



National Aeronautics and
Space Administration

MSFC-HDBK-1912A
DECEMBER 6, 1994

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

2nd Edition

SYSTEM ENGINEERING HANDBOOK

Volume 1 - Overview and Processes

Prepared by:
Science and Engineering
Systems Analysis and Integration Laboratory
Systems Definition Division

2nd Edition
System Engineering Handbook
MSFC-HDBK-1912

PREPARED BY:

Richard W. Smart

Richard W. Smart
Senior Engineer,
Sverdrup Technology/MSFC Group

L. Don Woodruff

L. Don Woodruff
Chief,
Systems Definition Division

APPROVED BY:

James N. Strickland

James N. Strickland
Director,
Systems Analysis and Integration Laboratory

George F. McDonough

George F. McDonough
Director,
Science and Engineering

Release Date: ____/____/____		Marshall Space Flight Center SPECIFICATION/DOCUMENT CHANGE INSTRUCTION		Page _____ of _____ Copy No.:
		Spec./Doc. No. <u>MSFC-HDBK-1912</u>		
Change No./Date	SCN/DCN No./Date	CCBD No./Date	Replacement Page Instructions	
—			INITIAL RELEASE	
change 1			REV A REPLACES INITIAL RELEASE IN ITS ENTIRETY.	

6/5/91
RELEASE
EH

12/21/94
RELEASE
CB

MSFC-Form 4140 (Revised September 1990)

NOTE: After revising the document, file this sheet in document preceeding Table of Contents

PREFACE

Performing system engineering for the wide range of projects and programs at MSFC is both a major goal and a major challenge. Effective system engineering can help ensure that projects will meet the needs of the customer, will work properly, and will be completed in a timely and cost-effective manner.

The system engineering process is dynamic, and the system engineer must keep pace with evolving technology and the increasing complexity of space systems. At the same time, MSFC is faced with the loss of increasing numbers of its more senior, experienced engineers to retirement. The need to capture their knowledge and lessons learned and make this information available to the next generation of system engineers gave rise to this handbook. In utilizing the handbook, it is important to recognize two facets of system engineering:

1. Basic system engineering process
2. Organizational roles and responsibilities

Primary emphasis throughout the handbook is to define the system engineering process. This process has evolved over a number of years and has been utilized successfully on numerous in-house development programs. Organizational structures and responsibilities may vary from program to program (i.e., matrix, dedicated project, product development team, skunk works, etc.); however, the basic system engineering process presented in Figures 9 and 12 is considered valid in each case. As previously stated, the process is dynamic and will continue to evolve with emphasis on concurrent engineering and the application of computer-aided engineering tools.

In performing system engineering for any project, the importance of early planning to identify and schedule tasks necessary to ensure complete systems requirements definition and implementation cannot be overemphasized. Use this handbook as a guide to the current system engineering process and procedures at MSFC, and tailor it, as needed, to your particular project or program. Also, take note of the lessons learned listed throughout Volume 2, especially in Section 7.0.

L. Don Woodruff
Chief, Systems Definition Division

ACKNOWLEDGMENTS

Many talented people have contributed to the preparation of this handbook. Although the total list is too long to include, their efforts and contributions are acknowledged and appreciated. Without their inputs, the resulting product would not have been possible. The principal authors would especially like to acknowledge the following primary reviewers and contributors:

Glen Ritter, MSFC/EL51
Lanny Taliaferro, MSFC/EL55
Stephen Rose, MSFC/EL56
James Parker, MSFC/EL56
Paul Craighead, MSFC/EL58
Thomas Rowell, MSFC/EL45

The principal authors, however, take responsibility for the content of this handbook.

Copies of this document can be obtained from the MSFC Document Repository, Mail Code CN22D. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to MSFC/EL51, Attn: L. Don Woodruff. A self-addressed Document Improvement Proposal form appears at the end of this document.

TABLE OF CONTENTS

TABLE OF CONTENTS i

LIST OF FIGURES v

LIST OF TABLES vi

LIST OF ACRONYMS AND ABBREVIATIONS vii

LIST OF REFERENCE DOCUMENTS xii

1.0 INTRODUCTION 1

 1.1 Purpose 1

 1.2 Scope 2

 1.3 Handbook Organization 3

2.0 OVERVIEW 5

 2.1 Systems and System Engineering 5

 2.1.1 System Engineering Organization at MSFC 7

 2.1.1.1 Program Development Directorate 7

 2.1.1.2 Safety & Mission Assurance Office 10

 2.1.1.3 Science and Engineering Directorate 10

 2.1.1.3.1 Chief Engineers 10

 2.1.1.3.2 Systems Analysis and Integration Laboratory 10

 2.1.1.3.3 Design Laboratories 14

 2.1.1.3.3.1 Propulsion Laboratory 15

 2.1.1.3.3.2 Structures and Dynamics Laboratory 15

 2.1.1.3.3.3 Astrionics Laboratory 15

 2.1.1.3.3.4 Materials and Processes Laboratory 15

 2.1.1.3.4 Mission Operations Laboratory 15

 2.1.2 Other Organizational Responsibilities at MSFC 16

 2.2 NASA Phased Project Description 18

 2.2.1 Pre-Phase A (Advanced Studies) 23

 2.2.2 Phase A (Preliminary Analysis) 23

 2.2.3 Phase B (Definition & Preliminary Design) 26

 2.2.4 Phase C (Design) 30

 2.2.5 Phase D (Development) 31

2.2.6 Phase E (Operations).....31

2.3 NASA Payload Classification..... 32

3.0 SYSTEM ENGINEERING PROCESS..... 35

3.1 Systems Planning and Definition..... 36

 3.1.1 Project Initiation Agreement 38

 3.1.2 Program/Mission Requirements 38

 3.1.3 Program/Project Plan..... 38

 3.1.4 Systems Analysis and Models 38

 3.1.4.1 Performance and Requirements Analysis 38

 3.1.4.2 Risk Management..... 39

 3.1.4.3 Cost Assessment..... 40

 3.1.5 Systems Trade Studies 40

 3.1.6 S&E Implementation Plan..... 41

 3.1.7 Mission Analysis 41

 3.1.7.1 Mission Requirements Analysis..... 42

 3.1.7.2 Mission Planning and Profile Generation 42

 3.1.7.3 Mission Performance Analysis..... 43

 3.1.8 Design Reference Mission 43

 3.1.9 Flight and Ground Operations Plan..... 44

 3.1.10 Safety 46

 3.1.11 Configuration Management 52

3.2 System Requirements Definition and Allocation 53

 3.2.1 Mission Planning and Requirements 55

 3.2.2 Operations Requirements 59

 3.2.3 Interface Requirements..... 62

 3.2.4 Preliminary Interface Definition 62

 3.2.5 Integration Requirements 65

 3.2.6 Systems Software Requirements..... 67

 3.2.6.1 Software Conceptual Phase 69

 3.2.7 Software Detail Requirements..... 71

 3.2.8 Hardware Subsystem/Component Design/ Verification Requirements..... 71

- 3.2.9 Verification Plan 73
- 3.2.10 Systems Verification Requirements 73
- 3.2.11 Software Test Planning 73
- 3.2.12 System Requirements Review (SRR) 74
- 3.2.13 Phase 0 Safety Review 74
- 3.3 Preliminary Design 76
 - 3.3.1 Flight Sequence and Timeline 79
 - 3.3.2 Design Analysis and Trade Studies 79
 - 3.3.3 Prototype Development 80
 - 3.3.4 Software Design 81
 - 3.3.5 Preliminary Design Review (PDR) 81
 - 3.3.6 Phase I Safety Review 81
- 3.4 Detail Design 83
 - 3.4.1 Instrumentation Program & Command List (IPCL) 83
 - 3.4.2 FMEA/Hazard Analysis 84
 - 3.4.3 Safety Compliance Data 86
 - 3.4.4 Systems Analyses, Models, and Simulations 87
 - 3.4.5 System Functional Schematics and Interconnect Diagrams 87
 - 3.4.6 Software Code/Debug 88
 - 3.4.7 Operations Simulations and Mockups 88
 - 3.4.8 Operations Procedures and Training 89
 - 3.4.9 Baseline Interface Definition 90
 - 3.4.10 Critical Design Review 90
 - 3.4.11 Phase II and III Safety Reviews 91
- 3.5 Fabrication and Assembly 92
- 3.6 Verification 94
 - 3.6.1 Verification Procedures 97
 - 3.6.2 Software Verification 98
 - 3.6.3 Software Validation 98
 - 3.6.4 Verification Report 98
 - 3.6.5 Verification Requirements Compliance 99
 - 3.6.6 Independent Verification and Validation 99

3.6.7 Software Operations and Maintenance Phase 100

3.6.8 Design Certification Review (DCR)..... 100

3.7 Pre-launch/Launch Operations 101

 3.7.1 Flight Readiness Review (FRR)..... 101

3.8 Flight Operations..... 102

3.9 Post-Mission Evaluation 104

 3.9.1 Hardware De-Integration and Return to Owners 104

 3.9.2 Engineering and Science Data Analysis..... 105

 3.9.3 Mission Evaluation Reports..... 105

LIST OF FIGURES

Figure 1. Phase B/C/D/E System Engineering (SE) Functions..... 6

Figure 2. MSFC Organization Chart..... 8

Figure 3. Total System Engineering for MSFC Projects..... 9

Figure 4. SAIL Organization Chart..... 11

Figure 5. Lab Lead Interfaces..... 13

Figure 6. NASA Headquarters Organization..... 17

Figure 7. NASA Program Phases 19

Figure 8. Typical Program Review Phasing 21

Figure 9. System Engineering Process - Phase A/B..... 22

Figure 10. MSFC Support Relationships In Project Phases 29

Figure 11. Payload Classification Process (MMI 8030.2) 34

Figure 12. Phase B/C/D/E System Engineering Process Flow 37

Figure 13. Principal Ground Integration Documentation 47

Figure 14. Principal Spacelab Mission Ground Integration Documentation 48

Figure 15. Ground Processing Flow Diagram Example 49

Figure 16. Payload Safety Review Process 51

Figure 17. System and Design Functional Relationship 54

Figure 18. System Specification Process Flow..... 56

Figure 19. Task Flow of Mission Operations Definition..... 58

Figure 20. Mission Operations Integration Task Flow 61

Figure 21. Sample Functional Block Diagram..... 63

Figure 22. Interface Control Document Process Flow 66

Figure 23. Experiment Payload Integration Process 68

Figure 24. System and Software Development Process..... 70

Figure 25. Systems Software Functional Requirements Process Flow 72

Figure 26. Preliminary System Design 77

Figure 27. Design Evolution 78

Figure 28. IPCL Development Process Flow 85

Figure 29. Verification Methods..... 95

LIST OF TABLES

Table I. Engineering Areas of Expertise..... 12
Table II. Design And Performance Requirements Breakdown 55

LIST OF ACRONYMS AND ABBREVIATIONS

AFE	Aeroassist Flight Experiment
AO	Announcement of Opportunity
AR	Acceptance Review
ASE	Airborne Support Equipment
ATP	Authority to proceed
AXAF	Advanced X-Ray Astrophysics Facility
C ²	Command and Control
CCB	Configuration Control Board
CCBD	Configuration Control Board Directive
CDMS	Command and Data Management System
CDR	Critical Design Review
CEI	Contract end item
CGF	Crystal Growth Furnace
CI	Configuration Inspection
CIL	Critical Items List
CM	Configuration Management
CPU	Central Processor Unit
DCR	Design Certification Review
DMS	Data Management System
DN	Discrepancy Notice
DoD	Department of Defense
DPD	Data Procurement Document
DR	Data Requirement/Discrepancy Report
DRM	Design Reference Mission
EB	Electronics and Information Laboratory
ECLSS	Environmental Control and Life Support System

ECP	Engineering Change Proposal
ECR	Engineering Change Request
EGSE	Electrical GSE
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EO	Mission Operations Laboratory
EPED	Experiment Payload Element Developer
EPEMR	Electrical Power and Energy Management Report
ERD	Experiment Requirements Document
FCI	Functional Configuration Inspection
FMEA	Failure Modes and Effects Analysis
FOSP	Flight Operations Support Personnel
FRR	Flight Readiness Review
GFE	Government Furnished Equipment
GIRD	Ground Integration Requirements Document
GN&C	Guidance, Navigation, And Control
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HOSC	Huntsville Operations Support Center
HST	Hubble Space Telescope
I/F	Interface
ICD	Interface Control Document
IIA	Instrument Interface Agreements
IOC	Initial Operational Capability
IPCL	Instrumentation Program & Command List
IPL	Integrated Payload
IRD	Interface Requirements Document
IRN	Interface Revision Notice

IRR	IPL Requirements Review/Integration Readiness Review
ISSA	International Space Station Alpha
IV&V	Independent Verification and Validation
IWG	Interface Working Group
JSC	Johnson Space Center
KHB	Kennedy Handbook
KSC	Kennedy Space Center
LCC	Launch Control Center
LSSP	Launch Site Support Plan
MCC	Mission Control Center
MCT	Mission Control Team
MGSE	Mechanical GSE
MM	Marshall Manual
MMI	Marshall Management Instruction
MPE	Mission Peculiar Equipment
MRA	Mission Requirements Analysis
MRB	Materials Review Board
MROFIE	Mission Requirements On Facilities/Instruments/ Experiments
MSFC	Marshall Space Flight Center
MSOE	Mission Sequence of Events
NAR	Non-Advocate Review
NASA	National Aeronautics and Space Administration
NHB	NASA Handbook
NMI	NASA Management Instruction
NSTS	National Space Transportation System

O&IA	Operations and Integration Agreement
OMRS	Operation and Maintenance Requirements and Specifications
PD	Program Development Directorate
PDR	Preliminary Design Review
PDT	Product Development Team
PED	Payload Element Developer
PERT	Program Evaluation Review Technique
PI	Principal Investigator
PIA	Project Initiation Agreement
PIP	Payload Integration Plan
PMM	Payload Mission Manager
POCC	Payload Operations Control Center
PRD	Project Requirements Document
PRSD	Preliminary Requirements Specification Document
QA	Quality Assurance
R&T	Research and Technology Office
RFP	Request for Proposal
RID	Review Item Discrepancy
ROM	Read-only Memory
S&E	Science and Engineering Directorate
S&MA	Safety and Mission Assurance
S/C	Spacecraft
SA&I	Systems Analysis and Integration
SAIL	Systems Analysis and Integration Laboratory
SOC	Spacecraft/Satellite Operations Center
SOW	Statement of Work

SRR	System Requirements Review
SS	System Specification
SSDD	System/Segment Design Document
STS	Space Transportation System
SWCDR	Software Critical Design Review
SWPDR	Software Preliminary Design Review
SWPRR	Software Preliminary Requirements Review
SWRR	Software Requirements Review
TBD	To Be Determined
TCRSD	Test and Checkout Requirements and Specifications Document
TCS	Thermal Control System
TDR	Test Discrepancy Report
TDRSS	Tracking and Data Relay Satellite System
TLM	Telemetry
TOPS	Technical Oversight Panels
TPS	Thermal Protection System
USAF	United States Air Force
Vdc	Volts Direct Current (DC)
VRSD	Verification Requirements and Specifications Document
WBS	Work Breakdown Structure

LIST OF REFERENCE DOCUMENTS

NASA Documents

<u>NUMBER</u>	<u>TITLE</u>
(Not numbered)	NASA Program/Project Management Initiative Lexicon
(Not numbered)	The NASA Mission Design Process
NHB 5300.4(1A)	Reliability Program Provisions for Aeronautical and Space System Contractors
NHB 7120.5	Management of Major System Programs and Projects - Detail Policies and Processes
NHB 9501.2	Procedures for Contractor Reporting of Correlated Cost and Performance Data
NMI 7120.4	Management of Major System Programs and Projects
NMI 8010.1	Classification of NASA STS Payloads
NSTS 1700.7	Safety Policy and Requirements for Payloads Using the STS
NSTS 13830	Implementation Procedure for STS Payloads System Safety Requirements
NSTS 18798	Interpretations of NSTS Payload Safety Requirements

Marshall Space Flight Center Documents (See Volume 2, Section 3.3 for a more complete list of system engineering-related MMs and MMIs)

(Not numbered)	PD Lead Engineer's Guide
JA-012	Payload Project Office Payload Safety Implementation Approach

JA-061	Payload Mission Manager Interface and Safety Verification Requirements for Instruments, Facilities, MPE, and ECE on Space Transportation System (STS) Spacelab Payload Missions
JA-062	Spacelab Integrated Payload System Verification Requirements
JA-081	Interface and Safety Verification Requirements for Instruments, Facilities, MPE and ECE on STS Partial Payload Missions
JA-082	System Verification Requirements for Integrated Payloads on Mixed Cargo Missions
JA-447	Mission Requirements On Facilities/Instruments/Experiments (MROFIE)
JA55-040	Safety and Interface Verification Plan for the Multiple Experiment Processing Furnace-Crystal Growth Furnace (MEPF-CGF) Experiment
MM 1107.1	MSFC Organization Manual
MM 7120.2A	Project Management Handbook
MM 8075.1	MSFC Software Management and Development Requirements Manual
MMI 1700.18A	MSFC System Safety Program
MMI 8010.5	MSFC Baseline Design Reviews
MMI 8030.2	Policy on MSFC Payloads
MMI 8040.15	Configuration Management
MSFC-HDBK-2221	Verification Handbook
MSFC-STD-555	MSFC Engineering Documentation Standard
SE 5330.6	Non-Conformance Reporting System
SE 5330.7	MSFC Material Review System

Other NASA Center Documents

KHB 1700.7

STS Payload Ground Safety Handbook

Other References

Blanchard, Benjamin S. and Fabrycky, Wolter J., Systems Engineering and Analysis, Prentice Hall, Inc., 1990.

Forrester, Jay W., Principles of Systems, Wright-Allen Press, Inc., 1968

Glossary, Defense Acquisition Acronyms and Terms, Fourth Edition, Defense Systems Management College, October 1989.

MIL-STD-499A, Engineering Management, 1974.

Systems Engineering Management Guide, U.S. Government Printing Office, 1986.

Systems Engineering Management Guide, U.S. Government Printing Office, January 1990.

1.0 INTRODUCTION

Systems engineering is defined in MIL-STD-499A as, "...the process(es) required to transform an operational need into a description of system performance parameters and a system configuration through the use of an iterative process of definition, synthesis, analysis, design, test and evaluation. It includes the integration of related technical parameters and ensures compatibility of all physical, functional, and program interfaces in a manner that optimizes the total system definition and design. In addition, systems engineering integrates reliability, maintainability, safety, survivability, and other such efforts into the total engineering effort to meet cost, schedule and technical performance objectives."¹

System engineering is a continuous, iterative process with a built-in feedback mechanism that is used throughout a project or program's life cycle to arrive at the best system architecture and design possible. Just when system engineering began to be practiced as a separate discipline is open to debate, but there seems to be general agreement that formal recognition and definition of the process started after World War II. Large, complex post-war development projects such as the first U.S. ballistic missiles and NASA's Apollo program exhibited the characteristics which created the need for system engineers.

Among these project characteristics are:²

- Large design teams with many highly specialized designers
- Multiple contractor involvement, widely separated geographically, complicating communications
- Multiple hardware and software subsystems in concurrent development
- Complex operational and logistic support requirements
- Constrained development time
- High level of advanced technology

A glance at this list shows that many, if not all, of the typical projects at MSFC exhibit these characteristics. Therefore, system engineering has the potential for having a major positive impact on all of the Center's activities. This handbook is intended to document system engineering techniques as practiced at MSFC.

1.1 Purpose

This handbook will help the reader gain an understanding of the diversity, necessity, importance, and effective use of resources that is system engineering. This document is intended to define system engineering and to describe the multi-disciplined combination of technical, managerial, and engineering skills required to

¹ MIL-STD-499A, Engineering Management, May 1, 1974.

² Systems Engineering Management Guide, U.S. Government Printing Office, 1986.

effectively conduct a system engineering program at MSFC. It is meant to be a working reference and guide to performing day-to-day system engineering tasks as well as an overview of the system engineering process throughout the life cycle of a project. The necessary flow charts, figures, references, clarifying examples and illustrations are included. The NASA phased project development process, including typical project reviews is also described herein, as well as interfaces among different laboratories, offices, contractors, and other NASA centers.

1.2 Scope

This document will not define system engineering from an academic viewpoint. Rather, it will equip a practicing system engineer and organizations/people who interface with system engineers with an understanding of the tools, techniques, and processes used at MSFC. It will also provide a better understanding of the importance, definition, and practice of the system engineering process.

This handbook is written from the point of view of the working-level system engineer in the Systems Analysis & Integration Laboratory (SAIL), with each system engineering job or function described in some detail via flow diagrams and accompanying text. Discussions of some classical (textbook) system engineering tools and techniques are included in Volume 2 for comparison and contrast with the MSFC methodologies. At MSFC, end-to-end system engineering is primarily the responsibility of the Systems Analysis and Integration Laboratory working in consonance with the chief engineers, but depending on the task scope or the engineering disciplines involved, other laboratories perform system engineering functions (see Section 2.1.2). This handbook attempts to delineate the processes of system engineering at all levels and organizations within MSFC.

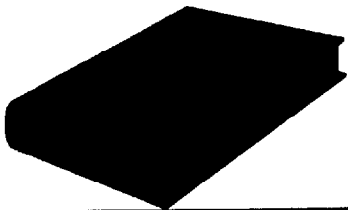
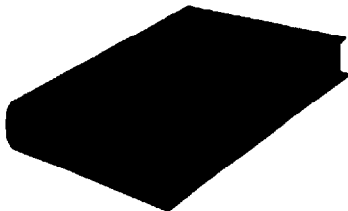
The processes and procedures described herein are used primarily on the typical, in-house project or program. Since each project or program tends to be unique, you should expect to find some deviations from the process described here on a project-by-project basis. As always, engineering and management judgment need to be applied to tailor this generic process to a specific project. By the same token, these processes and procedures require tailoring for use on smaller programs such as experiments. Where appropriate in the text, guidelines for tailoring have been included.

It should also be noted that for the typical contracted effort many of the processes described here will actually be performed by a contractor. The role, then, of the MSFC system engineer becomes one of monitoring and overseeing the contractor's activities. In addition, the system engineer should seek to add value to the contractor's effort by taking an active part in planning and independent analysis. In some sense, this role is even more demanding than the case where the work is done in-house in that the system engineer must work harder at staying in touch with the contractor's technical progress. Often, the contractor will not be collocated with MSFC, and frank and open communications will be essential to a successful project. This communication may be accomplished through technical oversight panels (TOPS) or working groups which relate to the various disciplines.

This volume is not intended to be a statement of policy, nor to recommend changes to any existing Center policies. It addresses the entire spectrum of system engineering at MSFC, and describes the complete project flow from concept to post-flight data analysis.

1.3 Handbook Organization

This handbook is divided into two volumes along with their associated appendices. Volume 1 - Overview and Processes describes the overall system engineering process flow throughout the life cycle of a project. Another important aspect of system engineering is the organization by which the process is performed. At MSFC, the system engineering effort is spread over multiple laboratories and includes Chief Engineers and project office personnel. This organization is also discussed in this volume. Volume 2 - Tools, Techniques and Lessons Learned contains "how to" fact sheets on system engineering tools and techniques, as well as checklists, document outlines and lessons learned to aid the working-level engineer. In essence, Volume 1 is the overall road map and guide book, whereas Volume 2 is the toolbox used to implement the process and produce the documents, analyses, and other output products of system engineering. This structure is illustrated in the following diagram. This handbook describes the "now" process and can be used as a basis for process improvement.

<p>Volume 1</p> 	<ul style="list-style-type: none"> • Overview and processes • Project life cycle • System engineering at MSFC • Phase A/B/C/D/E processes
<p>Volume 2</p> 	<ul style="list-style-type: none"> • Tools, techniques, and lessons learned • Document templates • Ref. to specs, standards, MMs, & MMIs • Analytical techniques • Design review guidelines • System engineering tools • Lessons learned

Volume 1 includes a definition and road map of system engineering as it is practiced at MSFC by the SAIL. This road map (Figures 9 and 12) is the key to the entire process description of Section 3.0, and the reader is encouraged to continuously refer back to these figures to place the entire process in perspective. To assist the reader, the individual blocks on Figure 12 show the paragraph number in the text where that function is described. Note, however, that some paragraphs in the text do not have corresponding blocks on Figure 12. This is primarily done to avoid over-complicating

the figure, and is limited to processes such as formal reviews and the functions of continuous processes such as safety and configuration management, to name a few. The complete system engineering process and the disciplines involved are described in detail, including the function, practice, and importance of each. Volume 2 contains numerous examples and illustrations to clarify the interfaces, personnel interactions, and their timelines in supporting typical project activities.

Bold-face type is used throughout the text for paragraph headings and to emphasize and highlight fundamental principles and important ideas.

2.0 OVERVIEW

2.1 SYSTEMS AND SYSTEM ENGINEERING

There are many definitions of a system. Two of these are listed below:

- A system is a set of interrelated components working together toward some common objective.¹

- A system is a grouping of parts that operate together for a common purpose. For example, an automobile is a system of components that work together to provide transportation. An autopilot and an airplane form a system for flying at a specified altitude.²

System engineering consists of applying iterative processes throughout the life cycle of the project. There are a multitude of diagrams in the literature depicting these processes including everything from the spiral or double helix concept given in the draft HQ NASA Systems Engineering Handbook³ to the simple functional schematic block diagram of the DoD Systems Engineering Management Guide.⁴ Rather than embracing any particular model here, we note that all of these depict similar functions with different terminology. Each begins with an input (usually some kind of requirement) and proceeds through a functional analysis of the requirements to decide **what** must be done (requirements definition and allocation) to satisfy them. After deciding what must be done, a synthesis process of deciding **how** it is to be done (concept definition and preliminary design) is followed by a decision process of selecting among alternative solutions. The best solution then is designed in detail, manufactured, verified and deployed to perform the mission or meet the original requirements (or the current version of the requirements). Throughout this series of processes there is provision for looping back to any previous stage and applying new knowledge gained to the refinement of the results and products of those stages. This system engineering function and feedback process as it is applied in this handbook to a typical MSFC project is depicted in Figure 1.

The role of the system engineer varies depending on the stage of the system engineering feedback process of Figure 1. Prior to System Requirements Review (SRR), the primary function of the system engineer is to conduct the necessary tasks and assure development of completed system requirements for review & baseline at SRR.

¹ Blanchard, Benjamin S. and Fabrycky, Wolter J., Systems Engineering and Analysis, Prentice Hall, Inc., 1990.

² Forrester, Jay W., Principles of Systems, Wright-Allen Press, Inc., 1968.

³ Shishko, Robert and Chamberlain, Robert G., Draft NASA Systems Engineering Handbook, September 1992.

⁴ Systems Engineering Management Guide, U.S. Government Printing Office, 1989.

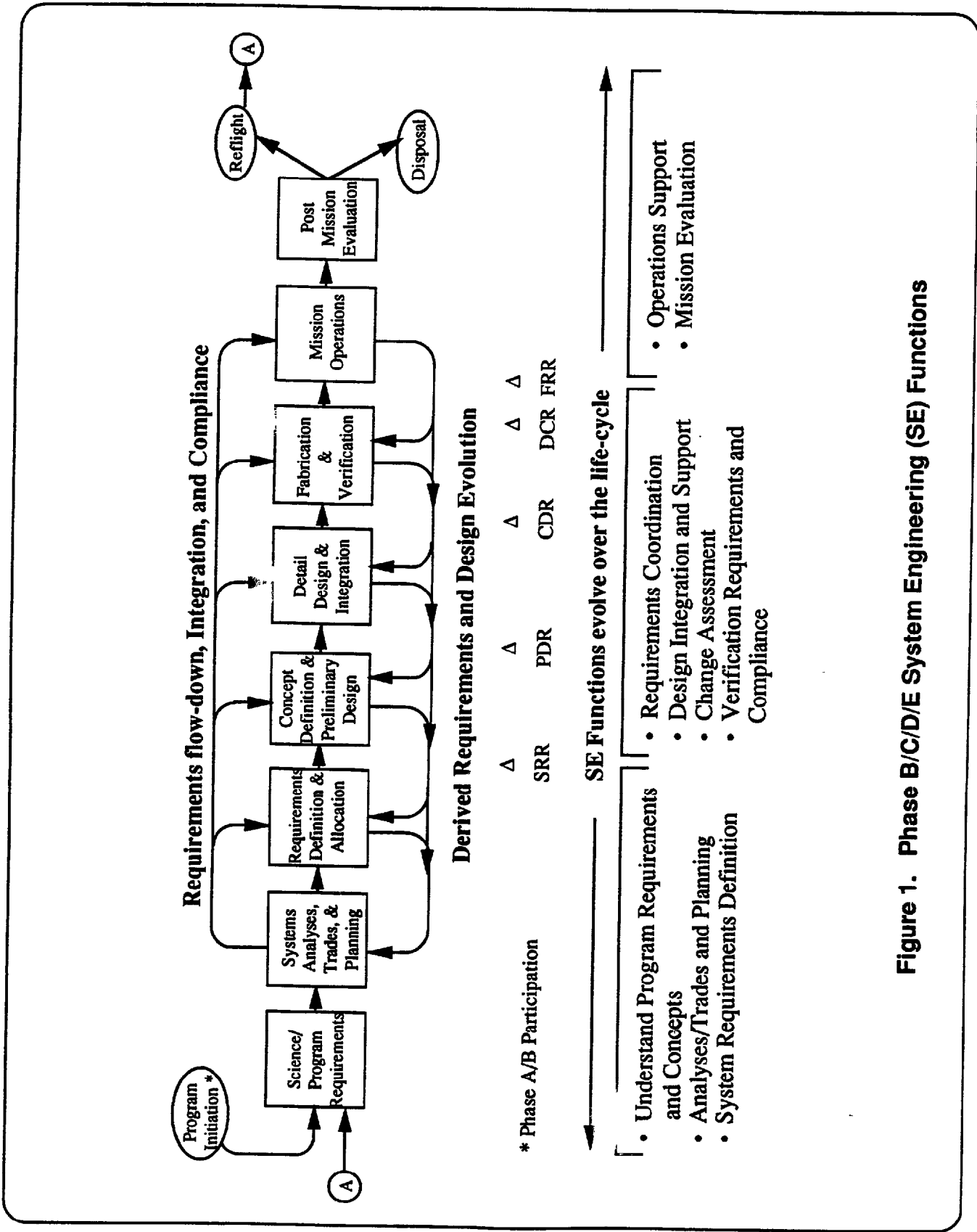


Figure 1. Phase B/C/D/E System Engineering (SE) Functions

Subsequent to requirements baseline (i.e., SRR), the system engineer's focus shifts to requirements maintenance and coordination with the design organizations to assure correct interpretation and compatibility of requirements during design implementation. Throughout the life of the program, the system engineer participates in evaluating program changes and identifying requirements changes and impacts. Throughout design implementation, derived requirements will necessitate changes in the system requirements, and the system engineer should view these changes as a normal part of the design process. Avoid the tendency to view the System Specification as something, once baselined, that is final and unchangeable.

2.1.1 System Engineering Organization at MSFC

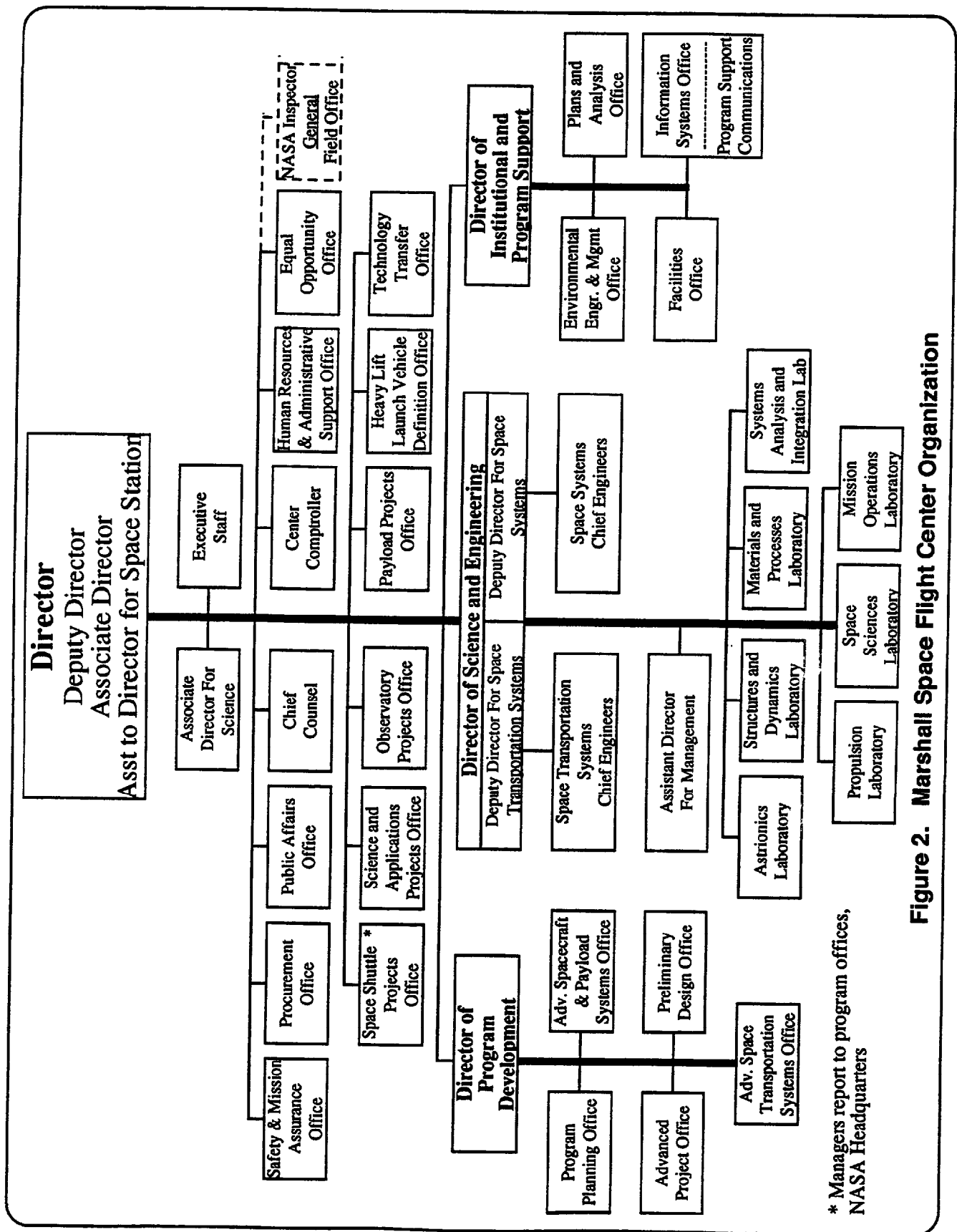
The system engineering organization at MSFC has evolved over the years. During the early years of the Center, work efforts were primarily concentrated on one or two major programs with the engineering organization dedicated to these programs. As the Center roles and missions expanded to encompass launch vehicle systems, space systems, spacecraft, experiments, payloads, and associated development and operations facilities, the system engineering organization transitioned from a program-oriented one to its present matrix alignment. Factors which accelerated this process include a shortage of experienced discipline engineering personnel and the application of newer and more complex technologies. The distinct advantage of the matrix organization is that it can provide system engineering to several programs with fewer discipline personnel, and can provide more flexibility as project needs change.

Although the program-dedicated engineering or Product Development Team (PDT) organization provides more effective support to the individual program, it is difficult to maintain when dealing with multiple programs and limited systems discipline staffing. As a result, as the number of programs managed by MSFC has increased, the centralized system engineering organization has provided dedicated staffing to the various PDTs and matrixed support to the remaining programs.

It should be noted that system engineering functions at MSFC are not concentrated in one organization. Rather, these functions are divided among the Project Office, Chief Engineer, Program Development Directorate, Systems Analysis and Integration Laboratory, several Design Labs, the Mission Operations Lab, and the Safety and Mission Assurance Office. Figure 2 shows the formal MSFC organizational structure as of this writing. The system engineering functions of the various organizations are discussed below and summarized on Figure 3. See MM 1107.1 for more detail on the roles and missions of each MSFC organization.

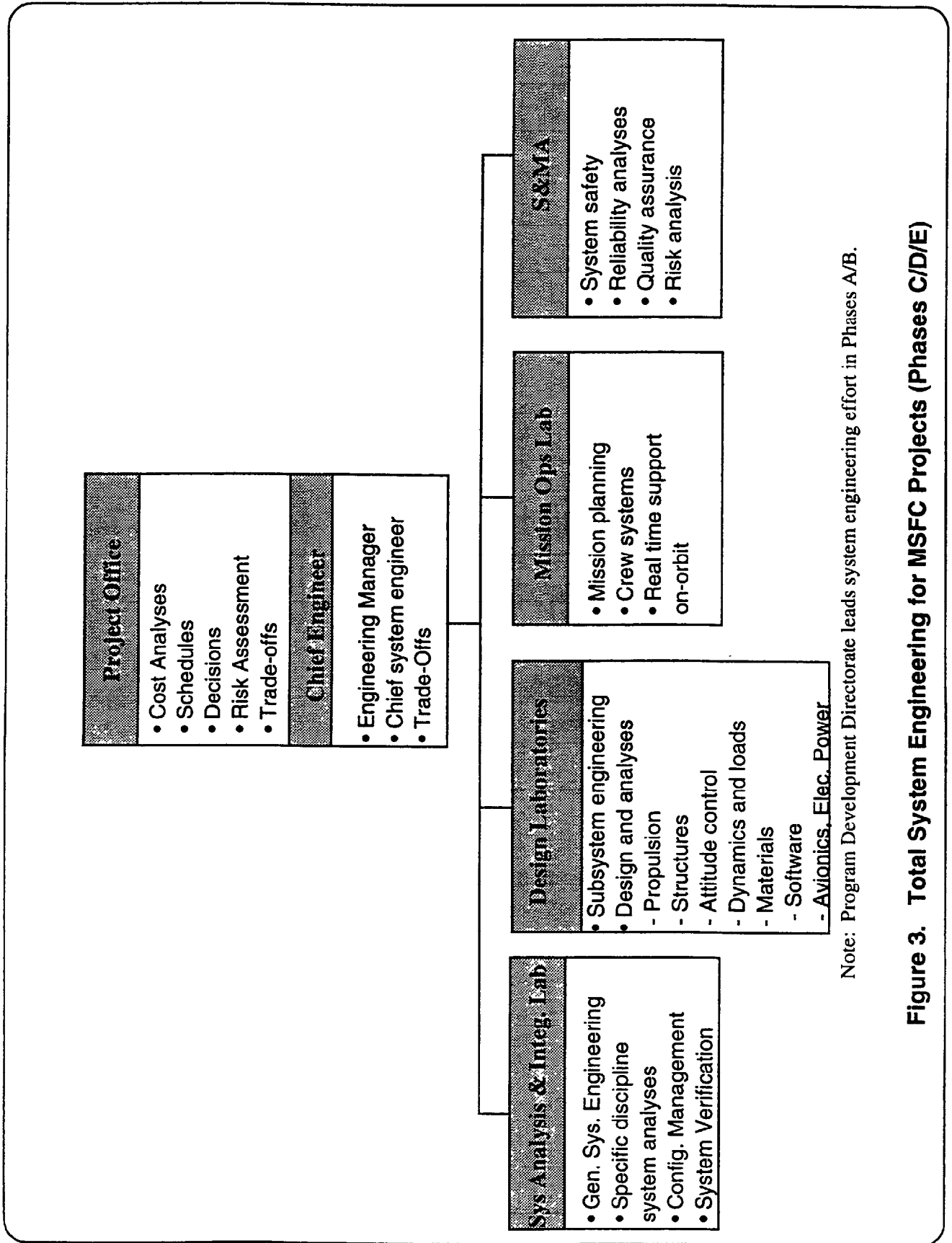
2.1.1.1 Program Development Directorate

During preliminary analysis and concept definition stages of a project's life cycle, system engineering functions are typically performed by the Preliminary Design Office within Program Development (PD). Within this office, most of the system and specialty engineering disciplines are represented and are applied to exploring feasible concepts for meeting mission needs. As a project matures and receives approval to enter



* Managers report to program offices, NASA Headquarters

Figure 2. Marshall Space Flight Center Organization



Note: Program Development Directorate leads system engineering effort in Phases A/B.

Figure 3. Total System Engineering for MSFC Projects (Phases C/D/E)

development, the primary system engineering responsibility shifts to the Science and Engineering Directorate.

2.1.1.2 Safety & Mission Assurance Office

System safety engineering is the responsibility of the Safety and Mission Assurance (S&MA) office. In addition, system engineering expertise in reliability analysis, quality assurance, and risk analysis exists within this organization.

2.1.1.3 Science and Engineering Directorate

2.1.1.3.1 Chief Engineers

At MSFC, the Chief Engineers are assigned to Space Transportation Systems (organization code EE) and Space Systems (organization code EJ) under the Director of Science and Engineering (S&E) (Figure 2). Although organizationally a member of S&E, the Chief Engineer is a key member of the project management team. **The program/project Chief Engineer serves as the Engineering Manager and chief system engineer for the project to ensure engineering adequacy.** One of the key functions of the Chief Engineer is to ensure the commitment and coordination of in-depth engineering support from the S&E Laboratories.

Problem solving and issue resolution are important functions of the system engineers, especially when issues involve two or more disciplines. At MSFC, the formal authority to resolve these issues rests with the Chief Engineer's Office. At MSFC, system engineering is considered one of the engineering disciplines. However, the system engineers can often be very effective in problem solving and issue resolution by virtue of their function in the organization. That is to say, if the system engineer exhibits broader knowledge of the system requirements and design and has integrated with the design teams, that person's assessment on issues will be based on what is best for the overall system. This may help resolve issues and problems very early after they are identified without referring them to the Chief Engineer's Office.

2.1.1.3.2 Systems Analysis and Integration Laboratory

During program design, development and implementation, system engineering support is provided primarily by the Systems Analysis and Integration Laboratory (SAIL, shown in Figure 4) within the S&E Directorate. The SAIL performs system engineering tasks to accomplish systems analysis, definition, and integration; define engineering criteria, trades, concepts, and design and performance requirements; payload integration, verification planning, and test and flight evaluation. **A primary function of the SAIL system engineers is to ensure end-to-end compatibility and performance of all system elements.** The SAIL also provides configuration management support and performs systems testing, where required, for all MSFC programs.

The SAIL staffing includes the primary and specialty engineering discipline areas of expertise including many of those identified in Table I. Typically, the

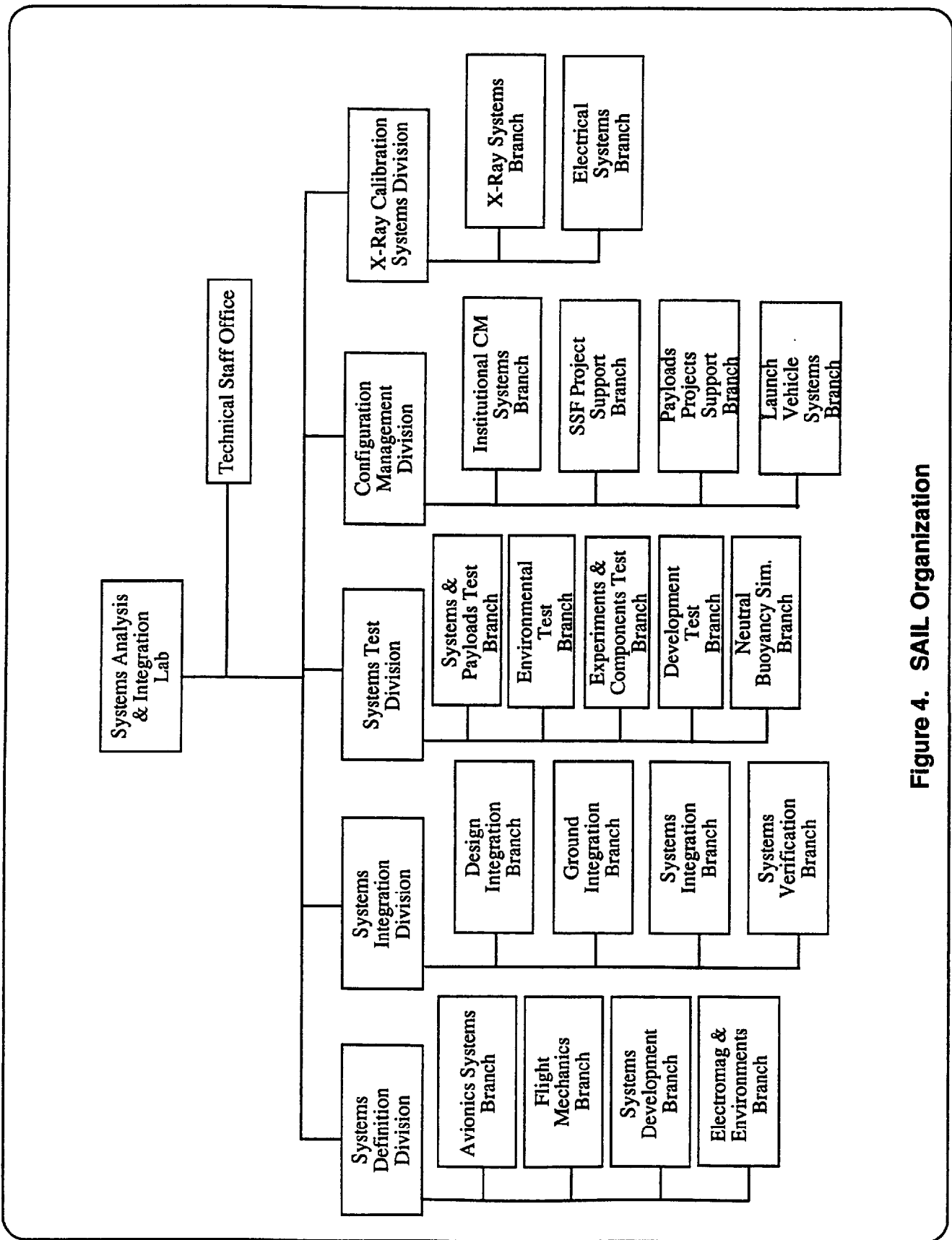


Figure 4. SAIL Organization

Table I. Engineering Areas of Expertise

Electrical/Electrical Power	Mechanical/Mechanisms
Structures	Conceptual Layout*
System Design	End-to-end Functional Schematics*
Orbital and Flight Mechanics*	Test Facility Planning and Operation
Contamination Control	Loads and Induced Environments
Guidance and Navigation (G&N)*	Data Management
Communications	Instrumentation
Measurement Systems	Software Requirements
Electromagnetic Compatibility/Interference *	Lightning Protection *
Interface Definition and Control*	Pointing and Stabilization
Alignment	Thermal Systems
Resource Utilization Reporting* (mass properties, electrical power, instrumentation and commands)	Propulsion
Ground Integration and Operations*	Flight Operations and Integration
Man-Systems Integration	Life Support and Environment Control
Materials	Systems Safety (FMEA/CIL/Hazard Analysis)
Launch Processing	System Verification Planning and Requirements Compliance*
Spacecraft Charging*	GSE Requirements*
Natural Environments* (space and terrestrial)	System Requirements*

* Primary responsibility for these disciplines resides in SAIL.

system engineering organization includes many of these disciplines. A key responsibility of the system engineer is to ensure that these disciplines (primary and specialty) are considered throughout the program life cycle.

It is critical to maintain this engineering expertise in the system engineering organization to ensure timely performance of analyses and initial requirements definition and allocation. Subsequent to establishing a requirements baseline, the system engineer is responsible for keeping requirements current and assuring correct interpretation of the requirements by the design organizations.

Within the SAIL, a Lab Lead System Engineer is assigned for each program to integrate the discipline expertise within the laboratory, coordinate with other laboratory lead engineers, and serve as the primary systems interface with the project Chief Engineer, as illustrated in Figure 5. The Lab Lead System Engineer is also responsible for planning and coordinating all the system engineering activities of the SAIL for the assigned project. For this reason, it is important that this system engineer have a thorough understanding of the project objectives, requirements, and design.

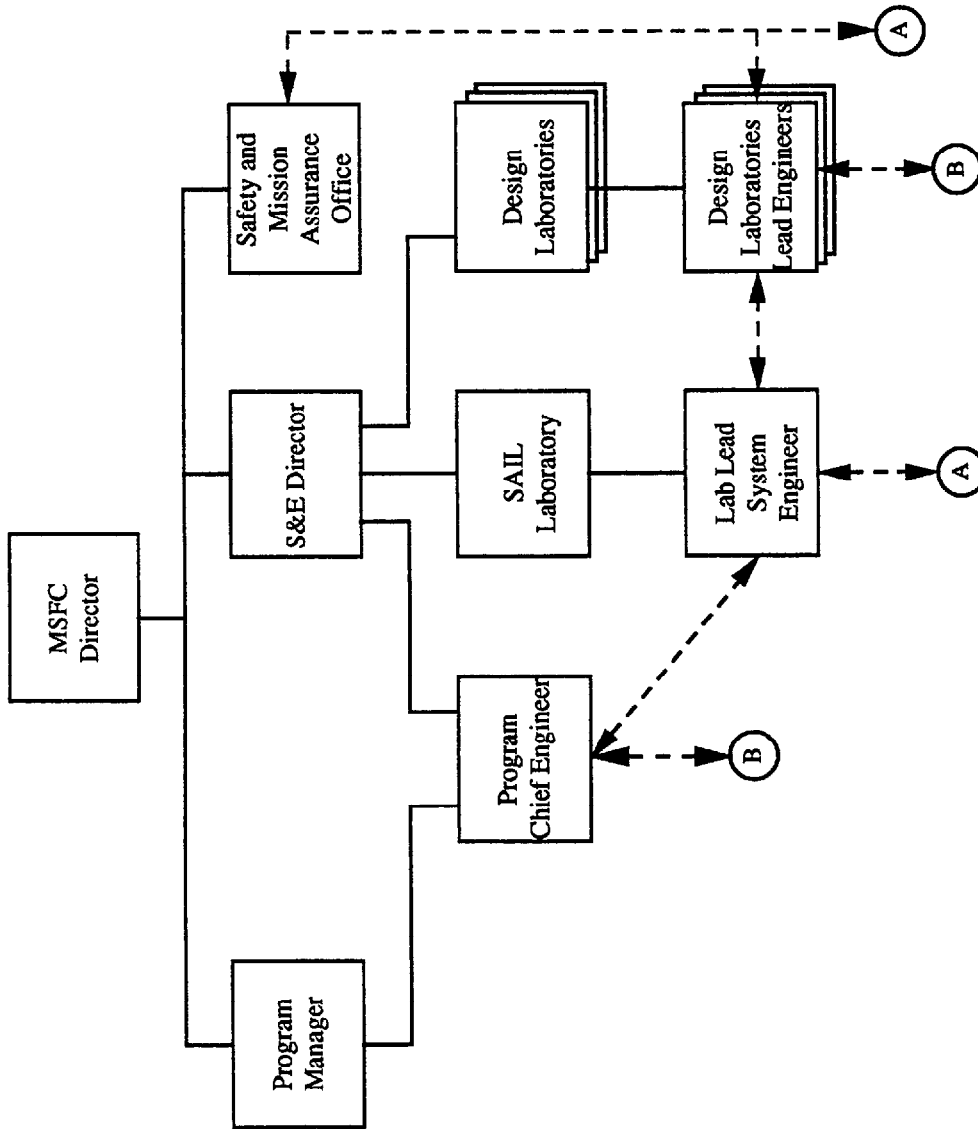


Figure 5. Lab Lead Interfaces

Specific tasks that fall to the Lab Lead System Engineer include:

- Serving as the point-of-contact for the SAIL for program system engineering;
- Participating in preparation of the Engineering Implementation Plan (EE/EJ function) for in-house programs;
- Defining specific SA&I tasks, program milestones and task schedules, developing a task/document tree (see Volume 2, Section 2.1.1) and required documentation outputs, manpower/skills required, and the SAIL organization responsible for each of the above;
- Monitoring timely developments and updates to the SA&I documentation, such as system requirements (the Lab Lead System Engineer is responsible for ensuring the System Specification is completed), Interface Control Documents (ICDs), verification/test requirements, analyses, and trade study reports;
- Keeping the appropriate SAIL organizations informed of meetings, tasks, schedules, and actions and coordinating systems activities with the Chief Engineer;
- Developing and maintaining current knowledge of the disciplines involved with the project in order to assess the design implementation to assure requirement compatibility and proper design integration;
- Working actions involving commitment or support of design laboratories or the Project Office through/by the appropriate Chief Engineer (EE/EJ);
- Maintaining a current list of systems issues and concerns to assist in identification of problems requiring resolution;
- Supporting the design reviews and serving as a Level IV Change Board member; and
- Briefing SAIL pre-board and board members prior to program board meetings.

One of the most important functions of this engineer is to assure the timely definition of the program system-level requirements.

2.1.1.3.3 Design Laboratories

The other S&E Laboratories plan, perform, and direct research, analyses, design, and development of components, subsystems, and related support equipment. They conduct required component and subsystem development, qualification, and acceptance testing. These Labs also conduct advanced technology studies and maintain state-of-the-art technical expertise in the various engineering disciplines. The scope of the subsystem engineering effort by these Labs encompasses most of the aspects of system engineering, and thus they are part of the overall MSFC system engineering organization.

2.1.1.3.3.1 Propulsion Laboratory

The Propulsion Lab (EP) performs the design, development, and integration of propulsion and mechanical subsystems, mechanisms, their components, and associated support equipment. Included are the propulsion subsystem research, design, development, integration, verification and test activities, and related facilities.

2.1.1.3.3.2 Structures and Dynamics Laboratory

Structures and Dynamics Lab (ED) performs structures and control subsystem requirements definition, design, analysis, and verification. Specific responsibilities include definition of space vehicle aerodynamic, aerothermodynamic, thermal, vibration, acoustic and life support for manned environments. In addition, this Lab analyzes the dynamic interaction of guidance, control, structure, and propulsion subsystems, and is responsible for structural design, stress and thermal analyses, design of thermal protection systems, and operates the fluid and gas dynamic facilities.

2.1.1.3.3.3 Astrionics Laboratory

The Astrionics Lab (EB) performs engineering analyses, develops requirements, designs, develops, integrates, and verifies avionics subsystems including guidance, navigation, control, electrical power, communications, data management, and optics for space vehicles, experiments, and payloads. Maintains EEE parts data base and performs parts failure analysis. This Lab also develops software specifications and performs software system engineering and development for flight and ground systems.

2.1.1.3.3.4 Materials and Processes Laboratory

Materials and Processes Lab (EH) evaluates physical characteristics and engineering properties of metallic, nonmetallic, and composite materials in aerospace applications. In addition, EH operates shops for hardware fabrication and assembly, including production of full-scale engineering models and mock-ups, process development tooling, test support equipment and fixtures, and flight hardware. This Lab also performs failure analyses of flight, qualification, and development hardware, and maintains the NASA database for material properties and processes.

2.1.1.3.4 Mission Operations Laboratory

The Mission Operations Lab (EO) performs mission operations engineering, analysis, and integration for operations control, man-systems integration, training and flight crew support, data management, flight and ground system requirements, mission integration, and orbit analysis. In addition, this lab manages and develops mission support systems, such as the Huntsville Operations Support Center, Payload Operations Control Center, Payload Crew Training Complex, and the Mission Planning System and provides real time on-orbit support.

2.1.2 Other Organizational Responsibilities at MSFC

Basic research in support of the space sciences including magnetospheric, solar, plasma physics, astrophysics, high energy and infrared astronomy, and low gravity science is carried out by the Space Science Lab (SSL). The scientific and engineering objectives, the enabling technologies, and the knowledge of hardware design, carrier capabilities, cost estimates, and mission design at MSFC are initially brought together in the Program Development (PD) Directorate. This directorate develops the concepts, preliminary system and subsystem requirements, and preliminary designs for future launch vehicles, payloads and missions, such as advanced space observatories, geo-platforms and scientific payloads. Advice for both science and technology is actively solicited from the external communities, and technical and scientific expertise is provided by the Science and Engineering (S&E) Directorate. Payload and mission concepts that complete the study phase and are successful in the competition for funding are transferred to a project office, responsible for managing the design and development phases.

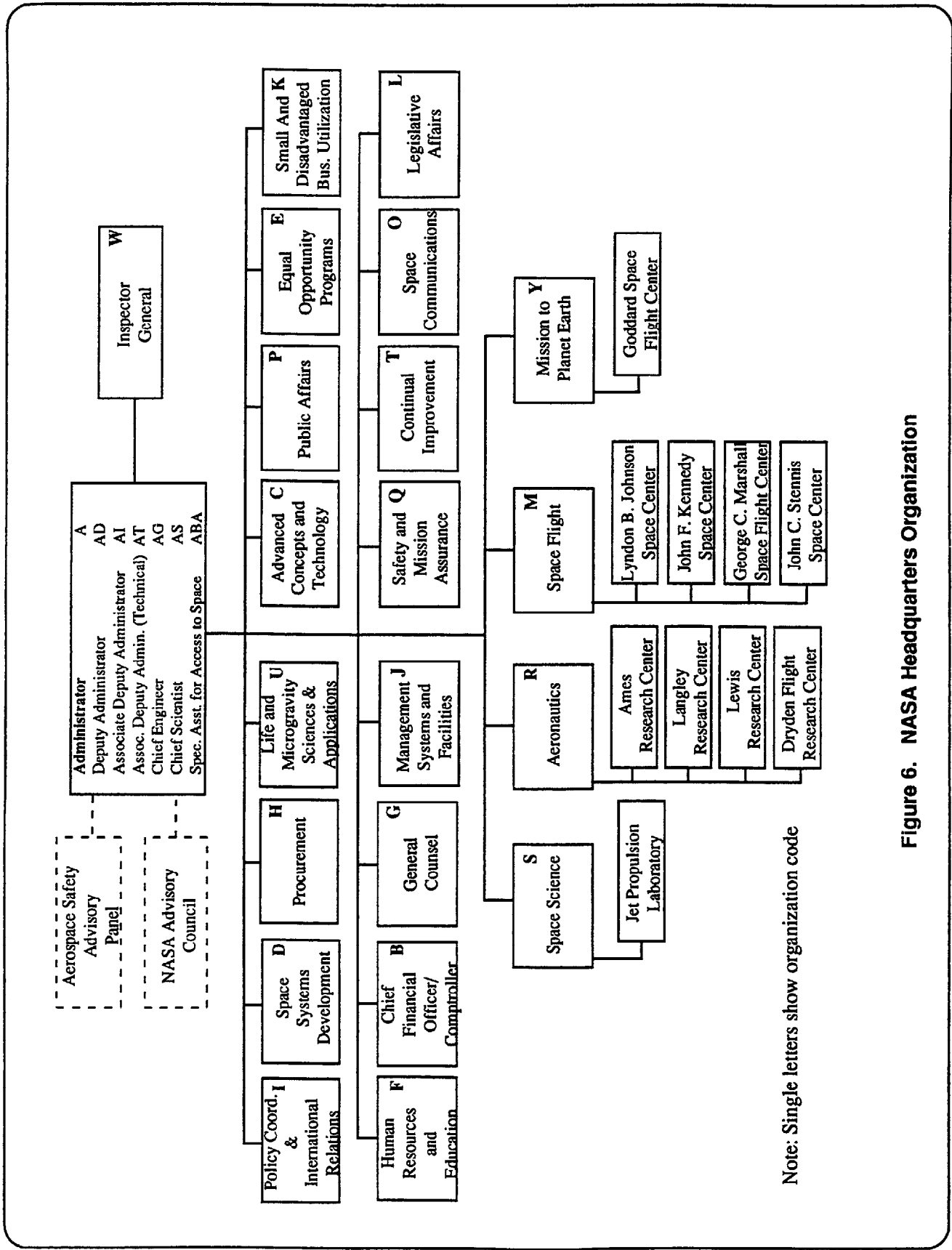
The laboratories in S&E support design development, vehicle/payload/mission integration, and subsequent flight activities throughout the lifetime of space missions. This approach of melding technical and scientific goals, enabling technologies, mission concepts, and project management has proven very beneficial for MSFC, resulting in major engineering and space science accomplishments.

The Safety and Mission Assurance (S&MA) organization is separate from S&E. The S&MA has two reporting channels; to the MSFC Center Director and directly to the Associate Administrator for S&MA at NASA Headquarters. More details on the roles of S&MA and other MSFC organizations which interface with the system engineering organizations can be found in Marshall Manual (MM) 7120.2, Project Management Handbook.

New space program initiatives are focused through various NASA Headquarters offices. Figure 6 depicts the NASA Headquarters organization. Examples of typical working relationships between each of the headquarters offices and MSFC are discussed below.

Codes D, S, and U have the responsibility for scientific satellite programs. Concepts for scientific initiatives are defined by the scientific community and there is always a multitude of exciting and worthy concepts. Program Development assists in furthering the development of these scientific concepts by performing mission feasibility and utility analyses. The process may start with little more than sketches of the optical path of a proposed telescope, for example. Alternatively, a satellite concept may be proposed. The process continues in ever increasing levels of detail until the concept for the telescope and a convincing satellite concept emerge. Initially, there is usually a judgment of cost: high or moderate.

New launch vehicle development is the responsibility of Code M. Congress sometimes requires that new launch vehicle developments be conducted jointly with



Note: Single letters show organization code

Figure 6. NASA Headquarters Organization

the USAF. Typically Program Development performs trade studies comparing vehicle sizing, engine type and thrust level, configuration options, flight performance, and advanced avionics on a continuing basis. Program Development, with support from the Science and Engineering Laboratories, also initiates, promotes, and supports technology development for engines and avionics.

Code C has the responsibility for technology development. Program Development maintains a detailed understanding of emerging technologies to permit evaluation of feasibility or desirability of new initiative launch vehicles, payloads and satellites. Often, preliminary design activities reveal the need for new start technology programs or increased emphasis on existing programs or the need to support and sponsor individual technology specialty groups.

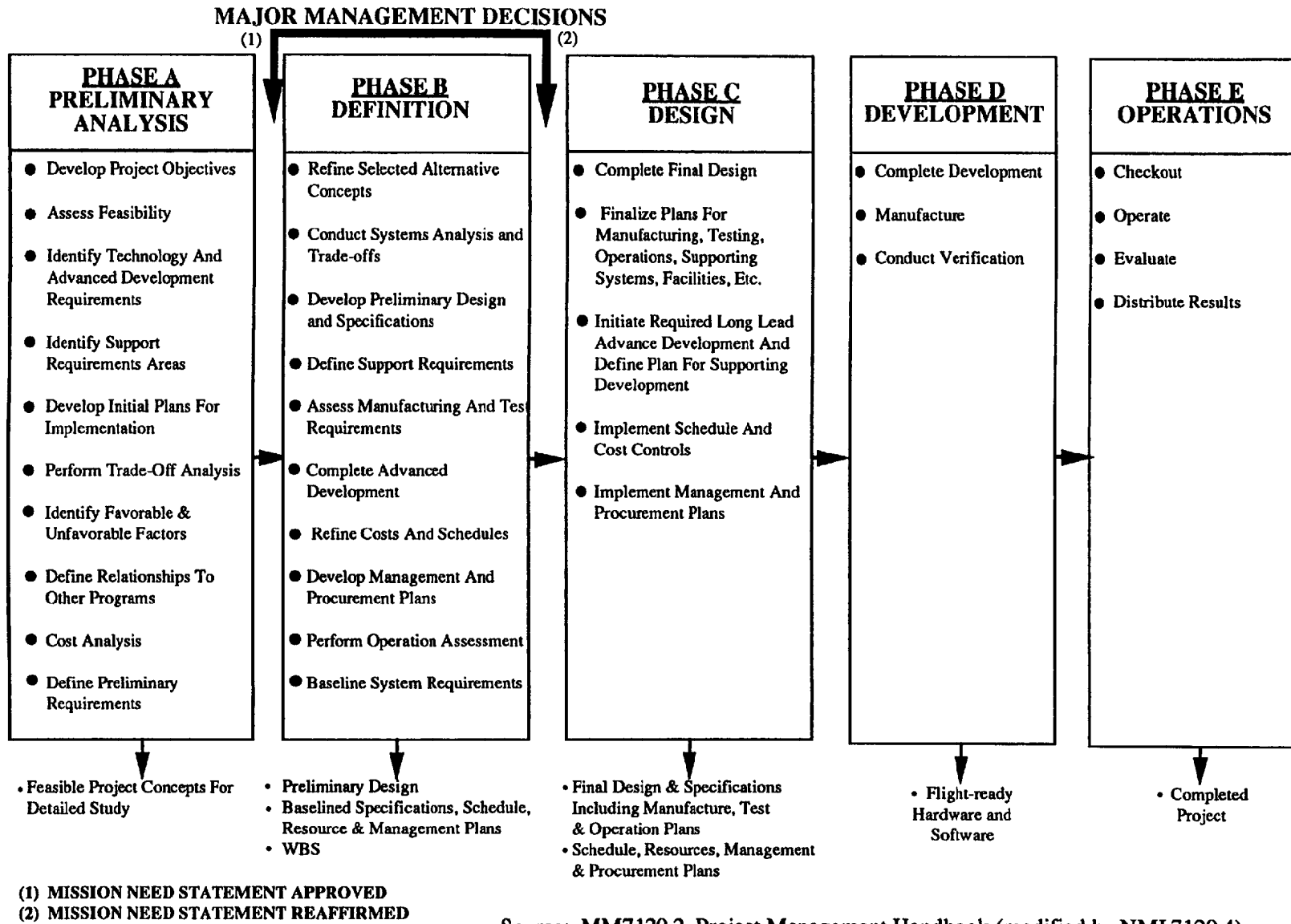
The focal point for new program initiatives at MSFC is the Office of Program Development. Program Development participates with the overall national and international space community and the appropriate NASA headquarters office in decisions leading to commitment for new program starts. Often the Science and Engineering Laboratories at MSFC become involved in supporting Program Development during these activities.

2.2 NASA Phased Project Description

It is extremely important, especially in the planning of major projects, that critical requirements be well defined and the necessary technology be available. If these criteria are met, there will be an acceptable level of risk in meeting technical goals with reasonable cost and schedule.

To ensure that the program is at a proper level of maturity when Congress approves major funding for design and development, projects go through various phases of analysis and definition. The reader is referred to NMI 7120.4 and NHB 7120.5 for additional material on the NASA project life cycle. There are five phases in the life cycle of a typical major project: Phase A (Preliminary Analysis), Phase B (Definition), Phase C (Design), Phase D (Development), and Phase E (Operations). Depending on the complexity of the system, funding availability, and launch schedules; a project may combine phases or add intermediate phases. Common variations would include combining Pre-phase A and Phase A, adding an Advanced Development phase between Phase B and Phase C, or combining Phase C and Phase D into Phase C/D. As a further example, the Space Shuttle program had both a Phase B' (B prime) and Phase B'' (B Double-prime) in order to further refine the definition and requirements of the system before proceeding into Phase C. Figure 7 depicts a typical phased project flow in which Pre-phase A has been combined with Phase A.

Safety is a critical system engineering function which must be considered during all program phases and in all studies and analyses. **In short, although safety is organizationally the responsibility of S&MA, it is a responsibility of all program participants and should be a primary consideration throughout the system engineering process.**



Source: MM7120.2, Project Management Handbook (modified by NMI 7120.4)

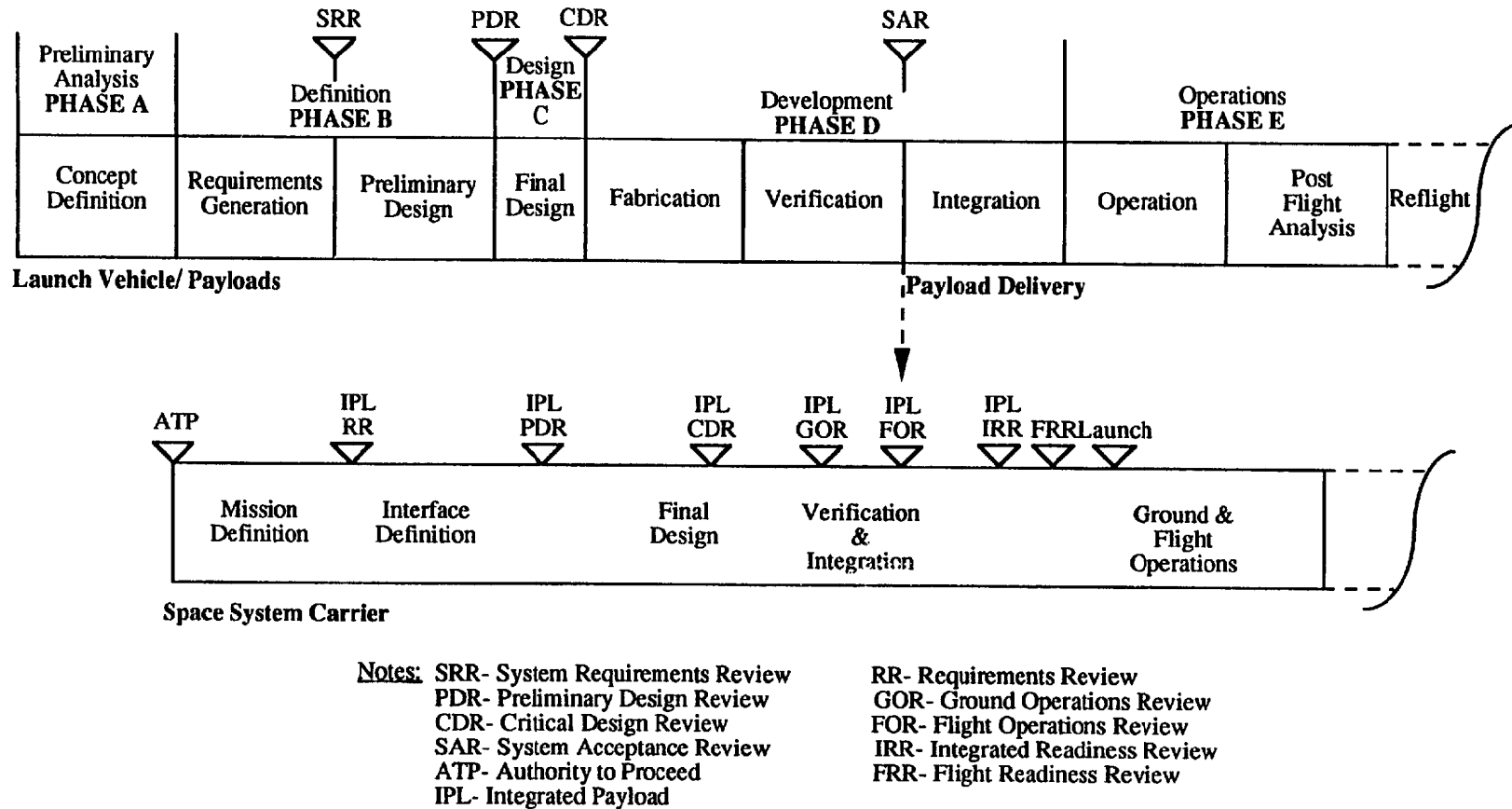
Figure 7. NASA Program Phases

Figure 7 shows the major activities in each phase, as well as the outputs and major decision points. Note that this description pertains to the typical program in which NASA contracts with industry to do the Phase C/D activity. Other types of programs include small, contracted efforts, as well as both large and small in-house programs where NASA may retain all or part of the design and development responsibility. The system engineering process, as described in section 3 of this volume, differentiates these different program types.

The typical program review phasing includes many more activities and formal reviews than are shown in Figure 7. For completeness, these are introduced here and shown in Figure 8. This figure also serves to relate the major reviews to the project phases and to show the more detailed integration activities associated with attached payloads and Spacelab kinds of experiments. Detailed discussions of these reviews and integration activities can be found in Section 3.0 of this volume and Section 5.1 of Volume 2. Note that applicability of individual reviews to a specific program are governed by NHB 7120.5 and the Program Manager.

At MSFC, the Program Development Directorate is responsible for nurturing new projects from idea conception through concept definition supporting preliminary design. System engineering is emphasized and utilized throughout this process, both in-house and during contracted studies. Typically, concepts that have matured through this process and gained "new start" approval to become official projects are then moved into project offices. The "new start" review and approval process begins approximately two years in advance of Phase C/D authority to proceed (ATP) at which point funds are applied to begin a major design and development effort. That two year period is used to execute the definition phase (Phase B) and prepare the request for proposal (RFP) for Phase C/D. The "new start" approval process includes a definition review or non-advocate review (NAR) generally conducted during the Phase B activity at a time when the Project Manager, Center management, and Headquarters Program Office deem appropriate. Results of the NAR are factored into the Phase C/D RFP, as well as the budget approval process. Note that this timeline pertains principally to large programs which include in-house and contracted efforts. The time frame could be much shorter for smaller projects such as experiments. Figure 9 depicts the overall system engineering process flow in Program Development.

The principal processes shown on Figure 9 are outlined in Sections 2.2.1, 2.2.2, and 2.2.3 which follow. In the course of developing the preliminary system requirements and the conceptual design, PD uses many of the same analysis tools and techniques that are employed by S&E in later program phases. The principal differences in the outputs of the two organizations are the quantity, format and maturity of the documentation and the level of detail in the analyses. In summary, the analyses and trade studies by S&E are to refine, not repeat, the concepts developed by PD in support of design implementation. PD develops the conceptual approach, and S&E develops the design implementation.



Note: Program Phases based on NMI 7120.4

Figure 8. Typical Program Review Phasing

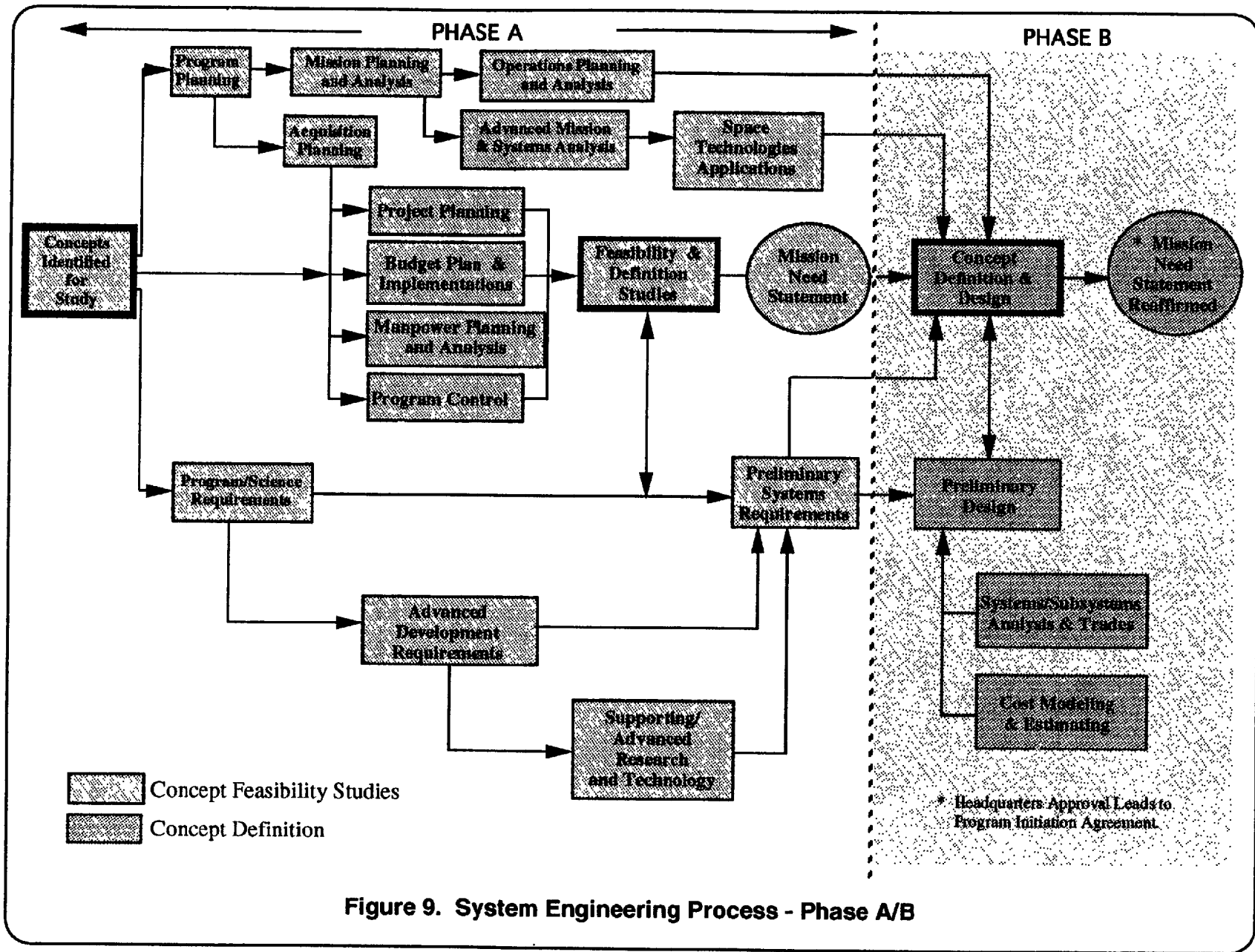


Figure 9. System Engineering Process - Phase A/B

2.2.1 Pre-Phase A (Advanced Studies)

Pre-Phase A occurs prior to the initiation of the program/project life cycle. A pre-Phase A study may be accomplished within the engineering capability of Program Development or contracted with funding from one of the major NASA Headquarters offices. Successful results from this study would provide justification to initiate a Phase A study or additional pre-Phase A studies. The genesis of new ideas requiring further study can come from a variety of sources: industry, the scientific community, university and research centers, MSFC contractors and associates, or from within MSFC itself. Typically, such ideas receive a top-level examination by cognizant MSFC/PD personnel. A quick assessment of objectives, requirements and the total mission concept is performed. Often, new ideas are shared with colleagues through proposals (either in response to an RFP or unsolicited), technical papers at professional society meetings, or "white papers" propounding the new idea/concept. From an MSFC in-house "weeding out" process, concepts are identified for further (Phase A) study.

System functional concept trades are performed during the pre-Phase A period, generally at a fairly cursory level of detail. This process eliminates architectures that are too costly or time-consuming to develop. They are conducted at a level sufficient to support the definition of the top level system requirements. These advanced studies support future programs by exploring potential needs and solutions. Architectural options are the result. Some of the primary sources for this identification of concepts include brainstorming, past experience, examination of other systems, and intuition.

Cost estimates are developed in pre-Phase A and are usually at a very preliminary level due to the lack of detailed systems definition. These estimates are based primarily on parametric comparisons. Known costs from past and current programs are adjusted for the new program, taking into account differences in mission, size, complexity and other factors.

2.2.2 Phase A (Preliminary Analysis)

A Phase A study is the preliminary analysis of a space concept. These concepts could have come from a pre-Phase A study or from other sources within or external to NASA. The majority of concepts that are studied at MSFC are assigned by NASA Headquarters and funded accordingly. This phase and Phase B are principally to establish mission need and a comprehensive definition of the project. Documentation in this Phase usually consists of study reports and briefing charts.

The mission need determination is the first step in a multi-faceted preliminary concept definition activity. This is the step that is first performed at a NASA Headquarters or Center level (or industry, university, etc.) and is the precursor to concept development. The mission need determination is that part of early mission planning that identifies a scientific knowledge need or gap that could be met with some kind of NASA sponsored activity. A set of Level I requirements is generally developed during or just prior to the activities described in the following paragraphs.

A utility analysis is conducted to determine the value of a project. The following criteria may be considered during this study: the needs met, the scientific knowledge acquired, the political benefits, or potential technology spin-offs and applications.

Certain satellites and/or instruments are selected for a more detailed level of design. The Preliminary Design Office of Program Development leads these studies. This office is a miniature replication of the capabilities of the laboratories at MSFC: Propulsion, Guidance, Navigation and Control, Electrical Power, Avionics, Structures, Operations, etc. Cost is an important differential, but often other factors, such as mission risk or incompatibility with other instruments that may be grouped on a common satellite, may predominate.

Schedules are developed during Phase A studies by Program Development in conjunction with the organization performing the study (contractor, PD, S&E). The schedules include an overall program schedule provided by MSFC and a detailed technical schedule developed by the contractor.

The overall program schedule depicts important milestones that establish the start and finish dates of each study phase, including design, development, launch, and operations. Programmatic milestones are also shown. These are dependent on the federal budget cycle plus proposal preparation and evaluation time. The contractor schedule depicts the major activities and phasing required to develop the hardware in time to meet the scheduled launch date. Since this is a concept study, the detail schedule is still at a relatively high level and would not show activity below the system level.

Cost estimates developed during Phase A are generated using a parametric cost analysis system in conjunction with the cost database discussed above. The MSFC has access to several cost estimating systems, both government and commercial. One example is the GE/RCA Price Model. Each model is unique with special capabilities and limitations. Complexity factors and Cost Estimating Relationships are applied to the estimating software using system weight as the independent variable. A factor is applied to the hardware/software costs to account for wraparounds such as project management, test and verification, percent new design, operational complexity, hardware complexity, similarity to other projects or development activities, and others. As each system is defined in more detail and the system weight is further refined, the cost estimates become more realistic and provide a higher confidence level in the results.

A cost/risk analysis and assessment is usually completed near the end of each Phase A study. The analysis is accomplished with special software that uses statistical techniques, including a Monte-Carlo simulation (see Volume 2, Section 4.5.1). The results predict the probability of completing the program within the estimated cost. A risk assessment, which follows the analysis, should identify areas of high risk that require further cost analysis or possibly further trade studies to look at alternate systems that would lower the potential costs without sacrificing technical capability.

As part of the study activity the contractor provides a detailed risk analysis and assessment to establish a high level of confidence for the program cost. The cost estimate established during this phase will provide NASA Headquarters with the funding requirements that will require approval from Congress to begin the development program.

Additional insight into the Phase A and B processes from an agency viewpoint is provided by The NASA Mission Design Process document which was principally developed by GSFC under the auspices of the NASA Engineering Management Council.

The processes occurring during Phase A include:

- Development of project objectives
- Assessment of project feasibility
- Identification of research and advanced technology requirements
- Identification of support requirements areas
- Performance of trade-off analyses
- Identification of favorable and unfavorable factors
- Definition of relationships to other programs
- Selection of systems concepts
- Identification of maintenance, technology insertion, and disposal concepts of payload and orbital debris
- Environmental Impact Analysis

The outputs from Phase A, which become the inputs to Phase B, include information on:

- Concept definition,
- Preliminary system requirements,
- Preliminary configuration layouts,
- Point designs,
- Preliminary Non-Advocate Review Report,
- Preliminary Integrated Program/Project Summary,
- Preliminary Program Plan,

- Project Definition Plan,
- Preliminary schedules,
- Independent Cost Estimate,
- Environmental impact,
- Mission Needs Statement, and
- Phase B/C/D Request for Proposal and Announcement of Opportunity (AO)

2.2.3 Phase B (Definition & Preliminary Design)

The Administrator's approval of the Mission Needs Statement shall constitute approval to proceed to Phase B. This phase of the project consists of the refinement and baseline of system requirements, cost estimates, schedules and risk assessments prior to starting final design and development.

Once the feasibility of an idea is established, the Concept Definition is begun to explore alternatives to meet the documented mission need. Competition and innovation should be employed to ensure that a wide variety of alternatives are identified and examined. Modeling and computer analysis are required to assess the best concepts.

The goal of a concept definition activity is to determine the best and most feasible concept(s) that will satisfy the mission and science requirements. Generally, the requirements available at this point in time are Level I (NASA Headquarters) requirements from preliminary activities.

Level I requirements are broad mission needs and objectives. Occasionally, there may be some Level II (project office level) requirements at this time.

Throughout the Phase B period, the concepts and requirements that were developed during Phase A are iteratively reviewed and analyzed. Using trade study techniques, the concepts' capabilities are compared to the system requirements. Those concepts that consistently satisfy the requirements are identified and refined. Any concepts that do not meet performance and other requirements are scrutinized very closely for possible elimination. Following the examination of those that do not perform well, assessments are made regarding their augmentation to discover the degree of change necessary to bring their performance into scope. The concepts that have to change too much or would experience severe budgetary and/or schedule impacts are deleted from the concept definition and analysis cycle. This allows the analysts' energies to be focused on those concepts that are valid and workable.

These trade studies provide a more detailed look at the architectural concepts and result in a narrowing of the field of candidates. Trades performed during this time consider such things as cost, schedule, lifetime, and safety. The evaluation criteria used

to assess alternative concepts are developed to a finer level of detail than for earlier system trades.

Cost estimates from Phase A are refined as further detailed requirements are identified during Phase B. The cost estimating process is still dependent on parametric analysis. The Program Development Cost Office works closely with the study contractor in evaluating costing methodology and continuously compares government cost estimates with those of the study contractor. Should a large discrepancy occur, the assumptions and schedule inputs of the study contractor are examined. If this examination yields valid assumptions and schedules, the NASA estimates are adjusted. The cost estimation process goes through continuous iterations during the study to reflect the evolution of detail resulting from trade studies.

Schedules are developed during Phase B by the Task Team Program Control personnel and by the study contractors. Schedules developed by the Task Team are expanded from the Phase A overall program schedules. Task Teams include membership from PD, S&E, and S&MA. In addition, other schedules are developed that include Phase C & D procurement strategies, cost phasing and project manning requirements. The study contractor schedules are expanded to lower levels of the Work Breakdown Structure (WBS) to include subsystem development, program management, manufacturing, verification, logistics planning, operations planning and other technical areas. The schedule detail would show the phasing of all major activities through launch and the follow-on operations.

The processes occurring during Phase B include:

- Development of an S&E Implementation Plan (in-house projects),
- Refinement of selected alternative concepts,
- Performance of trade-off analyses,
- Performance of system analyses and simulations,
- Refinement of system and support requirements,
- Definition and assessment of preliminary manufacturing and test requirements,
- Identification of advanced technology and advanced development requirements for focused funding,
- Refinement of preliminary schedules,
- Refinement of preliminary cost estimate and trade study results which support selection of baseline for cost estimate,
- Assessment of technical, cost, and schedule risks, and

- Reaffirmation of the Mission Need Statement.

The outputs from Phase B, which become the inputs to Phase C, may include information related to:

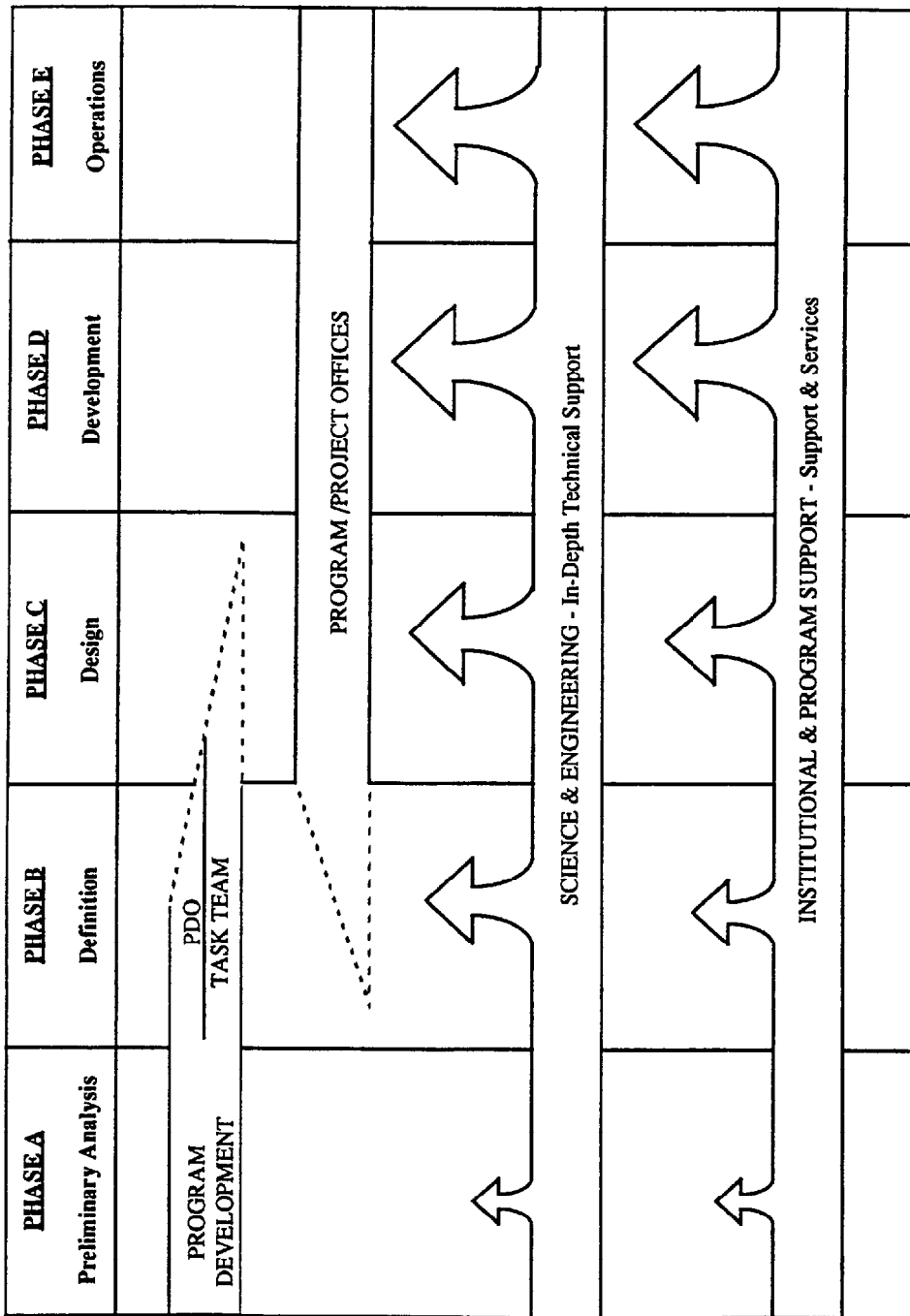
- Work breakdown structure (WBS),
- Baseline System Specification,
- Program Commitment Agreement (PCA),
- Preliminary Design Review (PDR) baseline,
- Project Plan for Phase C/D,
- Contractor Selection Decision and Instrument Selection Decision, if applicable, and
- Non-advocate Review Report.

A separate core of people are selected to form a task team to manage the Phase B contract. At the beginning of Phase B, a Chief Engineer is appointed to the Task Team (or Project Office) to provide consultation to the Task Team Manager on all related engineering matters. The Chief Engineer also helps ensure that the study contractor uses acceptable engineering practices and sound judgment during the course of the study. The Chief Engineer is often the deputy to the task team manager. The Chief Engineer's office has personnel resources available to support the project as needed during the study. Additional engineering support from S&E may be used at the discretion of the Chief Engineer. The Chief Engineer plays a key role in determining the state of technical maturity of the project for starting the final design and development phases.

At the conclusion of Phase B, the task team is converted to a project office, and is no longer under the direction of Program Development. On large projects, such as International Space Station Alpha, a project office might be created prior to Phase B; in which case Program Development support becomes minimal (such as cost estimating and limited programmatic) and S&E plays a major role in the Phase B engineering activities.

At MSFC, it is not uncommon to have more than one directorate providing engineering or technical support to a project throughout its life cycle. During Phase B, transition from a PD-focused concept and requirements definition activity to an S&E-focused design and implementation activity occurs as depicted in Figure 10.

Figure 10 shows that Program Development typically performs most of the technical support during Phase A. As the project life cycle evolves, the Science and Engineering (S&E) Directorate takes on a larger and larger role as PD's involvement



Source: PD Lead Engineer's Guide (Modified)

Figure 10. MSFC Support Relationships In Project Phases

tapers off. The exact point at which S&E gets involved varies depending on the size and priority of the project at MSFC, as well as the availability of S&E manpower resources.

Since the publication of the 1st Ed. of this handbook, there has been a noticeable trend toward earlier involvement of S&E in Phase B, in particular. In most cases, however, Phase C and D activities are exclusively the domain of S&E.

The extent of information and the level of detail resulting from Phase B to begin the Phase C design is variable, and is a function of the time and money made available for the conduct of Phase B studies. The hand-over of technical responsibility from PD to S&E is an interface which requires a great deal of attention to minimize transition issues and project disruptions. A key issue to be addressed is the type and content of documentation produced in Phases A and B. The recent trend toward earlier S&E involvement in phase B projects should help mitigate the rework needed.

2.2.4 Phase C (Design)

Approval to initiate Phase C (or C/D) is obtained through Administrator approval of the Program Commitment Agreement and Program Associate Administrator approval of the final Project Plan. This phase requires Congressional budget approval for projects large enough to be separate line items in the NASA budget submission. Funding must be approved and available at the start of Phase C. Detailed design is accomplished and plans are refined for final development, fabrication, test and operations.

The processes occurring during Phase C include:

- Completion of detail design,
- Performance of detailed system analyses,
- Development of final manufacturing, testing, verification, integration, operations, supporting systems, and facilities plans,
- Refinement of schedules and cost estimates, and
- Implementation of management and procurement plans.

The outputs from Phase C, which become the inputs to Phase D, include:

- CDR baseline, including,
- Baseline detail design and CEI specifications,
- Baseline interface control documents (ICDs), and
- Verification requirements and specifications.

It is typically at the beginning of Phase C, when industry is heavily involved in design and project funding is increased dramatically, that many formal documentation requirements are contractually imposed. This can contribute to large cost increases over previous estimates in Phases A and B, and dictates the need for early inputs from the S&E engineering organization to assure that design and performance requirement specifications and data requirements (DRs) are incorporated into initial cost estimates. For a list of system engineering DRs and core specifications and standards, see Volume 2, Sections 2.1.2. and 3.1, respectively.

At MSFC, the design phase is normally combined with the development phase to form a Phase C/D. The resulting contract takes the Phase B data, refines it into a final design, develops and fabricates the hardware, tests and flight qualifies it, and supports the flight/mission operations.

2.2.5 Phase D (Development)

During this phase of a project, flight hardware and software are developed, manufactured/coded, tested and qualified for flight.

The processes occurring during Phase D include:

- Development and test of prototype/protoflight hardware,
- Verification/Validation - Qualification of hardware and software for flight,
- Manufacture and integration of flight hardware,
- Checkout of flight systems,
- Launch operations, and
- Initial Flight operations including deployment, engineering evaluation, and operational acceptance characterization.

The outputs from Phase D include:

- Successful turnover of the system to the user,
- Documentation and evaluation of the on-orbit verification results and anomalies, and
- Documentation of lessons learned.

2.2.6 Phase E (Operations)

During this phase of a project, support is provided for the flight operations to satisfy the mission needs.

The processes occurring during Phase E include:

- Flight operations, and
- Retrieval or disposal of payload and orbital debris

The outputs from Phase E include:

- A successful mission,
- Documentation and evaluation of the results and anomalies, and
- Documentation of lessons learned.

In the early days of space flight, MSFC provided expendable propulsion systems, so most project activity terminated when launch operations were complete. As the mission of MSFC evolved into payloads and experiments, its role in the area of mission operations and maintenance greatly expanded and now provides an important function in present projects such as Spacelab, the National Space Transportation System (NSTS), Hubble Space Telescope (HST), the Advanced X-Ray Astrophysics Facility (AXAF), and the International Space Station Alpha (ISSA). These programs involve 15 to 30 years of technology insertion, operations, and maintenance activities that would justify a separate independent phase in their life cycles.

2.3 NASA Payload Classification

Payload classification provides a basis for mutual understanding, among all organizations involved, of the general approach taken with respect to safety, costing, document tailoring and the cost versus risk trade decisions for specific equipment. A payload is described as any equipment or material carried by the launch vehicle that is not considered part of the basic launch vehicle itself. Items in this category include free-flying automated spacecraft, coherent experiment units, individual experiments, payload support equipment, and instruments.

Figure 11 illustrates a typical payload classification process. This process consists of establishing the class (as shown in the figure), and then identifying any class-based requirement deviations. NASA Management Instruction (NMI) 8010 is the payload classification instruction documents currently in use at MSFC and should be consulted for details.

A summary of the payload classifications follows:

Class A Minimum Risk: payloads for which a minimum risk approach is clearly dictated. This could be due to a prohibitively high cost for the consequences of failure, or through an unacceptable combination of the costs and less tangible factors associated with failure. An example is the Hubble Space Telescope.

Class B Risk/Cost Compromise: payloads for which an approach, characterized by reasonable compromise between minimum risks and minimum costs, is appropriate

due to the capability of recovery from in-flight failure by some means. This would hold true even if it involved significantly high costs and/or highly undesirable intangible factors. An example is the Aeroassist Flight Experiment.

Class C Economically Reflyable/Repeatable: payloads for which reflight or repeat is planned as a routine back-up in the event of in-flight soft failure. A "soft failure" is one resulting in failure of a payload to meet its success criteria, without resulting in any safety hazard or propagation of failure to the launch vehicle or to other equipment. Two examples are the Crystal Growth Furnace and the ASTRO-1 payload.

Class D Minimum Single Attempt Cost: payloads that have objectives worth achieving at a cost not to exceed the amount required for a single, low cost attempt; where formal verification requirements are limited to those necessary for safety and compatibility. An example is the "get-away special" canisters for student-designed payloads.

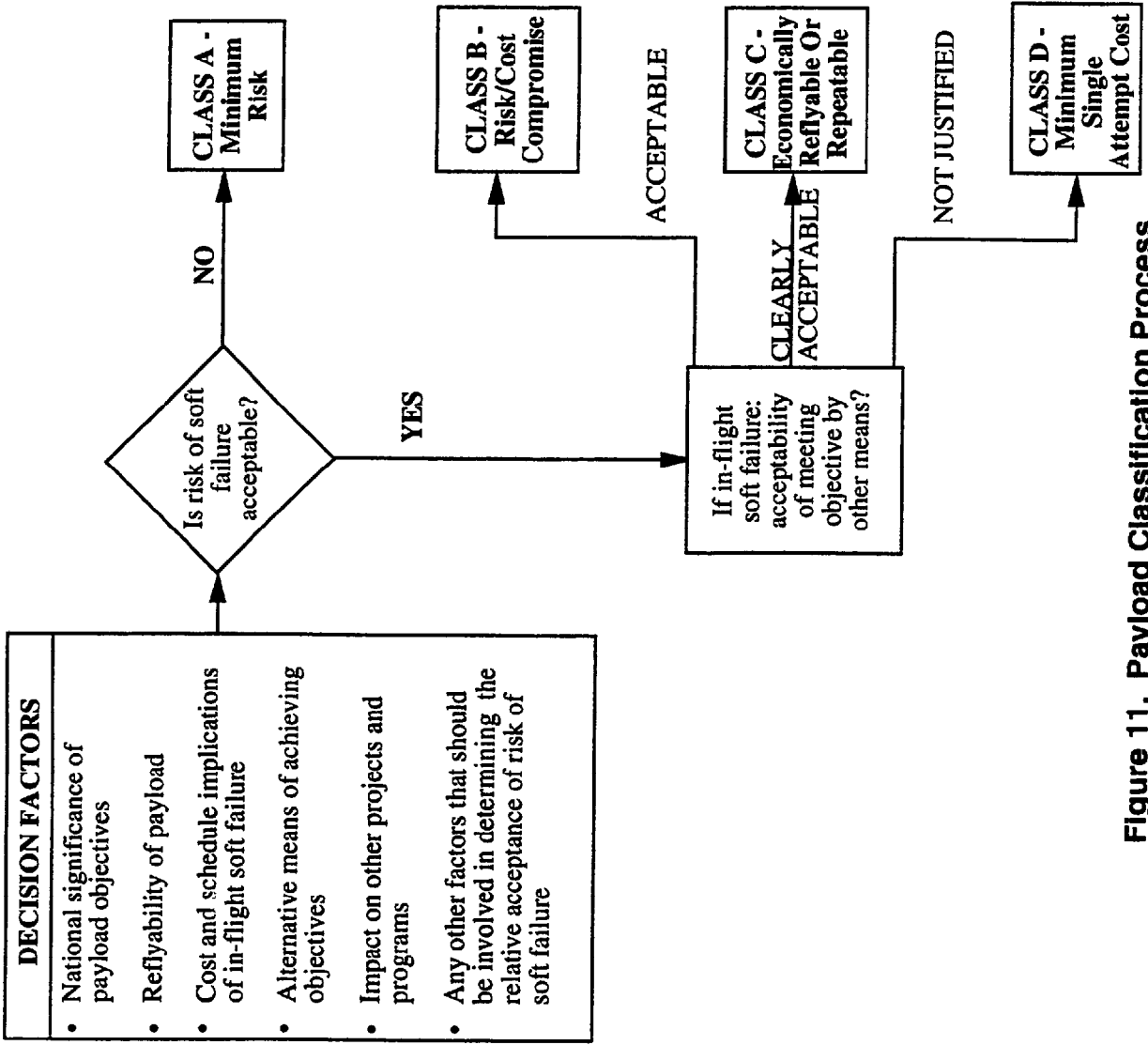


Figure 11. Payload Classification Process

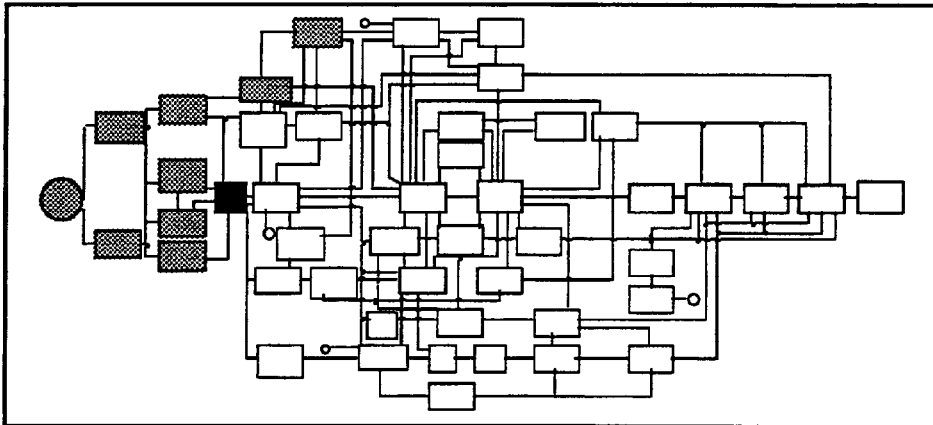
3.0 SYSTEM ENGINEERING PROCESS

As explained previously, programs go through many steps between conception and completion. The system engineering process is an important part of the overall process. This section will address the steps taken during performance of the system engineering activities, with emphasis on "how it is done at MSFC." Each of the sections will address the system engineering activities that go on during that portion of the process. Information as to what is going on in other organizations will be provided as needed, in order to put the system engineering activities in perspective.

Figure 12 is a flow diagram illustrating the entire system engineering process during Phases B/C/D/E. Figure 9 showed the equivalent process used by PD in Phases A and B. Not all of the functions shown on Figure 12 are performed by SAIL. System safety, for example, is the responsibility of the S&MA Office, but it is important for the system engineers in SAIL to have an understanding of how safety fits into the overall system engineering process. Similarly, the mission operations functions of Figure 12 are performed by the Mission Operations Laboratory.

Figure 12 is the "road map" for the rest of this volume. Each of the activities shown is described in detail in the numbered paragraph identified in the appropriate box. These activities have been organized into nine specific areas: (1) Systems Planning and Definition; (2) Systems Requirements Definition and Allocation; (3) Preliminary Design; (4) Detail Design; (5) Fabrication and Assembly; (6) Verification; (7) Launch Operations; (8) Flight Operations; and (9) Post-Mission Evaluation. Please note that not every sub-section in 3.0 has a corresponding box on Figure 12. These exceptions relate mainly to formal review and safety discussions.

3.1 SYSTEMS PLANNING AND DEFINITION



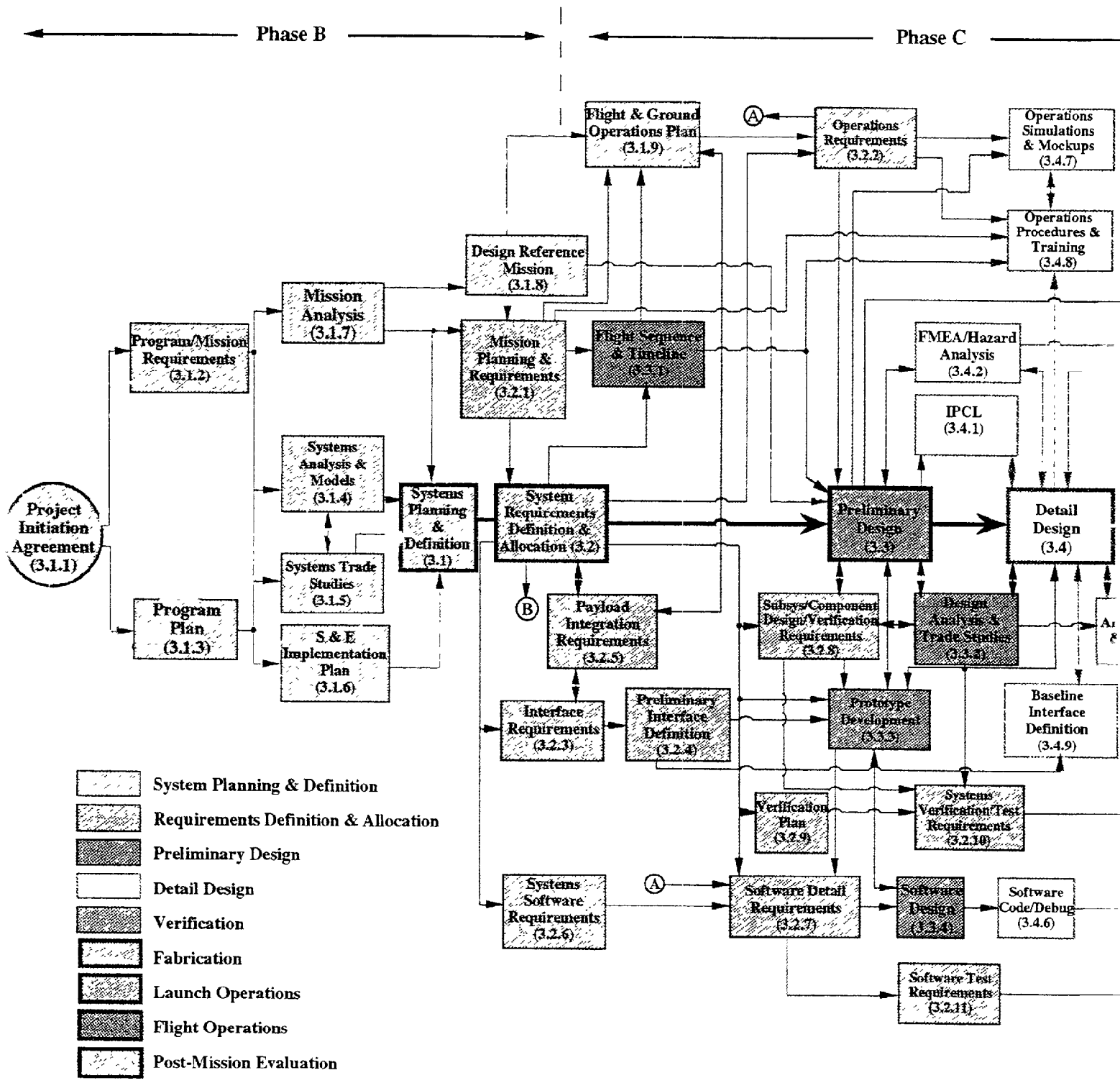
The mini-flow chart at the beginning of each major section to follow is a reference to Figure 12, the "road map" for the rest of this volume. The mini-flow shows the box representing the section heading in black with shading to show the subordinate boxes that are covered in the text under that section. This is done to assist the reader in relating Figure 12 to the individual paragraphs in section 3.0.

As mentioned in the Preface, one of the most important, but often neglected, aspects of system engineering is the basic planning function necessary to identify and schedule tasks and products. In addition to maintaining broad technical knowledge, the system engineer must recognize this inherent need for planning. Too often, we operate in a "reaction engineering" mode responding to one crisis after another. This can be a symptom of poor or inadequate planning up front.

To assist in identification of all required tasks, one should build a work breakdown structure (WBS) or documentation/task tree along with schedules for each identified task. An important step in this process is to establish the "system" definition for the specific program. As presented in Figure 17, this may be at the total vehicle/spacecraft level or may be a single experiment. Usually, the project WBS is produced by the project office or proposed by a contractor (see NHB 9501.2 for more details on the WBS). However, the WBS approach of breaking large tasks down into their sub-tasks is equally applicable to the overall system engineering effort. The tasks should be keyed and planned to support program milestones. This activity should be worked in close coordination with the Chief Engineer and Project Offices. The primary result should be early identification of all tasks and products necessary to support requirements definition and implementation.

This planning activity will also provide visibility for coordination with other S&E and project personnel and provide the basis for establishing manpower requirements. Sample documentation trees are in Volume 2, Section 2.1.1.

For programs involving many complex, interacting tasks, prepare flow charts for each major activity. These flow charts depict inputs, tasks, and outputs and identify need dates and the critical path. Critical activities are those, "... which when delayed



have an impact on the total project schedule"¹ These critical activities comprise the critical path. Refer to Volume 2, Section 2.1.5 for an example of this kind of flow chart, called a Program Evaluation Review Technique (PERT) chart.

3.1.1 Project Initiation Agreement

According to MM 7120.2, "The Project Initiation Agreement (PIA) is an agreement between the Program Associate Administrator (at Headquarters) and the Center participating in the project. The PIA outlines a new project's management and technical interfaces, procurement or in-house acquisition strategy, schedules, resource estimates, uncertainty (technical, schedule, environmental, and cost risks), contingency reserves and all other key ground rules. The PIA is superseded by the approved Project Plan."²

3.1.2 Program/Mission Requirements

The system engineering process must begin with a thorough assessment and understanding of program and mission objectives and requirements. Much of this information can be obtained from the Project Requirements Document and the Experiment Requirements Documents, if applicable.

3.1.3 Program/Project Plan

The Program or Project Plan is prepared in accordance with NHB 7120.5, and describes the overall plan for proceeding with a project. This plan supersedes the PIA, and the format and level of detail may vary with the size, complexity, sensitivity, and other characteristics of the project.

3.1.4 Systems Analysis and Models

3.1.4.1 Performance and Requirements Analysis

Performance and Requirements Analysis includes concept definition, preliminary engineering and trade analyses, subsystem analyses, mission planning and operability analyses, navigation and control analysis, flight mechanics and performance analysis, and operations planning analysis (both ground and flight operations).

System analyses and models are used to evaluate the various feasible approaches and predict performance. The output of these system analyses should reflect a preferred system configuration concept. The system engineering feedback provisions shown in Figure 1 are important in the requirements identification, analysis, and system definition activities. The role of the system engineer in this process is discussed in Section 2.1 of this volume.

¹ Glossary, Defense Acquisition Acronyms and Terms, Fourth Edition, Defense Systems Management College, October 1989, p. 30.

² MM 7120.2A, Project Management Handbook, June 1989, p. II-5.

Models and analyses are iteratively refined and the results are included/documentated in the form of design drawings, process specifications, analysis reports, and model (computer) documentation. End item specifications are refined with the incorporation of analysis and model results.

3.1.4.2 Risk Management

Risk management includes the related activities of risk planning, risk assessment, risk analysis, and risk handling.¹ In general, the project manager or another official in the project office should have responsibility for risk management, since the evaluation of risk is subjective and decisions on the extent of risk mitigation require consideration of a broad range of issues such as budget, technical, and programmatic. Each of the risk management activities will be briefly discussed below.

Risk Planning is the structured process of eliminating, minimizing, or containing the effects of risk. Generally, items are identified as risks if events can prevent the project from meeting its performance, cost, or schedule goals. The goal of the risk manager is to raise the awareness of all project participants to the need to continuously examine risk areas and solutions to identified risks.

Risk Assessments are conducted continuously to identify the risks to a program due to technology considerations (i.e., new designs, materials, processes, operating environments), availability of vendors, failure modes, schedule optimism, margin allocation, and requirement stringency, to name a few. During Phase C/D activities, risks identified during Phases A and B are reevaluated to determine whether they have been adequately controlled or eliminated. Also, it is necessary to identify any potential risks that arise as a result of design implementation and to incorporate risk mitigation. The key to an effective risk management program lies in the thoroughness and continuity of the risk assessment activity.² Additional details are given in MMI 1700.18.

Risk Analysis is the process of describing and quantifying the risk and developing alternatives for risk mitigation or elimination. Cause, effect, and magnitude of the risk are key outputs of this process, and these can be documented and tracked through a "watch list".³ This is an identification of the risk, its consequences, the warning signs or events which will trigger the risk, and risk handling steps. The "watch list" must be continually reviewed and revised during the project life cycle.

Risk Handling embodies the techniques and methods of reducing or controlling risks. Without risk handling there is no risk management. "Generally the techniques for reducing or controlling risks fall into the following categories: 1) avoidance,

1 Systems Engineering Management Guide, U.S. Government Printing Office, January 1990, p.15-1.

2 Systems Engineering Management Guide, U.S. Government Printing Office, January 1990, p.15-2.

3 Systems Engineering Management Guide, U.S. Government Printing Office, January 1990, p. 15-8.

2) prevention (control), 3) assumption (retention), 4) transfer, and 5) knowledge and research."¹

In summary, risk management is an essential element of a successful program. Although the system engineers are usually not charged with the overall responsibility for implementing risk management, they should be major contributors to identifying technical risks and developing alternative solutions. At MSFC, the S&MA Office has responsibility for risk analysis.

3.1.4.3 Cost Assessment

Primary costing in support of new programs is performed by the costing organization in PD. To support realistic cost estimates, MSFC keeps current a cost database including all completed NASA programs, and many unclassified DoD space flight programs, within the past 25 years. The data are categorized into manned and unmanned programs, and further separated into other cost subcategories such as recurring, non-recurring, hardware/software systems, design, development, manufacture, test, operations, and management.

Typically, costs are estimated during Phases A and B for contracted efforts. Cost and performance monitoring and tracking begin with Phase C. A study manager from the Program Development organization initiates discussions with the Program Planning office for cost estimating support. The cost estimating activity can be performed with varying degrees of resolution and accuracy depending on the fidelity of the inputs. For example, a cost estimate can be generated using only the estimated weight of the completed system. Other parameters that define the system such as computing requirements, mass storage, similarity to past projects, etc. can also be used by the cost estimating software. As more information (such as percent new design, performance characteristics, schedules, and better definition of the system) is generated, the cost estimates are refined. This is a highly iterative process and is essentially continuous throughout Phases A and B.

3.1.5 Systems Trade Studies

The system concept trades, performed by the Preliminary Design Office of Program Development during Phase A, are feasibility studies conducted with general assumptions and definitions. As the program progresses into Program Definition/Concept Validation (Phase B), the emphasis shifts to determining the optimum approaches for accomplishing the goals of the program. During Phase B, determination of program requirements and selecting the concept which best satisfies overall program requirements takes precedence. These early trade studies address the allocation of requirements and resources to the systems which will make up the program. It is at that time that risky technologies and/or highly complex systems are identified.

¹ Systems Engineering Management Guide, U.S. Government Printing Office, January 1990, p. 15-8.

As S&E support phases into the program, additional, more detailed trades and analyses are performed by S&E personnel. These trades primarily support the development of design and performance requirements and specifications. Objectives of system engineering trade studies in Phases C and D include providing the most cost-effective design implementation, integrating and balancing all design-for and engineering specialty requirements, and avoiding the tendency to go directly to a point design based on past experience.

Optimization of the total system design in meeting project requirements and mission needs is the responsibility of the system engineer. Engineers, by their nature and training, will seek to optimize the components, boxes, or subsystems for which they are responsible; however, optimization of the individual parts of the system may not result in the optimum total system. The system engineer, therefore, must constantly examine through, trade studies, the effects on the total system as the designs evolve. Where designer optimization of a subsystem impacts negatively on system optimization, the system engineering organization must provide recommendations to assist the program chief engineer in selecting design options. More details on trade studies are given in Volume 2, Sections 4.2.1 and 4.2.2.

3.1.6 S&E Implementation Plan

An S&E Implementation Plan (analogous in some ways to a System Engineering Management Plan in industrial settings) is a very important document that defines specifically what the organization performing the work is going to do for the project. For contracted (out-of-house) efforts this document is a deliverable which specifies the engineering tasks the contractor will perform in response to the Statement of Work (SOW). It includes manpower loading and schedule planning and is generally broken down organizationally.

The S&E Implementation Plan should be completed during Phase B or at the beginning of Phase C and is the lead document for defining S&E support for the program. It specifies tasks for the individual laboratories, such as, "SAIL shall develop ICDs and Structures and Dynamics shall perform the structural analysis." The Implementation Plan should be specific on what is requested/required from each laboratory. The program Chief Engineer has the lead responsibility for preparation, coordination, and maintenance of the Implementation Plan with the support and involvement of the S&E Labs, working through the Lab Lead Engineers. A sample Implementation Plan outline is in Volume 2, Section 2.1.3.

3.1.7 Mission Analysis

Mission analysis in S&E is the discipline within system engineering which develops, analyzes, and documents mission requirements leading to the definition of the most effective and efficient methods of satisfying mission objectives. Mission analysis may be defined as the process of translating the high level project requirements (Level I and II) for operating a system into a carefully analyzed, detailed mission profile. The activities required to perform mission analysis are divided into three

distinct areas as discussed in the following paragraphs: Mission Requirements Analysis, Mission Profile Generation, and Mission Performance Analysis.

3.1.7.1 Mission Requirements Analysis

Mission Requirements Analysis (MRA) is an orderly transformation of overall mission objectives into detailed mission requirements. This effort includes the identification, interaction and documentation of overall mission objectives, the breakdown of objectives into detailed mission requirements, the analysis of those requirements, and finally, the development of finely detailed mission requirements and their allocation to individual system elements. These steps can be summarized as follows:

- 1) Delineate the overall mission objectives.
- 2) Translate mission objectives into requirements.
- 3) Analyze and expound mission requirements, and
- 4) Allocate the mission requirements and input to the overall requirement allocation process described in Section 3.2.

3.1.7.2 Mission Planning and Profile Generation

Mission Planning and Profile Generation is the activity accomplished to analyze mission objectives, define system capabilities, and generate a mission profile that maximizes the achievement of mission objectives within hardware, software and mission constraints. Detailed mission requirements provide an input to this activity. The output of this process can be a preliminary mission profile or a detailed Design Reference Mission (DRM). This process can be summarized as follows:

- 1) Perform mission/system assessment
 - a. Trade study - Mission objectives vs. system capabilities
 - b. Define target conditions, data return, and other parameters
- 2) Conduct preliminary hardware/software assessment
 - a. Launch vehicle size/weight
 - b. Propulsion, guidance, and navigation systems
- 3) Develop trajectory design
 - a. Trajectory analysis
 - b. Guidance, navigation, and maneuver analysis

- c. Optimization analysis
- d. Range safety and reentry impact analysis
- e. Tracking/telemetry coverage study
- f. Performance capability analysis

4) Generate mission profile and input to the system design processes described in Sections 3.3 and 3.4 and the flight operations process in Section 3.8.

- a. Mission timeline design
- b. Launch window
- c. Trajectory event profile
- d. Ground track generation

3.1.7.3 Mission Performance Analysis

Mission Performance Analysis is the process of assessing the capability of the system design to satisfy mission requirements. It defines and prioritizes specific mission performance parameters and performs feasibility trade studies to determine and evaluate performance versus cost and risk. The scope of this activity can range from straight-forward parametric studies to sophisticated system simulation models. The steps in this process are described below:

- 1) Interpret mission requirements into a set of measurable performance parameters
- 2) Identify system design features which affect mission performance
- 3) Assess mission performance of system design
- 4) Determine sensitivities of mission performance parameters to selected system design parameters and operational constraints
- 5) Iterate, process, and provide feedback as design and operations concepts evolve

Specific tools and procedures used in Mission Analysis at MSFC are discussed in Section 4.3.1 of Volume 2 of this handbook.

3.1.8 Design Reference Mission

The mission of the end item system under study is more clearly defined during Phase B, but still not baselined. The purpose of defining the mission more clearly is to develop performance targets for the design team to aim for. Baselining does not occur at this point because there may still be multiple concepts under consideration. Once a

single concept is selected, at the end of Phase B and at the beginning of Phase C, the mission can be baselined.

Numerous design reference missions (DRMs) are assembled by the study team at this point in the development scheme. The DRMs are chosen by the program or project office as that mission, or set of missions, that have the greatest impact upon the design and performance specifications of the flight article. The DRMs are realistic missions (i.e., not three-sigma excursions). They are determined by cognizant authority (i.e., by the project office in concert with the user community), usually through a Preliminary Requirements Specification Document (PRSD).

These DRMs allow the designers to satisfy the mission objectives with the concepts under active consideration. The short-comings of the individual concepts are brought to light. The mission objectives that cannot be satisfied by any of the concepts are identified and reevaluation must take place. The concepts have to be augmented to satisfy the objectives, or the objectives must be rescoped, changed, or eliminated completely. This process adds an element of realism to the overall development activity and helps fine tune the development process to achievable goals. The DRMs are also used to place bounds on the anticipated mission drivers for each subsystem.

As previously mentioned, early in a program specific missions may not be finalized. To allow the design process to proceed, a series of DRMs will bound the various performance requirements. As the program matures and specific missions are baselined, the DRMs will be phased out.

3.1.9 Flight and Ground Operations Plan

The process of defining the mission operations is part of the mission operations integration activity. Mission operations integration ensures that the system design is consistent with the operations concept and operational requirements and that mission operations system elements needed during post Initial Operational Capability (IOC) operations are being designed and developed. Mission operations supports system integration by participating in the development, coordination, and baselining of system hardware, software and interface design, and ensuring compatibility with the operations concept.

Mission operations is required to prepare, as well as review and provide inputs to operational documentation. These documents vary depending on the project office/payload user, but typically are one of two types;

- 1) Operational Requirements and Integration - Payload Integration Plan (PIP), PIP Interface Control Document, Annexes, ICDs.
- 2) Implementation and Procedures - PIP annexes, Training Plans, Simulation Plans, Flight Control/Operations Handbooks. Volume 2, Section 2.2.5 provides more detail on PIPs and PIP annexes.

Mission Operations consists of supporting system conceptual definition tasks, identifying mission operations requirements, developing an operational concept based

on these requirements, and supporting the system development and integration phases to ensure that operational concerns are identified and resolved as early as possible.

Mission Operations activity begins during the conceptual phase of the system design process to ensure that operations considerations and concerns are integrated into the system requirements definition. This involvement continues throughout the remainder of the system development process to ensure that the hardware, software, data, documentation, and personnel elements of the system are designed, trained, integrated, tested, and deployed in a manner consistent with customer requirements.

Mission Operations activities permeate system organizational boundaries. The results of Mission Operations trade studies and analyses can have a significant impact upon system hardware and software design. Throughout the system developmental process, from pre-proposal studies through final delivery, Mission Operations is directly involved in system design, development and decision-making activities. This involvement is critically important during the early phases of system development when the basic structure of the system is being defined and the initial system documentation is drafted. Even though actual system operations may be years in the future, the Operational Concept must be established as early as possible to ensure that system development is based upon valid and comprehensive operations scenarios. This operations concept is maintained as a living document to grow and mature as the total project follows its development course.

General documentation such as the Mission Requirements On Facilities/Instruments/Experiments (MROFIE) document (JA-447), the experiment design documents, interface requirements, and spacecraft design documents are used as references and requirements sources for more specific documentation. Specific documentation is that documentation that is project or task specific. Documentation such as Ground Support Equipment (GSE) requirements or the Verification Requirements and Specifications Document (VRSD) are developed from the general project documentation that is available.

Input is also received from the Principal Investigators and designers as requirements and designs are refined into final products. Diagrams showing the relationships among these various documents for non-Spacelab and Spacelab mission payloads are included as Figures 13 and 14, respectively.

The interfaces between the various types of GSE and the experiment, spacecraft, or orbiter must be defined and documented. Personnel on each side of the interfaces must know what is required to ensure compatibility.

Flow diagrams are an integral part of Ground Operations System engineering. The ground operations flow diagrams are a visual representation of the processes for a project. These diagrams can be used to show relationships between activities and project milestones and to relate schedules of various groups of support personnel and engineering teams to the projects. An example flow diagram is shown in Figure 15.

3.1.10 Safety

Early in Phase B of a project, the element developers (if the procurement is a contracted effort) are required to develop a plan for assuring that the proper safety analyses are performed and hazard controls are in place. The contractor also ensures that reliability, maintainability, and quality assurance plans are developed for approval by NASA. If the development is an in-house effort, then the S&MA Office has this responsibility. Thorough knowledge and understanding of systems safety requirements are needed. Although this section is written from the point of view of payload development, similar requirements also apply for spacecraft/launch vehicle development.

The contractor should have personnel (or support from an integration contractor with dedicated personnel) who are familiar and conversant with, as a minimum, the latest revisions of the following documents: NHB 1700.7, "Safety Policy and Requirements for Payloads Using the NSTS"; NSTS 18798, "Interpretations of NSTS Payload Safety Requirements; and KHB 1700.7, "STS Payload Ground Safety Handbook." A knowledge of the technical requirements of NHB 1700.7 and KHB 1700.7 should be augmented by a basic understanding of the safety implementation requirements of NSTS 13830, "Implementation Procedure for STS Payloads System Safety Requirements" and JA-012, "Payload Project Office Payload Safety Implementation Approach." Additional safety specifications and standards are listed in Volume 2, Section 3.2.

A payload safety plan should, therefore, reference all the above noted documents, contain an approach for building the necessary data files, compile a list of the key personnel involved in the project, and demonstrate a thorough understanding of the safety data package development and review process.

The objective of the Safety Program is to protect flight and ground personnel, the launch vehicle, payloads, GSE, the general public, public and private property, and the environment from payload-related hazards. As defined in NHB 1700.7, a hazard is, "the presence of a potential risk situation caused by an unsafe act or condition."

Simply put, safety assurance consists of the following three steps:

1. Hazard Identification - This is the result of a "Hazard Analysis" in which the Payload flight and ground support equipment, along with its attendant flight and ground operations, are analyzed to determine potential hazards.
2. Hazard Control - The method in the design by which the hazard is controlled and/or eliminated. In certain cases this may be accomplished by operating procedures.

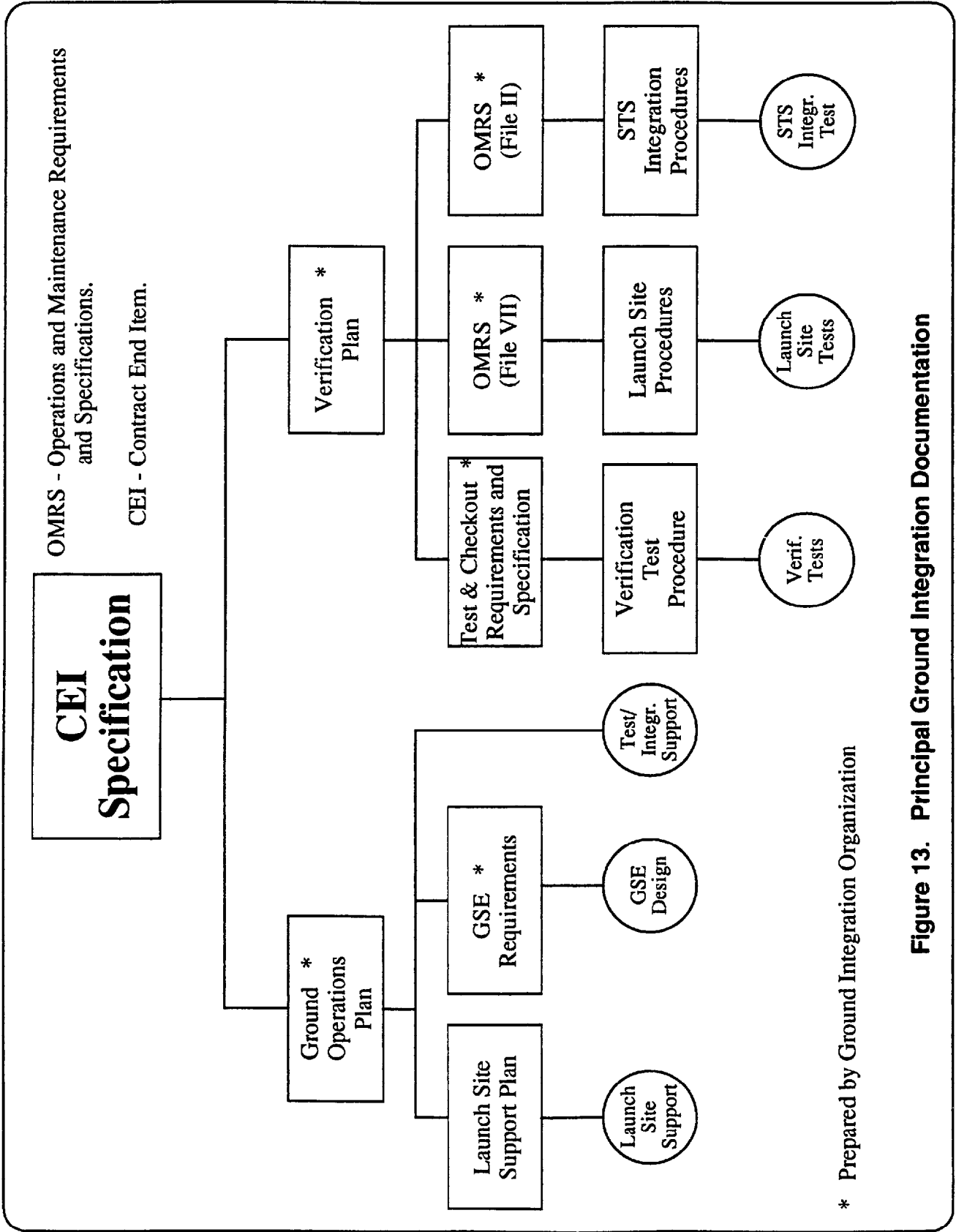


Figure 13. Principal Ground Integration Documentation

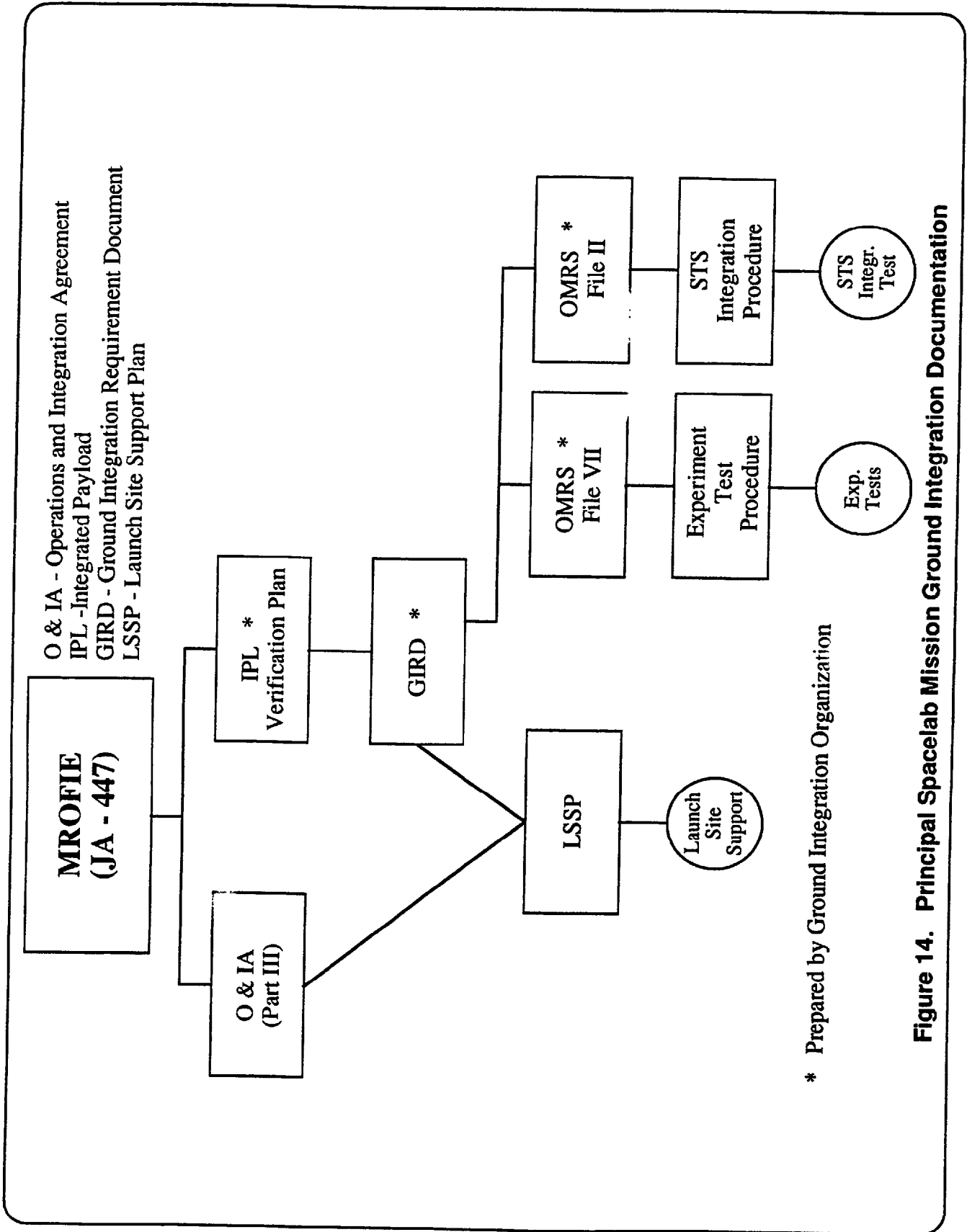


Figure 14. Principal Spacelab Mission Ground Integration Documentation

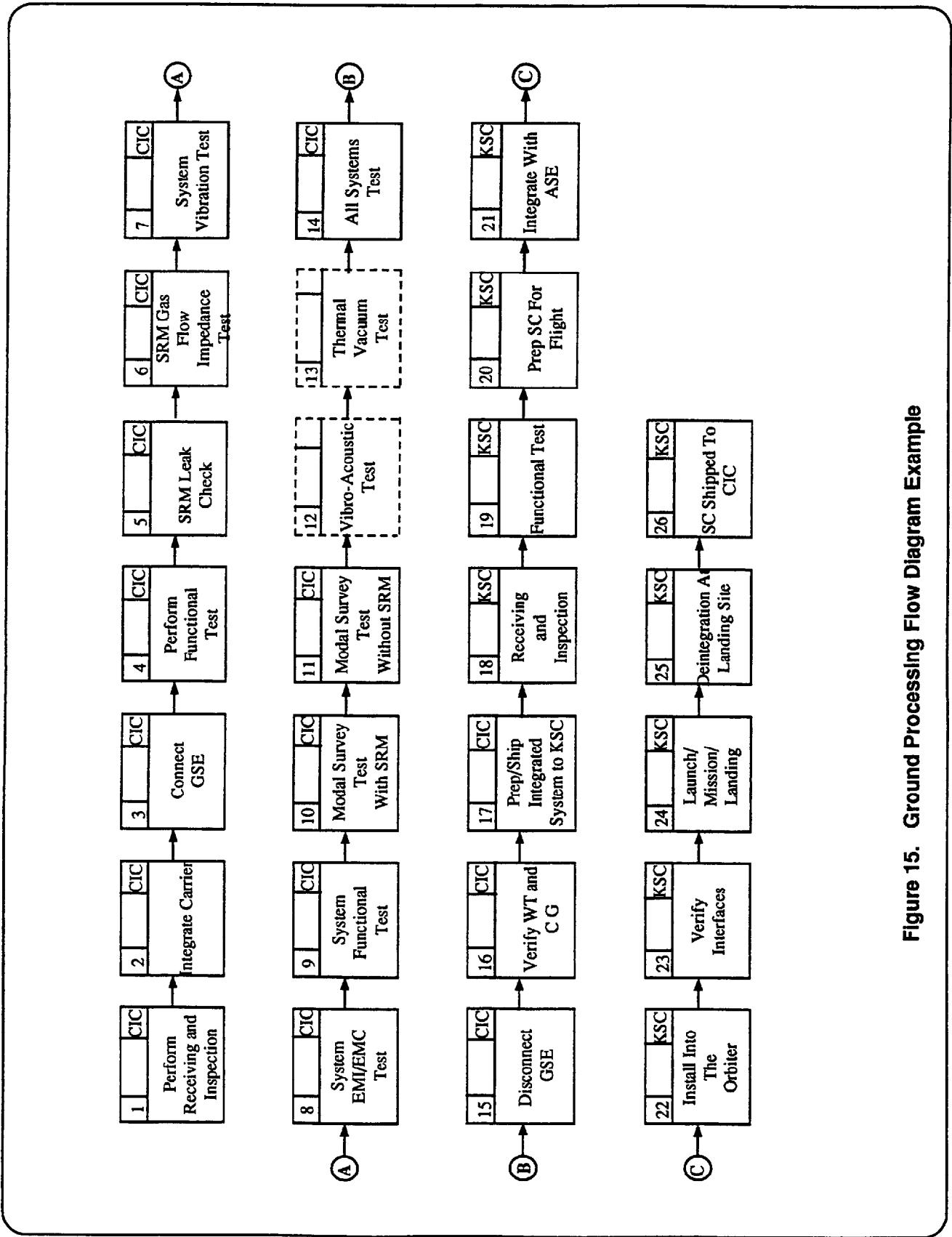


Figure 15. Ground Processing Flow Diagram Example

3. Hazard Control Verification - Demonstration by test, and/or analysis, and/or inspection that the hazard control method performs to specifications and does, indeed, control and/or eliminate the hazard.

The data/information from these steps are documented in "Hazard Reports" and supporting data which are required submissions at appropriate Payload/Program Reviews. These reviews are:

- The Payload Element Developer (PED) Payload Element Reviews and the Payload Mission Manager (PMM) Integrated Payload (IPL) Reviews which are described in Section 4.0 of JA-447.

- The Phase 0, I, II, and III Safety Reviews conducted with the NSTS Operators are described in Section 5.0 of NSTS 13830. The PMM assesses/incorporates the PED safety data given at the PED reviews into an overall Integrated Payload Safety Compliance Data Package which the PMM presents to the NSTS Safety Panels. The PED is encouraged (and in most cases will be required) to participate in these Safety Panel reviews.

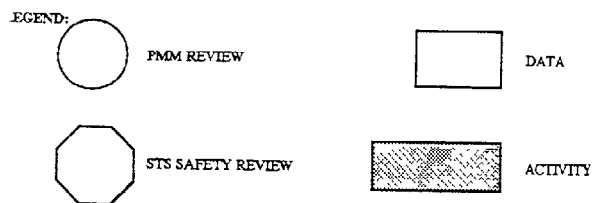
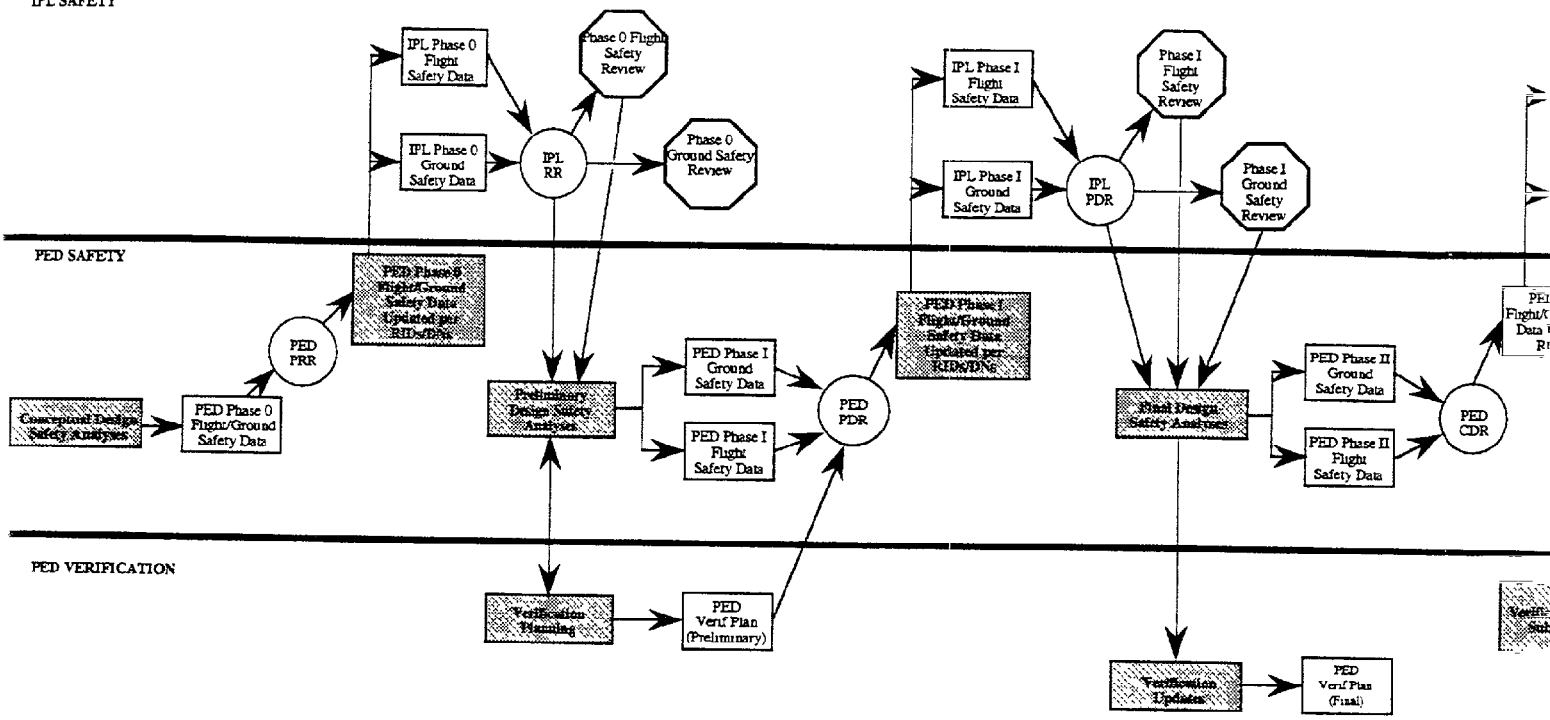
System safety compliance is certified through the completion of the payload safety hazard analyses and the safety review process. The configuration of the system is thoroughly assessed for potential hazards present due to system design or operating procedures. A separate list is prepared for flight equipment/operating hazards and ground equipment/operations hazards. During the assessment of the experiment design, performance, configuration, and planned operations, the evaluator takes a "devil's advocate" position to identify all potential hazards that could cause injury or illness to flight or ground crew personnel, or adversely affect the launch vehicle, Spacelab, or other payloads. No matter how remote the possibility of an occurrence, the evaluator should keep "Murphy's Law" in mind, and no potential hazard should be ignored or left unidentified just because stringent precautions have been taken to prevent the hazard from occurring.

The hazard reports are included as part of the safety compliance data package that is submitted as part of the phased safety reviews. The payload safety review process is as depicted in Figure 16. Each of the individual safety reviews will be discussed briefly in the appropriate sections of this handbook, but the reader is referred to JA-012 for full details.

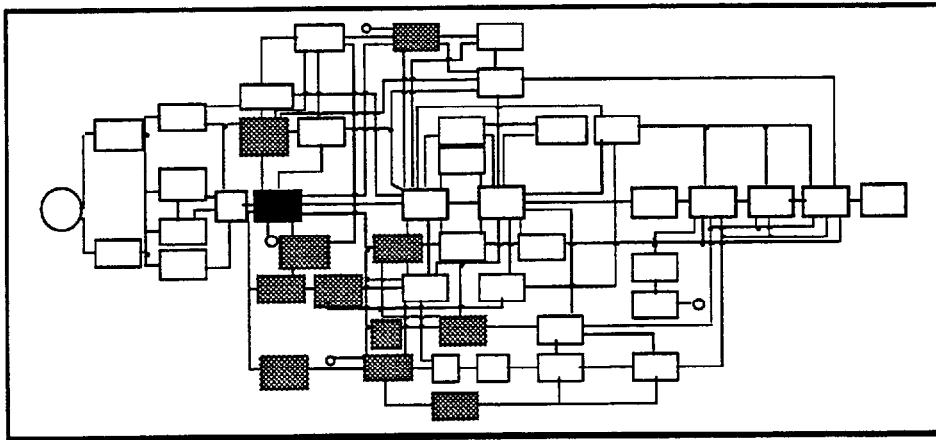
IPL SAFETY

PED SAFETY

PED VERIFICATION



3.2 SYSTEM REQUIREMENTS DEFINITION AND ALLOCATION

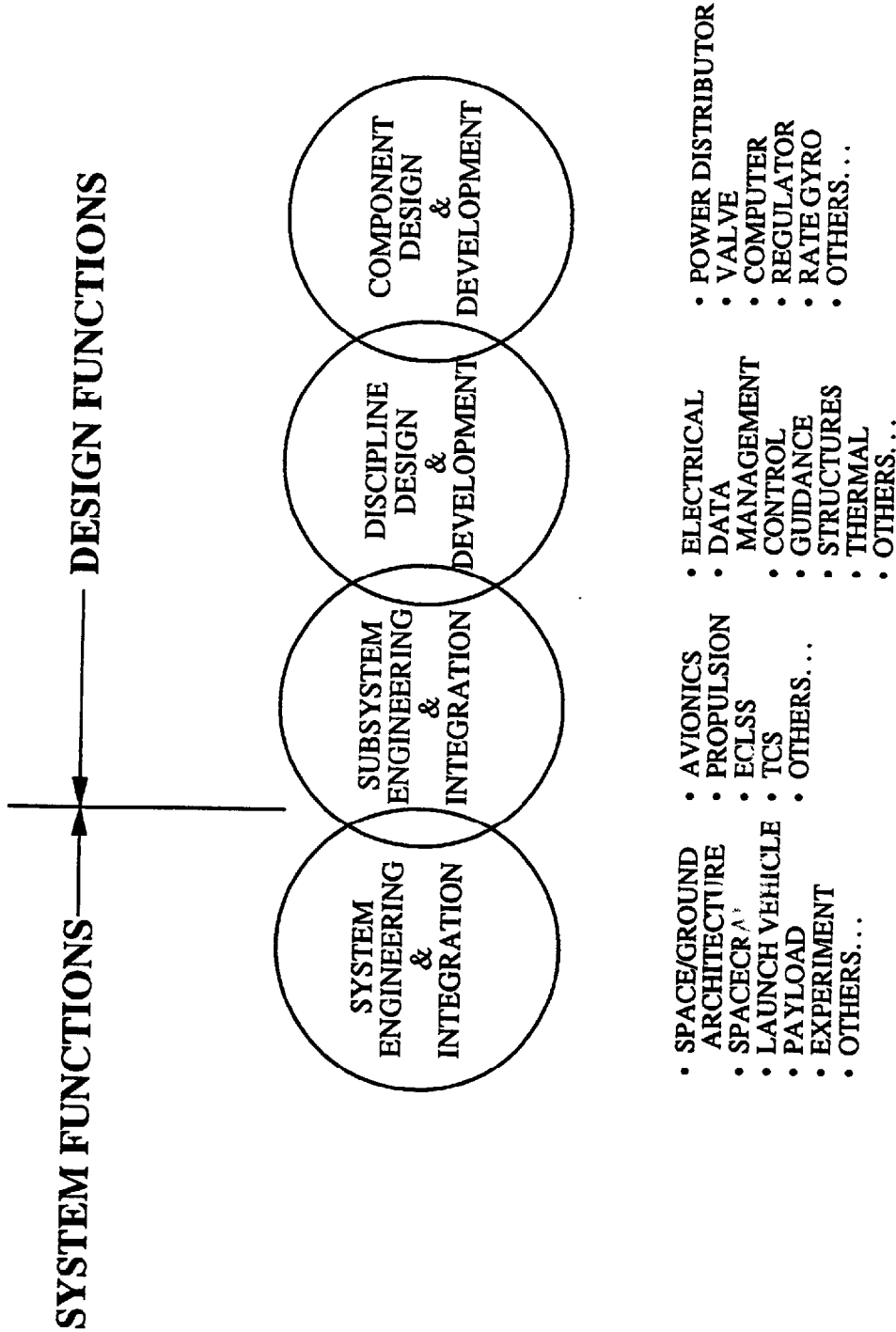


The requirements and concepts developed during Phase A are refined and expanded during Phase B and early in Phase C. This process helps ensure that all requirements are valid and that conflicting or redundant requirements are eliminated. Throughout Phase C, the system engineer monitors system requirements implementation and updates the System Specification (SS), as needed.

The relationship between system engineering and design is conceptually illustrated in Figure 17. The overlapping circles in the figure illustrate the difficulty, for example, in defining where system engineering stops and subsystems/design engineering begins. While it is clear that system functions are the responsibility of SAIL (except for some exceptions already noted) and the design functions are the responsibility of the various other labs in S&E, the responsibility for subsystem engineering and integration is not as easily identified. In general, subsystem engineering is the responsibility of the design labs. In any event, Figure 17 shows the functional relationship between system and design. As someone once said, "Every subsystem is someone else's system."

Requirements flow-down and resource allocation during Phase C are processes where system level functional and performance requirements and system resources are allocated among the various functional subsystems that make up the end item architecture. For example, each subsystem is assigned resources such as weight, volume, center of gravity location envelope, and power availability. **In allocating resources it is important to include adequate margins and contingencies.** See Volume 2, Section 2.5.1 for a discussion and examples of margins and contingencies.

Functions are also assigned to subsystems. For example, prime power generation and regulation would likely be allocated to an electrical power subsystem and structural support allocated to a structural/mechanical subsystem.



"Every Subsystem is Someone Else's System"

Figure 17. System/Design Functional Relationships

While some allocations appear obvious, others require engineering decisions. Temperature sensing could be allocated to command and data management, electrical power, avionics, or a separate thermal control subsystem. While requiring engineering judgment and analysis, this decision can be influenced by the workload in a given subsystem development organization, the responsibility for similar functions, historical influences, and other factors.

The System Specification contains the system level requirements and performance specifications. The document includes a general description of the vehicle/spacecraft or experiment system and a mission overview. The design and performance requirements for the end item are specified and these requirements are generically broken down into the areas shown in Table II.

Table II. Design And Performance Requirements Breakdown

* Mission Requirements	* Thermal Protection System (TPS)
* Operational Requirements	* Communications and Data Management
* Mechanical Performance Requirements	* Guidance, Navigation, and Control (GN&C)
* Electrical Performance Requirements	* Physical
* Airborne Support Equipment (ASE)	* Reliability
* Ground Support Equipment (GSE)	* Maintainability
* Operational Availability	* Propulsion
* Safety	* Storage
* Environment	* Design & Construction Requirements
* Transportability/Transportation	* Logistics
* Verification	* Personnel and Training
* Interface Requirements	* Human Factors

The process flow for developing the SS is shown in Figure 18, and a generic outline for the document is in Volume 2, Section 2.2.1 of this handbook.

3.2.1 Mission Planning and Requirements

Mission Planning and Requirements assessments are made to determine the following things about the mission of a project:

- Mission needs (e.g., orbit/inclination)
- Mission timing
- Special mission requirements
- Objectives to be accomplished

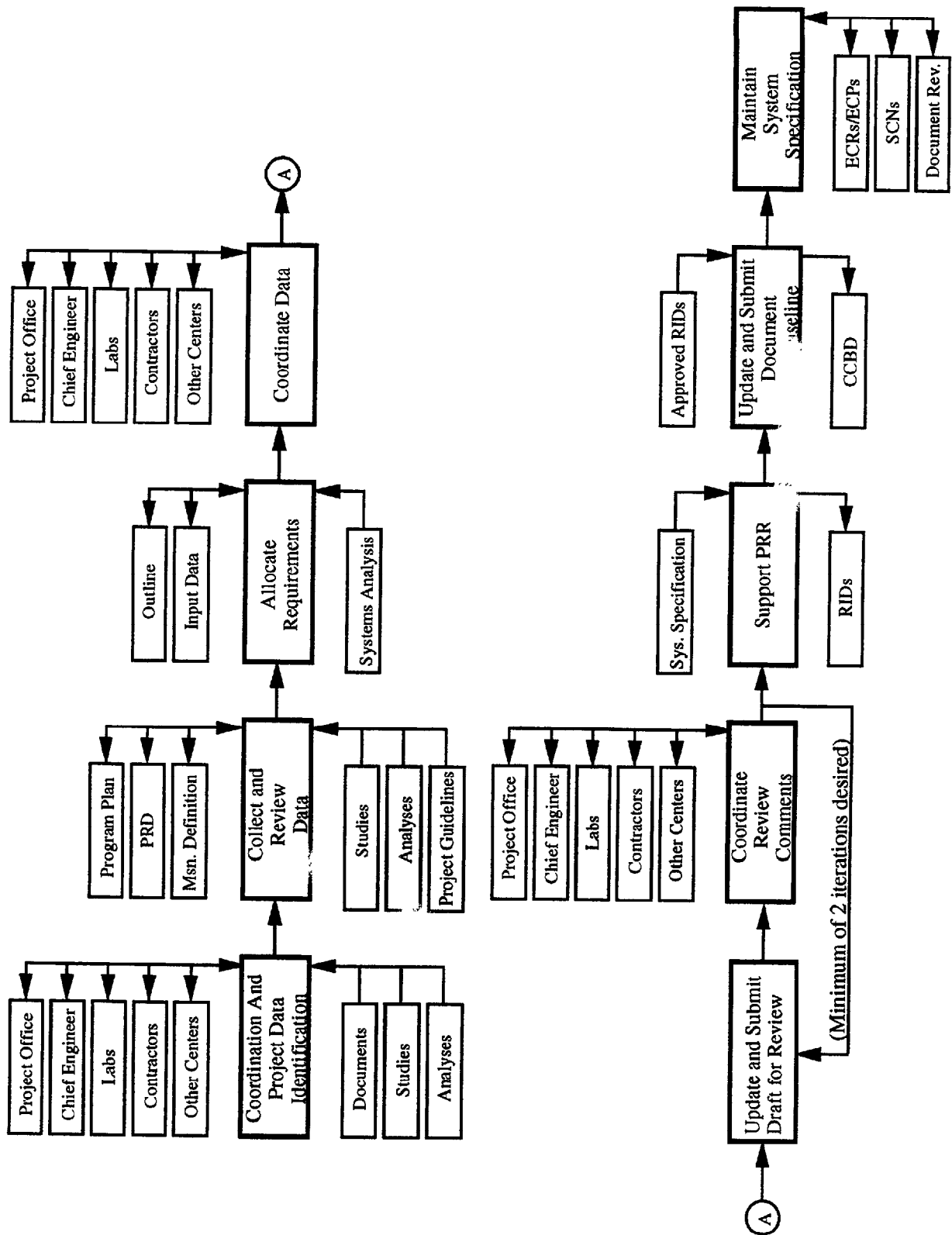


Figure 18. System Specification Process Flow

- Performance needs (propellant, thrust, etc.)
- Timelines on orbit
- Electrical power needs
- Data Transfer (uplink & downlink)
- Expendable resource needs
- Thermal cooling services required
- Crew-time needs.

The preliminary Operations Concept will be reviewed, modified, and approved by the project office/payload user community (if required). This process may require the project office to refine their requirements, designs, and goals. This may necessitate further trade studies and/or requirement reallocation, which in turn may impact the system preliminary design. This highly iterative process continues until a stable Mission Operations Concept results; one which is compatible with the system design, acceptable to the project office and user community and is operationally feasible. This Mission Operations Concept is then baselined and used in system design and development assessment activities.

Mission Operations requirements are reviewed to ensure full understanding of those requirements imposed by all external interfacing systems. These systems, which are fulfilling related operational requirements, will have operational limitations, constraints, and requirements not subject to modification. A full understanding of the environment in which the developing system must operate is mandatory.

The candidate operations requirements allocations are tested against the Operations Concept to validate the allocation criteria used, and to authenticate the Operations Concept. Figure 19 depicts the task flow for the tasks described above.

Inputs required to perform Mission Operations include:

a. Statement Of Work - The SOW is contained in the initial solicitation (RFP) and typically modified upon award of program contract. It will define Mission Operations Definition level and scope of work including:

- 1) Mission Type;
- 2) Mission Duration;
- 3) Operational Nodes;
- 4) Number of spacecraft;
- 5) Cost Objectives;
- 6) Preparation of Operations Requirements Documents.

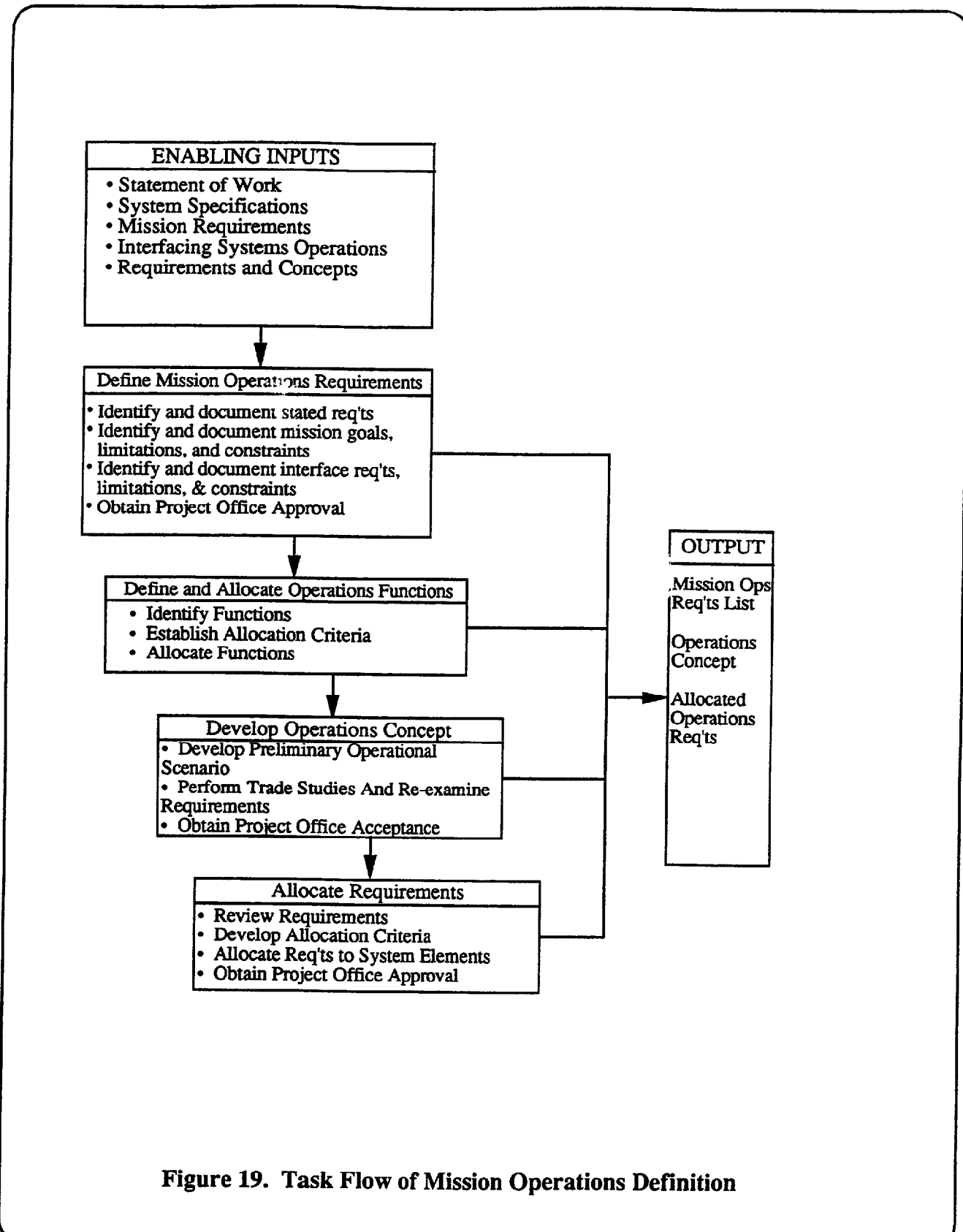


Figure 19. Task Flow of Mission Operations Definition

b. System Specifications - Hardware, Software, and Personnel Specifications including:

- 1) Control Console/Display type, capability and supporting software;
- 2) Spacecraft Subsystems capability and limitations including attitude control, Telemetry and Command (Word size, Uplink/downlink frequency and command mode, Electrical power (Solar array or battery, etc.).

c. Mission Requirements - Orbital parameters, spacecraft attitude, launch criteria, on-orbit support.

d. Mission Success Criteria - The project office will usually provide initial success criteria. These will be modified and added to during the early stages of Mission Operations definition. These criteria typically include:

- 1) Launch windows;
- 2) Data retrieval percentage;
- 3) Reliability numbers.

e. Interfacing Systems Operations Requirements and Concepts - These typically describe the project office operational nodes and could include the following NASA operations centers:

* JSC/MCC	* KSC/LCC
* JPL/POCC	* GSFC/TDRSS SOC
* MSFC/HOSC	* MSFC/POCC

As the system design develops from its initial concept through detail definition, the operational needs of the mission will be incorporated by direct participation of the Mission Operations organization in the activities of the system design team. This part of the process is iterative, and requires reevaluation and update as each program phase is completed (i.e., analysis, definition, design, development, and operations).

3.2.2 Operations Requirements

The overall mission operations integration process flow is shown in Figure 20. Each of the subtasks is discussed in the following paragraphs.

The first step in the operations requirements definition subtask is to identify all mission operations requirements in the enabling documentation (Statement of Work, system specification, mission performance requirements, mission success criteria, interfacing system operations requirements, and IPCL, if available). The specified requirements from these documents are studied to assure consistency of understanding of requirements across the project. These may be clearly identified as Mission

Operational requirements, or may be contained within other categories of the source documentation and thus derived to more clearly delineate operational needs. Trade studies are then conducted as necessary to ensure optimum allocation of each requirement.

The next step is to identify the Mission Operations requirements, limitations, and constraints imposed by any system which will provide an operational interface with the system under development. Requirements that are levied by interfacing external systems (e.g. NASA, joint center projects, payload user community) must also be identified and evaluated for operational compatibility, Command and Control (C²) efficiency, data exchange interfaces, and documented. This provides the basis for deriving those requirements which are not explicitly stated.

Next, the operational functions are analyzed and allocated consistent with the initial requirements. Mission operations requirements and constraints, in conjunction with mission goals, success criteria, etc., provide the input for developing and/or evolving the operations concept. This document describes the system operating procedures and critical command sequences, system interfaces, and system contingencies. A logical functions allocation criteria must be used. From a Mission Operations standpoint, the major concern is the establishment of criteria which are consistent and compatible with the operational structures and philosophies of interfacing systems and their control centers. These allocation criteria become an initial input to the operations concept development and vary with each mission or program. The goal is to allocate one function to each operational node or module.

Typical operational functions include:

- Command Development/Generation,
- Telemetry Monitoring,
- Data Monitor and Evaluation,
- Spacecraft Attitude Determination & Control,
- Power System Control,
- Thermal System Control,
- Spacecraft Configuration Control,
- Anomaly/Contingency Determination,
- Long Term Analysis,

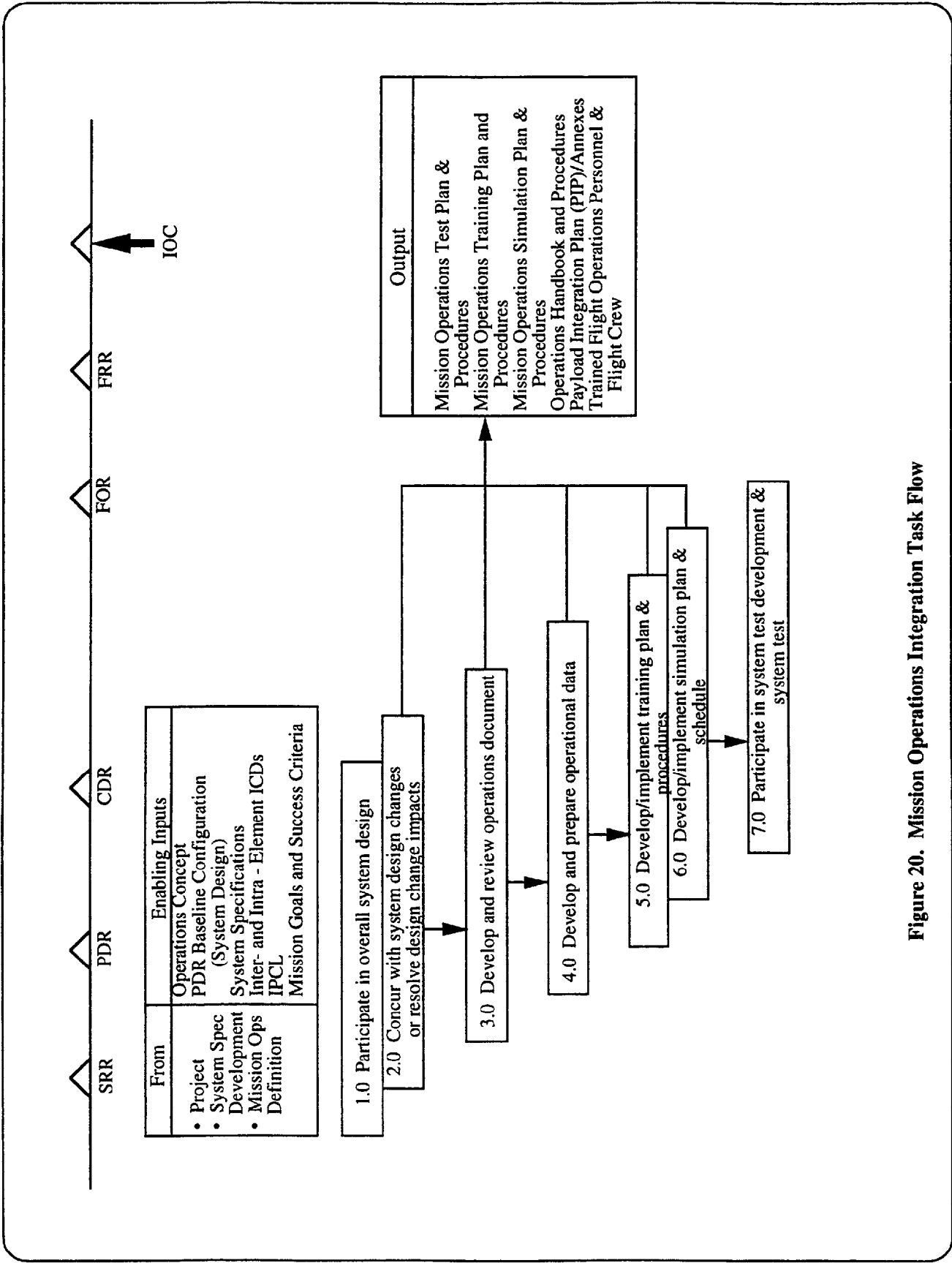


Figure 20. Mission Operations Integration Task Flow

- Life support metabolic compatibility, and
- Environment and Rack Service provision.

3.2.3 Interface Requirements

Precise interface definition early in the program is essential to a successful and timely development. Functional analyses are used for analyzing performance requirements and decomposing them into discrete tasks or activities. This involves the decomposition of the primary system functions into sub-functions at ever increasing levels of detail. Functional block diagrams are used to define data flow throughout the system and interfaces within the system. Once the segments and elements within the system have been defined, a top level functional block diagram is prepared as shown in Figure 21. The block diagrams are used to help develop interface data flows. In addition, they are used as the basis for reliability models and for failure modes and affects analyses which are performed by the S&MA Office.

In developing interface definition and control, consideration should be given to whether an Interface Requirement Document (IRD), an Interface Control Document (ICD), or both will benefit the particular program. In general, an IRD contains much more information than is required for interface control. The IRD normally is a collection of data which includes interface characteristics and related information in addition to the interface definition.

The IRD is most useful during early systems definition to ensure both parties understand the interface and its functional characteristics. The IRD also provides traceability from requirements to the interface definition in the ICD. **As the program definition matures, it is desirable to limit the formally controlled interface definition to only form, fit, and function information required for configuration control. This will greatly reduce change traffic and still retain required control. A generic IRD outline is shown in Volume 2, Section 2.3.1.**

3.2.4 Preliminary Interface Definition

Interface control is the process which ensures compatible physical and functional characteristics of hardware articles or software modules where they interact at a common boundary. The process identifies the characteristics of an item during its life cycle, controls changes to those characteristics, and provides information on the status of change actions. The control process can be applied to any element of a hierarchy from systems to piece parts or operating systems to subroutines. Generally, the process consists of system engineering and formal CM practices such as:

- Interface identification - concept and performance requirements established; development of preliminary interface requirements
- Interface requirements definition/documentation baseline- Interface Requirements Documents (IRDs) baselined subsequent to PDR

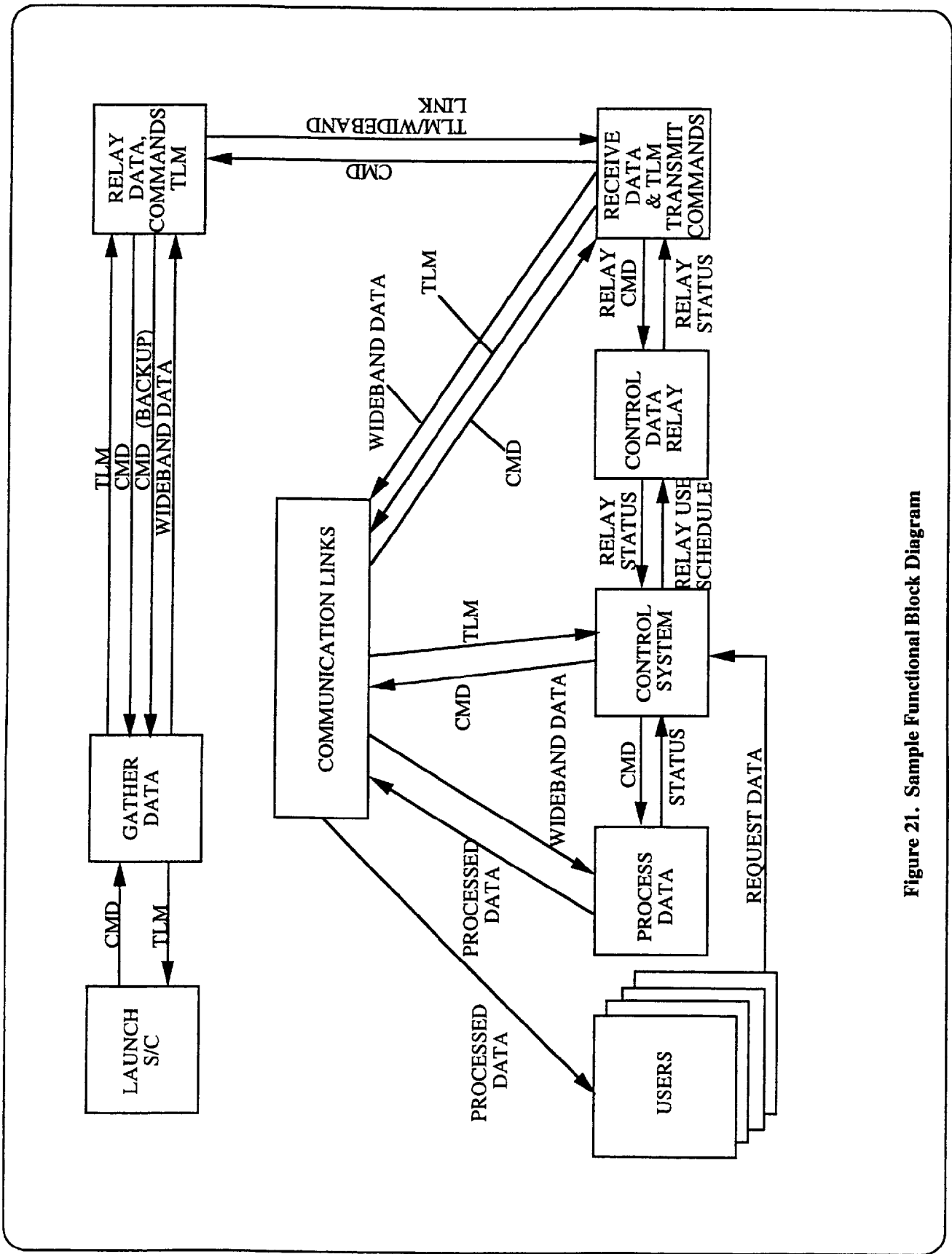


Figure 21. Sample Functional Block Diagram

- Interface documentation development - design solutions of requirements documented in Interface Control Documents (ICDs)
- Interface control documentation baseline - ICDs baselined in the CDR time frame
- Document change control per MSFC-STD-555, MSFC Engineering Documentation Standard (also see Volume 2, Section 5.2.2 for a discussion of the engineering change request process).
- Configuration audits - Compare configuration of as-built product with interface design solutions controlled by ICDs.

Interface control provides a means for presenting, identifying, and resolving incompatibilities and determining interface impacts of design changes. Program Management establishes interface control during the definition and development phases of a program.

The development of the interfaces begins following the definition of the system configuration. The interface definition consists of the following steps:

- 1) Establish a NASA and contractor team of specialists from parties involved in the interfaces (I/Fs);
- 2) Identify lead to direct the team to plan interface development strategy;
- 3) Review/determine program/system requirements for I/Fs;
- 4) Determine data required;
- 5) Prepare Preliminary Interface Definitions;
- 6) Resolve issues and incompatibilities, and
- 7) Document interface definitions.

Interface definition is exercised through the NASA/Contractor team called an Interface Working Group (IWG) consisting of the IWG Chairman, IWG Secretariat, and the contractors or other government agencies involved. An integrating contractor may also be involved, if one is required.

The primary functions of the IWG Chairman are to direct the identification of and to manage the system interfaces. This is accomplished by reviewing ICDs to assure that all interfaces are adequately defined or that a strategy exists to complete the definition. The IWG Chairman is responsible for preliminary management of all ICDs, resolution of issues, and for assuring that participants comply with the requirements as specified in program interface policies and procedures. **The ICDs describe the design of the interfaces. That is, the ICDs contain the design solution for the requirements described in the Interface Requirements Documents (IRDs).**

The ICDs are typically baselined near CDR, when approximately 90 percent of the design is completed. This means that they may be baselined (placed under configuration control) with issues still to-be-determined (TBD). A generic system ICD outline is in Volume 2, Section 2.3.2. The ICD Process Flow is shown in Figure 22.

Project interfaces at the intra-center level, especially between laboratories and project offices, are usually not documented in formal ICDs. Negotiations between the organizations on each side of the interface do occur, and are documented in design drawings. Experiment, payload, and component interfaces may also be documented in ICDs.

3.2.5 Integration Requirements

System integration is that process which takes place to ensure that the various segments and elements of the total system are in accordance with requirements and operate together and interface with the external environment as expected. This effort is primarily directed at identification of interfaces and an accompanying analytical assessment which considers all system elements (e.g., spacecraft, payload, launch vehicle, ground systems, airborne support equipment, Tracking and Data Relay Satellite System (TDRSS), flight planning and operations, and mission objectives) for compatibility and compliance with interface requirements. The system integration process encompasses all elements associated with the given program/project and begins with the interface definitions arising from the design concept.

The analytical integration process not only occurs between elements, but also internal to the elements. This latter process is known as design integration and is defined as the action(s) taken to ensure the various subsystems and components of a given system meet and operate together as required and expected. Design integration in any given element can occur independently of other elements. The principal function of design integration is to support the system integration requirements in the generation and documentation of ICDs, mass properties reports (see Volume 2, Section 2.5.1), configuration layout drawings, thermal budgeting and analyses, and electrical power reporting and assessments.

For attached payloads and Spacelab missions, there exist detailed and highly structured integration requirements. These are documented in the MROFIE and are summarized below.

The Mission Requirements On Facilities/Instruments/Experiments document (JA-447) establishes the approach to payload mission integration and operations, required documentation, and the control and flow to maturity of that documentation. The MROFIE document is applicable to all MSFC-managed NSTS attached payload missions. The NSTS attached payload missions include Spacelab dedicated missions, mid-deck payloads, and partial-payload missions. A partial-payload mission is a flight that is not a Spacelab dedicated (unique) mission and is shared with other payloads. Such missions are also referred to as mixed cargo missions. Partial payloads are defined as those payloads that do not require either a Spacelab module or the Spacelab igloo.

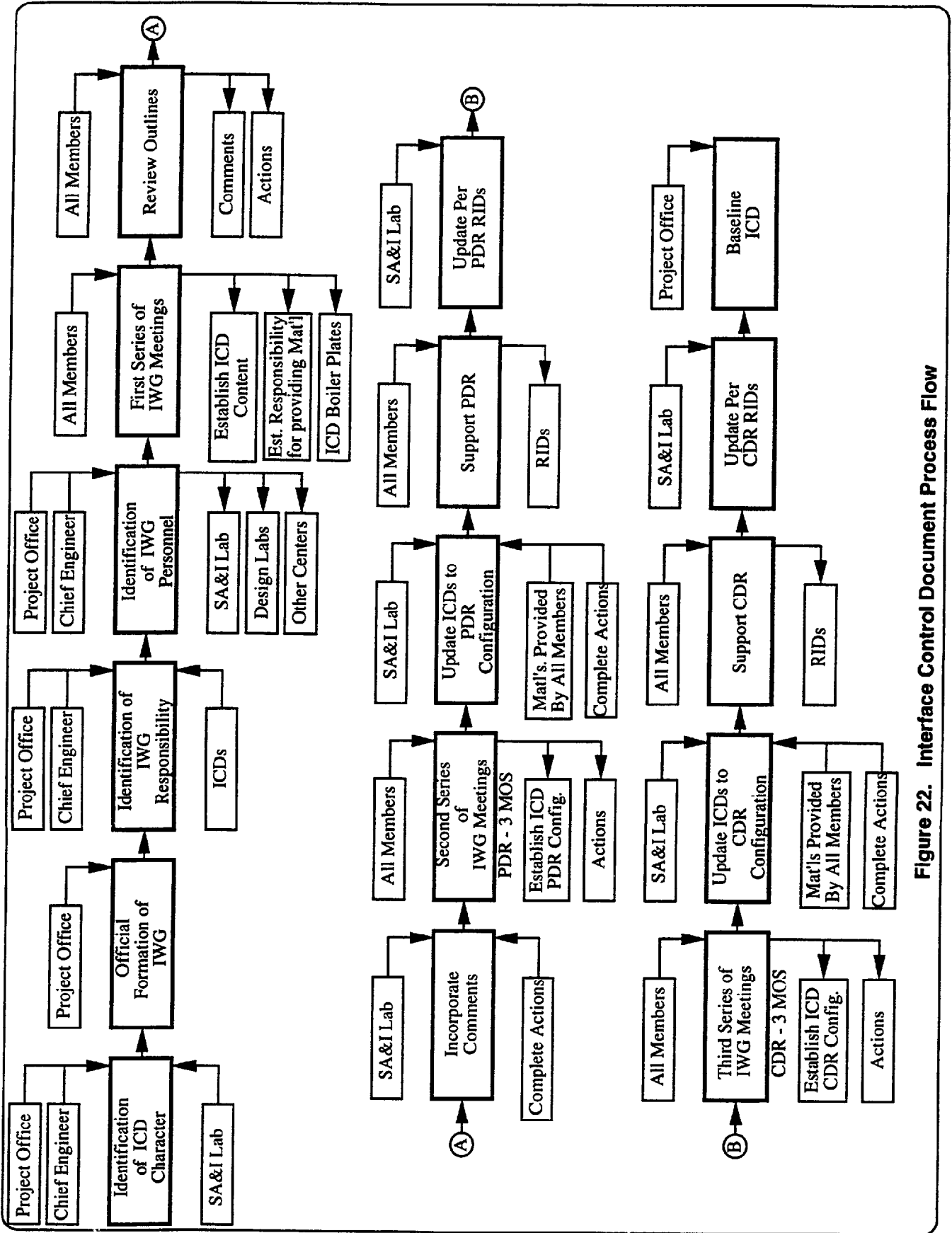


Figure 22. Interface Control Document Process Flow

The MROFIE is the source document for all requirements to be levied on Payload Element Developers (PEDs), and it defines the interfacing methods for them. Identification of the applicable requirements defined in the appendices or referenced documents is accomplished as a part of the preparation of the Instrument Interface Agreements (IIAs), the Operations and Integration Agreements (O&IAs), and the Verification Plan. For payloads developed under MROFIE, IIAs and O&IAs contain the information normally documented in an ICD. Mid-deck payloads do not require all of the identified documentation; however, an exchange of information to define and agree upon requirements is necessary. The method of documenting and agreeing to these requirements will be specified by the Payload Mission Manager (PMM) at assignment for development and integration.

The integrated payload definition and flight planning and operations necessary to ensure that the Principal Investigator's (PI) requirements are met are the responsibility of the Payload Mission Manager. The PMM also has the responsibility for verifying that the established safety requirements have been met by all payload elements and that the payload elements are compatible among themselves and with the launch vehicle. These responsibilities may be exercised by a contractor under the cognizance and direction of the PMM and staff. Figure 23 shows a typical experiment payload integration process.

After establishing the interfaces for an instrument or experiment, an Experiment Payload Element Developer (EPED) begins the development of the necessary hardware to accomplish the experimental objectives. The EPED aids the PI in the definition of the interfaces and IRDs, and develops the ICDs between the Experiment Specific Equipment and the experiment facility. Additionally, the EPED hardware and software must also satisfy the safety and interface requirements and constraints of other mission hardware. An outline for a Safety and Interface Verification Plan is provided in Volume 2, Section 2.4.2. Simultaneously with the development of an experiment or facility, the ICDs between that facility and the vehicle (either the launch vehicle or a Spacelab) are developed.

3.2.6 Systems Software Requirements

Software is defined as the, "...information content of a digital computer memory, consisting of sequences of instructions and data for the digital computer."¹ Another term often used in conjunction with software is firmware. Firmware is software converted or "burned into" read-only memory (ROM). The typical space project will also have both ground and flight software to be developed. For the purposes of this handbook, the development process described below is the same for both software and firmware, as well as ground and flight software. The primary reference for software development at MSFC is MM 8075.1, MSFC Software Management and Development Requirements.

¹ MM 8075.1, MSFC Software Management and Development Requirements Manual, January 22, 1991.

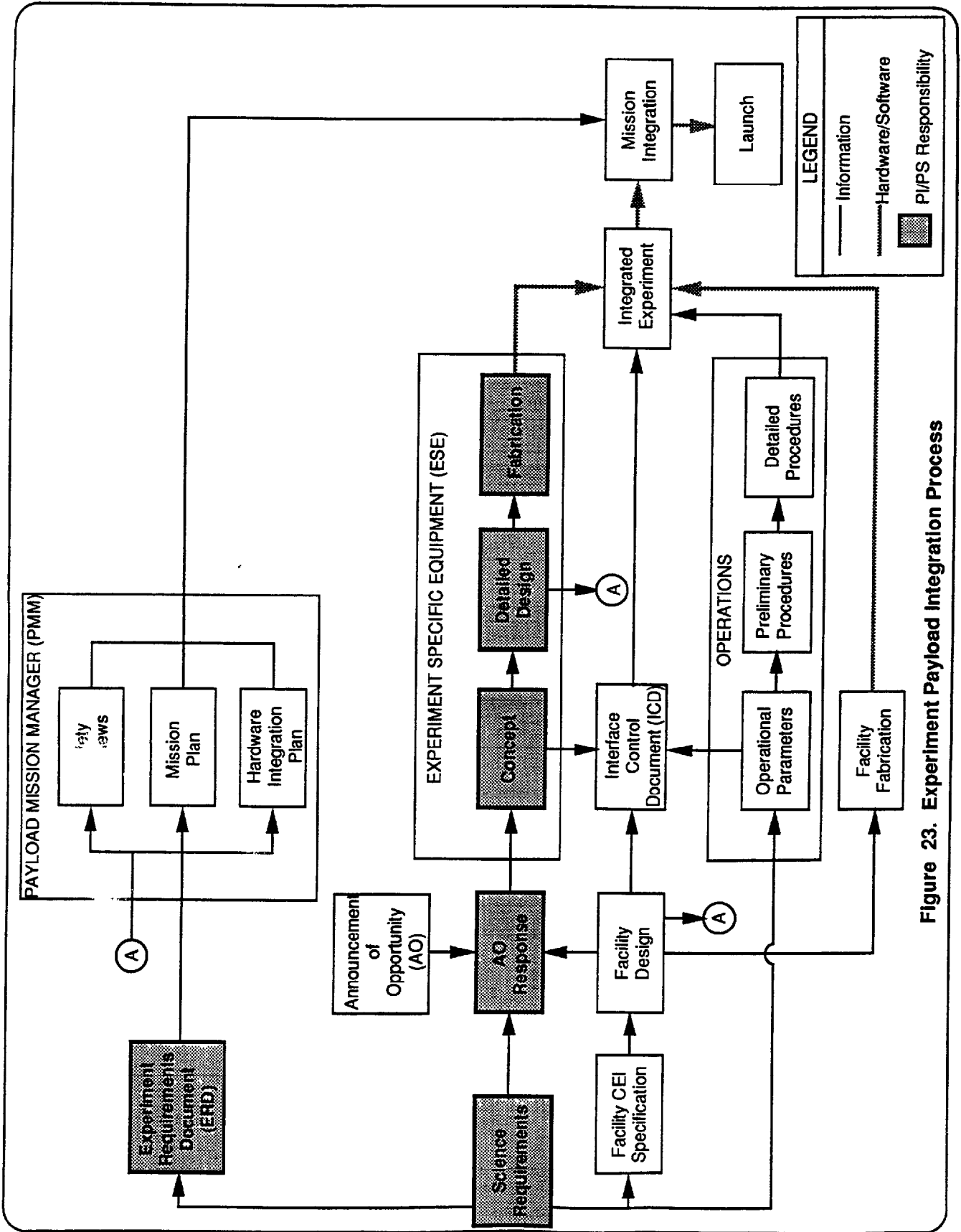


Figure 23. Experiment Payload Integration Process

The Software Development Process is illustrated in Figure 24 as separate, but closely related to, the systems development process. Once the systems functions are allocated to hardware and to software, the separate software development process begins. Finally, the hardware and software are brought together for systems integration testing and acceptance. The software development life cycle consists of the following phases:

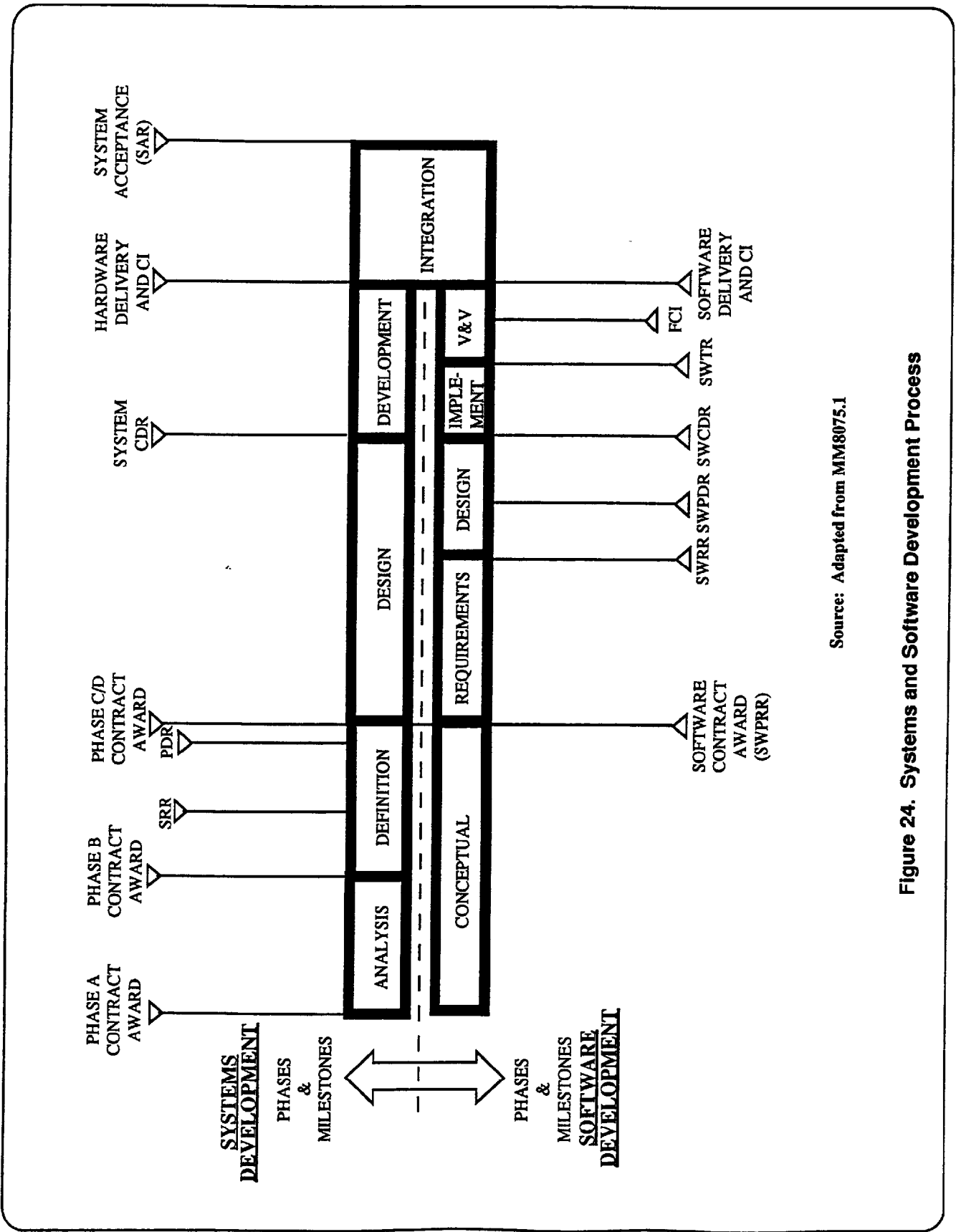
- Conceptual
- Requirements
- Design
- Code and Debug
- Verification
- Validation
- Systems Integration
- Operations and Maintenance

Not all software developments will include all of the phases. For example, if off-the-shelf software is being purchased, the conceptual and requirements phases will have already been completed. There may be a design phase where the software has to be redesigned to fit the capabilities of a particular system. There will be a debugging phase, which involves recoding. If so, there may or may not be a major independent verification and validation contract, although adequate software verification and validation must still be performed.

3.2.6.1 Software Conceptual Phase

This phase extends from inception of the task through the Software Preliminary Requirements Review (SWPRR). Key inputs to this process are the program requirements (Level I/II) and science requirements. System concepts are developed, and these naturally lead to both hardware and software concepts. Initial allocation of functions to both hardware and software is performed, and preliminary software configuration items are identified for planning purposes. Technical requirements for both hardware and software are documented in the Preliminary System Requirements Specification and reviewed at the systems SRR.

Early in this phase, a Preliminary Systems Software Functional Requirements Specification (SSFRD) is generated. Volume 2, Section 2.2.3 provides an outline for the SSFRD. Figure 25 depicts the Systems Software Functional Requirements Process Flow. These requirements are identified through analysis of the systems functions, subsystem and payload requirements and overall performance requirements. They are generally broad, high-level software requirements which require further expansion to the detail level for design purposes. Characteristics such as total data handling, throughput computer speed, mass storage, memory margins, and processor capabilities are identified in the Systems Software Requirements Specification. This document is placed under configuration control following the SWPRR (Figure 24).



Source: Adapted from MM8075.1

Figure 24. Systems and Software Development Process

3.2.7 Software Detail Requirements

The software requirements phase begins after the Conceptual Phase and extends through the Software Requirements Review (SWRR). The Preliminary Systems Requirements Specifications are updated during this phase, and the Interface Control Documents (ICDs) are drafted. The Software Management and Development Plans, the Software Quality Assurance (QA) Plan, and Software Standards and Procedures are also developed in this phase, in parallel with the corresponding system plans. The detail software requirement specification is configuration controlled following the SWRR.

3.2.8 Hardware Subsystem/Component Design/ Verification Requirements

Once the systems requirements of a program are determined and baselined and resources and constraints analyzed, an analysis of each proposed component of the system is performed to determine compatibility with the overall system. Hardware is then designed to satisfy the mission objectives. This design represents the system configuration, and is the responsibility of the design laboratories or organizations.

Based on the requirement allocation process, there are numerous qualitative requirements assigned to each subsystem and component. The subsystem design engineers then begin the process of deriving quantitative and performance requirements. An example of a qualitative requirement is: "The payload equipment shall be mounted in a mid-deck locker on the orbiter, and shall use mid-deck power." The quantitative subsystem requirements that result from this could be: "The equipment shall be 24 in. ± 0.05 in. wide, 10 in. ± 0.05 in. high, 18 in. ± 0.10 deep, and shall be compatible with Orbiter mid-deck power of 28 Vdc ± 4 Vdc at 5 Amperes."

As the subsystem requirements are determined they are documented in the end item specifications. If the effort is an out-of-house (contracted) procurement, this document is a Contract End Item (CEI) Specification. Volume 2, Section 2.2.2 contains a generic CEI Specification.

Subsystem and component verification requirements, as well as associated design requirements, are the responsibility of the design labs or the organizations responsible for hardware development. These are also documented in the CEI spec for hardware end items. Systems-level verification, which is a function of the SAIL, will be discussed further in Section 3.6 of this handbook.

Component specifications describe the physical, performance, functional, and other characteristics of the items. Traditionally, section 1 of the specification contains introductory material. Section 2 contains a list of applicable and reference documents. Section 3 contains the actual requirements. Section 4 contains a verification matrix. This matrix lists, for every requirement, the program development phase and verification methods that are planned for certifying that the hardware meets the requirement. See MSFC-HDBK-2221, Volume 2 for an example of a verification matrix.

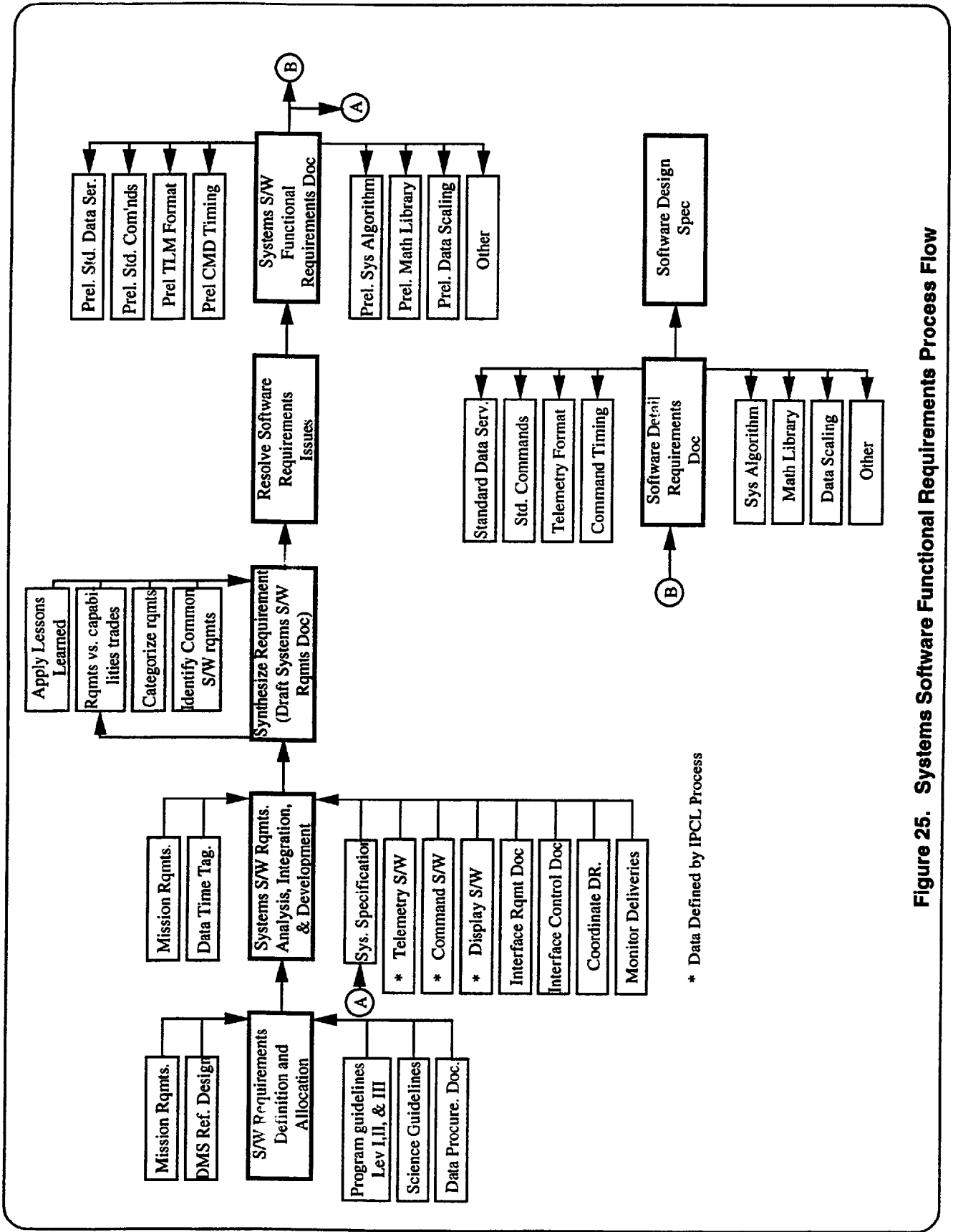


Figure 25. Systems Software Functional Requirements Process Flow

3.2.9 Verification Plan

The Verification Plan defines the activity for hardware assembly, development, qualification, analyses, and acceptance testing which are required to be performed to satisfy design, performance, safety, and interface requirements. The plan also describes the development and acceptance of the test software, the ground support equipment and the facilities necessary to support the verification activities. The methods and controls for these activities are also described, and the rationale for certain tests is provided. The plan is developed through a comprehensive review of the design specifications (e.g., CEI, SS, JA-061, and JA-081) and a close coordination with technical design disciplines. Agreement is sought on the types of tests and hardware configurations required to ensure compliance with design and performance requirements. The MSFC-HDBK-2221 contains more details on the Verification Plan.

The basic functions of the flight hardware/software are checked on the ground to help ensure proper in-flight performance. This is accomplished through environmental testing and simulation of the required flight performance.

Environmental testing helps to ensure that the hardware will function as required during and after the stress of the flight environment. Training and man/systems simulations involving man-in-the-loop provide additional information regarding operability, timelines, safety, and productivity involving both flight crew and ground controllers. Simulations are also used to check-out the software and hardware performance prior to flight. This is generally accomplished by the use of a check-out unit which simulates the flight computer interface and any ground computers. Hardware performance and communication between subsystems is verified and necessary changes to ensure the success of the mission are incorporated. The system is finally retested to assure compliance with requirements.

3.2.10 Systems Verification Requirements

At MSFC, no single document contains all verification requirements; however, system verification requirements are documented in the Verification Requirements and Specification Document (VRSD). These requirements and related pass/fail criteria include buildup, subsystem, and system-level testing of the hardware under environmental conditions to which the hardware will be subjected. See MSFC-HDBK-2221 for a VRSD outline.

3.2.11 Software Test Planning

Test planning addresses two activities: (1) code analysis and (2) testing. Analysis of the developed program code is performed to ensure that the code properly implements the software design and that software development standards have been followed. Software tools may be used to help identify actual or potential errors in the developed code, and to reformat and consolidate information to facilitate manual analysis. Since program analysis is performed in parallel with code development,

incremental code deliveries and modifications are analyzed as soon as possible to identify major coding problems for correction early in the code development process.

Independent tests are performed to determine compliance with software and system requirements. A comprehensive test plan is developed prior to testing and tests are planned at three levels:

- 1) Module testing to verify that individual software functions satisfy the corresponding software requirements;
- 2) Interface testing to verify that software/software and hardware/ software interface functions are properly implemented;
- 3) System testing to verify that the operational system possesses the required system capabilities and satisfies the appropriate performance requirements.

3.2.12 System Requirements Review (SRR)

The requirements definition and allocation process concludes with a formal SRR (see Figure 8). The SRR may be thought of as the culmination of the definition phase of a program. It is the final review before initiation (often contractual) of formal design and development of the program. Its purpose is to review and establish or update program requirements and to evaluate the management techniques, procedures, agreements, etc. to be utilized by all program participants. During the review the SRR team should verify configuration concepts and requirements, verify mission objectives, define the qualification approach, evaluate the system safety and quality assurance plans, and establish and approve the program requirements and system requirements baseline.

The SRR encompasses all major participants (both NASA and contractors), and an important product is the system specification which is formally baselined and placed under configuration management control subsequent to resolution of actions resulting from the review. This review is chaired by the Project Manager.

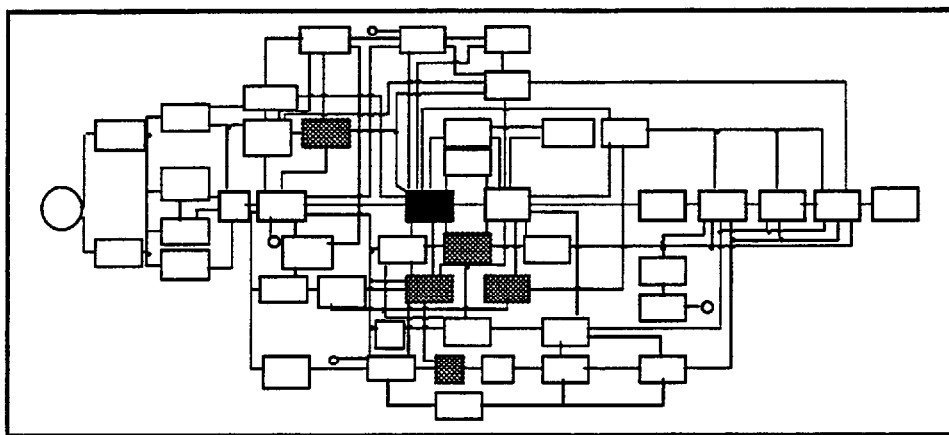
Additional guidance for all formal reviews is in NHB 7120.5 and MMI 8010.5. A checklist of SRR topics is in Volume 2, Section 5.1.

3.2.13 Phase 0 Safety Review

As shown in Figure 16, the initial safety assessment is of the conceptual design of the flight/payload hardware and comprises the Phase 0 safety data. These data are generated by the PED for the payload element SRR and then combined with other payload element safety data in an integrated payload safety data package for review at the IPL Requirements Review (IRR). The objectives of the Phase 0 review are: to assist the payload organization in identifying hazards, hazard causes, and applicable safety requirements early in the development of the payload/GSE; to adequately describe the hazard potential; to answer questions relative to the interpretation of the requirements of NHB 1700.7 or KHB 1700.7 or the implementation procedures of the safety data required for subsequent safety reviews.

The purpose of the Phase 0 hazard report is to document and scope the specific hazards identified. It is intended to be a working document for discussion and critique at the Phase 0 safety review and does not require concurrence signatures. One hazard report must be prepared for each unique hazard identified in the safety analysis and the hazards contained in the Phase 0 hazard reports should reflect the payload/GSE conceptual design and operations existing at the time of the review.

3.3 PRELIMINARY DESIGN



Preliminary design is addressed in Phase B by PD to support concept definition and selection. In Phase C, preliminary design is conducted by S&E to support design implementation. Preliminary system design begins with the technical baseline for the system as defined in a feasibility analysis. It proceeds from the translation of established system-level requirements into detailed qualitative and quantitative design requirements.

This design activity includes the process of functional analysis and requirements allocation, the accomplishment of trade-off studies and optimization, system synthesis, and configuration definition in the form of top-level specifications as illustrated in Figure 26. Inherent in the activities identified in the figure are the aspects of planning, implementing, and measuring with the necessary feedback provisions allowing for the incorporation of changes.

The system engineer must realize that requirements changes will likely be needed as design implementation proceeds (see Figure 1) and additional definition is accomplished. These requirements changes may be the result of additional knowledge gained or the inability of the design to meet a specific requirement. Regardless of the reason for the change, it is essential to update the requirements specifications when required so as to reflect current design status and assure a reliable, cost-effective product. Note that during this phase the role of the systems engineer shifts from requirements definition to one of ensuring requirements coordination and flow-down and working closely with the design engineering organizations to aid requirements understanding.

The process of design evolution is illustrated in Figure 27. All the activities shown should have the goal of meeting a specific set of requirements. The proper level of engineering effort must be applied to the system being developed. The steps presented in Figure 27 should be considered as a thought process, with each step being addressed to the extent and depth necessary to fulfill the requirements.

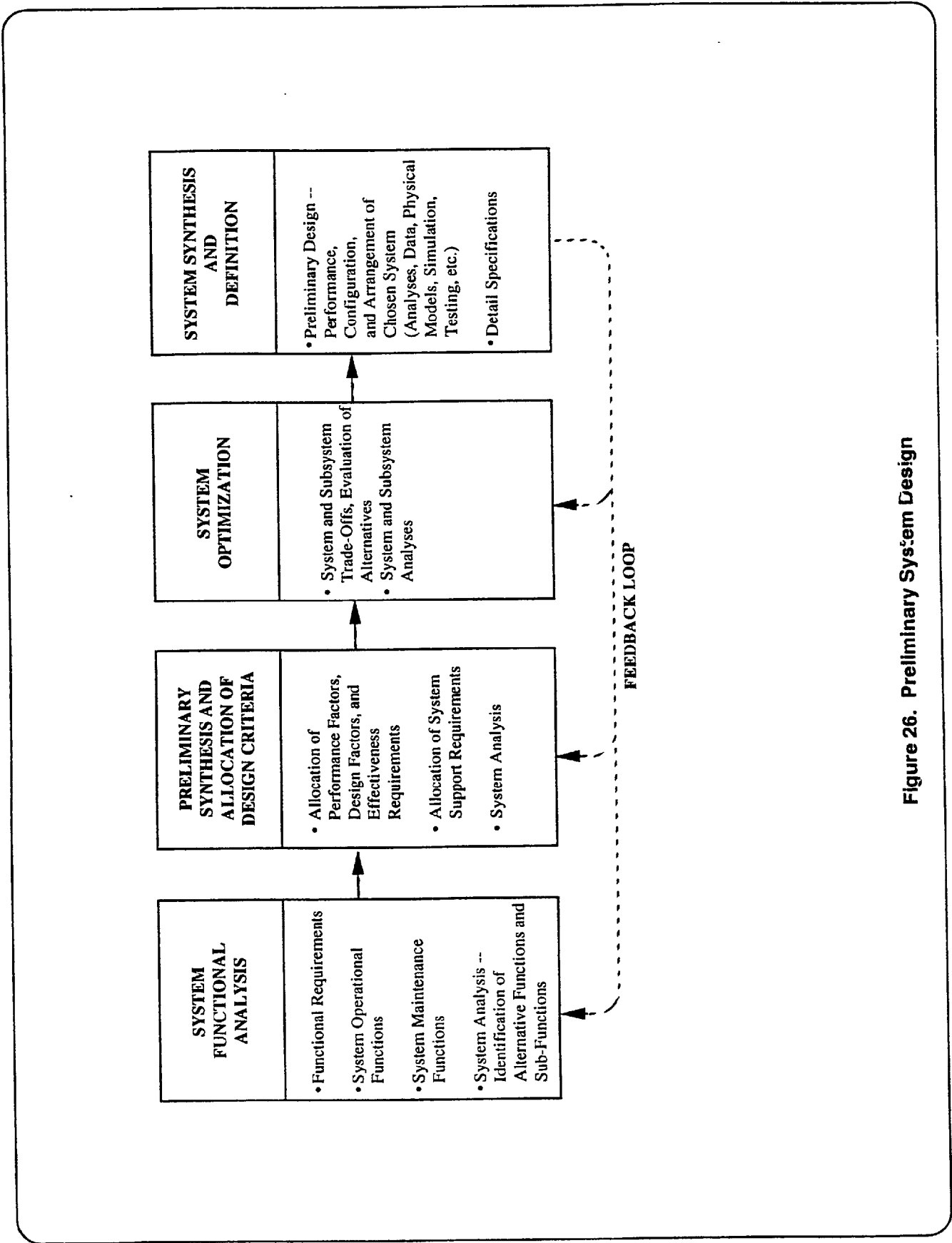


Figure 26. Preliminary System Design

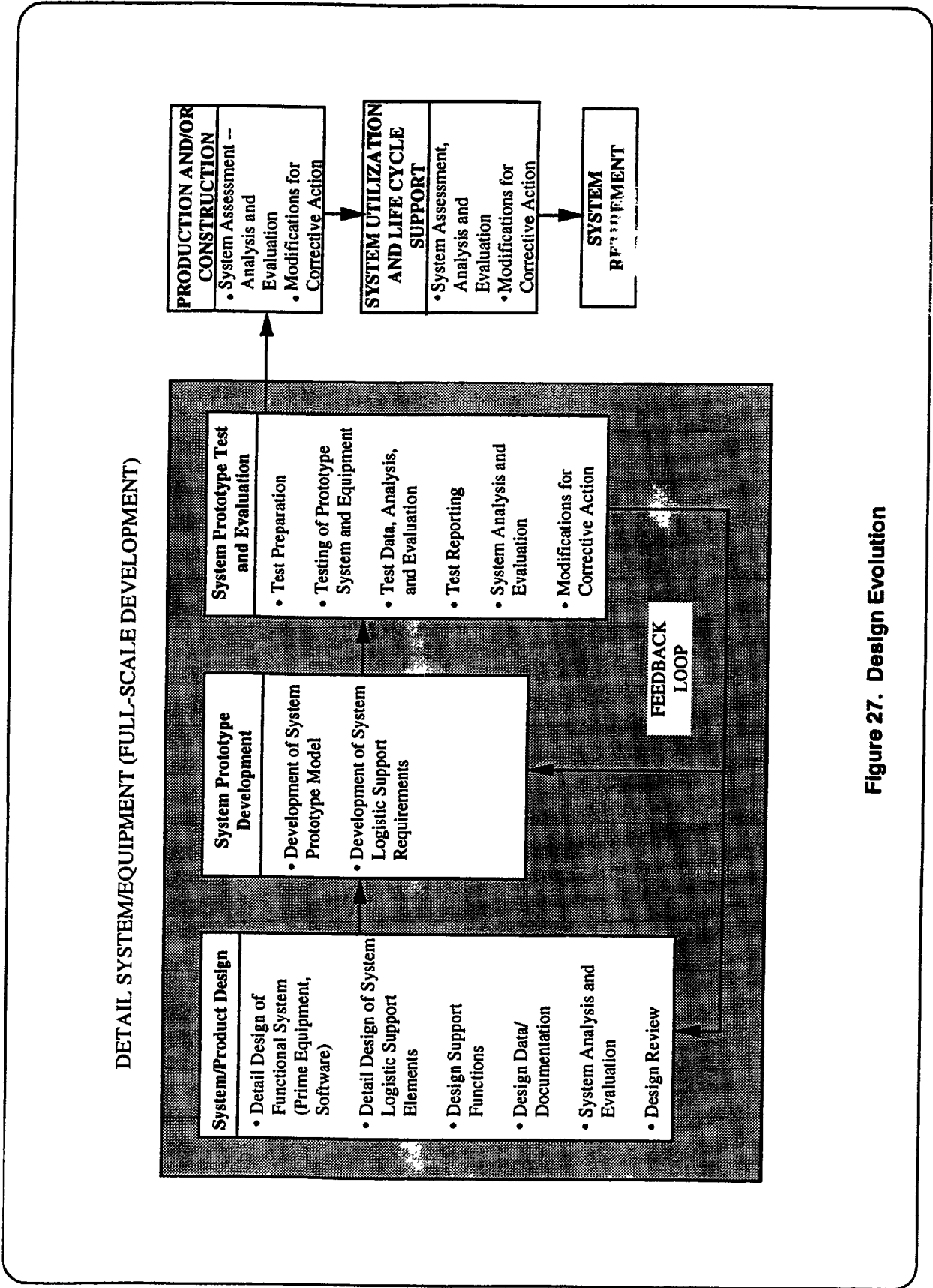


Figure 27. Design Evolution

Regardless of the system type and size, one commences with an identified need and a completed feasibility study for the purposes of establishing a set of requirements, constraints, and design criteria. Based on the results, functional analyses and allocations are generated to apportion the appropriate system-level requirements down to the subsystem, unit, and lower levels of the system.

3.3.1 Flight Sequence and Timeline

This subtask begins by developing or updating a customer-supplied, preliminary operational scenario based upon the mission operations requirements, mission goals and success criteria. This scenario, when finalized, provides a chronological and/or functional representation of how the system operates in performance of its mission. This includes mission sequence of events (MSOE), mission timelines, data flow (i.e., media-voice, computer, hard-line, satellite relay, etc.), personnel roles and responsibilities, contingency modes, maintenance and training considerations, identification of operational nodes/modules/elements and interface characteristics with these and other systems. The MSOE is a very key element of the Mission Operations concept in that it forms the basis for developing and performing training and simulations and becomes the "Flight Plan" (which includes: prelaunch operations, lift off, orbit insertion, on-orbit operations, de-orbit, and reentry) for on-orbit operations and support.

3.3.2 Design Analysis and Trade Studies

System and subsystem trade-offs provide a structured, analytical framework for comparative analysis of competing alternatives and provide the analysts or engineers with an understanding of the elements of the problem, their interrelationships, and the favored solution.

As the preliminary design continues, the emphasis of the trade studies shifts from definition of requirements to aiding the design process and to proving that the design meets the defined requirements. The preliminary design process allows the models used for analyses to be defined more realistically and in quantitative terms. This process is iterative as models are constantly improved and the design becomes more detailed. Also, as the design proceeds, the models are verified with test data, when available.

Many models of the system are generated with the total number and complexity depending on the program and its expected environment. The models generated in this phase address specific parameters of performance such as electrical power, guidance and navigation, structural dynamics, thermal, EMI/EMC, and lightning protection, to name a few. The outputs of the analyses which use these models are then applied in the refinement of the design. More details on analyses and models can be found in Volume 2 of this handbook. For illustrative purposes, a sample analysis and output product are discussed below.

Electrical power analyses include, but are not limited to, Solar Array Analysis, Voltage Drop Analysis, Fault/Fusing Analysis, and Grounding Analysis. In general, an

electrical power system analysis uses normal and worst-case subsystem/system interface conditions (voltage, current, and power) to evaluate the design for proper performance and compatibility. A grounding analysis is performed to assure that the electrical grounding configuration of all elements of the spacecraft, ASE, and Orbiter is consistent with performance specifications and that the various elements are compatible with each other during all phases of the mission. For detailed information regarding electrical power analysis tools and techniques, see Volume 2, Section 4.3.3.2.

Electrical Power and Energy Management Reports (EPEMR) provide engineering and management personnel with valuable information regarding a spacecraft's power and energy requirements versus its allocations. It provides solar array and battery output data per the mission timeline, and compares these values against the current load and time requirements of the spacecraft systems. The report is periodically updated to reflect the latest load and time information as the design evolves. The EPEMR is used to evaluate power system status, to track power margin changes throughout the program life cycle, and to evaluate contractor designs and proposals. Details of preparing and maintaining an EPEMR are covered in Volume 2, Section 2.5.1.2.

3.3.3 Prototype Development

Prototyping has been defined as, "The rapid development of a functional representation of a system capability that serves to provide a test bench on which system and user interface concepts can be tested prior to development."¹ In many cases, it is not feasible or cost-effective to build a full-scale working prototype of one-of-a-kind, custom-built hardware (for example, the Hubble Space Telescope). However, selected subsystems or assemblies may be prototyped to check performance, human engineering (ergonomics), payload fit and installation, and the physical operating range of moving elements.

Depending on how much of the system under development is prototyped, it may be possible to use the prototype article for system software checkout and verification. In any case, prototyping is one method of reducing risk in a program and should be given careful consideration in the early planning stages.

3.3.4 Software Design

This phase begins after the Software Requirements Review (SWRR) and concludes with a software design baseline at Software CDR (SWCDR). A Software PDR (SWPDR) is an intermediate milestone in this phase. The key software documents of the preliminary design are the Preliminary Software Design Specification and the Software Test Plan. The Systems Test Plan is also available early in this phase, along with an updated Preliminary System Design Document.

¹ NASA Program/Project Management Initiative Lexicon, Version 1.0, March 1990, p.106.

After the SWPDR, the detailed design occurs and concludes at the SWCDR. The results of the detailed design include the Software Detailed Design Specification, a Programmer's Handbook, and the Software Test Specification and Procedure. These documents are baselined at the SWCDR.

3.3.5 Preliminary Design Review (PDR)

The PDR is conducted when the basic design approach has been selected and the necessary documentation is available (usually when drawing preparation is approximately 10 percent complete). PDRs may be conducted at the program and/or project level. The PDR is a technical review of the basic design approach to assure compliance with program (Levels I and II) and project (Level III) requirements and is intended to accomplish the following:

- Establish the ability of the selected design approach to meet the technical requirements;
- Establish the integrity of the selected design approach;
- Establish the compatibility of the interface relationships between the specific end item and other interfacing items;
- Establish the producibility of the selected design;
- Establish the operability of the selected design; and
- Address cost and schedule relationships, producibility, test planning, and assessments for safety and reliability.

During the PDR, the preliminary engineering documentation is thoroughly reviewed, and any deficiencies or discrepancies are documented in a Review Item Discrepancy (RID). The RIDs are processed through a multi-level review board structure for disposition. All PDR RIDs should be closed prior to CDR. More details on the RID process can be found in Volume 2, Section 5.1.10.

The PDR and CDR are the only mandatory reviews required by NMI 7120.4. All other reviews are at the discretion of the Program Manager. See NHB 7120.5 and MMI 8010.5 for more details on this and other reviews. A checklist of PDR topics is given in Volume 2, Section 5.1.2.

3.3.6 Phase I Safety Review

Preliminary design safety analyses are reviewed as shown in Figure 16 by the PED and IPL at Preliminary Design Review. The Phase I flight and ground safety data are updated per RIDs and Discrepancy Notices (DNs) to produce a set of final design safety analyses. These become the Phase 2 flight and ground safety data.

Other safety-related data that is submitted in design reviews include accident or mishap investigation reports, disposition of waivers, and status of limited life items.

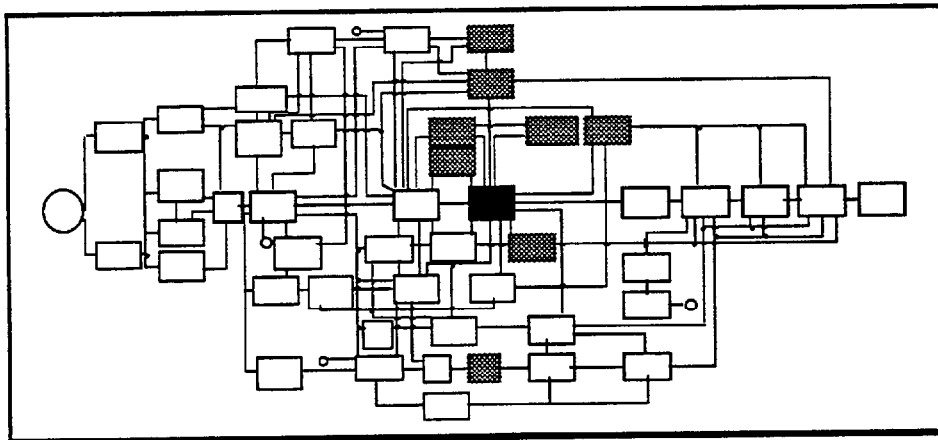
Essentially this includes anything else that could have a bearing on the over-all assessment of the safety of the system.

There are also separate safety reviews conducted at JSC and KSC. Flight related safety reviews are conducted at JSC while ground processing and launch site safety reviews are conducted at KSC.

Both ground and flight safety hazard analyses, at the preliminary design level, are required for the Phase I ground and flight safety data packages that are due at the PED PDR. Also due at the PED PDR is a preliminary version of the PED Verification Plan which includes description of the activities and the plan for verifying the hazard controls.

The purpose of the Phase I safety review is to obtain safety panel approval of the updated safety analysis that reflects the preliminary design and operations scenario of the payload/GSE. The safety analysis is refined such that: all hazards and hazard causes inherent in the preliminary design have been identified; all hazards have been evaluated for means of eliminating, reducing, or controlling the risk; and preliminary safety verification methods have been established. A preliminary identification of the payload interfaces and of the hazards presented by these interfaces is also made. A Phase I hazard report is prepared for each hazard identified as a result of the safety analysis on the preliminary design and operations scenario of the payload/GSE. Hazard reports are added to or deleted from those agreed upon during the Phase 0 review to reflect the updated safety analysis. Rationale for deleting a hazard agreed upon at Phase 0 is subsequently presented during the Phase I review.

3.4 DETAIL DESIGN



Detail design is accomplished by the S&E design laboratories (see Figure 2). For contracted efforts, the contractor does the detail design and the S&E design labs have a monitoring and oversight role. The drawings for jigs, tooling and other production fixtures are done at this time. A detailed cost estimate based upon Work Breakdown Structure is made. All equipment and hardware items are specified. Often the fabrication of some long lead components will be started during this phase as soon as their shop drawings are released.

3.4.1 Instrumentation Program & Command List (IPCL)

The IPCL is an avionics system engineering tool which is used primarily to identify, define, and control signal requirements and their applications to the end-to-end command and data management system (CDMS). The contents of an IPCL are specific, and a standard process is followed in development of each IPCL. Eventually this process (shown in Figure 28) involves all discipline engineers associated with the spacecraft design.

The IPCL defines the attributes of each signal that is required to design, test, and operate the spacecraft. Some of the attributes include a unique requirement number, its name, the rate of issuance or collection, and multiplexer channelizations to name a few. All of the attributes of each signal are contained in a database.

The purpose of an IPCL is broader than listing and controlling the signals desired on a particular spacecraft. In general, a CDMS IPCL engineer is assigned to each program with a goal to ensure that adequate numbers of signals are included in the design of the CDMS. The object is to ensure the design is sufficiently robust that adequate CDMS resource margins (e.g., memory, CPU, multiplexer channels, data bus traffic) are maintained to allow for growth and mission flexibility over the life of the program.

The IPCL is also used to monitor and document the configuration of the CDMS. By maintaining complete information about measurement and command signal flows of the spacecraft, the system engineer is able to examine resource allocation and use. In this case, the primary resources used and monitored are telemetry bandwidth and on-board data storage consumption.

The process flow for developing and using the IPCL is shown in Figure 28. This process flow is applicable to either in-house or contracted efforts. The IPCL process for contracted projects begins with the development of a Data Procurement Document (DPD) containing Data Requirements (DRs), statement of work (SOW), and the Project Requirements Document (PRD) which make up the Request for Proposal (RFP).

The process begins with the development of a preliminary IPCL to support a PDR. This preliminary IPCL will provide insight into potential CDMS or subsystem performance problems. The PDR version of the IPCL is released for review at least 30 days prior to the scheduled PDR. Sample IPCL format and preparation instructions can be found in Volume 2, Section 2.2.6.

The IPCL should be submitted for baselining following incorporation of the CDR RIDs. If the RIDs resulted in significant changes, a data analysis report should be performed to ensure design margins are still adequate. Once the IPCL is baselined, any proposed change must be submitted as an engineering change request (ECR) or engineering change proposal (ECP).

3.4.2 FMEA/Hazard Analysis

The Systems Safety Office of S&MA performs the Failure Mode and Effects and Hazard Analyses. During these activities, the group interfaces regularly with the detail design organization to assure the accuracy of the configuration, specifications, etc. when it is available historical data are used to support these reliability assessments.

A Reliability and Maintainability Program Plan is also produced during the early part of Phase C. This plan makes provisions for insuring that the parts and components designated for use in the system are of the level of reliability necessary to satisfy the requirements of NHB 5300.4 (1A-1). The plan also has procedures for insuring that if maintainability is a consideration (such as HST or ISSA) that the necessary analysis methods and specific analyses are specified to be performed.

The reliability analyses are coordinated with the appropriate cognizant laboratory within S&E. That is, the investigation surrounding an electronic part failure is conducted in concert with the EB lab. The interface with a contractor organization is in assuring that the contractor specifications contain the appropriate requirements and documentation, and that the contractor is properly implementing the requirements and procedures called out in his specifications.

Where applicable, a safety analysis is performed on flight hardware, software and associated GSE to identify hazardous elements and functions. The safety analysis should be initiated early in the design process to identify hazards, determine risks, and

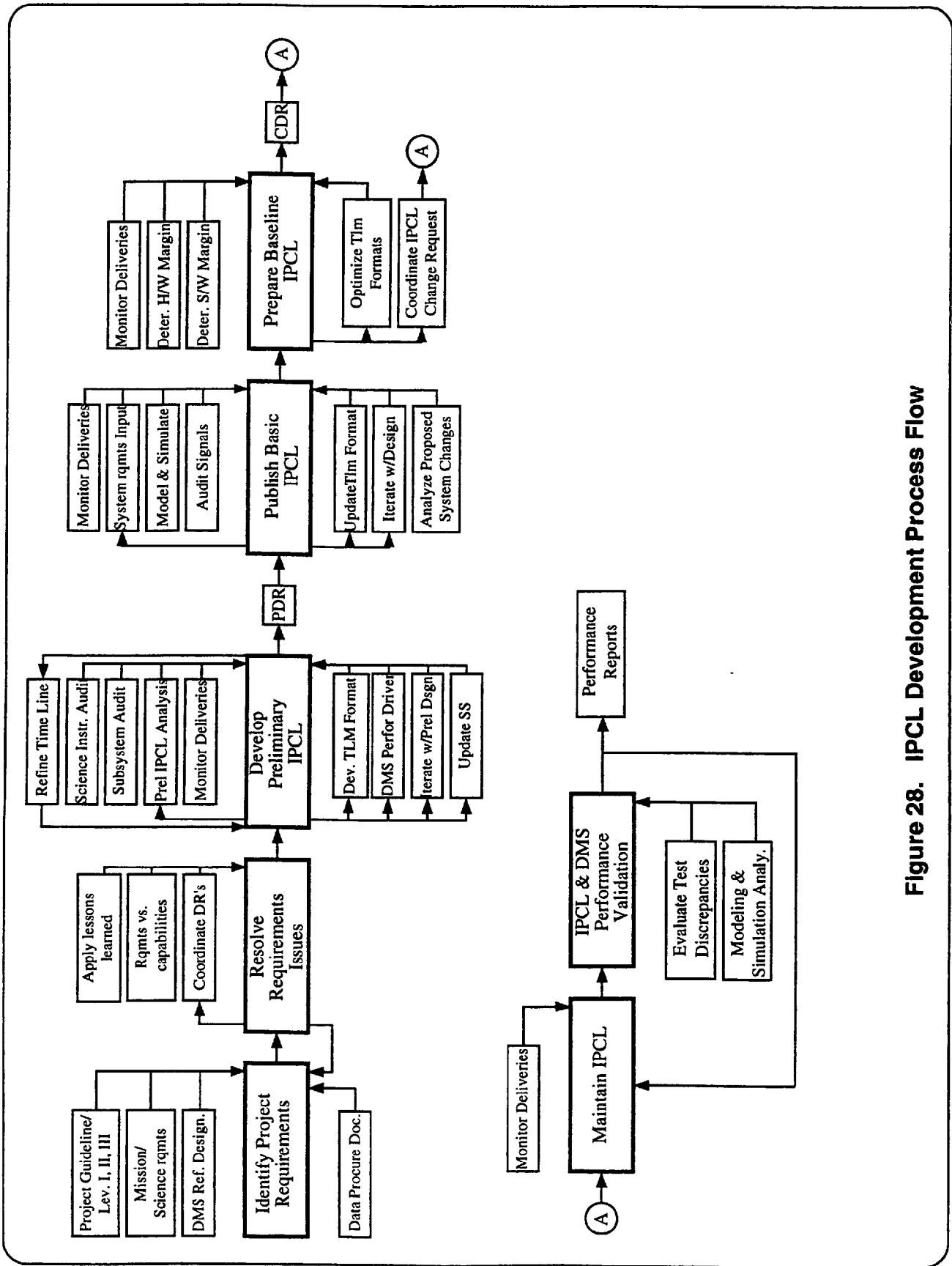


Figure 28. IPCL Development Process Flow

provide the basis for hazard elimination or control. This process should be applied to design/hardware changes throughout the program life cycle.

Maintainability requirements are outlined in NHB 5300.41. Long duration programs may be designed for on-orbit maintenance. The extent of on-orbit maintenance operations should be established during initial program requirements definition to ensure consideration in the initial design concepts. For example, the product assurance plan for the Hubble Space Telescope (HST) had separate maintainability, reliability, and safety sections.

3.4.3 Safety Compliance Data

Referring again to Figure 16, the next safety data iteration is at the final design level. This is the Critical Design Review (CDR) and is a review of the design to which the flight and ground hardware and software are to be manufactured. Thus, the finalization of the hardware description and operation, the hazard controls, and the verification methods to be implemented in verifying those controls are in the PED CDR data package. The PED Safety Compliance Data are assessed and combined by the PMM into an IPL Safety Compliance Data Package which is baselined following the IPL CDR, with the signature of each of the PEDs required.

After the IPL CDR, the PMM delivers the baselined IPL Safety Compliance Data Package to the NSTS Phase II Safety Review Panels for the Phase II safety reviews. The purpose of the Phase II safety review is to obtain safety panel approval of the updated safety analysis that reflects the completed design and operations scenario of the payload/GSE. The Phase II safety analysis is completed such that: all hazards and hazard causes have been identified; a means for eliminating, reducing, or controlling the risk has been defined and implemented; and specific safety verification methods (i.e., test plans, analysis procedures, and inspection requirements, etc.) have been finalized. Payload/GSE interfaces, mission and ground operations, procedures, and timelines that were not addressed during the Phase I safety review are assessed for safety hazards. The payload interfaces to be assessed include those between the Orbiter and the payload and among the various elements that comprise the payload (i.e., the spacecraft, upper stages, space platforms, pallets, experiments, ASE, ancillary flight equipment, GSE, GFE, etc.). Newly identified hazards are documented in additional hazard reports.

The Phase II hazard reports are prepared by updating/revising the Phase I hazard reports to reflect the completed payload/GSE design and flight/ground operating procedures. If the payload/GSE design is changed from Phase I to Phase II such that a Phase I hazard report may be deleted, a brief statement of rationale for deleting the report is given in the Phase II assessment report.

Following the CDR, which typically represents a level of design completion of 90 percent, the hardware is actually documented, produced, and verified. In the same timeframe as the Design Certification Review (DCR), the Phase III safety reviews are conducted. The Phase III hazard reports reflect the as-built design and operations of the payload/GSE. Ideally, by Phase III, all safety analyses efforts will have been completed.

The payload organization updates the Phase II hazard reports to (1) reflect the final payload/GSE design and operations, and (2) document the status and results of all completed verification work. All open flight verifications must be listed on the flight safety verification tracking log. Open ground verifications and open flight verifications that have been identified as a constraint against payload processing must be closed before the applicable ground operation can be performed.

The purpose of the Phase III safety review is to obtain safety panel approval of the completed safety analyses and of the safety certification data. The PED must submit data before the PED Integration Readiness Review (PED IRR), which confirms the satisfactory completion of all hazard control verification items and of all open safety items. These data are submitted by the PED in the form of requested changes (ECRs) to the PEDs section of the baselined IPL Safety Compliance Data Package. The Phase III safety review is the final determination of the safety compliance of the payload/GSE with the NSTS payload safety requirements.

The preceding paragraphs contain a brief description of the payload safety verification process. Complete descriptions of requirements, implementation approaches, and procedures are available in the safety documents listed in Volume 2, Section 3.2.

3.4.4 Systems Analyses, Models, and Simulations

The final system analyses utilize models that incorporate the detail design information and should be test verified. The purpose of this series of analyses is to predict the performance of the system as designed. Detailed mathematical models are used to determine if the system will meet the system requirements. Whenever possible, and especially when critical technology is involved, tests are conducted to verify the design and the models' accuracy.

Through this iterative process the models become more refined and confidence is gained that the results from the analyses are accurate. The individual models are then combined to determine system level interactions. The interactions are identified and an interface model generated. Further analyses determine if these interactions have a deleterious effect on the performance of the system.

As more test data become available, the accuracy of the models is continually checked and the models are modified to reflect the acquired information. Verification and refinement of the models continue throughout the design, development, and fabrication phases of the program. The final models are used both to justify the original assumptions of the program and to verify parameters of the system which cannot be tested directly.

3.4.5 System Functional Schematics and Interconnect Diagrams

The purpose and function of the systems diagrams and schematics are to provide end-to-end functional definition of electrical and fluid systems for analysis and troubleshooting. The system interconnect diagrams graphically depict the arrangement of external plumbing/electrical cabling which connects assemblies and

equipment. Diagrams for electrical and mechanical systems are prepared separately with appropriate cross references. A sample interconnect diagram is shown in Volume 2, Section 2.5.2.

The Electrical System Schematics illustrate and describe items with symbols placed such that a circuit may be traced from end-to-end in the sequence of its function. The placement and arrangement of these circuits follows a logical sequence of presentation to provide a clear description of the distribution, attendant interlocking, and content of the circuits.

Electrical System Schematics show electrical circuits of the spacecraft equipment which connect via direct electrical paths to all external interfaces. The schematics include all appropriate support equipment to accommodate the operational configuration. The circuits in the interfacing equipment are shown by reference. A sample of an electrical system functional schematic is found in Volume 2, Section 2.5.3.

Fluid system functional schematics provide integrated configuration definition of all fluid systems (vehicle, payload, or experiment) in one convenient reference. Schematics include all pertinent components (valves, regulators, pumps, filters, etc.) within the fluid system as well as pertinent interfaces with other compatible fluid systems (e.g., launch vehicle, ground support equipment (GSE), facilities, other projects). Schematics reference design drawings for configuration details and identify (by symbol and reference) power, command, and data interfaces. A sample of a fluid system functional schematic is in Volume 2, Section 2.5.3.

3.4.6 Software Code/Debug

The software is coded and tested in this phase. The level of testing is commonly referred to as debugging. When debugging is complete, a Test Review may be scheduled to assure conformance to test requirements and plans in the subsequent verification, validation, and systems integration tests.

The initial software delivery is made, though it is an internal delivery not usually available to the user. This delivery is intended to be made to the verification team. The internal delivery is under developer configuration control at the beginning of verification.

3.4.7 Operations Simulations and Mockups

Simulations and mockups generally fall into two categories; non-operational mockups and operational simulators. These two types of models serve two primary functions. Mockups are generally used for "form and fit" activities and to evaluate man-systems interface; later, they may be used for crew training and other purposes. Simulators are breadboard operational pieces of hardware which are used in lieu of the actual flight hardware to allow the system to be exercised in its various operational and off-nominal modes.

3.4.8 Operations Procedures and Training

The Mission Operations (EO) Laboratory plays a key role in the development and conduct of operations simulation and training as part of integration. Operational simulation capabilities are typically developed in conjunction with the design, development and build of the system hardware and software. The simulation system and/or simulators are used to exercise and validate system operational capability, verify interfaces, demonstrate overall system readiness, and provide operational system training for ground and flight operations (including flight crew) personnel. Mission operations typically defines the requirements, defines the functional capability of the math model, designs the support equipment and implements the simulations.

Any changes being considered to hardware or software elements of the current system design are reviewed by Mission Operations to ensure that fulfillment of operational requirements is not jeopardized. The operations concept impact is also assessed. This requires active participation in the configuration management process.

Mission Operations produces the operational data through reviewing the system design in conjunction with the mission operations concept. The mission operations concept will define the basic operational modules (e.g., MMDA-POCC, Orbiter/Aft Flight Deck, Upper Stage, Satellite, Launch Control Center, etc.) and inter- and intra-module data link and interface requirements. The data associated with each module must then be derived and documented.

Training requirements and plans are developed by the mission operations organization primarily from the operations concept and operations requirements as described above. Once this initial set of mission operations training requirements is established, training requirements are also established for the interfacing systems/operations elements. Next, the resources required to fulfill the training requirements are identified. These resources include items such as training aids, simulators, special documentation, system hardware and software configurations, secure training areas, etc. After preliminary training requirements and resources have been established, an operational training plan is developed that describes the operational training to be conducted, the resources required, the roles and responsibilities of all participants in the training program (including external interfacing participants from NASA centers, contractors, etc.), and the training schedule.

Mission operations simulations are accomplished to supplement and provide operational training to the Mission Control Team, crew, and appropriate Flight Operations Support Personnel (FOSP); to demonstrate the technical/functional performance of external interfaces; to assess system performance during specialized mission phases; and to demonstrate the operational performance and characteristics of the system.

Simulation requirements are derived from the operations concept, mission goals and success criteria, and consist of those functions and activities that must be performed in an operational environment in order to demonstrate system readiness. An example is receipt of operational data from an external source, processing of this data in

accordance with system mission requirements, and the transmission of the required processed results to the designated external recipient; all within the constraints of a valid operations timeline. Simulations of this nature will have some heritage from the project's integrated systems testing results. However, demonstration of operational capability, using a mission oriented scenario and timeline, will exercise many system capabilities and functions for the first time. For this reason, the identification of simulation requirements requires close coordination with system design, system test, and project management.

Mission operations participates in the program test planning and scheduling activity and participates in Test Working Groups, providing review and comment support to system test-related activities. The goal is to incorporate the mission operations requirements into the test planning and scheduling process. Mission operations also identifies and develops the unique operations tests, plans, and procedures not covered by the system test activity. In some cases, tests cannot be performed to evaluate/demonstrate some operational aspect of the mission (e.g., zero-gravity activities). These will usually be accomplished by analysis or similarity to past tests. Mission operations will independently plan, schedule, and perform operations-unique tests to demonstrate and verify operational concepts. These will typically form part of or operate in conjunction with simulation activities.

Finally, when the formal system test process begins, mission operations participates in conducting the test and subsequent data analysis, and ensures that actual system performance data are used to update system training materials and simulation plans and procedures.

3.4.9 Baseline Interface Definition

The Interface Control Documents that describe the design solutions for all the interfaces between hardware and software elements are baselined in the CDR time frame. These documents are then used as inputs to the end item specifications. Once the ICDs are baselined, the parties on each side of an interface are bound by the interface design contained in the ICD. Should one of the element developers determine there is a change required for the equipment to function properly, a change package is prepared. The change package is processed by the appropriate Change Control Board (CCB) to assess resulting impacts and ensure that interface compatibility is maintained.

3.4.10 Critical Design Review

The primary purpose of the CDR is to assess the detail design configuration documentation and establish a baseline for start of fabrication. Design drawings should be approximately 90 to 95 percent complete at the CDR milestone. The CDR provides assurance that the detail design is in accordance with the Part I CEI specification prior to its release to manufacturing.

By the start of CDR, all PDR RIDs should have been closed. The system engineering documentation in the CDR data package is thoroughly reviewed and

discrepancies are once again documented in RIDs. More details on the RID process can be found in Volume 2, Section 5.1.10.

Subjects that should be addressed include the design configuration, system compatibility, design integrity, reliability and safety assessments, and cost and schedule relationships. Test, verification/validation, and manufacturing and assembly plans should be available, as well as contract end item specifications. Additional details are in NHB 7120.5 and MMI 8010.5. A checklist of CDR topics is in Volume 2, Section 5.1.3.

The participants and chairmanships are basically the same as the project PDR. Generally, the level of NASA control, following the completion of the CDR, remains at the Part I CEI Specification, and the detail drawing control remains with the design contractor. However, NASA project management has the option of establishing control over the product baseline to include detail engineering drawings of the items to be manufactured.

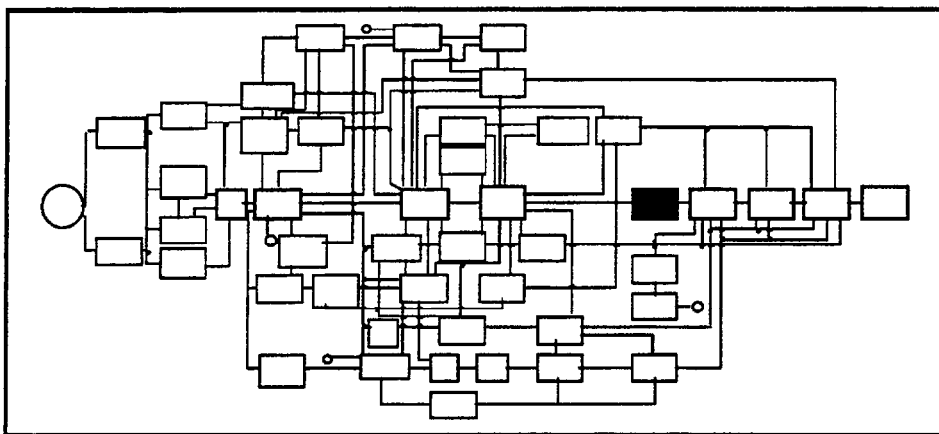
The primary product of the CDR is the formal identification of specific engineering documentation that will be authorized for use to manufacture the end items. This includes authorized release of the baselined design and the required data as shown above. After baselining the design, any proposed changes will require submission of an Engineering Change Request (ECR) or an Engineering Change Proposal (ECP). The ECR process is described in Volume 2, Section 5.2.2.

3.4.11 Phase II and III Safety Reviews

Referring to Figure 16, the Phase I flight and ground safety data are reviewed again at CDR to produce a Phase II flight and ground safety data baseline. Concurrently, a safety verification plan is developed and outstanding safety items are closed out. Hazard Reports are generated, as required, by the PED and IPL safety review teams at CDR.

The resulting Phase III ground and flight safety close-out data reports are statused by the PED team at the Integrated Readiness Review (IRR). Subsequently, the IPL conducts a review of the Phase III safety data and the PED/IPL teams jointly issue both flight and ground safety compliance certification reports. Hardware modifications made during final system integration result in a delta-Phase III flight safety readiness report prior to launch.

3.5 FABRICATION AND ASSEMBLY



The production of an end item (launch vehicle, spacecraft, payload, experiment) which meets project requirements and mission objectives is a key milestone in the overall system engineering process. Likewise, production planning and production capabilities must be factored into the system design from the beginning of the project if the most-effective solution is to be found. Among the production functions which the system engineer needs to consider are, "... material ordering, material handling, fabrication, processing, quality assurance, process control, assembly inspection, test, preservation, packaging, storage, shipping, and disposition of scrap, salvage, and waste materials."¹

The early and continuous consideration of these production functions in trade studies, cost analyses, risk management, schedules, and other products of the system engineering process is part of what is known as "concurrent engineering." This concept is best pursued as part of an overall Total Quality Management approach to project management. For our purposes here, suffice to say that the system engineer must include production functions in the system engineering process from the beginning of Phase A and throughout the life cycle. The balance of this section is given to a brief description of some of the other activities that occur during the fabrication and assembly process.

The fabrication and assembly processes are the critical final steps during which hardware is acquired (either manufactured in-house, contracted out, or purchased off-the-shelf). The components or subsystems are assembled to produce the end item system. This phase is not merely the assembly of components and/or piece parts into subassemblies, components, subsystems, or elements. It is the use of these elements in a final assembly process.

¹ Systems Engineering Management Guide, U.S. Government Printing Office, January 1990, p. 18-1.

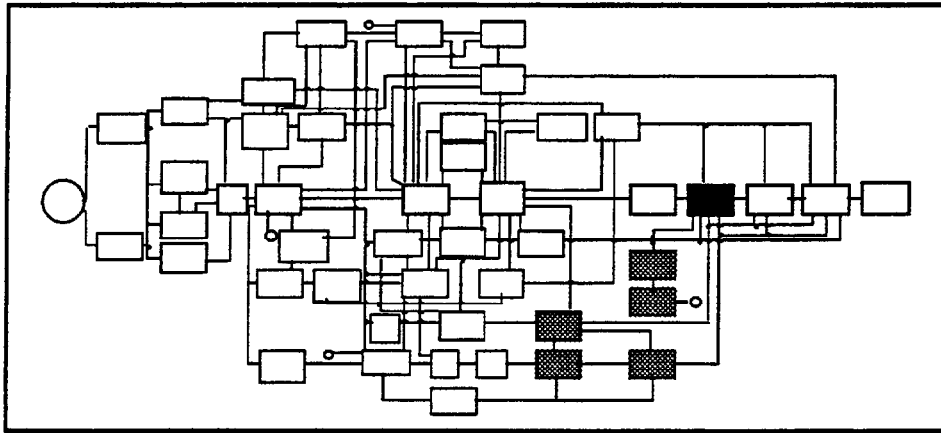
Before the elements, subsystems, or components can be developed, the parts that make them up must be obtained. This is a make or buy decision activity. Issues such as the number of items used, commonality, availability, material and reliability requirements, schedules, capabilities, and budgets are all traded off against the program requirements and constraints.

In all procurement activities, factors such as material requirements, material characteristics, reliability, and delivery schedule for raw material should be considered. Other important factors include production schedule, product delivery schedule, project schedule, budgetary considerations, and other requirements and constraints.

The integration of all the various elements of a system is usually accomplished in multiple locations. This activity is the assembly of all the discretely defined end items into a homogeneous system. The assembly of parts and components that comprise the elements and subsystems is accomplished prior to this phase, with the exception of some Mission Peculiar Equipment (MPE).

Several locations are typically involved in this physical integration activity because the system assembly is often staged or conducted in parts. That is, each of the hardware element developers performs a certain amount of assembly at their facility. Next the assembled subsystems (or elements) are transported to an integration site. Sometimes elements are shipped to an integration site where another developer performs further assembly. All the hardware elements, components, subsystems, and MPE are ultimately delivered to KSC for processing. At KSC all the final assembly and check-out operations are conducted to prepare the payload for its mission.

3.6 VERIFICATION



Verification programs are established for flight and ground systems to ensure safety interfaces, design and performance requirements, and specifications are met. See MSFC-HDBK-2221 for a complete discussion of the verification process. Verification is accomplished through the two primary techniques of testing and assessment as illustrated in Figure 29.

Verifications are performed at all levels of development and integration, including tests during assembly and simulated flight environments. Verification requirements are derived from Level I through Level IV requirements documents and are defined by the Verification Requirements and Specifications Document (VRSD). The Verification Requirements Compliance Document provides the evidence of compliance to each Level I through Level IV requirement and to the requirements of the VRSD. A flow-down of Level I through Level IV requirements including the requirements of the VRSD provides traceability of all project requirements. See MSFC-HDBK-2221, Section 2.1.1.11, for a discussion of the Verification Requirements Compliance Document. The results of the verifications are documented in a verification report which provides the result of each verification activity, a description and disposition of non-conformances, and conclusions and recommendations.

Testing falls into two major categories, as shown on Figure 29: functional testing, and environmental testing.

Testing of a vehicle/payload or experiment ensures that performance of the flight systems, hardware and software, are in accordance with the design and performance requirements. The test activities include in-process testing, functional testing, and environmental testing, at ambient and in a simulated flight environment. Simulators are generally used where flight hardware is missing, where man-in-the-loop activities are required to verify operability, and at interfaces to ensure that the systems function properly.

In-process testing is performed during the hardware assembly phase. This testing satisfies requirements that cannot easily be verified after the hardware is assembled. A typical in-process test would be to verify the bonding of equipment to the structure.

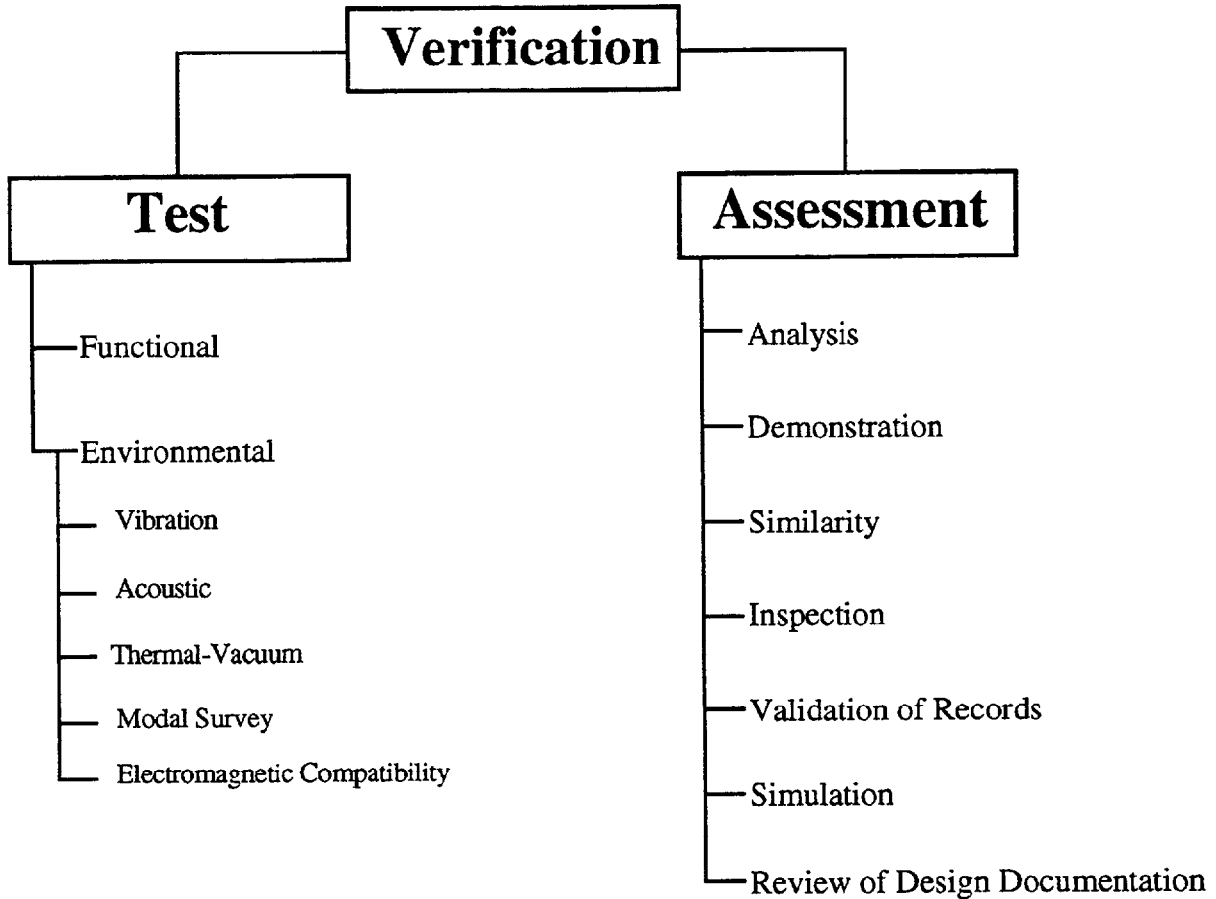


Figure 29. Verification Methods

Functional testing consists of performance tests conducted on flight or flight-configured hardware and software usually at ambient conditions. Its purpose is to establish that the system performs in accordance with design and performance specifications. Functional tests are performed before and after environmental tests.

Note that it is very important to specify what the ambient conditions are for functional testing, otherwise it is left open to interpretation by the tester. Commands and telemetry are exercised to the extent possible, and redundant equipment and hardware configurations are verified where possible. After all subsystems and equipment have been tested, the vehicle/payload or experiment is tested as an integrated unit to ensure the compatibility of the systems.

Environmental testing consists of performance tests conducted on flight or flight-configured hardware and software under conditions approaching those expected

in flight. Environmental tests may include modal survey, vibration, acoustic, and thermal-vacuum tests. Electromagnetic Compatibility (EMC) testing is sometimes considered part of functional testing, but in MSFC-HDBK-2221 EMC is included under environmental testing.

A functional test of the system at ambient conditions is performed after each environmental test to ensure that systems experience no degradation after exposure to the environmental conditions. An inspection of the payload or experiment is also performed to ensure no visible damage occurred due to the environmental exposure.

Major guidelines influencing the integrated system requirements verification are as follows:

- All items being integrated at the system-level must have been verified at the component level prior to delivery.
- All new system interfaces, hardware and software must be verified. If an interface is broken, it must be re-verified.
- GSE safety and interfaces with the total system must be verified.
- Interface verification must ensure wiring continuity and functional operation across the interface.
- Verification of system compatibility must be assured.

Some requirements cannot be verified by test, and must be verified by various assessment methods; normally analysis, demonstration, inspection, similarity, validation of records, simulation, and review of design documentation (see Figure 29 preceding).

Verification by analysis includes the techniques of system engineering analysis, statistics and qualitative analysis, computer and hardware simulations, and computer modeling. Analysis may be used when it can be determined that rigorous and accurate analysis is possible, testing is not feasible or cost-effective, similarity is not applicable, or verification by inspection is not adequate.¹

Verification by demonstration is a method used where actual demonstration techniques are used to verify compliance to a requirement. This includes requirements such as serviceability, accessibility, transportability, and human engineering.² Verification of crew hardware interfaces and accessibility for on-orbit equipment removal and replacement would be by demonstration, for example.

Verification by inspection is the physical evaluation of equipment and/or documentation to verify design features. Inspection is used to verify construction

¹ MSFC-HDBK-2221, Verification Handbook, February 1994.

² MSFC-HDBK-2221, Verification Handbook, February 1994.

features, workmanship, dimension and physical conditions such as cleanliness, surface finish, and locking hardware.¹

Verification by similarity is a process of assessing requirements compliance by review of prior test data or hardware configuration and application. This is used where the hardware item is similar or identical in design and manufacturing process to another hardware item that has previously been qualified to equivalent or more stringent specifications.² This method of verification is used mostly at the component level. Caution must be used to make sure the intended application environment of the component is identical to or less stringent than the previous application environment. In each case, however, ensure that the flight hardware to be verified by similarity meets all applicable requirements.

Validation of records is the process of using manufacturing records at end-item acceptance to verify construction features and processes for flight hardware.³

Simulation is the process of verifying design features and performance using hardware or software other than flight items.⁴

Review of design documentation is the process of verifying the design through a review of documentation during the Preliminary and Critical Design Reviews.⁵

Verification is performed at various times in the project life cycle. These verification phases are defined periods of major project activity and include the development, qualification, acceptance, pre-launch, and flight/mission phases. See MSFC-HDBK-2221, Section 2.1.1.3.2 for more details on the verification phases.

3.6.1 Verification Procedures

Procedures define the sequence of events and provide detailed information on objectives, support requirements including software support, configurations, environmental conditions, constraints, and special instructions. The Verification Procedures are generated by the test organization to satisfy requirements defined by the VRSD. Procedures are tailored to a verification phase, a particular test, and a given hardware level and contain all the characteristics and design criteria to be tested for acceptance or rejection. This could involve an automated test or a manual verification. Once the procedure is approved, it is subject to change control.

¹ MSFC-HDBK-2221, Verification Handbook, February 1994.
² MSFC-HDBK-2221, Verification Handbook, February 1994.
³ MSFC-HDBK-2221, Verification Handbook, February 1994.
⁴ MSFC-HDBK-2221, Verification Handbook, February 1994.
⁵ MSFC-HDBK-2221, Verification Handbook, February 1994.

3.6.2 Software Verification

The Verification Phase is conducted on the debugged software by a group independent from the coders and debuggers. The software is checked against the Software Requirements Specification in a facility which simulates a closed loop system using as much hardware from the flight system or prototype, as feasible. Logic paths and operating mode are verified as well as reasonable failure modes. This phase concludes with the delivery of a verified program and a Functional Configuration Inspection (FCI). This FCI reviews the verification and design results to assure functional conformance with software requirements. The "as-built" design and code and verification reports are baselined at the FCI. The change control and problem report processes are in formal use beginning with verification.

3.6.3 Software Validation

Validation is a step beyond verification in that more hardware is used in the testing. Emphasis is on system/software compatibility and subsystem performance. Validation is system integration testing with emphasis on assuring software performance within the system environment. The final software delivery and Configuration Inspection (CI) conclude this phase. A Detailed Software Design Specification Document (as-built) and a Software User's Manual are released at the CI along with the Software Validation Test Report. Often verification and validation are performed by a third party and not the software developer.

Systems integration is the systems level test that provides a final test of the software at the highest possible level of testing. It can be considered a higher level validation or an extension of the validation process. A hardware/software integration and compatibility test at the systems level is the goal. This phase ends with the Systems Acceptance Review (SAR). The final software update delivery may be made at SAR, and all previous software documentation is updated, as required.

3.6.4 Verification Report

The Verification Report provides the results of all verification activities on the hardware and software, including any special tests and ground support equipment. The report includes the specific result of each procedure requirement, including performance data and data plots and describes any deviations from nominal results. The report also provides the objectives of the test, a description of all non-conformances and failures, disposition of non-conformances, corrective actions, and retest activities. A conclusion relative to the success of the verification is included. The report will contain a copy of the as-run test procedure, if the procedure will more clearly show how results compare against applicable specification requirements.

3.6.5 Verification Requirements Compliance

The requirements for which compliance will be identified are normally defined in two separate documents. One document contains the requirements resulting from a flow-down of Level I requirements through Level IV. The second document contains the requirements defined by the VRSD. Compliance to the requirements that have been flowed-down and to the requirements of the VRSD ensures the Level I design and performance requirements have been met. Verification assessment process flow diagrams can be found in MSFC-HDBK-2221.

A Verification Requirements Compliance process is used to identify how compliance to requirements was achieved in relation to the verification program. Compliance to a requirement is established when the documents referenced show and certify the adequacy of the method used in the verification process and that the verification result is compliant with requirement specifications and criteria. Compliance must be defined for requirements at all levels, including derived requirements.

The compliance information provided for each requirement includes the verification method, the compliance data, and any non-conformance to the requirement specification or criteria. The compliance data would be that information which provides the actual data or the reference to the actual data that shows compliance to the requirement.

3.6.6 Independent Verification and Validation

Independent software Verification and Validation (IV&V) is the process of determining that the software is developed in accordance with the stated specifications, that it performs satisfactorily in the mission environment the functions for which it was designed, and that it does not perform unintended functions. IV&V is an independent, systematic evaluation of a software developer's product throughout the software life cycle.

As a management tool, IV&V ensures an orderly process of software development by identifying errors early in the development cycle rather than in later phases where corrections are much costlier. This process supplements the developer's software QA process because IV&V is performed by an organization independent of the software design group.

IV&V is designed to address each critical phase of the software development process (Figure 24). Software development is comprised of many subactivities or tasks and IV&V assures that each development task has been completely and correctly performed. The IV&V process occurs in three phases as described below.

This IV&V consists of two parallel activities: 1) requirements analysis, and 2) test planning. Verification of software requirements is performed to ensure that system and interface requirements (documented in the system specification) are correctly allocated to software requirements. The IV&V organization also compiles a detailed test plan for evaluating the software, in parallel with the requirements analysis phase.

The requirements analysis consists of two activities, equation and design analysis and facility development. The software design defines both the executive control logic and algorithms to perform each software function. A balance of analysis techniques must be selected to verify both of these elements of the software design. Design analysis techniques to be utilized for any particular function are dependent upon the nature of the function (such as filtering, display output, device interfacing). The proposed design of each software function is verified by using the selected method to determine the extent to which it satisfies the software requirements. Control logic is similarly verified to ensure proper interaction between software functions. Any deficiencies in the software design are documented and forwarded through the Project to the Developer. The facility development provides for the development of test tools such as simulations, flow charters, editors, and other automated tools required to implement the testing phase.

Software test planning was discussed in Section 3.2.11 above. Once the tests are run, test results are recorded and any anomalous results are confirmed by analysis before the results are presented to the Project. An IV&V Final Report documents the results of the IV&V effort and presents conclusions regarding the operational performance of the system.

3.6.7 Software Operations and Maintenance Phase

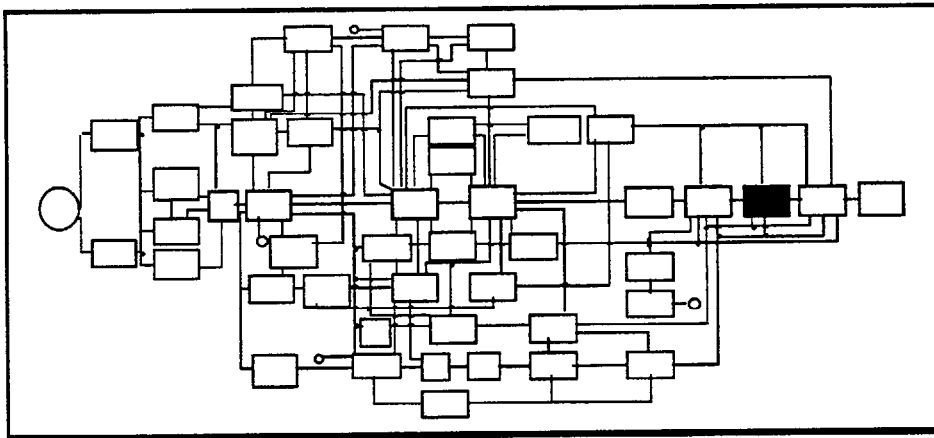
This final phase runs for the balance of the project life cycle, and requires a strict configuration control process be maintained. At the end of this phase (end of project), the final software configuration and documentation should become a permanent MSFC record in case a project is reactivated or the software can be used in future projects.

3.6.8 Design Certification Review (DCR)

After completion of fabrication and assembly and the verification process, a DCR may be conducted to evaluate the results and status of verification planning, testing, and analysis necessary to certify the design. Generally, it is scheduled after CDR and prior to FRR and shipment of flight hardware to the launch site; but depending on program structure, the DCR may occur subsequent to other significant events such as completion of verification flights. The DCR should address the design requirements, make an **as-designed** comparison, assess what was built to meet the requirements and review substantiation (including CEI verification plan and requirements, ICDs, design requirements, and CCBDs), determine precisely what requirements were actually met, review significant problems encountered, and assess remedial action taken.¹ A list of DCR topics is given in Volume 2, Section 5.1.6.

¹ MM7120.2, Project Management Handbook, June 1989.

3.7 PRE-LAUNCH/LAUNCH OPERATIONS



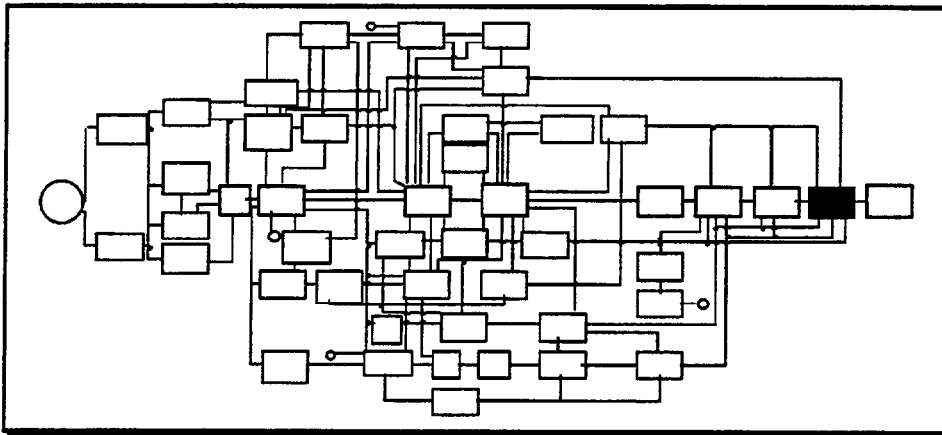
Pre-launch and launch operations are conducted primarily at KSC, although the MSFC Huntsville Operations Support Center (HOSC) may be manned and in a support role for MSFC-managed missions. This support may include providing technical analysts, technical advisors, system engineers, and/or direct operations support personnel to monitor data and verify performance prior to launch.

The technical specialists and system engineers assigned to augment the support personnel of the Mission Operations Laboratory (EO), will be assigned to a position, either on-site or off-site, and will perform evaluation and checkout functions during the pre-launch final countdown. They may also participate in the GO/NO GO decision process. After liftoff, the flight operations process takes over and will be described in Section 3.8.

3.7.1 Flight Readiness Review (FRR)

Shown in Figure 8, the FRR is a detailed review by which the system is certified as flight-worthy. It includes review of the system verification process (both testing and analysis), system compatibility, operational planning, and team preparedness. The review will result in certification of flight readiness of the operational team, the acceptability of the vehicle for each flight, and the readiness of the system to achieve all flight objectives. A checklist of FRR topics is in Volume 2, Section 5.1.9.

3.8 FLIGHT OPERATIONS



The full compliment of FOSP/Mission Control Team (MCT) personnel will be active in the on-orbit control and operations of the payload/spacecraft. The following is a list of typical, but not all-inclusive, functions that the FOSP/MCT performs:

- Provide tasking instructions to Command Controller for uplink to spacecraft (S/C)
- Analyze real-time health and status telemetry data
- Perform long-term trend analysis
- Determine S/C attitude and generate ephemeris data
- Resolve anomalies
- Interface with Project Office
- Provide communications links between the flight crew and ground controllers/Pis
- Provide replanning responses to minimize impacts of payload contingencies
- Manage allocation of resources among payloads

Inputs required to perform the operations support task are:

- Trained Personnel - Trained and certified MCT, FOSP, HOSC and POCC Personnel, and flight crew.

- Approved Flight Operations Documents - System schematics, specifications, software listings, flow diagrams, logic diagrams, operational procedures, and handbooks.
- Simulation/Test Results - Parametric and procedure data that can be used for system/subsystem analysis, mission reconstruction, anomaly resolution and replanning.

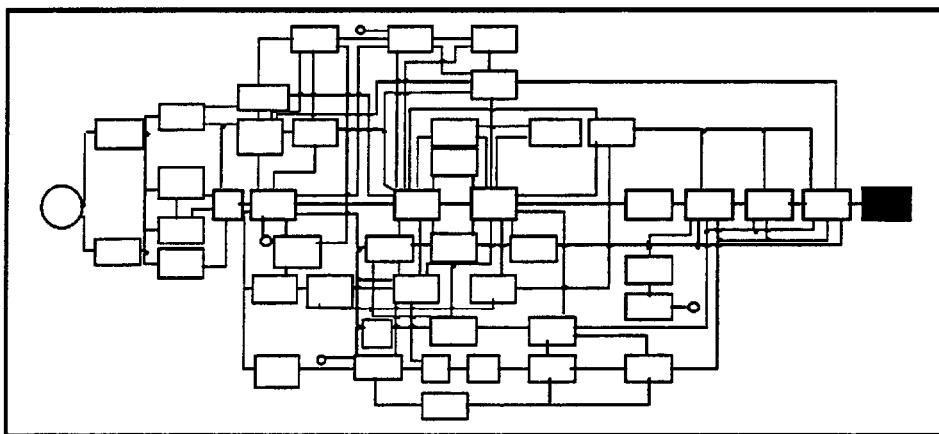
Outputs resulting from this task include:

- Mission Operations Performance Evaluation - Ongoing mission operations performance evaluation presented and reviewed at project meetings, data reviewed for impact to next mission flight planning, timelines, etc., to ensure mission assurance compatibility.
- Retraining/Recertification Requirements - These new requirements will be a result of ongoing and post-mission personnel performance evaluation. Mission scenario training will use trainer and simulator facilities.
- Historical Data - This data will include: Telemetry/Data tapes (unprocessed and processed); daily logs, anomaly history and resolution, and history/data tapes, meeting minutes, etc.
- Trend Data and Projection Analysis.
- Post Mission Evaluation Report - A finished, bound, hard-copy report, representing Mission Success overview.

The system engineering contribution to Mission Support during the flight covers the following tasks:

- Providing flight hardware system expertise
- Monitoring the health of the hardware and software
- Monitoring the engineering performance of the system
- Performing ground analysis/calibration for subsequent uplink
- Responding to anomalies which affect system performance
- Coordinate software patches for anomaly correction
- Providing status information to/from the Science Operations leads, management, KSC and JSC, as appropriate

3.9 POST-MISSION EVALUATION



There are numerous activities that occur in the life of a payload following the completion of the orbital flight, re-entry, and landing segments of a mission. Some principal post-mission functions include hardware de-integration, data analysis, and the preparation of post-mission reports. These are discussed below.

3.9.1 Hardware De-Integration and Return to Owners

Following landing and subsequent safing of the orbiter systems, the shuttle is returned to KSC for de-integration of the payload(s) and refurbishment of the shuttle. When necessary a few experimental results are extracted from the shuttle very soon after landing. However, even in these few cases, the hardware is not removed.

Once the shuttle is delivered to KSC, the hardware is de-integrated and the various components, elements, subsystems, and experiments are returned to their source. Sometimes flight anomalies require some limited on-line or off-line testing of the carrier prior to complete de-integration. In the event the payload carrier is to be re-used for another flight, in the same configuration, it will be stored at KSC until needed for final integration on the next mission. If a carrier requires reconfiguration or refurbishment, it is returned to the integration site or developer's facilities for these activities.

Prior to and during the hardware de-integration activities, the hardware is inspected for general condition and failures or anomalous conditions. The condition of the hardware system is carefully observed and documented at completion of the de-integration activity.

There is very little storage space available at KSC due to the large number of payloads being processed for flight at any given time. Thus, very seldom is hardware retained unless it will re-fly in the same configuration (i.e., same MPE, same electrical interfaces; requiring only experiment and orbiter integration to be ready for flight again).

3.9.2 Engineering and Science Data Analysis

Very large amounts of engineering and science data are typically collected during a mission. When required, data are usually downlinked to the Mission Control Center (MCC) or Payload Operations Control Center (POCC) during the mission for preliminary analysis and display purposes. Data may also be stored within the experiment or its carrier to be retrieved post-mission. Most of the data storage is accomplished using magnetic tape recorders or, more recently, in non-volatile mass memory.

Some of the downlinked data is analyzed while the mission is still on-going. Engineering data that can help provide early assessments of success, on systems that can be adjusted on-orbit if the first run(s) is flawed, are often analyzed immediately following their receipt. Principal Investigator (PI) curiosity often leads to science data downlinking requests during the mission. Most science data analysis, however, occurs following the landing and retrieval of tapes from the tape recorders.

Science data analysis is performed by the PIs in their own (or their sponsor's) facility. Analysis techniques and algorithms will not be discussed here as they are peculiar to the specific PI and sponsoring institution, whether government or civilian.

3.9.3 Mission Evaluation Reports

Mission operations support personnel will conduct the necessary studies and analyses to permit rapid and accurate assessment of Flight Vehicle/Spacecraft performance, personnel (Flight Crew and Flight Operations Support Personnel and Mission Control Team) performance, identification of flight hardware/software anomalies and/or malfunctions, establishment of remedial action and identification and documentation of lessons learned.

Complementing the anomaly investigations, the post-mission evaluation report is another key area of activity for the system engineer. This report typically contains information such as:

- 1) Mission Summary
- 2) Carrier (or experiment) performance
 - a) Hardware
 - b) Software
 - c) System
 - d) Flight procedures

3) Ground Support Performance

- a) Ground displays/analysis tools
- b) Procedures
- c) Personnel
- d) Ground interfaces/protocol

4) Anomaly Investigation Summaries

- a) What happened?
- b) Why did it happen?
- c) How it will be corrected (or a plan established to obtain this answer)?

5) Lessons Learned/Conclusions

COMMENTS CONTINUED:

[Empty rectangular box for comments]

FOLD, STAPLE OR TAPE CLOSED, AND SEND TO:

**MFSC/EL51
ATTN: L. Don Woodruff
MARSHALL SPACE FLIGHT CENTER AL 35812**