segment (FOS) manages and controls the EOS spacecraft and instruments. The FOS is responsible for mission planning, scheduling, control, monitoring, and analysis in support of mission operations for U.S. EOS spacecraft and instruments. The FOS also provides at the investigator’s sites ECS software (the Instrument Support Terminal (IST) tool kit) to connect a Principal Investigator (PI) or Team Leader (TL) facility to the FOS in remote support of instrument control and monitoring. PI/TL facilities are outside the FOS, but connected to it by way of the EOSDIS Science Network (ESN). The Flight FOS focuses on the command and control of the flight segment of EOS and the interaction it has with the ground operations of the ECS. The FOS’s functions and requirements are described in more detail in Reference 304-CD-001-001 “FOS Segment Requirement Specification”.

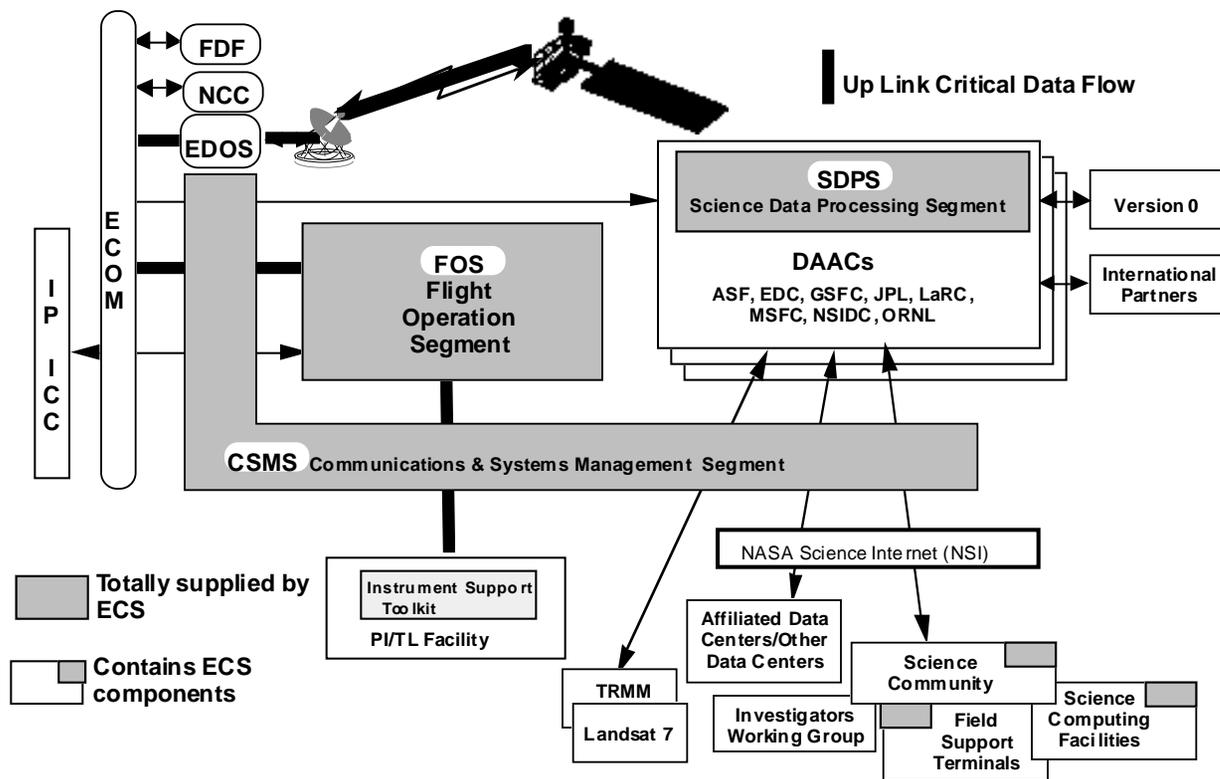


Figure 3-1. Up Link Critical Data Path

3.1.2 Down Link Critical Data Flows

The down link path originates at the flight hardware and ends at “first capture”. Figure 3.3 highlights the Down Link Critical data flows. The Science Data Processing Segment (SDPS) receives, processes, archives and manages all data from EOS and other NASA Probe flight missions. The FOS captures the real-time telemetry and produces real time reports as to the health and status of the flight hardware. The SDPS’s functions and requirements are described in more detail in Reference 305-CD-002-001 “Science Data Processing Segment (SDPS) Design Specification for the ECS Project”.

The Communications and System Management Segment (CSMS) focuses on the system components involved with the interconnection of user and service providers and with system management of the ECS components. Three subsystems have been identified in the CSMS area. The Internetworking Subsystem comprises the physical, data link, network, and transport layers. The Internetworking Subsystem supports alternative transports between communicating end-stations, alternative networking methods between end systems and intermediate systems, and alternative circuit, packet or cell-based LAN and WAN distribution services. The Communications Subsystem is comprised of the session, presentation, and application layers, and provides support for peer-to-peer, advanced distributed, messaging, management, and event handling communications facilities. The System Management Subsystem uses management applications, communications services, and an information model that defines the information flow between the manager and the managed objects. The manager also uses several applications to monitor and configure system resources (managed objects) as required. The CSMS’s functions and requirements are described in more detail in Reference 305-CD-003-001 “Communications and System Management Segment (CSMS) Design Specification for the ECS Project”.

3.2 ECS Segments that Contain Critical Software Items

3.2.1 FOS

The FOS is responsible for commanding the flight segment as well as first capture of the down linked telemetry. The software critical items are discussed in Section 4.

3.2.2 SDPS

The EDOS is responsible for first capture of all the down linked data. This captured will be archived for at least 30 days, see Reference 560-EDOS-0502.0001 “Earth Observing System (EOS) Data and Operations System (EDOS) Operations Support Plan” Section 3.1.8 .

3.2.3 CSMS

Critical data flows pass through CSMS but all such paths are fully redundant and use very stable COTS software packages (TCP/IP for example). CSMS provides infrastructure for FOS and SDPS and as such it does provide critical functions for FOS. These critical functions will be covered in the FOS section.

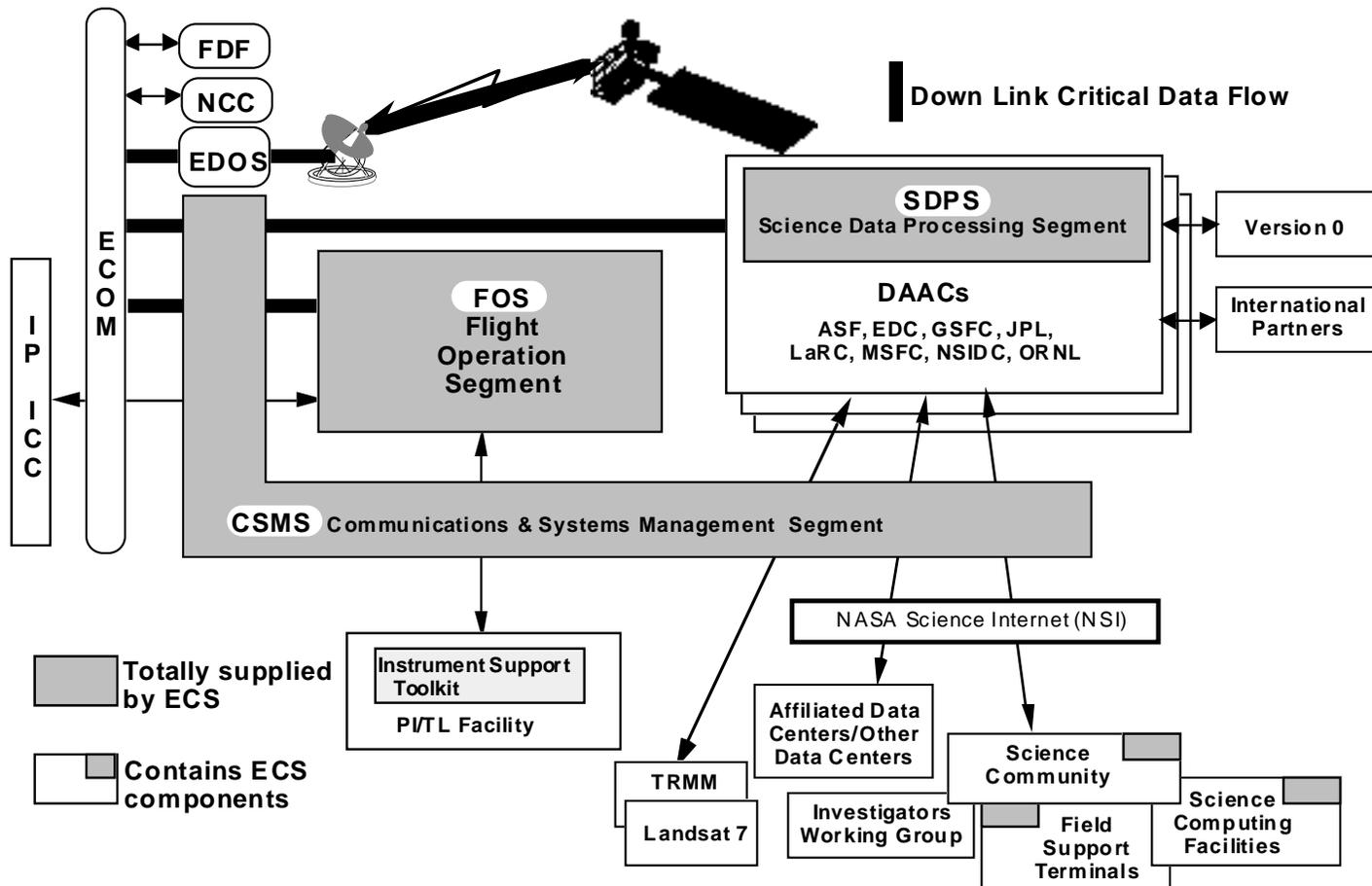


Figure 3-2. Down Link Critical Data Path

4. Flight Operations Segment (FOS)

4.1 FOS Overview

The Flight Operations Segment (FOS) provides the operations center for the U.S. EOS spacecraft and the U.S. EOS instruments, and coordinates mission operations for other non-U.S. EOS instruments on-board the U.S. spacecraft. FOS supports the EOS mission life cycle, which includes supporting pre-launch, launch, and on-orbit operations that occur in parallel with operator simulations training as well as interface tests, system tests, and end-to-end tests. FOS also supports concurrent operations with maintenance, system upgrades, and sustaining engineering activities. In addition, FOS supports command, control, and analysis of multiple spacecraft and their instruments simultaneously.

The FOS consists of two elements -- the EOS Operations Center (EOC) and the Instrument Support Toolkit (IST). The EOC will be located at Goddard Space Flight Center. It is responsible for the high-level monitoring and control of all instruments on-board the U.S. EOS spacecraft. It will maintain spacecraft and instrument health and safety, monitor spacecraft performance, perform spacecraft engineering analysis, perform high-level monitoring of the mission performance of the instruments, and provide periodic reports to document the operations of the spacecraft and instruments.

The IST is a software toolkit that will be delivered to the Principal Investigator/Team Leader (PI/TL) sites for U.S. EOS instruments. An IST provides access to the EOC functions for those individuals who are not physically located at the EOC. It enables PIs and TLs to participate in the planning, scheduling, commanding, monitoring, and analysis of their instruments.

The FOS is implemented with a high degree of redundancy in its hardware architecture as illustrated in Figure 4-1.

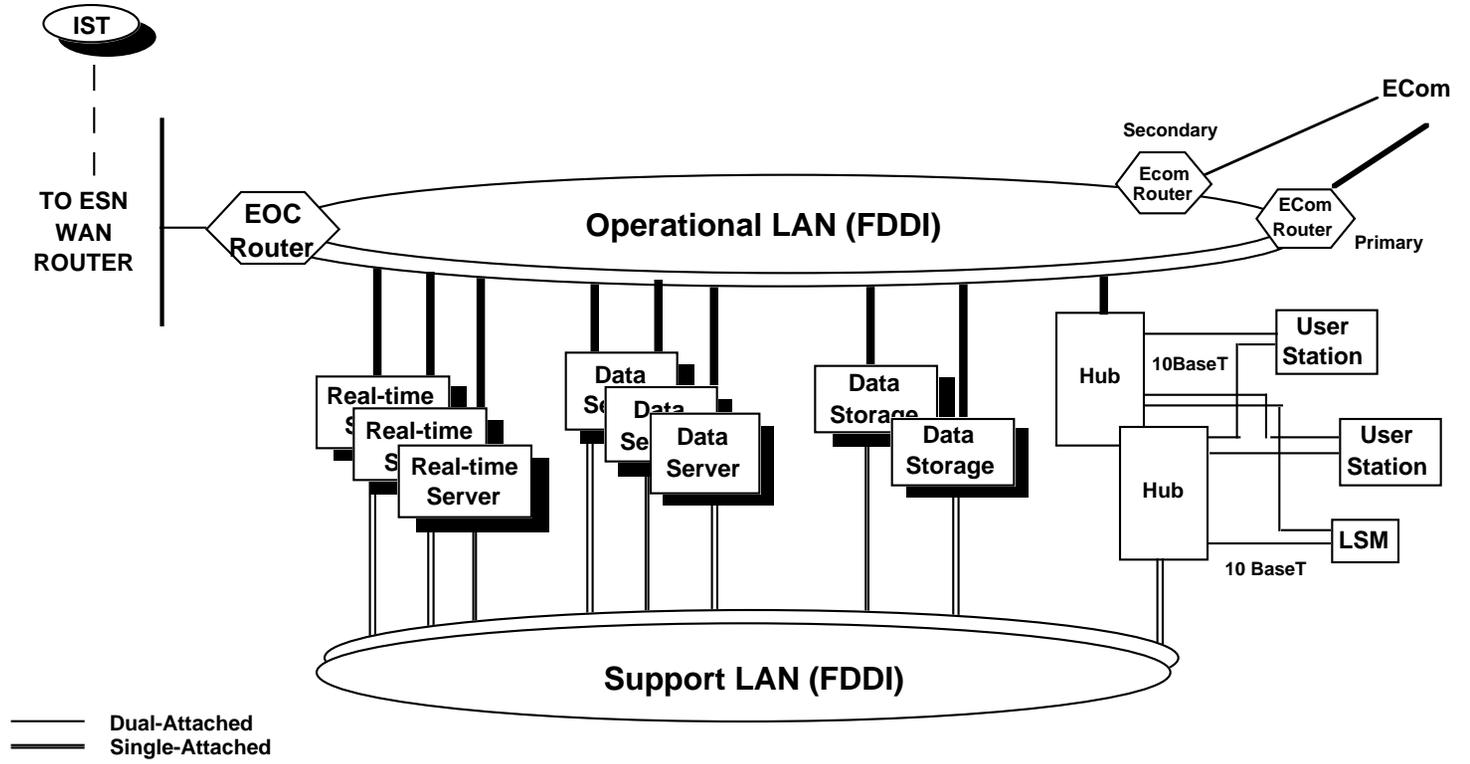


Figure 4-1. FOS Conceptual Architecture

4.2 FOS Subsystems

FOS has been partitioned into nine distinct subsystems. An individual FOS subsystem does not consist of an integrated hardware and software component. Rather, the FOS hardware is a distributed system where multiple subsystems perform operational tasks on the same hardware unit, see Figure 4-2. Thus, a subsystem, as defined for the FOS, consists of the software and operations associated with the performance of system requirements. In this document, the design of the FOS subsystems emphasizes the software component and includes operations information, as applicable.

A summary description of the nine FOS subsystems is provided below (A “*” indicates that this subsystem contains Critical Software Items.):

- * **Scheduling:** The Planning and Scheduling Subsystem integrates plans and schedules for spacecraft, instruments, and ground operations. The Planning and Scheduling Subsystem provides the operational staff with a common set of capabilities to perform "what-if" analyses and to visualize plans and schedules.
- * **Command Management:** The Command Management Subsystem manages the preplanned command data for the spacecraft and instruments. Based on inputs received from the Planning and Scheduling Subsystem, the Command Management Subsystem collects and validates the commands, software memory loads, tables loads, and instrument memory loads necessary to implement the instrument and spacecraft scheduled activities.
- * **Command:** The Command Subsystem is responsible for transmitting command data (i.e., real-time commands or command loads) to EDOS for uplink to the spacecraft during each real-time contact. Command data can be received in real-time by the operational staff or as preplanned command groups generated by the Command Management Subsystem. The Command Subsystem is also responsible for verifying command execution on-board the spacecraft.
- * **Telemetry:** The Telemetry Subsystem receives and processes housekeeping telemetry (in CCSDS packets) from EDOS. After the packet decommutation, the telemetry data is converted to engineering units and checked against boundary limits.
- * **Analysis:** The Analysis Subsystem is responsible for managing the on-board systems and for the overall mission monitoring. Its functions include performance analysis and trend analysis. It also cooperates with the Telemetry Subsystem to support fault detection and isolation.
- * **Resource Management:** The Resource Management Subsystem provides the capability to manage and monitor the configuration of the EOC. This includes configuring the EOC resources for multi-mission support; facilitating operational failure recovery during real-time contacts.

- * **Real-Time Contact Management:** The Real-Time Contact Management Subsystem is responsible for managing the real-time interface with the NCC and EDOS, as well as with the DSN station, as applicable.

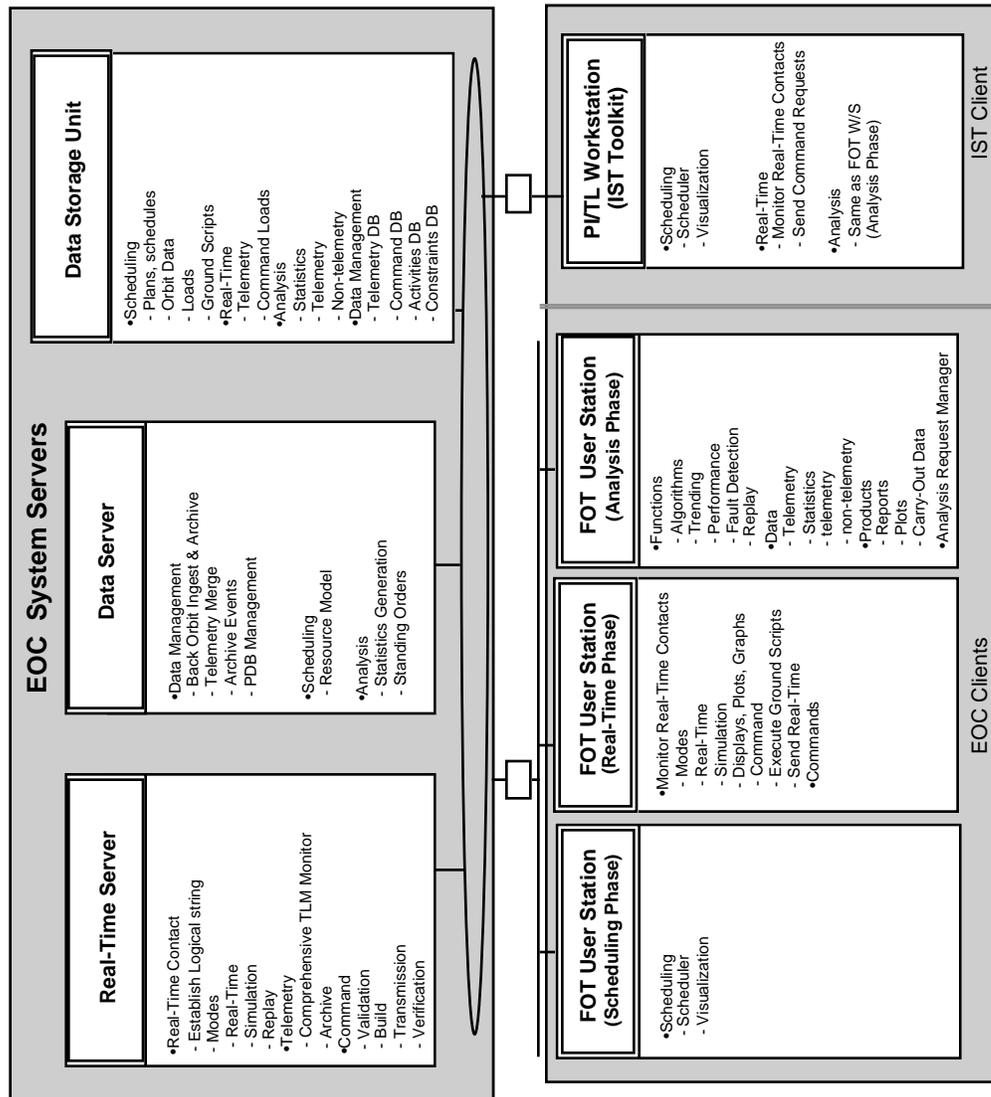


Figure 4-2. FOS Software Architecture

- * **Data Management:** The Data Management Subsystem is responsible for maintaining and updating the Project Data Base (PDB) and the FOS history log.
- * **User Interface:** The User Interface Subsystem provides character-based and graphical display interfaces for FOS operators interacting with all of the aforementioned FOS subsystems.

The following is a summary of all CSCI that contain critical software items and the acronyms that are used in the rest of the tables in this section.

FOS CSCI Acronyms

CSCI	FOS subsystem
ANA	Analysis
CMD	Real-Time Command
CMS	Command Management System
DMS	Data Management System
FUI	FOS User Interface
RCM	Real-Time Contact Management
RMS	Resource Management System
TLM	Telemetry System

CSMS CSCI Acronyms

CSCI	CSMS subsystem
CSS	Communications System
ISS	Internetworking System
MSS	System Management Subsystem

4.3 FOS Real Time Phase

The real-time phase focuses on the functions that are performed during the pre-contact, contact, and post-contact phases, see Figure 4-3.

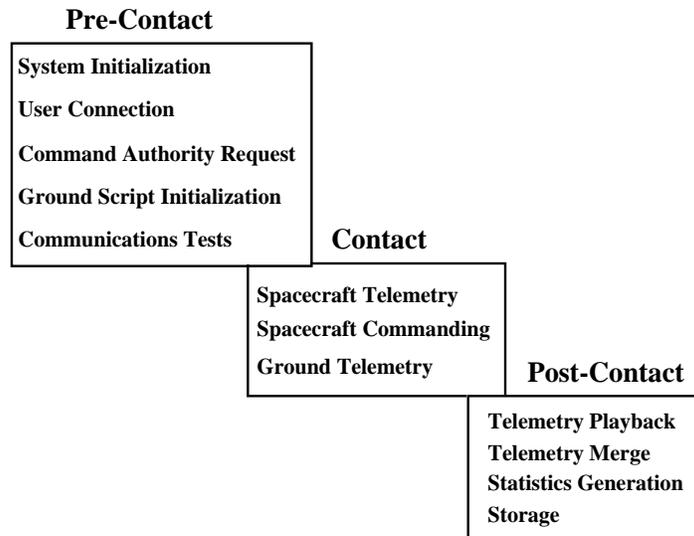


Figure 4-3. FOS Scenario Phase Mapping

These phases include the execution and control of the ground script; the uplink of spacecraft loads, instrument loads and real-time commands; command verification; ingest and monitoring of the real-time housekeeping telemetry and replay telemetry; and the capture and recording of real-time deviations to the planned ground script to ensure that the as-flown schedule is accurate. The functionality for the real-time phase is partitioned between six subsystems -- the Command, Telemetry, Resource Management, Real-Time Contact Management, User Interface, and Data Management subsystems. The ground script and the command load files generated during the scheduling phase are the primary products used for pre-contact, contact, and post-contact operations for each EOS spacecraft.

4.3.1 Pre-Contact Scenario

The ground script for the applicable EOS spacecraft and time-frame is initiated from the Command Activity Controller's User Station during the pre-contact period. The ground script includes all ground directives and spacecraft command directives (e.g., command load requests, and real-time commands) that are to be executed. Each ground directive and spacecraft command directive included in the ground script has a unique time stamp. The status of each executed directive (pass/fail) is monitored by the Command Activity Controller.

The User Interface Subsystem executes the ground script and displays the pertinent ground script information to the users on a display window. It sends the ground configuration directives to the Resource Management Subsystem and the spacecraft command directives to the Command Subsystem. The status of the executing ground script, including recently executed directives, the current directive to be executed, and upcoming directives, is maintained on the ground script display window.

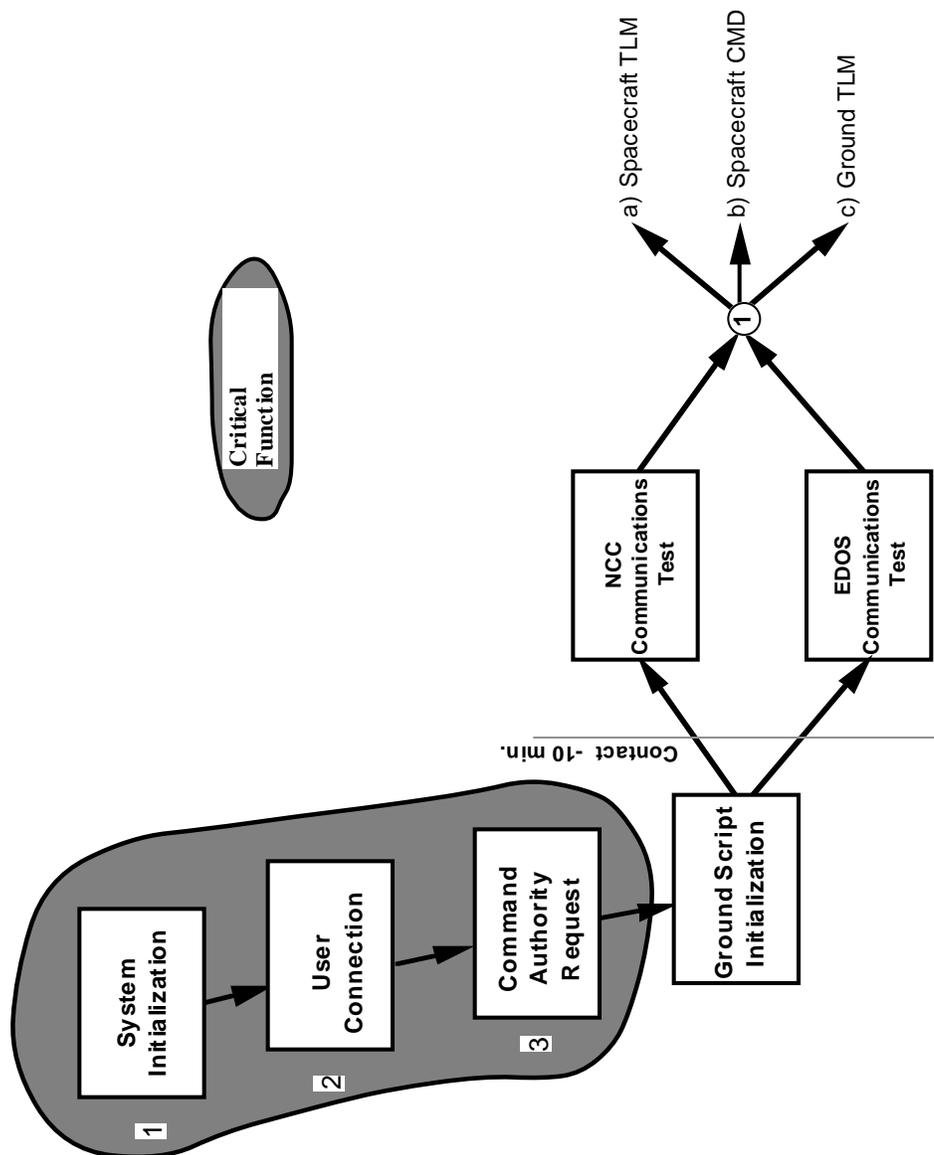


Figure 4-4. Pre-Contact Scenarios

During pre-contact, ground configuration links are verified and the operational environment is established. This includes identification of the Command Activity Controller with spacecraft command authority, establishing the logical string in the EOC for telemetry monitoring and commanding, and loading updated telemetry and command data bases.

The Resource Management Subsystem is responsible for controlling the logical strings for telemetry monitoring and command -- i.e., it enables FOS users to receive and monitor telemetry from one or more spacecraft and one or more instruments. In addition, the Resource Management Subsystem receives requests from a Command Activity Controller for command authority -- i.e., a request to be able to send commands to an EOS spacecraft. The Resource Management Subsystem grants this privilege to authenticated users, and ensures that only one person has command authority for a single spacecraft at any one time.

The following Pre-Contact functions contain critical software items:

- 1- System Initialization
- 2- User Connection
- 3- Command Authority Request

Tables 4-1 through Table 4-3 maps these critical functions to software components.

Table 4-1. Threads & Components for Box 1

Activity Phase	Thread	Component	CSCI
Infrastructure - Comm	Communications	Comm I/F to SDPS	DMS
Infrastructure - Comm	Communications	Network	ISS
Infrastructure - Comm	Communications	Security	ISS
Real-Time Operations	String Initialization	Configure CMD	RMS
Real-Time Operations	String Initialization	Configure RCM	RMS
Real-Time Operations	String Initialization	Configure TLM	RMS
Real-Time Operations	String Reconfiguration	Notify CMD of Configuration Change	RMS
Real-Time Operations	String Reconfiguration	Notify TLM of Configuration Change	RMS
Real-Time Operations	String Termination	Transfer Mission Critical Activity	RMS
Real-Time Operations	String Reconfiguration	Update String Configuration	RMS
Segment	System Failure Recovery	CMD S/W Failure Recovery	RMS
Segment	System Failure Recovery	Component Failure Detection	RMS
Segment	System Failure Recovery	Component Failure Recovery Rqst	FUI
Segment	System Failure Recovery	DMS H/W Failure Recovery	RMS
Segment	System Failure Recovery	RCM S/W Failure Recovery	RMS
Segment	System Failure Recovery	RMS S/W Failure Recovery	RMS
Segment	System Failure Recovery	RTS H/W Failure Recovery	RMS
Segment	System Failure Recovery	TLM S/W Failure Recovery	RMS
Segment	System Failure Recovery	User Station H/W Failure Recovery	RMS
Support - DMS	Data Base	Activity Validation	DMS
Support - DMS	Data Base	ASTER PDB Validation	DMS
Support - DMS	Data Base	Cmd PDB Validation	DMS
Support - DMS	Data Base	Constraint Validation	DMS
Support - DMS	Data Base	Tim PDB Validation	DMS

Table 4-2. Threads & Components for Box 2

Activity Phase	Thread	Component	CSCI
Real-Time Operations	Connection Support	User Authorization & Authentication	CSS, MSS

Note: CSS (Communications System) and MSS (System Management Subsystem) are parts of CSMS.

Table 4-3. Threads & Components for Box 3

Activity Phase	Thread	Component	CSCI
Real-Time Operations	Managing Command Privilege	Update CMD Privilege ACL	RMS
Real-Time Operations	Managing Configuration Privilege	Update ConFig Privilege ACL	RMS
Spacecraft Commanding	Command Authorization	Command Authorization Approval	RMS
Spacecraft Commanding	Command Authorization	Notify CMD of new Commander	RMS

4.3.2 Contact Scenarios

4.3.2.1 Spacecraft Telemetry

The Telemetry subsystem receives the housekeeping telemetry in real-time from the spacecraft using the CCSDS formats via the Ground Station interface. It decommutates the telemetry parameters, and performs engineering unit conversion, and limit checking based on the definitions in the Telemetry Data Base. In addition, the Telemetry Subsystem also sends telemetry subsets (i.e., attitude sensor data) to the FDF.

The following Contact Spacecraft telemetry functions contain critical software items:

- 4- EOC Telemetry Acquisition
- 5- EOC Telemetry Storage
- 6- Telemetry Processing
- 7- Spacecraft State Check

Table 4-4 through Table 4-7 maps these critical functions to software components.

Table 4-4. Threads & Components for Box 4

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Manual Commanding	Ecom Interface Connectivity	ISS
Telemetry	Configuring Telemetry Processing	Adjusting Parameter Selection	TLM
Telemetry	Collecting S/C Attitude Information	Collecting Attitude Data for FDF	TLM
Telemetry	Configuring Telemetry Processing	Determining Current/Default Time Config	RMS
Telemetry	Configuring Telemetry Processing	Enabling/Disabling Telemetry Archiving	TLM
Telemetry	Configuring Telemetry Processing	Selecting Limit Set (context switch)	TLM
Telemetry	Configuring Telemetry Processing	Selecting Limit Set (user)	TLM
Telemetry	Configuring Telemetry Processing	Selecting Telemetry Stream	TLM
Telemetry	Configuring Telemetry Processing	Telemetry Configuration Modification	RMS
Telemetry	Real-Time Monitoring	Tim Data Dropouts - Event	TLM
Telemetry	Real-Time Monitoring	Time Proc - Context Switches	TLM
Telemetry	Real-Time Monitoring	Time Proc - Decom	TLM
Telemetry	Real-Time Monitoring	Time Proc - EU Conversions	TLM
Telemetry	Real-Time Monitoring	Tim Proc - Packet Processing	TLM

Note: ISS (Internetworking System) is part of CSMS.

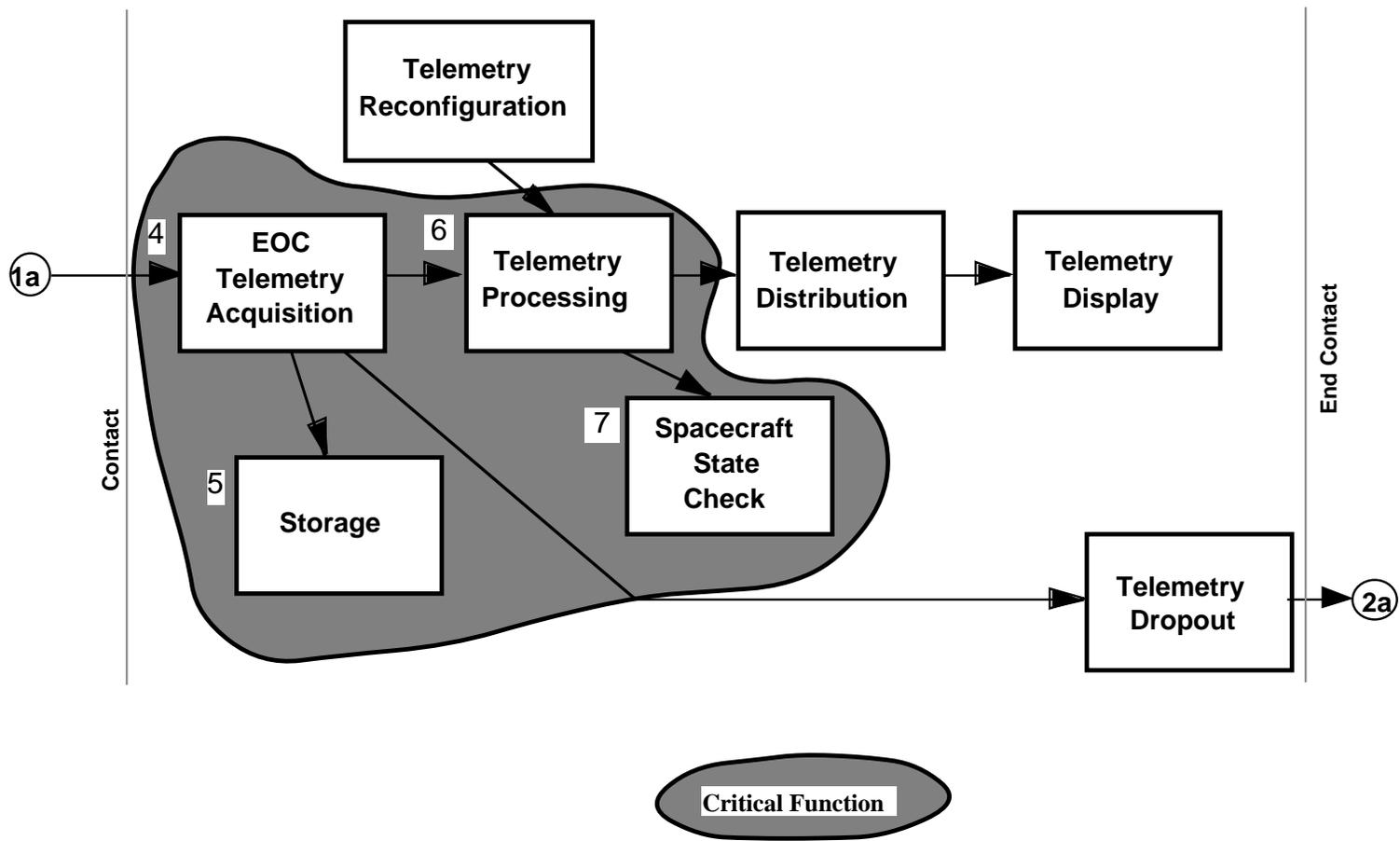


Figure 4-5. Contact SC TLM Scenarios

Table 4-5. Threads & Components for Box 5

Activity Phase	Thread	Component	CSCI
Telemetry	Real-Time Monitoring	Storing Telemetry	TLM

Table 4-6. Threads & Components for Box 6

Activity Phase	Thread	Component	CSCI
Telemetry	Real-Time Monitoring	Processing Derived Parameters	TLM
Telemetry	Real-Time Monitoring	Selecting Limit Set (context switch)	TLM
Telemetry	Real-Time Monitoring	Selecting Limit Set (user)	TLM

Table 4-7. Threads & Components for Box 7

Activity Phase	Thread	Component	CSCI
Segment	Clock Correlation	Calculating Clock Error	ANA
Segment	Checking Spacecraft State	Comparing Expected State with Telemetry	TLM
Segment	Memory Management	Maintain Ground Reference Image	CMS
Segment	Clock Correlation	Processing RCTDs	RCM
Segment	Checking Spacecraft State	Processing Telemetry	TLM
Segment	Clock Correlation	Processing TTMs	RCM
Segment	Memory Management	Update Ground Reference Image	CMS
Segment	Memory Management	Update Memory-to-Command Map	CMS

4.3.2.2 Spacecraft Commanding

During the contact, command loads and real-time commands are up linked to the spacecraft from the EOC through the Ground Station interface. (Note: the Ground Station interface is through EDOS and Ecom for a real-time contact to the spacecraft for both telemetry and command, while the Ground Station interface to the spacecraft simulator is through Ecom). The Command Subsystem receives the spacecraft command directives specified in the ground script to uplink command loads and real-time commands to the spacecraft. It can also receive real-time command directives from the Command Activity Controller and/or the IP-ICC when deviations to the ground script are necessary.

For a command load, the Command Subsystem sends the command load binary data previously produced by the Command Management Subsystem to the spacecraft via the Ground Station interface. The Command Subsystem builds the real-time command bit pattern to be up linked to the spacecraft using data from the Command Data Base.

Command loads are verified by the down linked housekeeping telemetry. The real-time commands are verified via Control Link Control Words (CLCW) in down linked telemetry (i.e., command receipt verification) as well as the down linked housekeeping telemetry (i.e., execution verification). For those command loads and real-time commands that are not successfully verified, re-transmissions can be made to a specified retry limit.

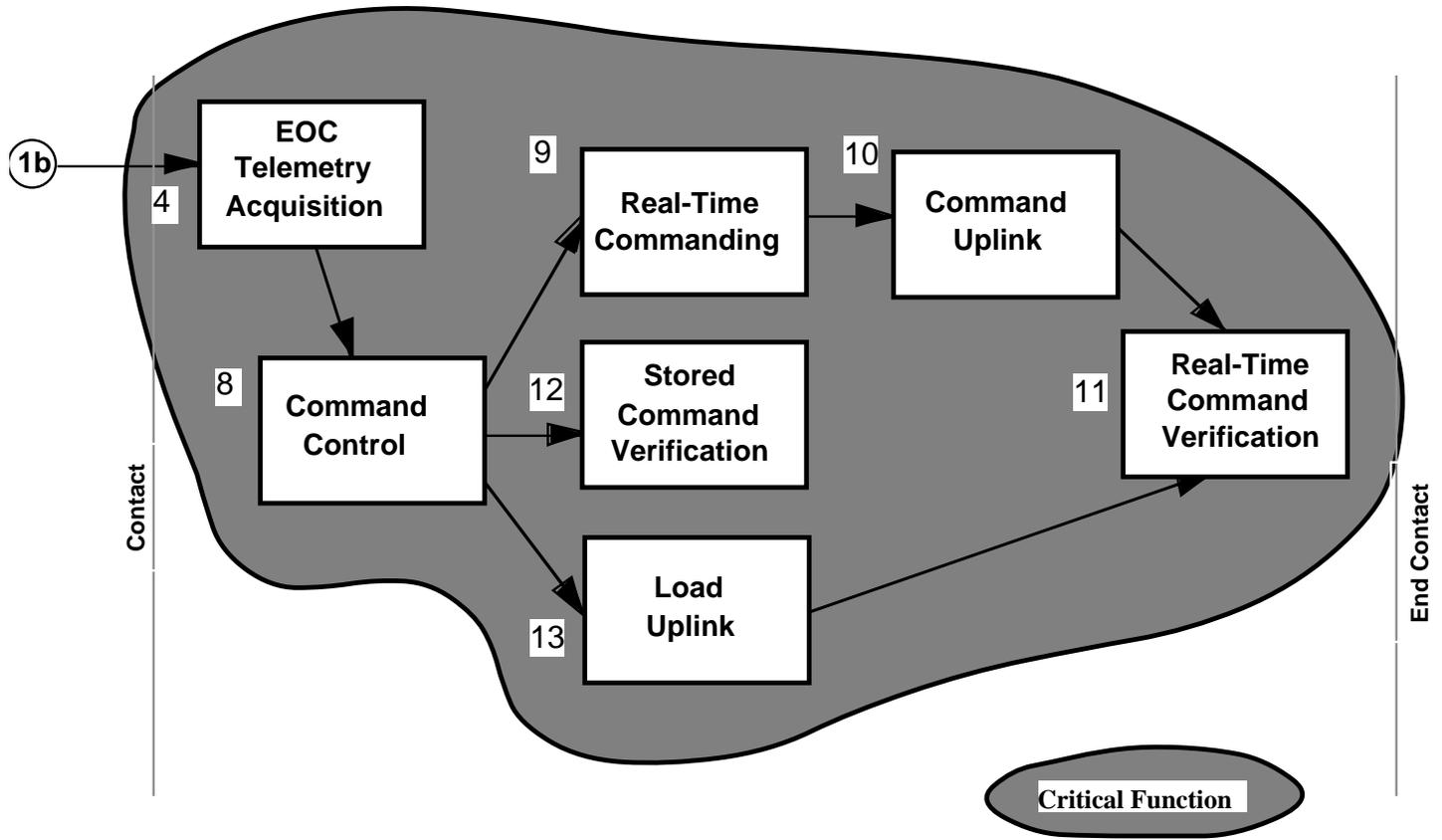


Figure 4-6. Contact SC CMD Scenarios

The Command Subsystem also sends the instrument uplink status to the IP-ICC. In addition, the Command Subsystem sends instrument command notification messages to the IP-ICC when emergency/contingency instrument commands are issued.

The Command Management Subsystem receives notification from the Command Subsystem after a command load has successfully been loaded on-board the spacecraft. This information is used to update its current copy of the spacecraft ground reference image.

The following Spacecraft commanding functions contain critical:

- 4- EOC Telemetry Acquisition
- 8- Command Control
- 9- Real-Time Commanding
- 10-Command Uplink
- 11-Real-Time Command Verification
- 12-Stored Command Verification
- 13-Load Uplink

Table 4-8 through Table 4-13 maps these critical functions to software components. See Table 4-4 for EOC Telemetry Acquisition.

Table 4-8. Threads & Components for Box 8

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Ground Script Commanding	Command Criticality	CMD
Spacecraft Commanding	Manual Commanding	Command Criticality	CMD

Table 4-9. Threads & Components for Box 9

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Ground Script Commanding	Command Generation	CMD
Spacecraft Commanding	Manual Commanding	Command Generation	CMD

Table 4-10. Threads & Components for Box 10

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Ground Script Commanding	Command Transmission to EDOS	CMD
Spacecraft Commanding	Manual Commanding	Command Transmission to EDOS	CMD

Table 4-11. Threads & Components for Box 11

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Ground Script Commanding	Command Validation - DB Lookup	CMD
Spacecraft Commanding	Manual Commanding	Command Validation - DB Lookup	CMD
Spacecraft Commanding	Ground Script Commanding	Command Validation - Prereq State Check	CMD
Spacecraft Commanding	Manual Commanding	Command Validation - Prereq State Check	CMD
Spacecraft Commanding	Manual Commanding	Command Verification - Telemetry Verification	CMD
Spacecraft Commanding	Manual Commanding	Command Verification - Receipt Verification	CMD
Support - User Interface	Directive Input	Validate Preplanned Command Procedure	CMD

Table 4-12. Threads & Components for Box 12

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Stored Cmd Verification	Command Validation - DB Lookup	CMD
Spacecraft Commanding	Stored Cmd Verification	Command Verification - Telemetry Verification	CMD

Table 4-13. Threads & Components for Box 13

Activity Phase	Thread	Component	CSCI
Spacecraft Commanding	Load Processing	Load Command Validation	CMD
Spacecraft Commanding	Load Processing	Load Criticality	CMD
Spacecraft Commanding	Load Processing	Load Transmission	CMD
Spacecraft Commanding	Load Processing	Load Verification	CMD

4.3.2.3 Ground Telemetry

The Real-Time Contact Management (RCM) Subsystem receives periodic status information from EDOS and the NCC during the real-time contact. This status information includes monitor blocks and operational data messages. The Real-Time contact Management Subsystem also can send ground configuration directives to NCC during a real-time contact, as applicable.

Spacecraft and Instrument Evaluators monitor the real-time housekeeping telemetry on the User Stations. The telemetry can be presented on a telemetry display window in a variety of forms -- e.g., text, graphical, plots, etc. The user can define the telemetry displays that enable him/her to focus on a particular area (e.g., monitoring the Power Subsystem or the CERES instrument), and quickly focus on anomalies that occur (e.g., graphical page that highlights an area where a red limit violation has occurred). An event area is also set aside on the User Station by the User Interface Subsystem to display event messages that have been generated by the Telemetry Subsystem during its processing.

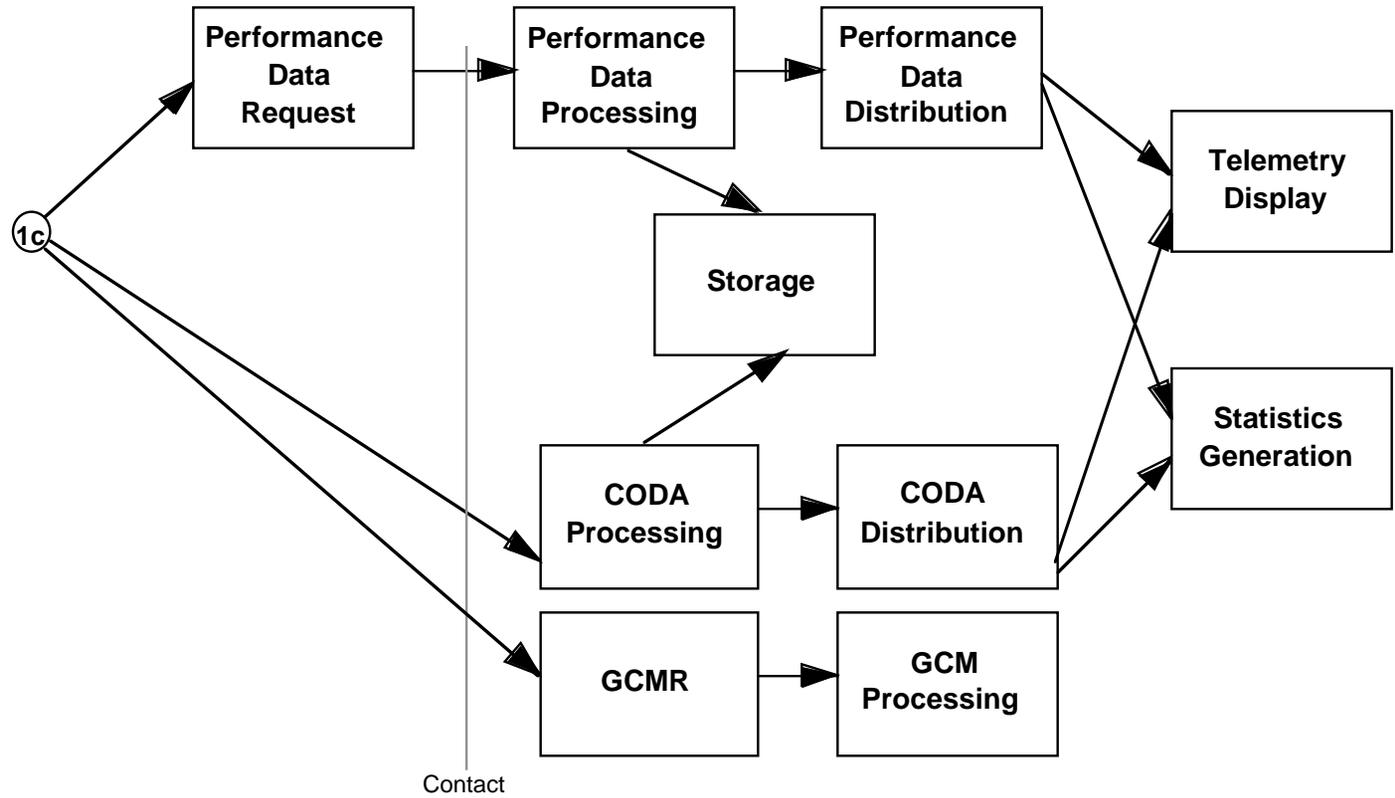


Figure 4-7. Contact Ground TLM Scenarios

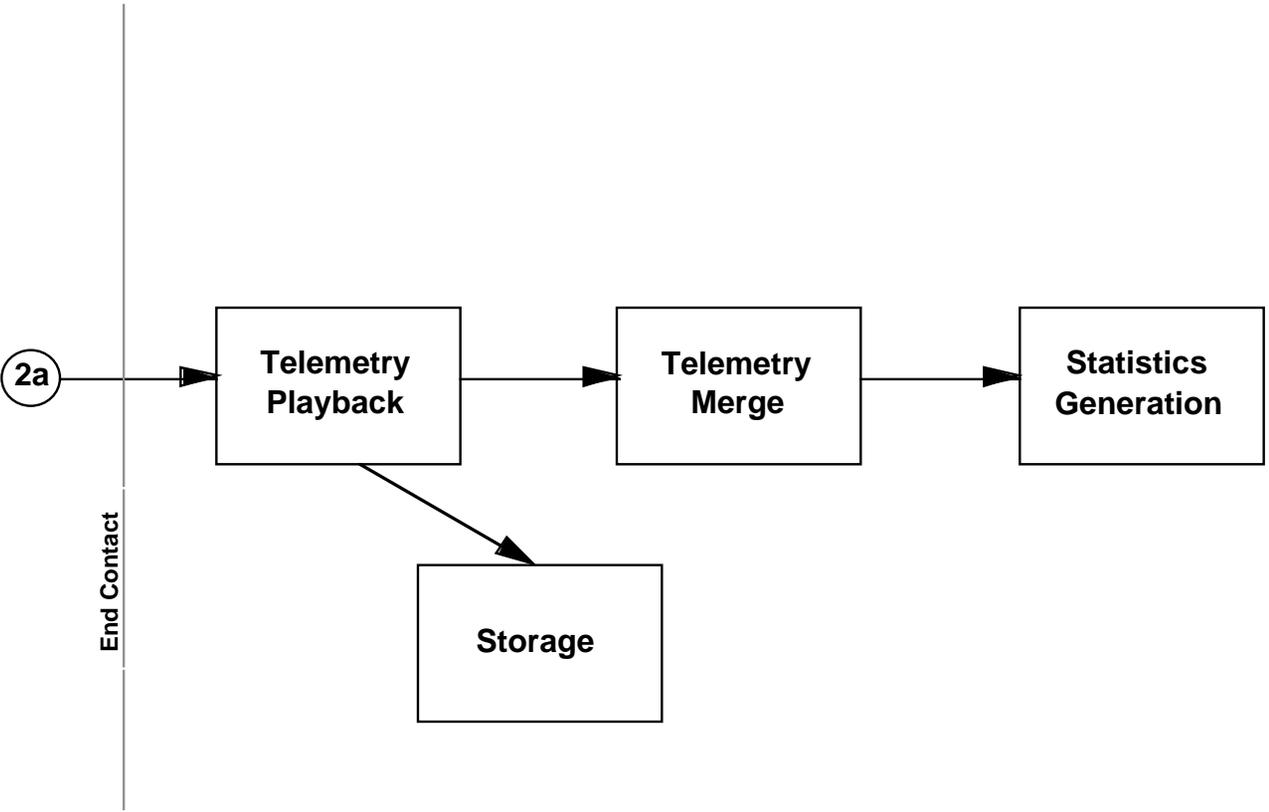
No critical subsystems are identified in the Ground Telemetry scenarios.

4.3.3 Post-Contact Scenario

During post-contact operations, the focus in the EOC is on receiving and storing the spacecraft recorded housekeeping telemetry and quick-look data from the Ground Station interface. The spacecraft recorded housekeeping telemetry is the full set of housekeeping telemetry recorded on-board the spacecraft. This data is ingested into the EOC by the Telemetry subsystem. It is merged with the real-time telemetry and archived to disk for subsequent trending and history analysis operations by the Data Management Subsystem. If requested by a user, the Telemetry Subsystem also replays historical data at a user selected rate. The processing is identical to real-time processing with the only distinction being the source of the data -- i.e., the Data Management Subsystem instead of the real-time Ground Station interface.

The User Interface Subsystem displays the applicable event information pertaining to the pre-contact, contact, and post-contact activities. This information includes telemetry displays, telemetry status, configuration status, and command status.

The Data Management Subsystem provides the access to the telemetry and command data bases and the command load files. In addition, the Data Management Subsystem receives and archives all event messages produced during the real-time operations. Note that deviations to the originally planned ground script are included in these event messages. This information is subsequently used by the Planning and Scheduling Subsystem to create the as-flown schedules.



No critical subsystems are identified in the Post-Contact scenarios.

Figure 4-8. Post-Contact Scenarios

5. Software Hazard Analysis

All of the ECS software critical items identified in this document have been located in the FOS segment. Therefore, software hazard analysis and mitigation will only address FOS.

5.1 Hazard Mitigation Through Design

The FOS segment of the ECS program is based on a large percentage of heritage design and code. This provides many advantages including the “lessons learned” on how to design and implement a robust satellite control system. The systems that provided this design and code (HST POCC for example) have demonstrated operational stability and the ability to protect their critical resources. Many of the features of these operational systems have been incorporated in the design of FOS thereby reducing the risk normally associated with designing and coding a critical software item.

Table 5-1 identifies the paragraphs in DID-305 “Flight Operations Segment (FOS) Design Specification and FOS Database Design and Database Schema Specifications,” where design has been completed / reused which specifically addresses software critical items identified in this document.

Table 5-1. Design Mapping

4.1.2.3	Event handler - notification (DB)
4.1.2.5	Telemetry, string configuration, telemetry processing
4.1.2.6	Data Server - Modeling analysis to prevent input/output bottleneck with data server
4.2.1	Network redundancy
4.2.3	Real Time Server - failure redundancy
4.2.4	Data Server - failure redundancy
4.2.6	Data Storage - no single point of failure
4.3.1	Data base validation - Local data storage
4.3.3	Contact Scenario - critical items
4.5.3	Failure Recovery
4.5.3.2	Real Time Server
5.2.3.4.1.3	Validate command procedure
6.1.1	Resource Management Subsystem
6.1.3.5.1	Backup logical string
6.1.3.9&10	Command authority scenarios
6.1.3.11	Real Time Server Failover
6.2	Command Subsystem
6.2.2	Command object model
6.2.3	All scenarios - command related
6.3	Telemetry subsystem
6.3.2.8	Spacecraft state check
6.3.3.1.3	Telemetry processing
6.3.3.2.3	Derived parameters
6.3.3.3.3	Adjust limit sets

5.2 Hazard Mitigation Through Testing

The ECS program employs an organized approach to risk minimization by maximizing the effort of critical software testing. Specifically, verification tasks are performed by three Segment Development organizations (i.e. FOS, SDPS, CSMS), three Segment/System Test organizations (i.e. FOS I&T, SDPS I&T, CSMS I&T), the Independent Acceptance Test Organization (IATO) and the Independent Verification and Validation (IV&V) contractor.

5.2.1 Verification Levels and Responsibilities

For each ECS segment (i.e. FOS, CSMS, SDPS), as coding for each computer software configuration item (CSCI) is completed, the individual CSCI is tested to ensure that its allocated requirements (i.e. the requirements allocated up through the next release) are satisfied. This is performed for all critical as well as non-critical CSCIs at the unit level. Following unit testing by the development organization and integration of all inter- and intra-segment CSCIs, the

Segment/System Test Organization performs verification activity to ensure all level 3 and level 4 requirements are satisfied. The verification activity at this level includes testing of all software critical CSCIs as well as non-critical CSCIs and is based on the build/thread approach (see Section 5.2.2).

To further ensure software robustness of CSCIs, scenario based testing is performed by the Independent Acceptance Test Organization (IATO). Testing at this level includes broader based end-to-end testing of all segments as they interact together. The Maintenance and Operations (M&O) organization provides a high level of operational support to IATO acceptance test planning and test scenario development to ensure adherence to actual operational functionality and to ensure thorough testing of software critical items at the scenario level.

Finally, the IV&V contractor performs an independent assessment of the functionality and performance of ECS releases, with an emphasis on "critical path" end to end interface testing.

5.2.2 Build/Thread Approach to Testing

The build/thread concept, which is based on the incremental aggregation of functions, is used to plan the Segment/System I&T activity of the ECS for each segment (i.e. FOS, SDPS, CSMS). A thread is a CSCI or set of CSCIs that implement a function or set of functions. The aggregate set of threads of each ECS segment comprise a release. Before testing begins, all CSCIs (both critical and non-critical) are identified and labeled via a build/thread diagram. At the Segment/System level, critical CSCIs are assigned a separate test case or set of test cases to ensure conformity to both level 3 and level 4 requirements. Specific test cases are also designed at this level to ensure intra-thread functionality, inter-thread functionality and intra-segment functionality and subsequent requirement conformance. A build (or turnover) is the assemblage of threads forming the overall system capabilities of a given release. Following each turnover, operational scenario based tests are designed, written and performed by the IATO organization to ensure operational functionality of the overall ECS design and assigned functionality of individual ECS segments and their CSCIs.

By designing the ECS test program using the build/thread approach, testing of critical CSCIs is performed early in the test cycle, and greater software test coverage is achieved, allowing for the maximization of level 3 and 4 requirements conformance and the minimization of risk.

5.3 Hazard Mitigation Through Maintenance and Operations

The Maintenance and Operations (M&O) organization will apply all approved ECS Software Configuration Management practices to ECS developed and delivered software in use by M&O in support of the EOS Spacecraft. These configuration management practices will also encompass all databases, data, Users Guides and Operational Instruction material pertinent to the correct and safe operation of the ECS software.

These practices are similar to ones employed by the M&O Organization on other missions, past and present and incorporate procedures and activities specifically intended to safeguard mission critical resources. The M&O Organization will work with the FOS Organization as an integrated team to develop, seek approval, and deploy those configuration management practices.

In addition, M&O will establish, as on other missions, rigorous initial training and proficiency exercises for all M&O personnel in the appropriate use of all ECS software.

M&O will develop and execute acceptance tests for FOS maintainability, repeatability and correctness, using actual command data and data from the Spacecraft simulator. Each subsequent software delivery, along with databases, will undergo similar acceptance and regression tests.

Abbreviations and Acronyms

ACL	Access Control List
ANA	FOS Analysis subsystem (CSCI)
ASTER	Advanced Space borne Thermal Emission and Reflection Radiometer (formerly ITIR)
CCR	commitment, concurrency, and recovery (protocol)
CCSDS	Consultative Committee for Space Data Systems
CD	compact disk (optical disk)
CDRD	contract data requirement document
CDRL	contract data requirements list
CERES	Clouds and Earth's Radiant Energy System
CLCW	command link control word
CMD	FOS Command subsystem (CSCI)
CMS	FOS Command Management System (CSCI)
COTS	commercial off-the-shelf (hardware or software)
CPCI	Computer Program Configuration Item
CSCI	computer software configuration item
CSMS	Communications and Systems Management Segment (ECS)
CSS	CSMS Communications System (CSCI)
DB	direct broadcast (AM-1)
DBMS	database management system
DCN	document change notice
DDSRV	SDPS - Document Data Server CSCI in the Data Server Subsystem
DID	data item description
DMS	FOS Data Management System (CSCI)
DSN	Deep Space Network
DSS	Decision Support System
ECS	EOSDIS Core System
EDOS	EOS Data and Operations System
EDU	EDOS Data Unit

EOC	Earth Observation Center (Japan);
EOS	Earth Observing System
EOSDIS	Earth Observing System Data and Information System
ESH	EDU Service Header
ESN	EOSDIS Science Network (ECS)
EU	Engineering Unit
FDF	flight dynamics facility
FOS	Flight Operations Segment (ECS)
FUI	FOS User Interface (CSCI)
GSFC	Goddard Space Flight Center
HW	Hardware
ICC	Instrument Control Center (ECS) (ASTER)
INGST	SDPS Ingest Subsystem
INS	SDPS Ingest Subsystem
IP	international partners
ISS	CSMS Internetworking System (CSCI)
IST	Instrument Support Terminal (ECS)
LAN	local area network
MD	Master Directory
MSS	CSMS System Management Subsystem (CSCI)
NAS	National Academy of Science
NASA	National Aeronautics and Space Administration
NCC	Network Control Center (GSFC)
OTS	Off the shelf
PA	payload accommodations
PDB	project data base
PDR	Preliminary Design Review
PI	principal investigator
RCM	FOS Real-Time Contact Management Subsystem (CSCI)
RTS	relative time sequence
SC	Space craft

SDPS	Science Data Processing Segment (ECS)
SDR	Software Design Review
SDSRV	SDPS - Science Data Server CSCI in the Data Server Subsystem
SE	System Engineering
SSR	Solid State Recorder, spacecraft data recorder.
STMGT	SDPS - Storage Management CSCI in the Data Server Subsystem
SW	science workstation / software
SWCI	software configuration item
TCP/IP	Transmission Control Protocol / Internet Protocol
TL	team leader
TLM	FOS Telemetry Subsystem (CSCI)
WAN	wide area network

This page intentionally left blank.

Glossary

Active parameter	parameter state status which indicates that the telemetry parameter is being updated.
APID	Application Identifier, number assigned by spacecraft mission management which represents the on-board application which generated the telemetry data.
Boundary limit	range value associated with a warning or alarm.
CCSDS	Consultative Committee for Space Data Systems, recommendations for spacecraft telemetry and telecommand packet format and protocol.
Comprehensive telemetry monitor	telemetry software residing on the Real-Time Server that provides complete parameter processing with temporary limit definition controlled by user with ground configuration authority
DDSRV	SDPS - Document Data Server CSCI in the Data Server Subsystem
Delta limit	maximum allowable value change in successive samples of a given parameter.
EDU	EDOS Data Unit, message packet generated by EDOS which contains the reconstructed spacecraft telemetry packet
ESH	EDU Service Header, contains EDU time tag, quality, and accounting information
ESN	EOSDIS Science Network (ECS)
EU	Engineering Unit, unit of measure assign to a given parameter (e.g. volts, amperes, degrees)
Ground configuration authority	privilege granted to one FOT user per logical string to alter the configuration of the comprehensive telemetry monitor
Ground script	a collection of time-stamped, time-ordered directives that provides an automated approach to planned activities
Ground telemetry	status and accounting data for the ground system
Logical string	collection of FOS resources that support shared access to real-time contacts, simulations or replay of historical data
Mirrored telemetry	telemetry software residing on user workstations that provides complete parameter processing with temporary limit definition controlled in parallel with the comprehensive telemetry monitor
Multicast	message addressing technique in which data is sent over a network for capture by multiple nodes
Static parameter	parameter state status which indicates that a telemetry parameter is not currently being updated.

STMGT

SDPS - Storage Management CSCI in the Data Server Subsystem

Tailored telemetry

telemetry software residing on user workstations that provides selective parameter processing and limit settings controlled by the individual user