NASA

National Aeronautics and
Space Administration

NASA CR-188330

Lyndon B. Johnson Space Center
Houston, Texas 77058

AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION FOR SPACE GENERIC OPEN AVIONICS ARCHITECTURE (SGOAA)

July 1994

John R. Stovall
Richard B. Wray

Prepared by:

Lockheed Engineering & Sciences Company
Houston, Texas

Task Order 060-EK-AB1
Contract NAS 9-19100

for

FLIGHT DATA SYSTEMS DIVISION
JOHNSON SPACE CENTER

LESC-31195

AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION FOR SPACE GENERIC OPEN AVIONICS ARCHITECTURE (SGOAA)

July 1994

John R. Stovall, Advanced Systems Engineering Specialist
Richard B. Wray, Advanced Systems Engineering Specialist

APPROVED BY:

G.L. Clouette, Project Integration Specialist Flight Data Systems Department	D.M. Pruett, Manager, Advanced Programs Flight Data Systems Division

Prepared by:

Lockheed Engineering & Sciences Company
Houston, Texas

Task Order 060-EK-AB1
Contract NAS 9-19100

for

FLIGHT DATA SYSTEMS DIVISION
JOHNSON SPACE CENTER

LESC-31195

PREFACE

This document has been produced by Mr. John R. Stovall and Mr. Richard B. Wray of Lockheed Engineering and Sciences Company (LESC), the codevelopers of the Space Generic Open Avionics Architecture (SGOAA) Standard and the Avionics Scenario and Command Model Descriptions presented in this document. The contributions of Mr. Ben Doeckel of LESC who participated in early development of the concepts for the avionics architectures is gratefully acknowledged. Special acknowledgment is also given to Mr. Dave Pruett of the National Aeronautics and Space Administration (NASA) Johnson Space Center (JSC) for his support of the Advanced Architecture Analysis, and his assistance in the development of the open avionics architecture.

DOCUMENT CHANGE RECORD

The following table summarizes the change activity associated with this document.

ISSUE AND DATE	CHANGE SUMMARY	SECTION

CONTENTS

Section **Page**

Section **Page**

TABLES

FIGURES

Figure		Page

ACRONYMS

BIT	Built-In-Test
CBIT	Continuous Built-In-Test
CLL	Common Lunar Lander
C&T	Communications and Tracking
DBM	Data Base Manager
DSM	Data System Manager
ECS	Environmental Control System
EPD	Electrical Power Distribution
EPS	Electrical Power Subsystem
FDSD	Flight Data Systems Division
FDIR	Fault Detection, Isolation and Recovery
FSS	Flight Support System
GN&C	Guidance Navigation and Control
GSS	Ground Support System
IMU	Inertial Measurement Unit
IOSM	Input/Output Data Services Manager
JSC	Johnson Space Center
KSFC	Kennedy Space Flight Center
LESC	Lockheed Engineering & Sciences Company
LVS	Lander Vehicle System
NASA	National Aeronautics and Space Administration
OS	Operating System
POST	Power-on Self Test
Prop	Propulsion
PWR	Power

RF	Radio Frequency
RSEL	Real Time Systems Enbgineering Laboratory
SAE	Society of Automotive Engineers
SATWG	Strategic Avionics Technology Working Group
SDS	Space Data System
SDSM	Space Data System Manager
SDSS	Space Data System Services
SGOAA	Space Generic Open Avionics Architecture
SOCS	Space Operations Control Subsystem
TLI	Translunar Injection
TM	Telemetry

1. INTRODUCTION

This paper presents a description of a model for a space vehicle operational scenario and the commands for avionics. This model will be used in developing a dynamic architecture simulation model using the Statemate CASE tool for validation of the Space Generic Open Avionics Architecture (SGOAA). The SGOAA has been proposed as an avionics architecture standard to the National Aeronautics and Space Administration (NASA), through its Strategic Avionics Technology Working Group (SATWG) and has been accepted by the Society of Automotive Engineers (SAE) for conversion into an SAE Avionics Standard. This architecture was developed for the Flight Data Systems Division (FDSD) of the National Aeronautics and Space Administration (NASA) Johnson Space Center (JSC) by the Lockheed Engineering and Sciences Company (LESC), Houston, Texas. This SGOAA includes a generic system architecture for the entities in spacecraft avionics, a generic processing external and internal hardware architecture and a nine class model of interfaces. The SGOAA is both scaleable and recursive and can be applied to any hierarchical level of hardware/software processing systems.

The SGOAA is documented in Reference [WS94], the proposed standard itself and in Reference [WS92], the technical guide for the proposed standard. Relevant definitions from [WS94] are included in this document as Appendix A. An extension of the SGOAA development effort is a simulation of the actual dynamic behavior of the SGOAA in a demonstration system design. Modes and states analysis [DW93] provides a valid approach for the description of dynamic system behavior. Understanding of the dynamic behavior of a system by development of a system model in the early stages of a project will eliminate much of the uncertainty now inherent in the design process.

The SGOAA is based on a partitioning between logical and direct avionics system requirements. It includes architectural functions, hardware, software and interfaces for all avionics hardware/software processing systems. The SGOAA requirements description includes both system service software and applications software for a generic hardware/software processing system, the Space Data System (SDS). The SGOAA Interface Model is used to define how system requirements are to be applied at the appropriate system level to determine the logical and direct interface points. System logical data flow requirements are created for each client/server entity identifying the source of the data and the end-user of the data, functions to be performed by the server and the characteristic attributes required of the data. As a service entity, the functions of the SDS that are to be modeled to validate the SGOAA model are the functions or services to be performed for the client entities represented by the commands for services. In certain instances such as initialization, the SDS is both client and server.

A typical unmanned space vehicle, the Artemis Common Lunar Lander (CLL) was chosen as a reference vehicle for defining the client/server relationships and functions to be performed and to provide part of a mission scenario for this analysis. Although the CLL program was not continued beyond the Phase A stage, the command scenario presented in this paper addresses the functions of the SDS and as such is sufficiently generic to be applicable to most spacecraft data systems. References [KIL92], [STA92], [STB92] and [SHU93] present technical descriptions of the CLL.

This scenario and the accompanying command description is based on a program consisting of a transportation segment and payload segment. The transportation segment consists of launch services and the lander system. The lander system consists of three subsystems: the lander vehicle system (LVS), the ground support system (GSS) and the flight support system (FSS). Both the GSS and FSS are ground facilities. The GSS is the control authority prior to launch and the FSS is the control authority after launch. Command and control is provided through a generic capability referred to as the Space Operations Control System (SOCS). SOCS functions may be allocated to both ground mission control facilities (FSS and GSS) and to the onboard space vehicle (LVS) facilities for autonomous execution.

Section 2 describes the mission scenario to be modeled in the SGOAA simulation. Section 3 provides a description of the behavior in the scenarios of the mission, vehicle and system elements. Section 4 provides the detailed command and response tables in the SGOAA model mission scenario addressing the commands (functions) that the SDS must perform as a service provider for the avionics subsystems. Appendix A provides some key definitions from [WS94]. Appendix B describes the CLL system and its external and internal interfaces. Appendix C describes the detailed combinations of the modes and states allowed in the analysis in a typical mission scenario. Appendix D describes and contains the activity charts, statecharts and their associated data base for the first phase of a SGOAA simulation developed using the Statemate modeling tool for the mission scenario described in this report.

2. SGOAA MODEL MISSION SCENARIO

The scenario shown in Figure 2-1 and described below represents the mission sequence adapted from the Artemis Common Lunar Lander program requirements, with additional assumptions (not fully implemented) of orbital activities to include space station behaviors [SDAT93]. Three mission phases are generally envisioned (with specific mission modes as shown in Figure 2-1):

- Pre-flight mission phase
- Flight mission phase
- Terminal mission phase

Scenario behaviors are described by mission phase, based on the modes in [DW93]. Not all states can be implemented by the systems in response to specific mode commands (see Appendix C for detailed descriptions of combinations of the possible modes and states). This section summarizes key features of the scenario elements. The "Spacecraft Command Response Tables" in Section 4 were derived from Table 3-3 SDS Functional Interfaces of [SHU92]. Additional commands required to be added to section 4 were based upon the scenario developed in this section and are shown in bold type in the tables in Section 4. The modes described in paragraph 3.1 and the mission scenario as described in paragraph 2.2 form the basis for the overall sequence of events.

System and subsystem states described in Section 3 result from commands generated in response to mode inputs. Commands initiated on the vehicle are indicated as such by the source being the Command Processor referred to hereafter as SOCS. Commands initiated by ground control are indicated as such by the source being the GSS prior to launch and the FSS following launch. Known generic commands are shown in quotation marks. An example of a command is: "Arm Pyro". The resulting state of the pyro device is that it is armed. The generic commands are expanded upon to include commands to each affected system and related to the "Spacecraft Command Response Tables" by Primary Command number shown in parenthesis. The command number for "Arm Pyro" is (3). Functions that are not tied to a specific defined command are shown in italics and require identification of specific additional commands. An example is *(emergency ground commands from FSS).*

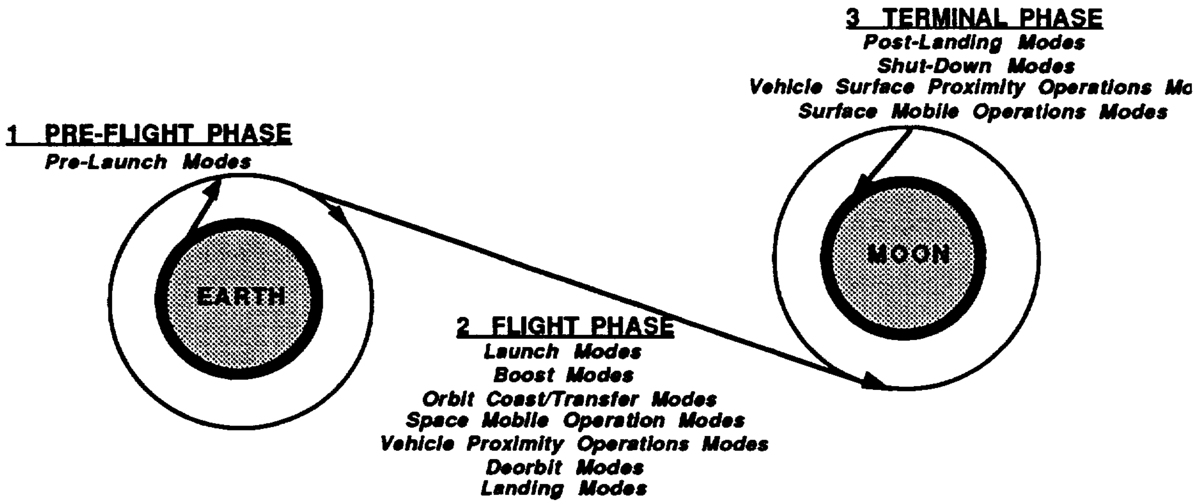


Figure 2-1. A Model of the Mission Scenario

2.1 GROUNDRULES

Groundrules used to develop and implement the scenario are reviewed below.

- The SDS processor will be powered up, perform Power On Self Test (POST) and will then boot SDS system software from non-volatile memory whenever power is applied to the vehicle (following this activation sequence all commands to power other systems can be routed throughout the SDS). The SDS processor will also send the results of POST over the communication link to the GSS or FSS whenever POST occurs.
- Loading of application software for Guidance, Navigation and Control (GN&C), Communications and Tracking (C&T), Instrumentation, Power, Propulsion and SOCS will occur when commanded by the GSS under SDS system software control following loading of the system software.
- Application software will remain in a non-active state until initially enabled by GSS command. The GSS is the priority command authority for the vehicle is on the ground. The FSS is the priority command authority for the vehicle following launch. In a normal operation mode the vehicle is under command control of the SOCS. SOCS will control the specific state (going to a state defines what functions the software will perform) of the application software.
- Power is individually applied to all systems.

- The following states are defined for each item of electronics:
  - SDS Processor (1 unit): Operational (Wait for commands and Processing) and Test (POST and Interruptive).
  - Doppler Radar (1 unit): Power-on (idle), Active Ranging (radiating energy) and Test (POST and Interruptive). This unit goes from idle to active ranging with a commanded mode change.
  - Radar Altimeter (1 unit): Power-on (idle), Active Ranging (radiating energy) and Test (POST and Interruptive).
  - Star Tracker (1 unit): Power-on (idle), Active Tracking and Test (POST and Interruptive)
  - Inertial Measurement Unit (IMU - 1 unit): Operational and Test (POST and Interruptive)
  - Propulsion (8 sets): Power-on, Test, Open and Close Engine Valves
  - Pyrotechnics (TBD # of sets): Power-on, Test, Arm Fire
  - Thermal (TBD # of Heaters): Heater Power-on, Test
- It is assumed that provisions are made in the design for the capability to activate the Star Tracker and the Radio Frequency (RF) hardware (Doppler Radar, Radar Altimeter, and the C&T Transponder) on the launch pad in the Integrated System Test mode.
- The C&T Transponder powers up into a listen only state (no transmissions) until commanded to do a state change and then it starts transmitting telemetry. Commanding a state change when it is transmitting causes it to go back to the listen only state.
- A "Pwr Up All Sys" command (10.28) will cause the SOCS to issue the appropriate individual commands to the Electrical Power Distribution (EPD) System to power up all systems. A "Pwr Dwn Sys" command (10.30) will cause the SOCS to issue the appropriate commands to power down all systems. In addition, systems may be individually powered up or down by the appropriate command.

2.2 MISSION SCENARIO

All subsystems will be activated prior to launch with a full sequence of commands and data for a normal mission/trajectory stored onboard [STB92]. No orbital verification phase is expected. The major mission modes consist of the following events:

- Pre-launch (controlled by launch control via the checkout consoles)
- Launch (controlled by launch vehicle)
- Boost to Earth orbit insertion (controlled by launch vehicle)
- Translunar injection (TLI) from Earth orbit is controlled by the LVS
- Mid-course correction to orbit coast (calculated by FSS and uplinked to LVS for implementation)
- Follow-up corrections (optional to orbit coast) (calculated by FSS and uplinked to LVS for implementation)
- Lunar orbit insertion
- Follow-up correction (optional from orbit coast)
- Lunar deorbit
- Powered descent initiation and autonomous landing
- Post landing and shut-down
- Operations by the payload or science mission support systems in the terminal area (in the CLL, payload operations are treated separately from the spacecraft).

Operations functions are similar for each of the burns following Translunar Injection (TLI). Each burn is preceded by a period of tracking. The FSS uses this data to calculate new position updates and uplinks these updates along with changes to stored commands (may include trajectory corrections) as needed to the LVS. The LVS (GN&C) then autonomously calculates and executes the burn. Telemetry is sent documenting LVS performance during the burn based on a preplanned timeline or upon command from the FSS. A state vector update is performed after landing on the lunar surface and then the FSS commands the LVS (SOCS) to safe and deactivate.

3. BEHAVIOR IN THE SCENARIOS

The behavior of an avionics system depends on the scenarios required of it as it performs the missions of the vehicle. This means the mission and vehicle behavior must be well defined, and the system behavior must be complementary to and consistent with the mission and vehicle behavior. This section describes the modes and states which constrain the allowable behaviors in the system as it performs its mission. The subsequent behaviors are then described for each mission phase.

3.1 MODES AND STATES

Modes and states were defined by studying the interfaces for a space vehicle. The skin of the spacecraft was defined to be the boundary for partitioning between external and internal interfaces. The boundary between modes and states was based on partitioning between activities planned and directly controlled by humans (i.e., a mode) and those activities directed, in response, by the machine (i.e., a state).

This report only presents a top level overview of the modes and states analysis performed. [DW93] presents a detailed description of the modes and states defined as applicable to space generic avionics. The modes and states as described in [DW93] are applied to the CLL reference vehicle in this paper and are to be implemented in the dynamic simulation.

Presented in the following paragraphs are the definitions of modes and states and how the modes and states analysis in [DW93] has been applied to the CLL reference vehicle. Appendix C presents an in-depth discussion of the detailed combinations of modes and states allowed in the analysis.

3.1.1 MODES AND STATES DEFINED

A mode is a predefined set of hardware and software configurations, and associated procedures used to organize and manage the conditions of operation for an avionics system's behavior, as planned (in advance) or directed by a human. Modes may have several levels of expanding detail. Mode models were developed to define the set of modes and mode transitions governing the behavior of a generic mission or vehicle. Generic mode transition diagrams illustrating mode models are provided in [DW93] Tailoring of these models to a specific mission or vehicle such as CLL requires identification of the set of allowable commands and responses for each mode.

States are the activities that a system or subsystem adopts in response to a mode input. A system/subsystem may step though several states in transitioning between one mode and another. The key difference between a mode and a state is that a mode is planned in advance or directed by a human, while a state is the response configuration adopted by a processing controlled system/subsystem. A state may be a complex configuration with many subsets, or it may be a simple configuration at the lowest level consisting of a switch setting such as on-off. State transition models (state transition diagrams) for space generic avionics were developed and are provided in [DW93].

These definitions from [DW93] are consistent with the definitions for modes and states found in [SDAT93] and [SSF93]. The definitions in [DW93] are the definitions accepted for use in this scenario.

3.1.2 SUMMARY OF MODES

To accomplish the mission scenario described above in Section 2.2, the mission modes shown in Figure 3-1 are needed. For each of these mission modes, ground control can command the vehicle modes shown in Figure 3-2. The mode categorizes the mission or vehicle behavior needed in the scenario.

As a result of these mode commands, the avionics system may take one of the states shown in Figure 3-3, while the SDSS function can take one of the states shown in Figure 3-4. The state categorizes the resulting system behavior as the avionics implements the mode commands. Specific commands (as described below) are generated by the system to implement each mode command.

The Pre-Flight Mission Phase consists of pre-launch operations. The Flight Mission Phase consists of launch, boost, orbit coast/transfer, space mobile, vehicle proximity, deorbit, and landing operations. The Terminal Mission Phase consists of post-landing, shut-down, vehicle surface proximity, and surface mobile operations. These mission phases are described in the following sections.

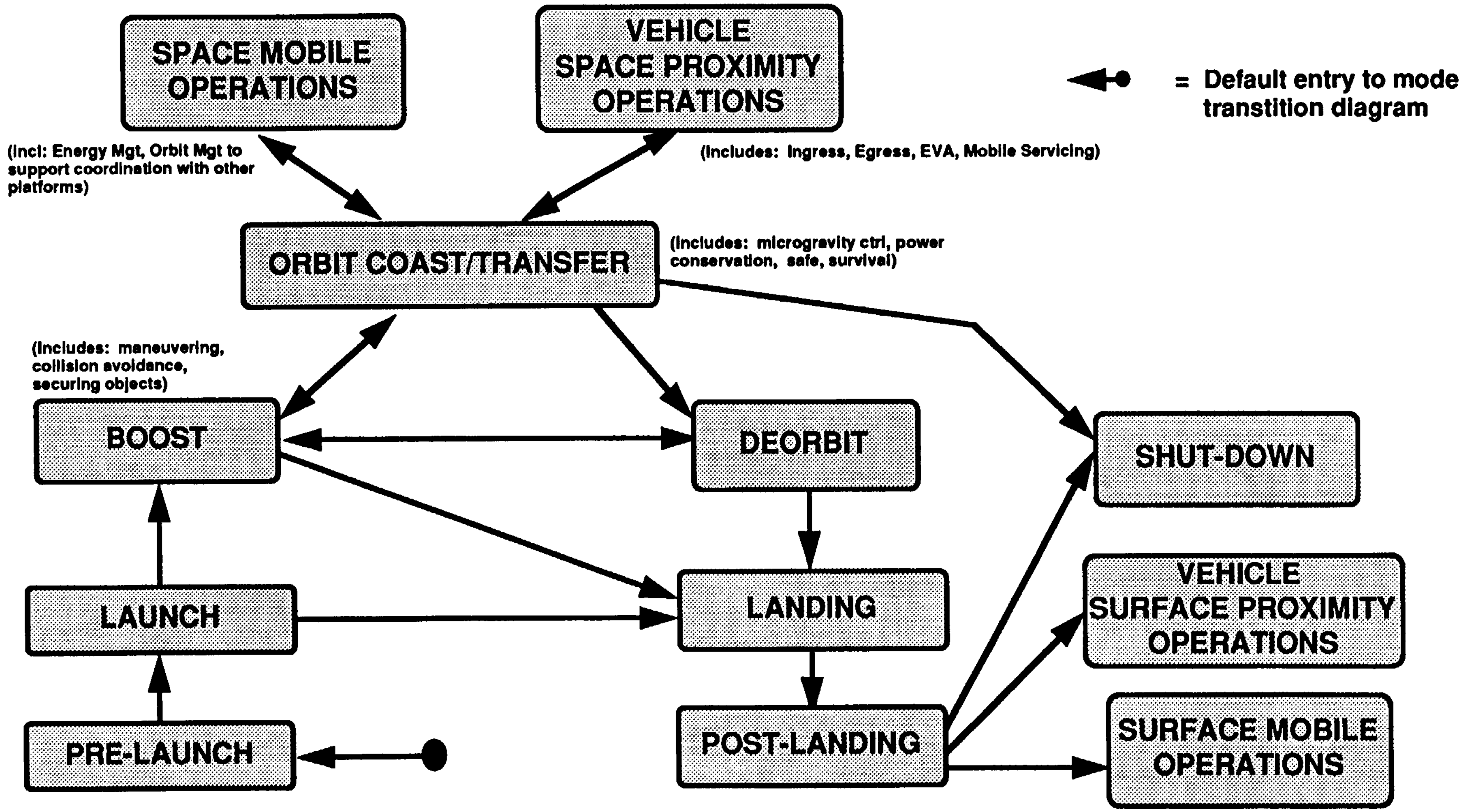


Figure 3-1. Mission Modes for Spacecraft Operations

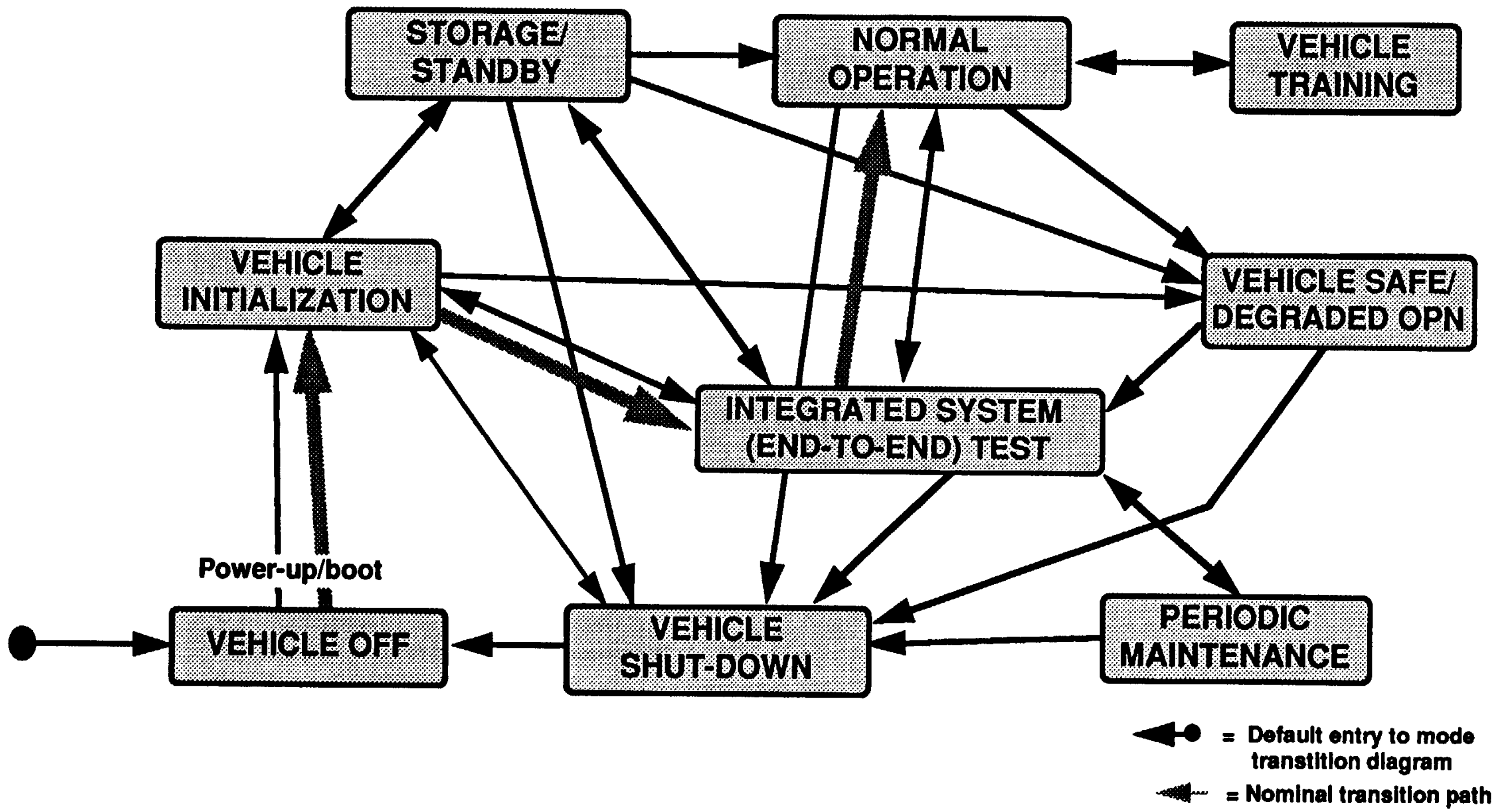


Figure 3-2. Vehicle Modes for Spacecraft Operation

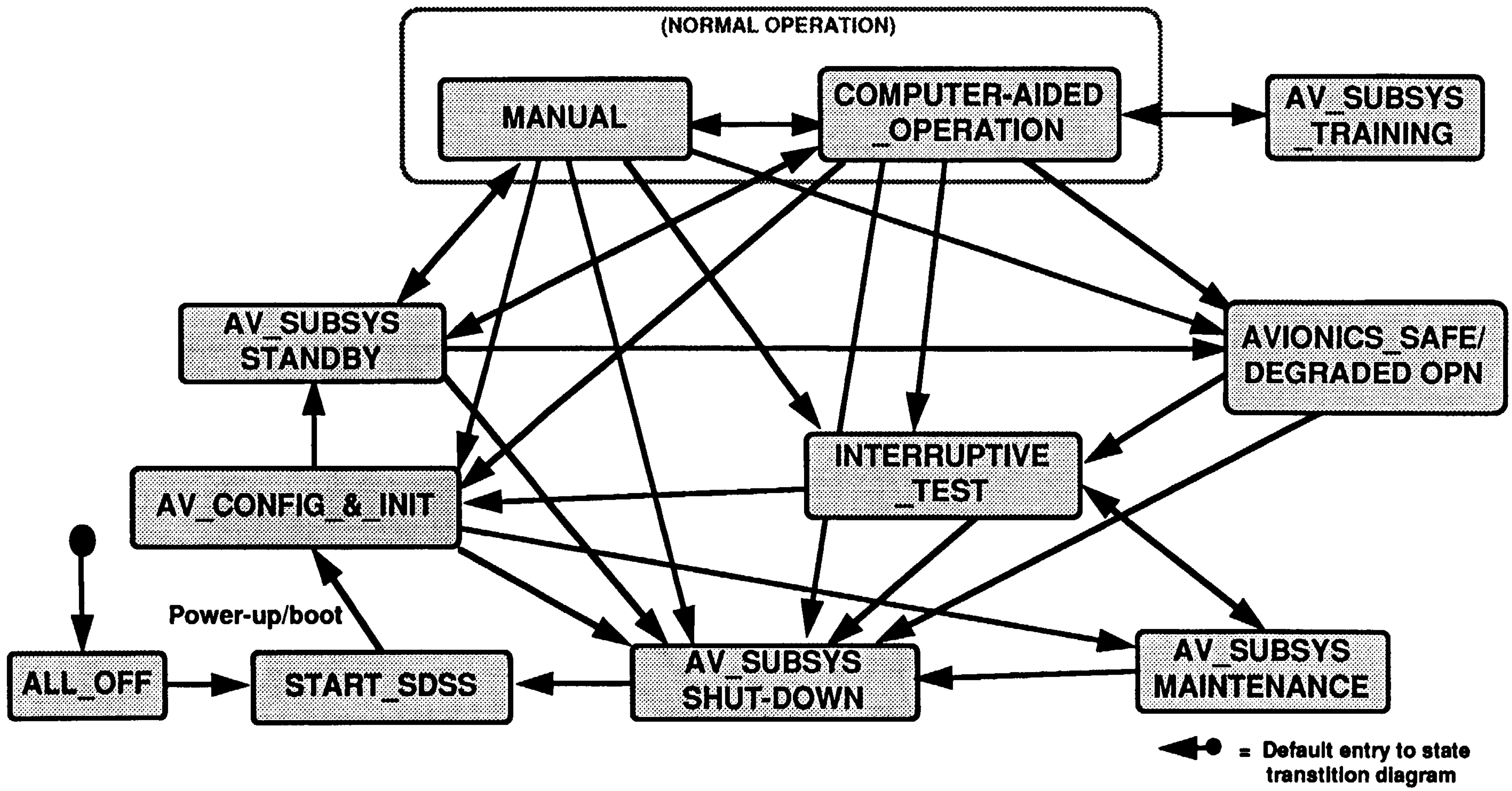


Figure 3-3. Avionics States for Implementing Ground Control Commands

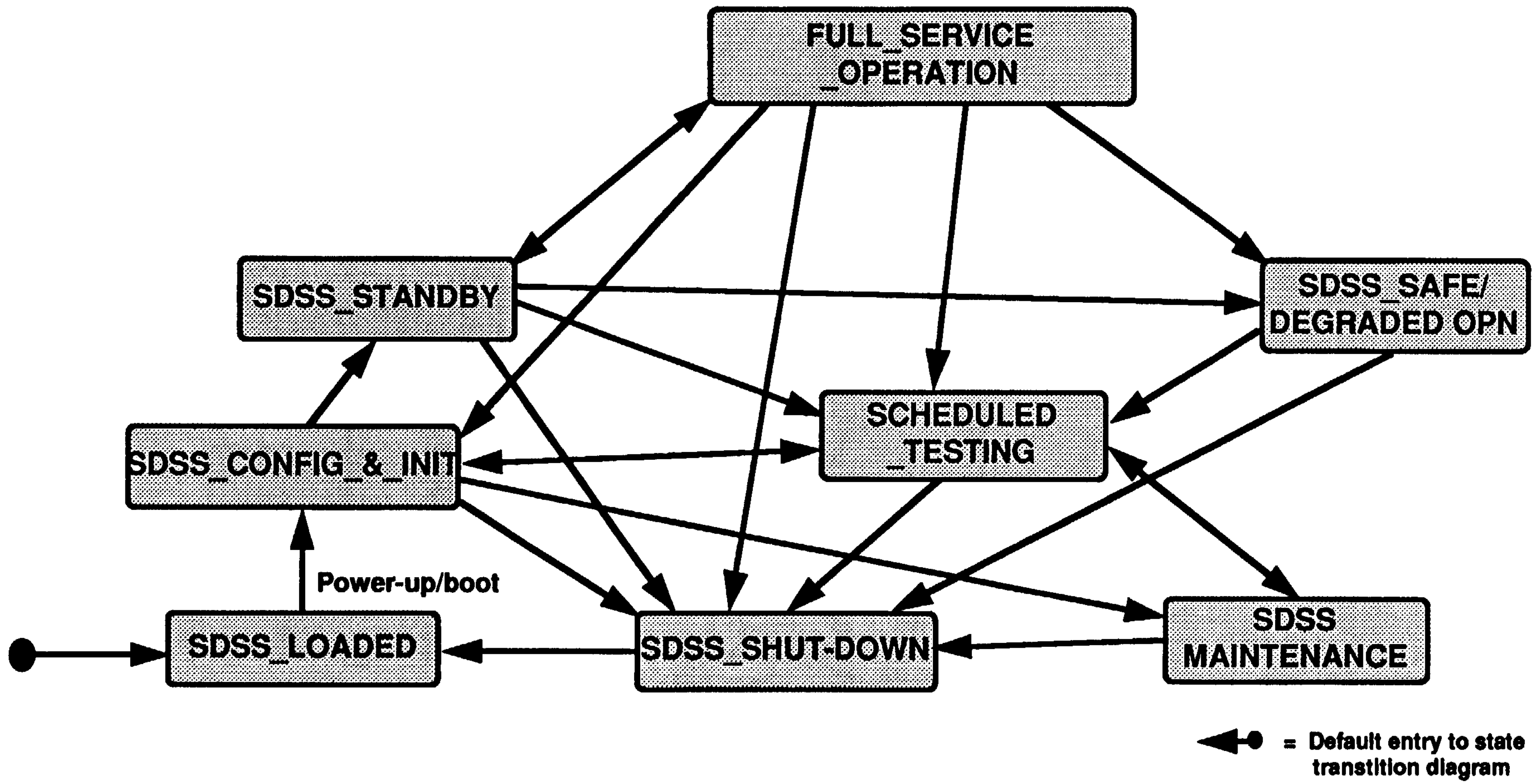


Figure 3-4. SDSD Function States for Implementing Ground Control Commands

3.2 PRE-FLIGHT MISSION PHASE

The Pre-Flight Mission Phase can enable or inhibit specific vehicle modes and avionics states while the spacecraft is being prepared for a mission (prior to launch), depending on implementation of the SOCS ground rules built into the systems and by relay of GSS ground control commands during startup. The following subsections describe the overall pre-flight command processing available to support vehicle mode commands to startup the vehicle subsystem processing.

The numbers shown in ( ) in the following sections are the number of the command from the command response tables contained in Section 4.

3.2.1 VEHICLE OFF MODE

- GSS issues command to "Load Application software" (10.26)
- GSS issues command "Enable Power System software" (10.12)
- GSS issues command "Power Up All Systems" (10.28) to Power System software, transitioning the LVS from the Vehicle Off Mode to the Vehicle Initialization Mode.

3.2.2 VEHICLE INITIALIZATION MODE

- The Power system software in the SDS (already running) will then request SOCS issue the following sequence of state change commands:
  - "Doppler power on" (5.2)
  - "Altimeter power on" (6.2)
  - "Transmitter power on" (8.2)
  - "Star Tracker power on" (14.2)
  - "IMU power on" (18.2)

3.2.3 INTEGRATED SYSTEM TEST MODE

- GSS issues the following series of state change commands to SOCS to perform test and monitoring and health and status checks.

- "SDS processor self test" (10.29)
- "Dump SDS processor memory" (10.3)
- "Enable GN&C" (10.14)
- "Enable C&T" (10.16)
- "Enable Prop" (10.18)
- "Enable command processing (SOCS)" (10.10)

- GSS issues the following series of state change commands to applications to perform test and monitoring and health and status checks. It is assumed that once a test is commanded the test will run to completion and the test results will be sent over the ground link to the GSS. The GSS can command the test be executed multiple times.
  - "Arm pyros"(2.1)
  - "Un-arm pyros" (2.2)
  - "Heater Group On" (3.1)
  - "Heater Group Off" (3.2)
  - "Valve control circuits self test" (4.4)
  - "Doppler self test" (5.6)
  - "Altimeter self test" (6.6)
  - "Transponder self test" (8.7)
  - "Antenna selection control circuits self test" (9.3)
  - "Set time" (10.2)
  - "Request time" (7.1)
  - "Dump request" (10.3)
  - "Star Tracker Self Test (14.5)
  - "IMU Self Test" (18.5)
  - "SDS processor hard reset" (10.4). Note: A hard reset causes an automatic (hardware controlled) recycle of power to the SDS processor, an automatic reboot of system services software and will send the following power on

commands to turn on any system that was inadvertently turned off during the reset.

- - "Doppler power on" (5.2)
- - "Altimeter power on" (6.2)
- - "Transmitter power on" (8.2)
- - "Star Tracker power on" (14.2)
- - "IMU power on" (18.2)

- The SDS processor will then issue the following state change commands after being put in a "hard reset" state without receiving any external commands.
  - "Load application software" (10.26)
  - "Enable power system software" (10.12)
  - "Enable GN&C" (10.14)
  - "Enable C&T" (10.16)
  - "Enable Prop" (10.18)
  - "Enable command processing (SOCS)" (10.10)
- GSS continues the issuing of the following series of state change commands to SOCS to perform test and monitoring and health and status checks
  - "SDS processor soft reset" (10.5). Note: A soft reset causes an automatic reboot of system services software and will send the following power on commands to turn any system on that was inadvertently turned off during the reset.

    - - "Doppler power on" (5.2)
    - - "Altimeter power on" (6.2)
    - - "Transmitter power on" (8.2)
    - - "Star Tracker power on" (14.2)
    - - "IMU power on" (18.2)
- The SDS processor will then issue the following state change commands after a "soft reset" without receiving any external commands.
  - "Load application software" (10.26)

- "Enable power system software" (10.12)
- "Enable GN&C" (10.14)
- "Enable C&T" (10.16)
- "Enable Prop" (10.18)
- "Enable command processing (SOCS)" (10.10)

- GSS will issue the following series of state change commands to the SOCS to test the ability of disabling and enabling application software.
  - "Disable power system software" (10.13)
  - "Enable power system software" (10.12)
  - "Disable GN&C" (10.15)
  - "Enable GN&C" (10.14)
  - "Disable C&T" (10.17)
  - "Enable C&T" (10.16)
  - "Disable Prop" (10.19)
  - "Enable Prop" (10.18)

- GSS will issue the following series of commands and associated test command sequences to the SOCS to test the ability to operate on stored sequences of commands.
  - "Immediate command" (10.20)
  - "Store command sequence, absolute time" (10.21)
  - "Store command sequence, relative time" (10.22)
  - "Start stored sequence", (10.23)
  - "Stop command sequence" (10.24)
  - "Delete command sequence" (10.25)

- GSS will issue the following series of state change commands to the SOCS to test the LVS systems.
  - "Touchdown" (1.0)
  - "State vector update" (13.0)

- "Select antenna" (9.1)
- "Send Telemetry (TM) Packets" (8.5)
- "Trans Stdby" (8.8)
- "Record " (15.0)
- "Playback " (16.0)
- "Doppler Track" (5.5)
- "Doppler Stdby" (5.7)
- "Altimeter Range" (6.5)
- "Altimeter Stdby" (6.7)
- "Star Tracker Track" (14.3)
- "Star Tracker Stdby" (14.4)

- GSS will issue the following series of commands to the SOCS to gather status of all systems. It is assumed that the system is designed such that all status data will be sent to the GSS over the umbilical by the SDS.
  - "Get SDS status" (12.1)
  - "Get GN&C status" (12.2)
  - "Get C&T status" (12.3)
  - "Get Prop status" (12.4)
  - "Get Therm status" (12.5)
- FSS or GSS will issue the command to "Power off" (10.30) based on health monitoring
- FSS issues command to "Go to Prelaunch Ready Mode" (19.1)

NOTE: DETAILED COMMANDS FOR THE FOLLOWING SECTIONS AS INDICATED BY [ ] will be defined during simulation build

3.2.4 PRELAUNCH READY MODE

- FSS issues command to "Go to Launch Mode" (19.2)

- FSS or SOCS issues command to "Go to Interruptive Test Mode" based on health monitoring if a problem is detected in one of the systems. Based on problem criticality, a command to "Go to Vehicle Shutdown Mode" may be issued.

3.3 FLIGHT MISSION PHASE

Upon completion of the vehicle startup activities, the spacecraft is ready to start its flight mission. Specific commands can enable or inhibit specific vehicle modes and avionics states, depending on implementation of the ground rules built into the systems and relay of ground control commands from the FSS during flight.

The numbers contained in ( ) in the following sections are the number of the command from the command response tables contained in Section 4.

3.3.1 LAUNCH MODE COMMANDS

- If a problem is detected prior to launch commit, the GSS or SOCS issues a command to "Go to Prelaunch Ready Mode" based on health monitoring.

Note: For CLL, the system is under control of the launch vehicle and no commands are issued by or for the LVS. All systems are in a wait for command state.

3.3.2 BOOST TO EARTH ORBIT INSERTION MODE COMMANDS

- SOCS issues command to "Activate Attitude Control" (4.1)
- SOCS issues command to "Activate Third Stage Propulsion System" (4.5)
- GN&C issue a command to "Fire Third Stage Propulsion System" (4.6)
- *[issue attitude control commands for TLI from GN&C]*
- *[emergency ground commands from FSS]*

3.3.3 ORBIT COAST/TRANSFER MODE COMMANDS

3.3.3.1 Orbit Transfer to Translunar Coast Flight Commands

- SOCS issues command to "Shutdown Third Stage Propulsion System" (4.7) based on GN&C calculations.

- SOCS issues command to "Arm Pyrotechnics (Pyros)" (2.1) based on a timeline following third stage shutdown
- SOCS issues command to "Fire Pyros" (2.3) based on a timeline to effect third stage separation
- SOCS issues command to "Go to Orbit Coast Mode " (19.3) following confirmation of a successful separation.

3.3.3.2 Orbit Coast In Normal Translunar Flight Commands

- *[Emergency ground commands and command over rides from FSS]*
- FSS issues command to "Update Position" (10.31)
- FSS issues command to "Update Velocity" (10.32)

NOTE: THE FOLLOWING SERIES OF COMMANDS ARE ISSUED BY THE SOCS BASED ON A TIMELINE FOLLOWING SEPARATION OF THE THIRD STAGE

- GN&C directs SOCS to issue a command to "Deploy LVS Legs" (2.4)
- SOCS issues command to "Deploy Solar Panels" (2.5)
- SOCS issues command to "Deploy Antennas" (2.6)
- SOCS issues command to "Start Active Ranging" (8.9)
- SOCS issues command to "End Active Ranging" (8.10)
- SOCS issues command to "Transmit Telemetry" (8.5)
- SOCS issues command to "End Transmission of Telemetry" (8.6)

NOTE: THE FOLLOWING SERIES OF COMMANDS ARE CREATED BY CONDITIONS OR EVENTS AND ARE NOT COMMANDED BY THE TIMELINE

- *[GN&C issues commands to propulsion (open and close engine valves) to maintain proper trajectory and attitude including entering the lunar parking orbit]*
- SOCS issues command "Go to Vehicle Safe/Degraded Operation Mode" (19.4) based on health monitoring

- SOCS issues command to "Go to Lunar Orbit Insertion Mode " (19.5) based on GN&C calculations or on a FSS command.

3.3.3.3 Orbit Coast Mid-course Correction Commands

Mid-course corrections during orbit coast may be issued any time during coast.

- FSS issues command to "Update Position" (10.31)
- FSS issues command to "Update Velocity" (10.32)
- FSS issues command to "Update Target Attitude" (10.33)
- FSS issues command to "Update Target Trajectory" (10.34)
- FSS issues command to "Update Timeline" (10.2)
- *[GN&C issues commands to propulsion open and close engine valves} to go to new attitude and/or trajectory including entering the lunar parking orbit]*

3.3.3.4 Orbit Transfer to Lunar Orbit Insertion Commands

NOTE: THE FOLLOWING COMMANDS ARE ISSUED BY SOCS BASED ON A TIMELINE FOLLOWING LUNAR ORBIT INSERTION

- SOCS issues command to "Start Active Ranging" (8.9)
- SOCS issues command to "End Active Ranging" (8.10)
- SOCS issues command to "Transmit Telemetry" (8.5)
- SOCS issues command to "End Transmission of Telemetry" (8.6)

NOTE: THE FOLLOWING SERIES OF COMMANDS ARE CREATED BY CONDITIONS OR EVENTS AND ARE NOT COMMANDED BY THE TIMELINE

- *[GN&C issues commands to propulsion {open and close engine valves} to enter the lunar parking orbit]*
- FSS or SOCS issues command to "Go to Vehicle Safe/Degraded Operation (19.4) Mode" if a problem is detected by health monitoring
- FSS or SOCS issues command as directed by GN&C to "Go to Deorbit and Landing Mode" (19.6) (from SDS normally or from FSS in abnormal situation)

3.3.3.5 Orbit Coast Follow-up Corrections to Lunar Orbit Commands

While in lunar orbit, follow-up corrections to the orbit coast will be made only if needed.

- FSS issues command to "Update Position" (10.31)
- FSS issues command to "Update Velocity" (10.32)
- FSS issues command to "Update Target Attitude" (10.33)
- FSS issues command to "Update Target Trajectory" (10.34)
- FSS issues command to "Update Timeline" (10.2)
- *[GN&C issues commands to propulsion (open and close engine valves) to go to the new attitude and/or trajectory to modify the lunar parking orbit]*

3.3.4 SPACE MOBILE AND VEHICLE PROXIMITY OPERATIONS MODE COMMANDS

The CLL is an uncrewed spacecraft, with no capability for coordinated space mobility operations nor for monitoring and controlling proximity operations around the spacecraft. These modes are not addressed further in this paper.

3.3.5 DEORBIT MODE COMMANDS

3.3.5.1 Lunar Deorbit Reconfiguration Commands

NOTE: THE FOLLOWING COMMANDS ARE ISSUED BY SOCS BASED ON A TIMELINE FOLLOWING THE LUNAR DEORBIT COMMAND (19.6).

- "Turn Altimeter Power On" (6.2)
- *[SOCS issues command to "Jettison Unneeded Equipment" (2.7) (whatever needs to be jettisoned)]*
- *[SOCS issues commands to reconfigure for landing (whatever else needs to be done)]*

3.3.5.2 Powered Descent Initiation Commands

NOTE: THE FOLLOWING SERIES OF COMMANDS ARE CREATED BY CONDITIONS OR EVENTS AND ARE NOT COMMANDED BY THE TIMELINE

- *[GN&C issues commands to propulsion (open and close valves) to maneuver in attitude to correspond with deorbit burns]*

- GN&C issues command to "Start Altimeter Ranging" (6.5)
- GN&C issues command to "Go to Full Throttle" (4.2) (open engine control valves for all eight engines for Phase 1 braking)
- *[GN&C issues commands to "Go to -15 degrees Pitch Attitude"(for Phase 1 braking)]*
- *[GN&C issues commands to "Go to 60 degree pitchup to vertical at 1.2 degrees per second rate" (Phase 2 braking)]*
- *[GN&C issues commands to reduce throttle by shutting down pairs of engines every 20 seconds until only two engines are running for 25% of throttle (Phase 2 and Phase 3 braking)]*

3.3.6 AUTONOMOUS LANDING MODE COMMANDS

- Landing sensor discrete (1.1) to SOCS from mechanical sensor indicating landing complete
- SOCS issues commands to for "Engine Off" (4.3) for the remaining two engines after receiving landing discrete (1.1)

3.4 TERMINAL MISSION PHASE

After landing, the spacecraft must be made safe for ground operations and the start of payload/science mission processing.

3.4.1 POST-LANDING MODE COMMANDS

The following commands must thus be issued:

- SOCS issues command to "Vent all compressed materials" (4.8)
- SOCS issues command to "Do active ranging" (8.9)
- SOCS issues command to GN&C to "Calculate position" (10.35)
- SOCS issues command to "Transmit telemetry(position and system status)" (8.5)

3.4.2 SHUT-DOWN MODE COMMANDS

- SOCS issues command to "Stop telemetry transmission" after completion (8.6)

- SOCS issues commands to shut down all systems (10.30)

3.4.3 VEHICLE SURFACE PROXIMITY AND MOBILE OPERATIONS MODE COMMANDS

There was no requirement for surface operations support by the CLL. These modes are not addressed further in this paper.

4. SPACECRAFT COMMAND RESPONSE TABLES

The "SGOAA Model Mission Scenario Command Response Table 4-1" contained in this section was derived from the SGOAA Mission Model Scenario contained in Section 2 of this document and from Table 3-3 "SDS Functional Interfaces" of [SHU92]. Additional commands required in addition to those defined in Table 3-3 of [SHU92] are shown in bold type in Table 4-1. The modes and states described in Section 3.0 and the mission scenario as described in Section 2 form the basis for the overall sequence of events. System and subsystem states result from commands generated in response to mode inputs.

In the Table 4-1, the Primary (Pri) Command (CMD) is the initiating or source command and the secondary (SEC) CMD are those generated by the application software as a result of the Pri CMD being issued. The software (S/W) responsible for implementing the command is also shown. Commands initiated on the vehicle are indicated as such by the source being the Command Processor referred to in this table as SOCS. Commands initiated by ground control are indicated as such by the source being the GSS prior to launch and the FSS following launch. Also shown are the expected responses that result from the commands.

Table 4-1. SGOAA Model Mission Scenario Command Responses

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
1.0 Touchdown					
1.1 Touchdown Notice	Mech	SDS	SDSM	Notice to GN&C(1.2)	Action sequence started
1.2 Touchdown Event	SDS	GN&C	SOCS	-	Start S/W routine based on (see 1) event
2.0 Mech Commands					
2.1 Arm Pyro	SOCS	EPD	SOCS	Apply pwr to arm Pyro	Pyro is armed
2.2 Unarm pyro	**SOCS**	**EPD**	**SOCS**	**Remove pwr to Pyro**	**Pyro is unarmed**
2.3 Fire Pyro	SOCS	EPD	SOCS	Apply pwr to fire Pyro	Pyro is fired
2.4 Deploy LVS Legs	**GN&C**	**SOCS**	**SOCS**	**2.3 Fire Pyro**	**Pyro fired, legs deployed**
2.5 Deploy Solar Panls	GN&C	SOCS	SOCS	2.3 Fire Pyros	Pyro fired, panels deployed
2.6 Deploy Antennas	GN&C	SOCS	SOCS	2.3 Fire Pyros	Pyros fired, antennas deployed
2.7 Jettison Equip	GN&C	SOCS	SOCS	2.3 Fire Pyros	Pyros fired, equip jettisoned
3.0 Thermal Commands					
3.1 Heater Group On	SOCS*	EPD	SOCS	Apply power to heater	Heater is turned on
3.2 Heater Group Off	SOCS*	EPD	SOCS	Remve pwr frm heater	Heater is turned off

*Command issued based on analog temperature measurements processed by the SDSM

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
4.0 Prop Commands					
4.1 Activate	**Att Cntrl**	SOCS	GN&C	GN&C	**Start Att Cntrl S/W**
4.2 Engine On	GN&C	LVS Valves	GN&C	Target valve open	LVS Eng Valve Opens
4.3 Engine Off	GN&C	LVS Valves	GN&C	Target valve close	LVS Eng Valve closes
4.4 Valve Self Test	**SOCS**	**LVS Valves**	**GN&C**	**Target valve close**	**Controller self tests**
4.5 Act 3rd Stge	**SOCS**	**GN&C**	**GN&C**	**Arm**	**3rd Stage Eng is Armed**
4.6 Fire 3rd Stage	**GN&C**	**Prop**	**GN&C**	**Fire 3rd Stage**	**3rd Stage Engine Fires**
4.7 Shtdwn 3rd Stge	**GN&C**	**Prop**	**GN&C**	**Engine Off**	**3rd Stage Engine Shuts Down**
4.8 Vent Systems	**SOCS**	**Prop**	**SOCS**	**Discretes to vents**	**All Vent Valves Open**
5.0 Doppler Cmds					
5.1 Activate Doppler	GN&C	C&T	SOCS	See 5.2	SOCS generates pwr on
5.2 Doppler Power On	SOCS	EPD	SOCS	Doppler pwr on	Power applied to doppler
5.3 Deactivate Doppler	GN&C	C&T	SOCS	See 5.4	SOCS generates pwr off
5.4 Doppler Power Off	SOCS	EPD	SOCS	Doppler pwr off	Power removed from doppler
5.5 Doppler Track	**GN&C**	**C&T**	**GN&C**	**Mode change**	**Doppler goes to trk mode**
5.6 Doppler Self Tst	**SOCS**	**C&T**	**SOCS**	**Mode change**	**Doppler goes to self test**

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
5.7 Doppler Stdby	GN&C	C&T	SOCS	Mode change	Doppler goes to stdby
6.0 Altimeter Cmds					
6.1 Activate Alt	GN&C	C&T	SOCS	See 6.2	SOCS generates pwr on
6.2 Alt Power On	SOCS	EPD	SOCS	Altimeter pwr on	Power applied to altimeter
6.3 Deactivate Alt	GN&C	C&T	SOCS	See 6.4	SOCS generates pwr off
6.4 Alt Power Off	SOCS	EPD	SOCS	Altimeter pwr off	Power removed from altimeter
6.5 Alt Range	GN&C	C&T	GN&C	Mode change	Altimeter starts ranging
6.6 Alt Self Test	**SOCS**	**C&T**	**SOCS**	**Mode Change**	**Alt goes to self test**
6.7 Alt Stdby	GN&C	C&T	SOCS	Mode Change	Alt goes to stdby
7.0 Clock Commands					
7.1 Request Time	C&T	SDS	OS	Output time to clock	OS puts Clock time on bus
8.0 Transponder Commands					
8.1 Activate Trans	SOCS	C&T	SOCS	See 8.2	SOCS generates pwr on
8.2 Trans Power On	SOCS	EPD	SOCS	Trans pwr on	Pwr applied to trans
8.3 Deactivate Trans	SOCS	C&T	SOCS	See 8.4	SOCS generates pwr off
8.4 Trans Power Off	SOCS	EPD	SOCS	Trans pwr off	Pwr removed from trnas 16

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
8.5 Send TM Packets	C&T	SDS	SDSM/OS and C&T	Output TM packets	DS outputs TM packets
8.6 Stop TM Packets	C&T	SDS	SDSM/OS and C&t	Stop TM	DS stops TM packets
8.7 Trans Self Test	SOCS	C&T	SOCS	Mode Change	Trans goes to self test
8.8 Trans Stdby	SOCS	C&T	SOCS	Mode Change	Trans goes to standby
8.9 Trans Range	GN&C	C&T	SOCS	Mode Change	Trans goes to ranging
8.10 Trans Stop Range	GN&C	C&T	SOCS	Mode Change	Trans stops ranging
9.0 Antenna Commands					
9.1 Select Antenna	GN&C	C&T	SOCS	See 9.2	SOCS generates Command
9.2 Antenna Selection	SOCS	Ant Switch	SOCS	Switch antennas	Antenna switches positions
9.3 Antenna Self Test	SOCS	C&T	SOCS	-	Antenna switch circuits self test
10.0 Grnd (GSS), uplink (FSS) & onboard (SOCS) commands	GSS/FSS/SOCS				
10.1 Any Onbrd Cmd	GSS/FSS	SDS	SOCS	Any onboard cmd	Respond to GSE request
10.2 Set Time	GSS/FSS/SOC	SDS	SOCS	See 10.2.1	Cmd Processor gen cmd
10.2.1 Set Time	SDS	SDS	OS	-	Time is reset

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
10.3 Dump Request	GSS/FSS	SDS	DBM	-	Dump data
10.4 Hard Reset	GSS/FSS	SDS	DSM	-	Hard reset
10.5 Soft Reset	GSS/FSS	SDS	DSM	-	Soft reset
10.6 Soft Reset & Wait for Cmds	GSS/FSS	SDS	DSM	-	Respond to ground cmd
10.7 Execute BIT & Report Status	GSS/FSS/SOC	SDS	DSM	-	Respond to ground cmd
10.8 Resume After Wait	GSS/FSS	SDS	DSM	-	Resume operations
10.9 Memory Failure Mgt & Prog Reload	GSS/FSS/SOC	SDS	DSM	-	Respond to ground cmd
10.10 Enable SOCS	**GSS/FSS**	**SDS**	**DSM**	-	**SOCS S/W activated**
10.11 Disable SOCS	**GSS/FSS**	**SDS**	**DSM**	-	**SOCS S/W deactivated**
10.12 Enabl Pwr S/W	**GSS/FSS**	**SDS**	**SOCS**	-	**Pwr sys S/W activated**
10.13 Disab Pwr S/W	**GSS/FSS**	**SDS**	**SOCS**	-	**Pwr sys S/W deactivated**
10.14 Enable GN&C	**GSS/FSS**	**SDS**	**SOCS**	-	**GN&C S/W deactivated**
10.15 Disable GN&C	**GSS/FSS**	**SDS**	**SOCS**	-	**GN&C S/W deactivated**
10.16 Enable C&T	**GSS/FSS**	**SDS**	**SOCS**	-	**C&T S/W activated**
10.17 Disable C&t	**GSS/FSS**	**SDS**	**SOCS**	-	**C&T S/W deactivated**

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
10.18 Enable Prop	GSS/FSS	SDS	SOCS	-	**Prop S/W activated**
10.19 Disable Prop	GSS/FSS	SDS	SOCS	-	**Prop S/W deactivated**
10.20 Immediate Cmd	GSS/FSS	SDS	SOCS	?	Set immediate response state
10.21 Store Cmd Seq [seq], Absolute Time	GSS/FSS	SDS	SOCS	-	Processor stores sequence
10.22 Store Cmd Seq [seq], Relative Time	GSS/FSS	SDS	SOCS	-	Processor stores sequence
10.23 Start Stored Seq (see 10.21 & 10.22)	GSS/FSS	SDS	SOCS	-	Start cmd sequence
10.24 Stop Cmd [seq]	GSS/FSS	SDS	SOCS	-	Implement stop cmd sequence
10.25 Delete Cmd [seq]	GSS/FSS	SDS	SOCS	-	Implement delete cmd seq
10.26 Load Software	GSS/FSS/SOC	SDS	DSM	-	Respond to GSE request
10.26.1 Load SOCS	GSS/FSS	SDS	DSM	-	Respond to GSE request
10.26.2 Load GN&C	GSS/FSS/SOC	SDS	DSM	-	Respond to GSE request
10.26.3 Load C&T	GSS/FSS/SOC	SDS	DSM	-	Respond to GSE request
10.26.4 Load ELS	GSS/FSS/SOC	SDS	DSM	-	Respond to GSE request
10.27 Calibrate Clock	GSS/FSS/SOC	SDS	SOCS	See 10.2 above	Calibrate clock

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
10.28 Pwr Up All Sys	GSS/FSS	SDS	SOCS	See all apply pwr cmds	Respond to GSE request
10.29 SDS Processor Self Test	GSS/FSS	SDS	DSM	Mode Change	SDS Processor self tests
10.30 Pwr Dwn Sys	GSS/FSS/SOC	SDS	SOCS	Shut Down All Sys	Respond to GSE & Landing Event
10.31 Update Pos	GSS/FSS/SOC	SDS	GN&C	-	GN&C executes position update routines
10.32 Update Vel	GSS/FSS/SOC	SDS	GN&C	-	GN&C executes velocity update routines
10.33 Update Att	GSS/FSS/SOC	SDS	GN&C	-	GN&C executes attitude update routines
10.34 Update Trajec	GSS/FSS/SOC	SDS	GN&C	-	GN&C exectues trajectory update routines
10.35 Cal Position	GSS/FSS/SOC	SDS	GN&C	-	GN&C calculates present position
11.0 FSS Cmd Integrity		C&T	SOCS	C&T	As req'd to Test C&T Cmd integrity
12.0 Get Subsys Status Commands					
12.1 Get SDS Status	GSS/FSS	SDS	C&T/DSM/SOCS	As req'd to sys	Subsys send status

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
12.2 Get GN&C Status	GSS/FSS	SDS	C&T/GN&C /SOCS	As req'd to sys	Subsys send status
12.3 Get C&T Status	GSS/FSS	SDS	C&T/SOCS	As req'd to sys	Subsys send status
12.4 Get Prop Status	GSS/FSS	SDS	C&T/GN&C /SOCS	As req'd to sys	Subsys send status
12.5 Get Therm Status	GSS/FSS	SDS	C&T/SOCS	As req'd to sys	Subsys send status
13.0 State Vector Update	FSS	GN&C	SDSM/ GN&C	GN&C updates state vector (from ground)	
14.0 Star Tracker Commands					
14.1 Activate Str Trk	GN&C	GN&C	SOCS	See 14.2	SOCS generates Command
14.2 Str Trk Power On	SOCS	EPD	SOCS	Str Trk pwr on	Power applied to Str Trk
14.3 Str Trk Track	GN&C	GN&C	SOCS	Mode change	Star Tracker begins track
14.4 Str Trk Stdby	**GN&C**	**GN&C**	**SOCS**	**Mode Change**	**Star Tracker goes to stdby**
14.5 Str Trk Slf Tst	**SOCS**	**GN&C**	**SOCS**	**Mode Change**	**Star Tracker self tests**
14.5.1 Deactivt Str Trk	GN&C	GN&C	SOCS	See 14.6	SOCS generates Command
14.6 Str Power Off	SOCS	EPD	SOCS	Str Trk pwr off	Power removed from Str Trk

Table 4-1. SGOAA Model Mission Scenario Command Responses - continued

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
15.0 Record	GN&C	SDS	SOCS	-	Processor records data
16.0 Playback	GN&C	SDS	SOCS	-	Processor plays back data
17.0 Schedule Request	GN&C	SDS	(OS)Ada RTE	-	Respond to request
18.0 IMU Commands					
18.1 Activate IMU	**GN&C**	**GN&C**	**SOCS**	**See 18.2**	**SOCS generates pwr on**
18.2 IMU Power On	**SOCS**	**EPD**	**SOCS**	**IMU pwr on**	**Power applied to IMU**
18.3 Deact IMU	**GN&C**	**GN&C**	**SOCS**	**See 18.4**	**SOCS generates pwr off**
18.4 IMU Power Off	**SOCS**	**EPD**	**SOCS**	**IMU pwr off**	**Power removed from IMU**
18.5 IMU Self Test	**SOCS**	**GN&C**	**SOCS**	**Mode Change**	**IMU goes to self test**
18.6 IMU Read	**GN&C**	**GN&C**	**SDSM**	**-**	**IMU Registers are read**
19.0 Vehicle Mode Change Commands					
19.1 Enter Prelaunch mode	GSS/FSS	SDS	SOCS	SDS S/W Mode change	Respond to GSE command
19.2 Enter Launch Mode	GSS/FSS	SDS	SOCS	SDS S/W Mode change	Respond to GSE command
19.3 Enter Orbit Cst Mode	**SOCS**	**SDS**	**SOCS**	**SDS S/W Mode**	**Respond to SOCS Command**

Table 4-1. SGOAA Model Mission Scenario Command Responses - concluded

PRI CMD	FROM SYS	TO SYS	S/W	SEC CMD	RESPONSE
19.4 Enter Veh Safe/Degraded Op Mode	SOCS	SDS	SOCS	SDS S/W Mode change	Respond to SOCS Command
19.5 Enter Lunar Orbit Insertion Mode	SOCS	SDS	SOCS	SDS S/W Mode change	Respond to SOCS command
19.6 Enter Deorbit Landing Mode	SOCS	SDS	SOCS	SDS S/W Mode change	Respond to SOCS command

NOTES:

1. SDS = Space Data System
2. EPD = Electrical power distribution(the H/W that is controlled by the "Power" system application for turning hardware on and off).
3. A description of the systems these Commands apply to is contained in the "Final Report for Transportation Segment Lander Vehicle System Space Data System" dated 1/6/93.
4. Commands not included in the "Final Report for Transportation Segment Lander Vehicle System Space Data System" dated 1/6/93 are shown in **bold type**.
5. SOCS and the Command Processor are the same entity.
6. The Valve Controller Software is included in the GN&C Application Software package.
7. The Radar Handler than handles the Doppler Radar and the Radar Altimeter is a part of the GN&C Application software package.
8. The Time Keeper software is a part of the OS.
9. When power is applied to the vehicle power is applied to the SDS processor. The SDS processor performs POST on itself, boots sufficient OS to enable it to operate and load application software and then GOs to a Wait State. This is all in the Start_Avionics Chart.

5. REFERENCES

[DW93] Wray, R. B., "An Analysis of the Modes and States for Generic Avionics", Job Order 60-911, Contract NAS9-17900 for the JSC, LESC-30749, July 1993.

[WS92] Wray, R. B. and Stovall, J. R., "Space Generic Open Avionics Architecture (SGOAA) Reference Model Technical Guide", Job Order 60-430, Contract NAS9-17900 for the JSC, LESC-30347, December 1992.

[WS94] Wray, R. B. and Stovall, J. R., "Space Generic Open Avionics Architecture (SGOAA) Standard Specification", Job Order 60-EK-AB1, Contract NAS9-9-19100 for the JSC, LESC-30347-C, June 1994.

[SDAT93] Software Design Architecture Team, "Space Station Freedom Integrated Avionics Software Design Document", PSAR Review, IBM, 1 September 1993

[KIL92] Kilbourn, M. B., "Artemis Conceptual Flight Profile", JSC-26017, September 1992.

[STA92] Stecklein, J. M., "System Specification for Artemis Transportation Segment Lander Vehicle System", Preliminary Draft, September 1992.

[STB92] Stecklein, J. M., "System Specification for Artemis Transportation Segment Flight Support System", Preliminary Draft, September 1992.

[SHU92] Shuler, R., "Final Report for Artemis Transportation Segment Lander Vehicle System Space Data System (SDS)", January 1993.

[SSF93] "Flight System Software Requirements (Integrated Station Executive Software)", DR SY-34.1, SSP 30610, Rev A, Work Package 2, May 1993.

APPENDIX A
SGOAA DEFINITIONS

APPENDIX A
SGOAA DEFINITIONS

Definitions are taken from the POSIX P1003.0 Draft Guide or [LAP90] where applicable or otherwise established as shown.

Application is defined as in POSIX as the use of capabilities (services/functions) provided by an information system specific to the satisfaction of a set of user requirements.

Application Platform (AP) is defined as in POSIX as the set of resources that supports the services on which an application or application software will run. Also known as a host platform.

Application Program Interface (API) is defined as in POSIX as the interface between the application software and the application platform, across which all services are provided.

Application Software is defined as in POSIX as software that is specific to an application and is composed of programs, data and documentation. Application software has uniquely defined interfaces.

Architecture is defined as the structure of Application Software, API, AP, and External Environment Interfaces (EEIs) which describe the organization and interfaces of a system.

Avionics System is defined for the purpose of this standard as the set of all electronic and processing based subsystems on a space vehicle, including all hardware, software and other electronics needed to control and operate the space vehicle. It is the collection of system elements and allocated capabilities that provides the coordinated functionality for end-to-end processing in handling the information needed to interface the space vehicle's major components, to control its interaction with its environment, and to respond to human commands. (Adapted from [JSC 31000])

Control Subsystem is an application which selects and implements alternative actions based on a-priori criteria or real time guidance.

Core Avionics is defined as the control subsystems and the supporting avionics (hardware and software) needed to enable these control subsystems to function. Core avionics include the controls for each of the traditional space avionics hardware subsystems (such as Guidance Navigation and Control (GN&C) and Communications and Tracking (C&T)). The avionics hardware sensors and effectors are outside the core avionics boundary.

Data Base Manager (DBM) is the control subsystem which manages structured data files, file transfers and file redundancy management.

Data Processing Subsystem (DPS) is an application subsystem providing data processing services. Data processing subsystems do not perform control subsystem functions.

Data System (for example the Space Data System - SDS) is a network of data system services, onboard computational resources, data storage, and human-machine interface devices which provide onboard command and control, data transmission, computation/processing, and operating application software to support a space vehicle's users (crew and controllers), interfacing systems, applications and subsystems.

Data System Manager (DSM) is the control subsystem which manages the housekeeping and status control services for the SDSS.

Data System Services (for example the Space Data System Services - SDSS) is a service subsystem with a generic functional architecture designed to provide a comprehensive set of services to all vehicles and subsystems.

Degraded mode is a system condition wherein some system elements (such as hardware, software, human, or procedural) are sufficiently unhealthy that the system cannot operate normally.

Error is defined as in [LAP90] to be that part of the system state which is liable to lead to subsequent failure.

Failure is defined as in [LAP90] as a deviation of the delivered service from the specified service, where the service specification is an agreed description of the expected function and/or service.

Fault is defined as in [LAP90] as the adjudged or hypothesized cause of an error.

Fault Tolerance is defined as in [LAP90] as providing a service complying with the specification in spite of faults. Fault tolerance is carried out by error processing and fault treatment. Error processing is aimed at removing errors from the system state, if possible before failure occurrence; fault treatment is aimed at preventing faults from being activated – again.

Fault Treatment is defined as in [LAP90] to be the actions taken in order to prevent a fault from being re-activated. The first step in fault treatment is *fault diagnosis*, which consists of determining the cause(s) of error(s), in terms of both location and nature. This is followed by *fault passivation*, which prevents the fault from being activated again. If the system is no longer capable of delivering the same service as before, then a reconfiguration may take place.

Flight Critical Function is a function which, if it fails, could cause loss of vehicle control resulting in loss of the vehicle and, if present, crew.

Function is an action/task that the system must perform to satisfy customer and end user needs.

Generic Architecture is an architecture where the elements of the architecture do not depend on any one mission or program for their definition. The elements of a generic architecture can be tailored to apply to many different missions and programs.

Input/Output Data Services Manager (IOSM) is the interface handling subsystem that manages the services that process requests for interaction between sensors, effectors, applications and other services.

Interface is the shared boundary between two functional units, defined by functional and other physical characteristics, as appropriate.

Mode is a predefined set of hardware and software configurations, and associated procedures used to organize and manage the conditions of operation for an avionics system's behavior, as planned, pre-planned or directed by a human.

Network Services Manager (NSM) is a control subsystem which manages peer-to-peer communication between application software running on distributed processing elements communicating over a network.

Operating System (OS) is the layer of software that isolates services and application software from the application platform hardware element. The OS provides services for at least management, allocation, and deallocation of the processor, memory, timing and input/output (I/O) processing resources for application and service software.

Service delivered by a system is its behavior as it is perceived by its user(s).

Service Subsystem is service software on an application platform, which provides transparent services to the using control or data processing subsystem.

Software is defined as in POSIX as the programs, procedures, rules, and any associated documentation pertaining to the operation of a data processing system.

Source is the originator of data passed across a logical interface.

Space Data System (SDS) - See Data System definition.

Space Data System Services (SDSS) - See Data System Services definition.

Space Generic Open Avionics Architecture (SGOAA) is defined as the target open architecture standard being developed to provide an umbrella set of requirements for applying a generic architecture interface model to the design of specific avionics hardware/software systems. This standard defines a generic set of system interface points and establishes the requirements for applying appropriate low level detailed implementation standards to those interfaces points. The generic core avionics system and processing hardware architecture models provided by the standard are robustly tailorable to specific system applications and provide a platform upon which the generic interface model is to be applied.

Space Operations Control System (SOCS) is the high level integrating command and control functional entity for a space vehicle and mission. SOCS functions may be allocated to both ground mission control facilities and onboard space vehicle facilities. SOCS functions replace all crew controlled functions for an unmanned vehicle.

Standard Data Services Manager (SDSM) is the interface handling subsystem that manages the services that process requests for interaction between sensors, effectors, application software and other services.

Standard is a document established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the maximum degree of order in a given context.

State is a set of hardware and software configurations which identify the intervening or instantaneous organization and constraints on the condition of operation for an avionics subsystem's behavior, resulting from mode commands as established by the system.

System is defined as in [SYSB-1] as the composite of equipment, material, computer software, personnel, facilities and information/procedural data that satisfies a user need.

System Services Software is common software, independent of application software, which is needed to run application software and enable it to interface to data within a system or across the EEI. This is similar to the POSIX entity, system software, which is defined as the application independent software that supports the running of application software.

Task is defined as a software entity that is executed in parallel with other parts of a software program to perform an action. [BOOCH87]

User is another system (human or physical) which interacts with the target system.

APPENDIX B
ARTEMIS COMMON LUNAR LANDER VEHICLE SUMMARY

APPENDIX B
ARTEMIS COMMON LUNAR LANDER VEHICLE SUMMARY

The purpose of the Artemis Program was to gather vital scientific and engineering data by conducting robotics exploration missions on the lunar surface both prior to and concurrent with human exploration missions. It included rapid, near-term development of small experimental and operational payloads, a low-cost capability to deliver these payloads to any location on the lunar surface, and an analysis of the data returned. The conceptual flight profile for the Artemis is contained in [KIL92].

The Artemis Program consisted of two segments, a transportation segment and a payload segment. The transportation segment consists of Launch Services and a Artemis Lander System. In the Artemis Lander System there are three systems: They are the Lander Vehicle System (LVS), the Ground Support System(GSS) and the Flight Support System (FSS). This scenario will primarily address the LVS, but will also include those commands issued to the LVS from the GSS during pre-launch activities and from the FSS after launch. A functional block diagram of the FSS is shown in Figure B-1.

B.1 LANDER VEHICLE SYSTEM

The LVS is the spacecraft which carries the Artemis Payload to a soft landing on the lunar surface. LVS functions include providing a simple structural interface for the Artemis Payload, providing an interface to the launch vehicle, and performing all in-transit functions on the way to the Moon. The LVS provides a controlled, soft landing on the lunar surface and provides an inert platform from which the payload can operate. The Lander does not provide any Avionics support functions to the payloads. The LVS automatically configures itself for flight and automatically executes all flight functions under the supervision of the FSS. The LVS periodically receives ground-computed position updates and will use onboard attitude updates to compute its state vector and perform targeting and burn execution functions.

The Lander consists of several subtier elements. These elements consist of avionics, structure, mechanisms, thermal control, propulsion and power. This report focuses on the SDS contained within the avionics element. [SHU92] is the Artemis final report on the avionics element. The avionics element is responsible for functions of the LVS which require electronics including digital equipment and software. This element handles active

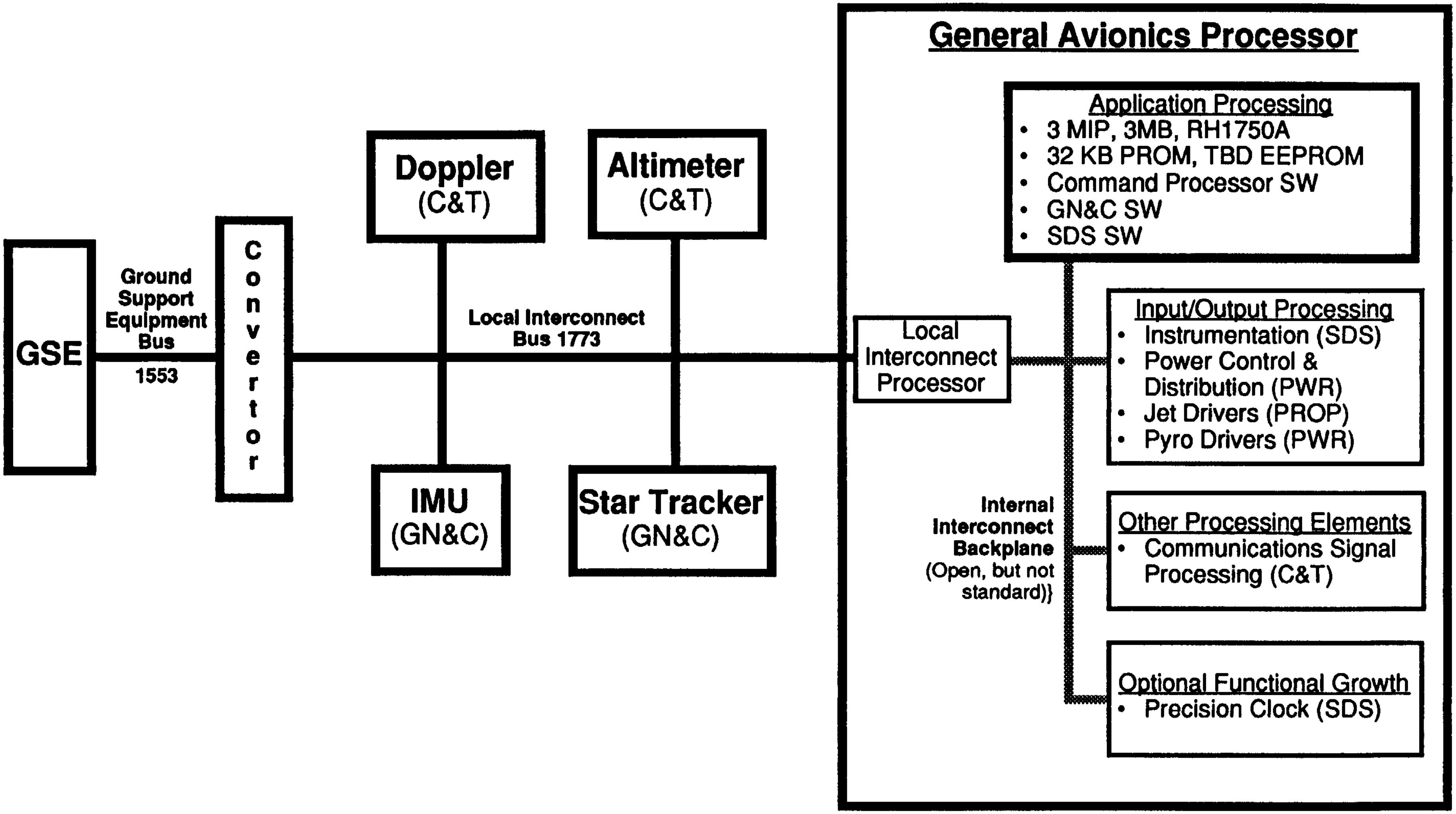


Figure B-1. CLL Avionics Element Functional Block Diagram ranging, telemetry, transmission ,command receipt and processing and other communications related functions. It also handles data management functions such as system monitoring, telemetry stream development, event sequence monitoring, and subsystem command generation. As shown in Figure B-1, the avionics element is partitioned into the SDS, GN&C, C&T, Propulsion System (Prop), Power System(Pwr) along with associated software. The CLL has no active Environmental Control and Life Support System (ELS) and no interface to payloads. The Command Processor issues all commands to the ELS. Figure B-2 from the SGOAA Standard [WS94] defines the SGOAA Class 4D Space Data System Services (SDSS) Software to Applications Software Direct Interfaces. The avionics element subsystem functions are discussed below:

- SDS as defined in [WS94] is a network of Data System Services (data system software), onboard computational resources, data storage, and human-machine interface devices which provide onboard command and control, data transmission, computation/processing, and operating of application software to support a space vehicle's users (crew and controllers), interfacing systems, applications and subsystems.
- Space Data System Services (SDSS) consists of standard data services management (SDSM), network services management (NSM), data base management (DBM), data system management (DSM), and an operating system (OS). The functions performed by each of these services is as follows:
  - The Input/Output Data Services Manager (IOSM) provides all interface to the system users for data processing and data communication services including data acquisition, standard services data distribution and reports generation.
  - The Common Lunar Lander does not require a Network Services Manager NSM) as it is a centralized processing system. Communication between the SDS and Other Avionics is via a 1553B Local Bus. The driver software for the 1553B is considered in SGOAA to be an extension of the Operating System software.
  - The Data Base Manager (DBM) is the service which manages storage and retrieval of data.

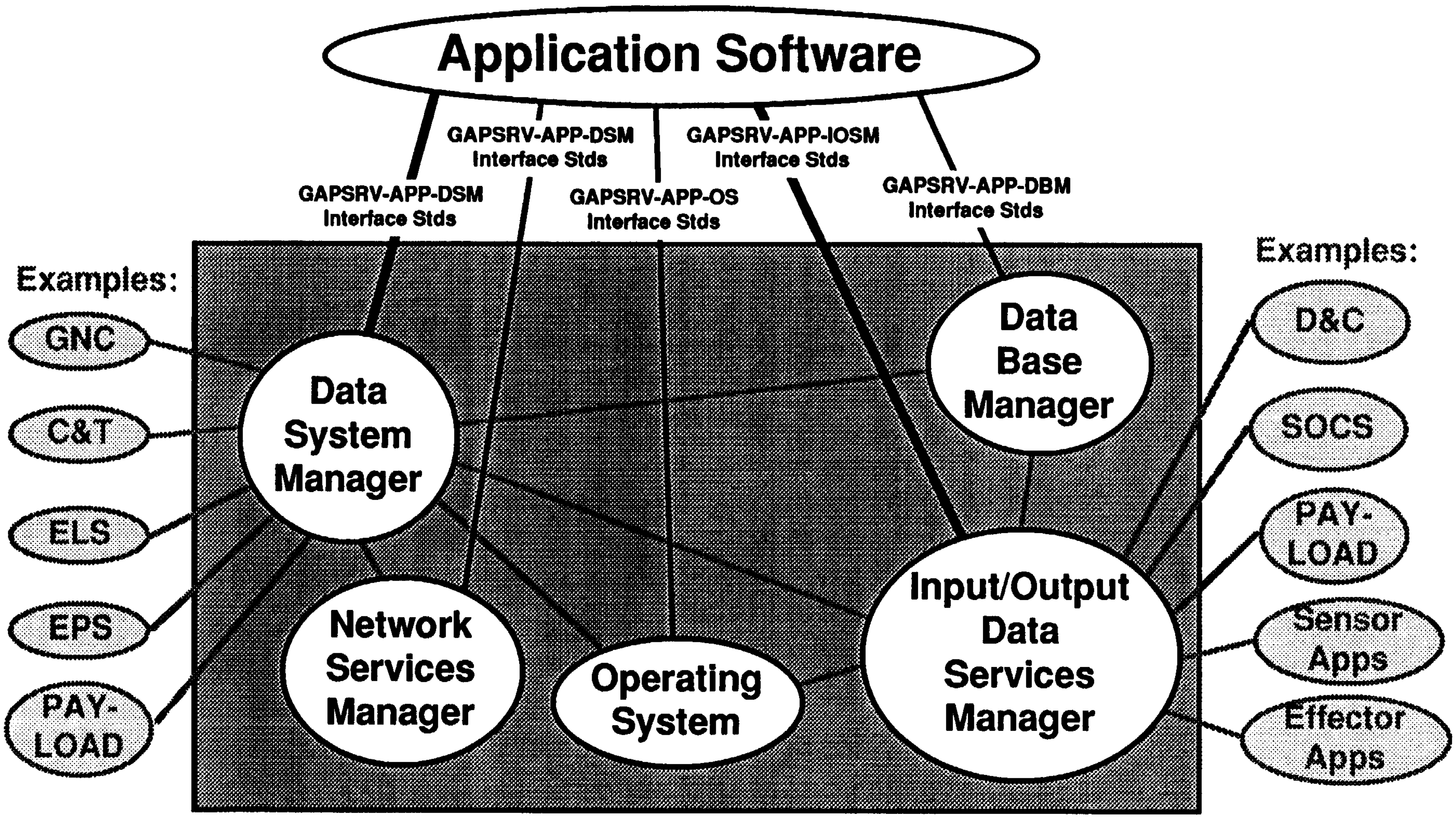


Figure B-2. Services to Applications Interfaces

- The Data System Manager (DSM) is the service which manages the housekeeping (configuration management) and status control services for the SDS. Fault management services provided include built-in test management, error detection, reporting and recovery functions for the SDS operational environment and a dump utility for communicating error by telemetry to the FSS.
- The Operating System (OS) is the layer of software that isolates services and application software from the application platform hardware element. The OS provides services for at least management, allocation, and deallocation of the processor, memory, timing and input/output (I/O) processing resources for application and service software. An Ada Run Time Environment is provided.

- GN&C applications software includes guidance functions such as maneuver targeting calculations and maneuver plan updates, and navigation functions for propagating inertial state vectors, processing state vector updates, and for determining vehicle attitude. Control functions for controlling spacecraft attitude and velocity by commanding thruster firings are also GN&C functions. Valve Controller Driver Software is included in the GN&C application software. GN&C hardware consists of the Inertial Measurement Unit (IMU), and Star Tracker. GN&C provides direct commands to the propulsion hardware by way of the Valve Controller Driver.
- C&T application software is provided to handle telemetry formatting and active ranging. C&T Tracking hardware is provided for directly determining lunar altitude and velocity upon request from GN&C. C&T hardware consists of the Doppler Radar, Radar Altimeter and a Transponder. The transponder provides for telemetry transmission and active ranging with the NASA Deep Space Network (DSN).
- Electrical Power System (EPS) application software is provided to control the EPS. The EPS hardware consists of the batteries, solar panels, power distribution switches, and power conditioning modules. The power element is responsible for electrical power generation, power distribution, and electrical noise suppression.

- The Command Processor applications software is equivalent to the SGOAA Space Operations Control Subsystem (SOCS) software. This software is the high level integrating and control functional entity for the space vehicle.
- The Propulsion System applications software is provided to control the Propulsion System. This systems hardware consists of the fuel tanks, fuel lines, valves to control fuel flow and the thruster engines. The Lander Vehicle propulsion element is responsible for providing the thrust indicated for state vector modifications and for providing the thrust needed in attitude maintenance.
- The Thermal System has no application software. The heaters can be turned on and off by the Command Processor software and are then controlled by built-in thermocouples. The Thermal Control System controls the temperatures of the various vehicle hardware. The Thermal Control System is a subset of the Environmental and Life Support (ELS) system shown in Figure B-2.
- The structural element provides the physical support for other lander systems, structural interface to the payload, and interface to the launch vehicle.
- Lander mechanisms perform derived functions such as those needed to deploy items such as landing legs and solar arrays.

B.2 INTERFACE DEFINITIONS

B.2.1 EXTERNAL COMMAND INTERFACES

External to the LVS is the Lander Vehicle's interface with the launch vehicle. The primary interface with the launch vehicle is structural. There may also be electrical interfaces for event triggers such as stage burnout's and separations.

Also external to the LVS is the Lander Vehicles interface to the Payload Segment. The Lander provides a simple structural interface to the payload and an electrostatic discharge path from the Lander to the surface.

The Lander Vehicle does not include operational support functions. For this function, the system has external interfaces with the FSS and the GSS. The FSS provides the vehicle with flight operations support for navigation updates and for system configuration monitoring and control when needed. The GSS provides the Lander Vehicle with its preparations for launch including transportation, testing, storage, handling, maintenance and servicing. The Avionics Subsystem or element provides the external interfaces for the data flow between the Lander Vehicle and the GSS and FSS.

B.2.2 INTERNAL COMMAND INTERFACES

The following discussion with regard to interfaces is limited to electronic interfaces between the Avionics and the other Lander subsystems. The Avionics Subsystem collects health and status data, collects development flight instrumentation data and distributes commands throughout all operational modes to all LVS Subsystems. Specific command functions performed by the Command Processor are:

- Issue commands to control power on and power off of the vehicle.
- Automatically provide for the selection and transition between vehicle modes.
- Accept and issue commands to all onboard systems and modify onboard data bases as directed by the GSS and the FSS.
- Issue commands to transmit telemetry.

GN&C functional software issues commands to the vehicle's rotation and translation effectors as required to execute maneuvers.

APPENDIX C
MODES AND STATES IN MISSIONS AND VEHICLES

APPENDIX C
MODES AND STATES IN MISSIONS AND VEHICLES

The following paragraphs contain short descriptions of the modes and states as extracted from [STA92] and modified to conform to [DW93]. Where [STA92] and [DW93] names differ the [STA92] name is shown in parenthesis.

Four types of mode and state models were defined:

- A Mission Mode model governing mission element behavior as shown in Figure C-1. The Mission Modes addressed in this paper are based in part on the CLL and are: Pre-launch, Launch, Boost, Orbit Coast, Deorbit, Landing, and Post-Landing including Shutdown.
- A Vehicle Mode model governing internal vehicle behavior is also shown in Figure C-1.
- A Subsystem State model identifying potential subsystem element behavior, with the Avionics Subsystem used as an example is shown in Figure C-2. Note that the action of any specific avionics subsystem state may vary depending upon which modes are in effect at the time the state is entered.
- A Function State Model identifying potential functional element behavior, with the Space Data System Services (SDSS) is used as an example in Figure C-2.

Not all possible combinations of mission and vehicle modes, and avionics subsystem and SDSS function states are allowed. The following subsections identify allowable combinations of modes and states.

C.1 <u>PRE-FLIGHT MISSION PHASE MODES AND STATES ALLOWED</u>

C.1.1 MODES ALLOWED IN THE PRE-LAUNCH MISSION PHASE

The Pre-Flight Mission Phase consists of the Pre-Launch Mission Mode as shown in Figure C-3. It includes all applicable vehicle modes up to launch. They are the Vehicle Off (Power Off), Vehicle Initialization, Integrated System (End to End) Test, Vehicle Shutdown and the Standby vehicle modes.

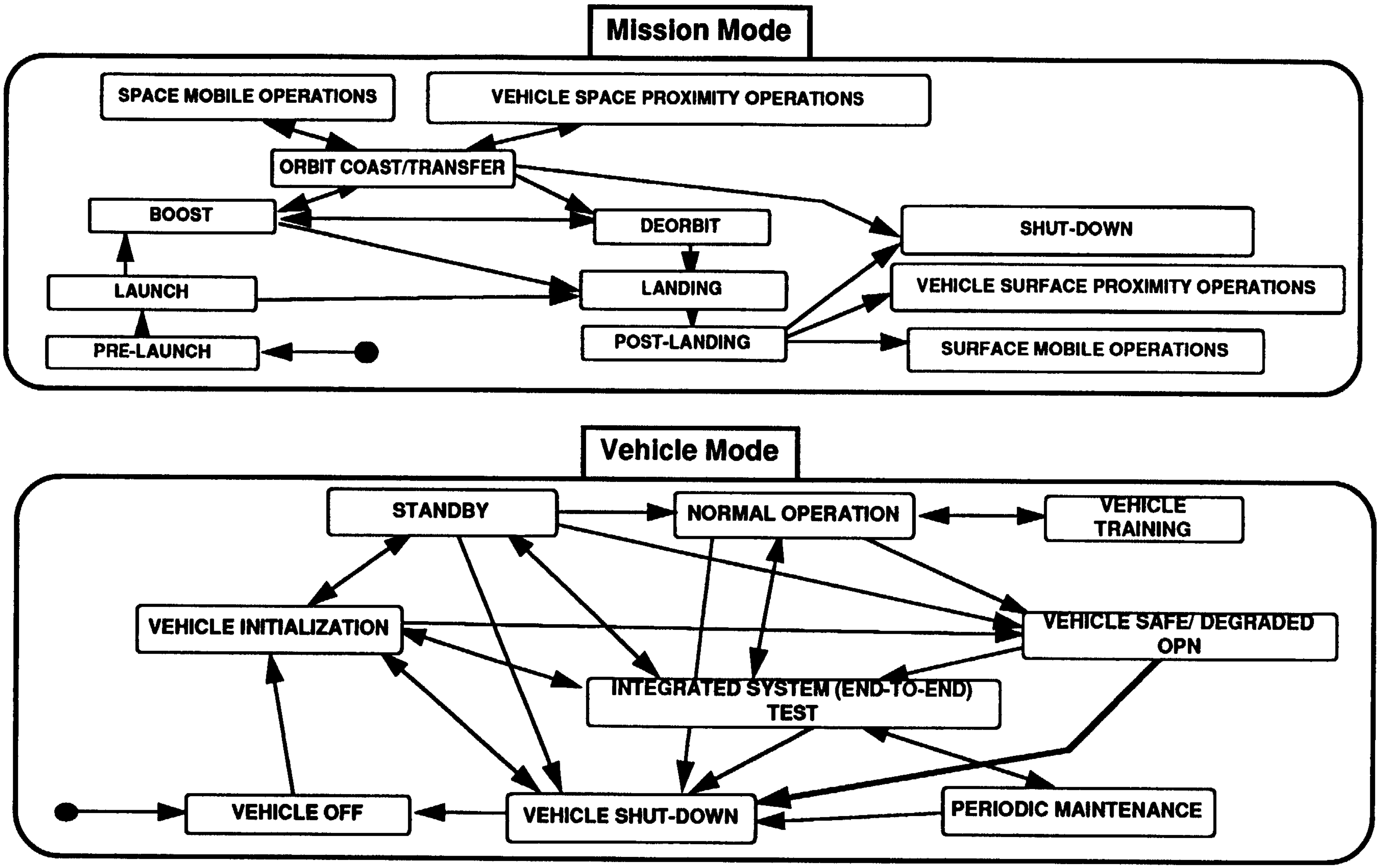


Figure C-1. Mission and Vehicle Modes

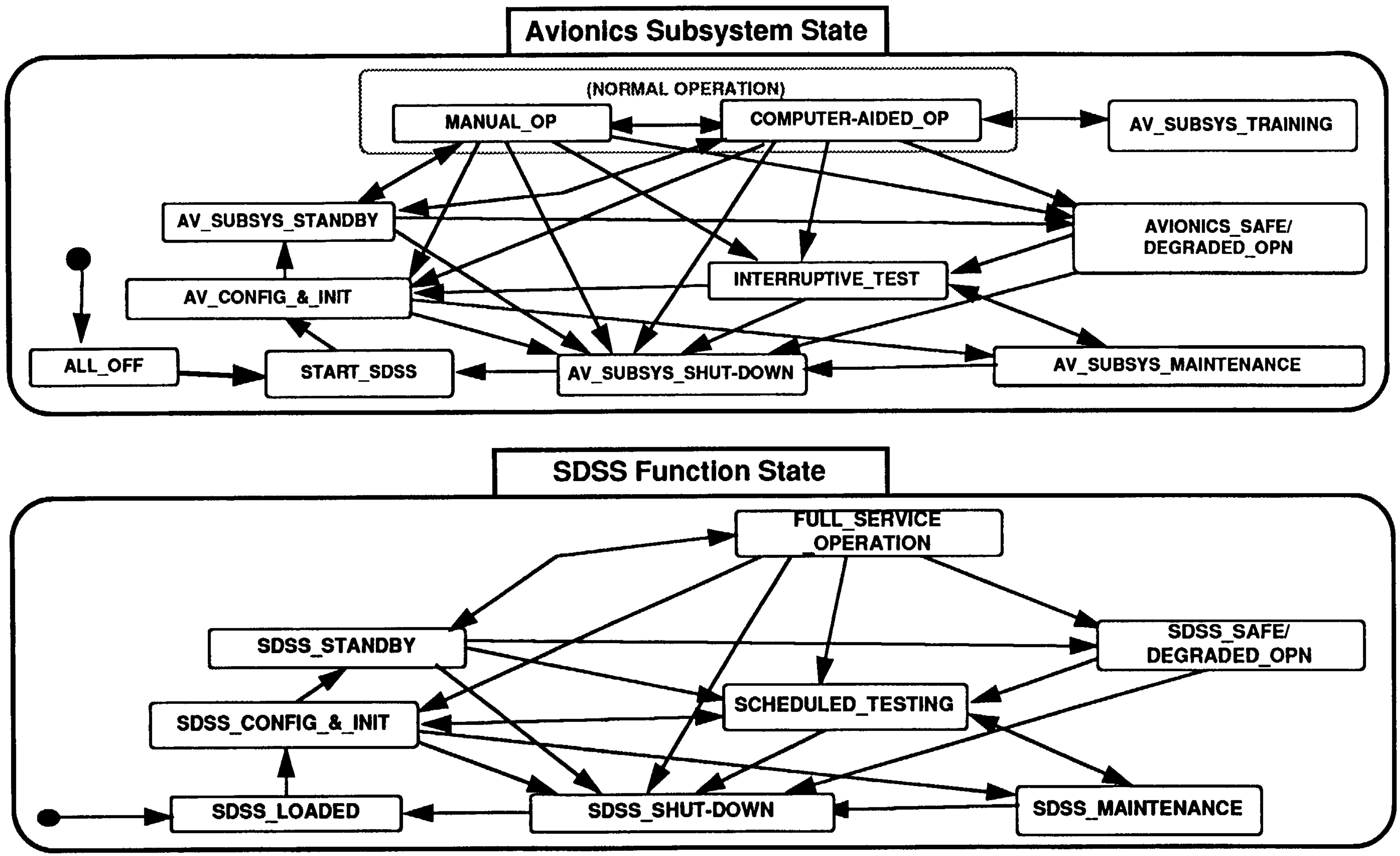


Figure C-2. Avionics Subsystem and Space Data System Services Functional States

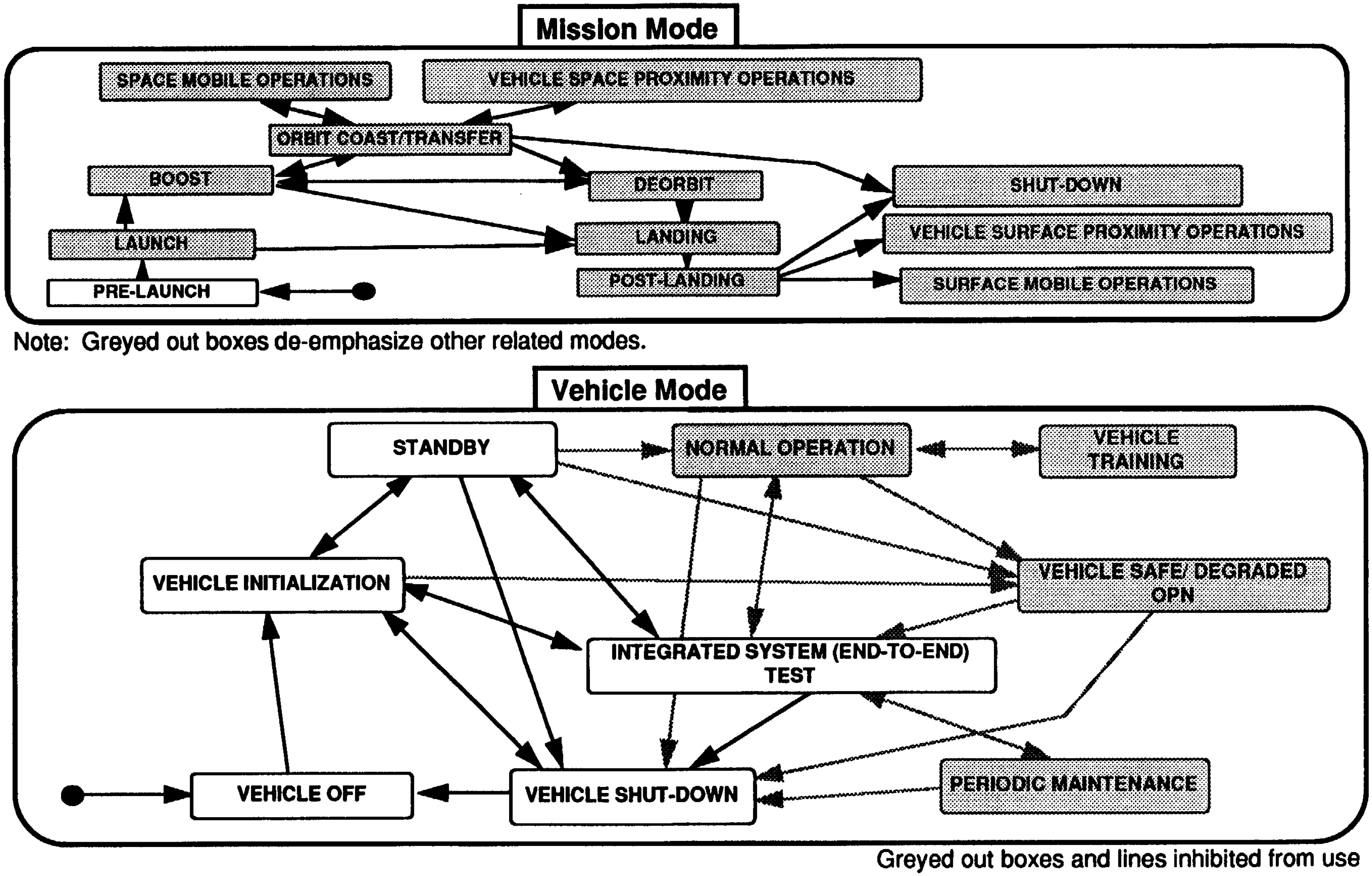


Figure C-3. Prelaunch Mission Modes

- Vehicle Off Vehicle Mode is the configuration in which the vehicle does not have power applied and is inert. The vehicle transitions out of this mode only into the Vehicle Initialization Vehicle Mode and can only be put in this mode from the Vehicle Shutdown Mode. A power up command causes the spacecraft to enter the Vehicle Initialization Mode. A power down command causes the spacecraft to enter the Shut-Down and then Vehicle Off modes sequentially.
- Vehicle Initialization Vehicle Mode is the mode that implements the startup process. This mode ensures that the flight vehicle systems are started up in the proper sequence. As a part of the initialization process,, each hardware item performs Power On Self Test (POST) and reports the results to the SDSS DSM. If failures are detected, the vehicle will be put into either the Integrated System Test, Standby or the Vehicle Shutdown Mode depending upon the failure(s) encountered.
- Integrated System Test Vehicle Mode is the mode used during prelaunch processing and in which the vehicle can perform health and status checks and be monitored and queried. This mode provides for primary processing to perform end-to-end system tests. There may be special test programs and equipment installed to support this testing. At the conclusion of the testing, the vehicle's systems should be purged of any special test data and code (to preclude impact on subsequent vehicle operations). From this mode the vehicle can enter the Vehicle Shut-down Mode upon a command, the Standby Mode upon command, or the Vehicle Initialization Mode upon a command to reset or complete vehicle systems initialization from the GSS.
- Vehicle Shut-Down Vehicle Mode is the mode where the vehicle is prepared for a safe shutdown; with backing up of any needed data bases, completion of diagnostic storage and implementation of the proper shutdown sequence for the various subsystems. From this mode only the Vehicle Off mode can be entered.
- Standby Vehicle Mode is the mode where the vehicle is configured and awaiting further commands with power usage and vehicle activity. This is a normal vehicle mode for use in the Pre-Launch Mission Mode. In this mode, final software loads have been made, the vehicle has performed health and status monitoring and is ready to accept commands. Key subsystems may be operating, such as communications, antenna pointing,, and continuous built-in test to ensure systems continue to function. Most subsystems will be operating at low

power and ready for use but not active, such as radar's and transmitters ready and able to be engaged upon command. From this mode the vehicle can only transition back to Vehicle Initialization, Integrated System Test or Vehicle Shut-Down Vehicle Modes upon command. When the mission mode transitions into the Launch Mission Mode, then the Normal Operation Vehicle Mode and others become available for activation upon command from the GSS.

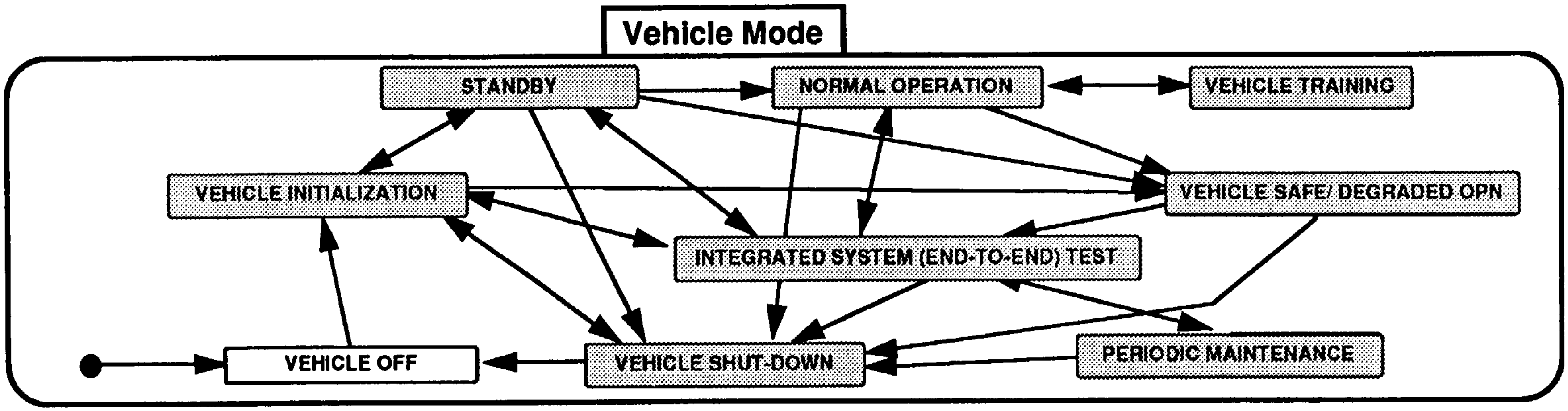
C.1.2 STATES ALLOWED IN PRE-LAUNCH MISSION MODE

In the Pre-Launch Mission Mode which begins with the vehicle installed on the launch pad and declared ready to be checked out and prepared for launch, the vehicle modes which can be utilized are Vehicle Off, Vehicle Initialization, Integrated System Test, Vehicle Shut-Down, Standby and Periodic Maintenance . Normal Operation, Vehicle Training and Vehicle Safe/Degraded Operation Modes are not available in the Pre-Launch Mission Mode. In the Integrated System Test Mode, the primary mode for the Pre-Launch Mission Mode, many of the same SDS functions are performed as in the Normal Operations Mode, but safeguards are in place to prevent unsafe or harmful system operation. Vehicle Training Mode is not appropriate during the checkout of a vehicle for launch. A failure in a vehicle system will initiate either a shutdown or continuation in the test mode and not a mode change to Vehicle Safe/Degraded Operation as there is no mission threat during prelaunch checkout. The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

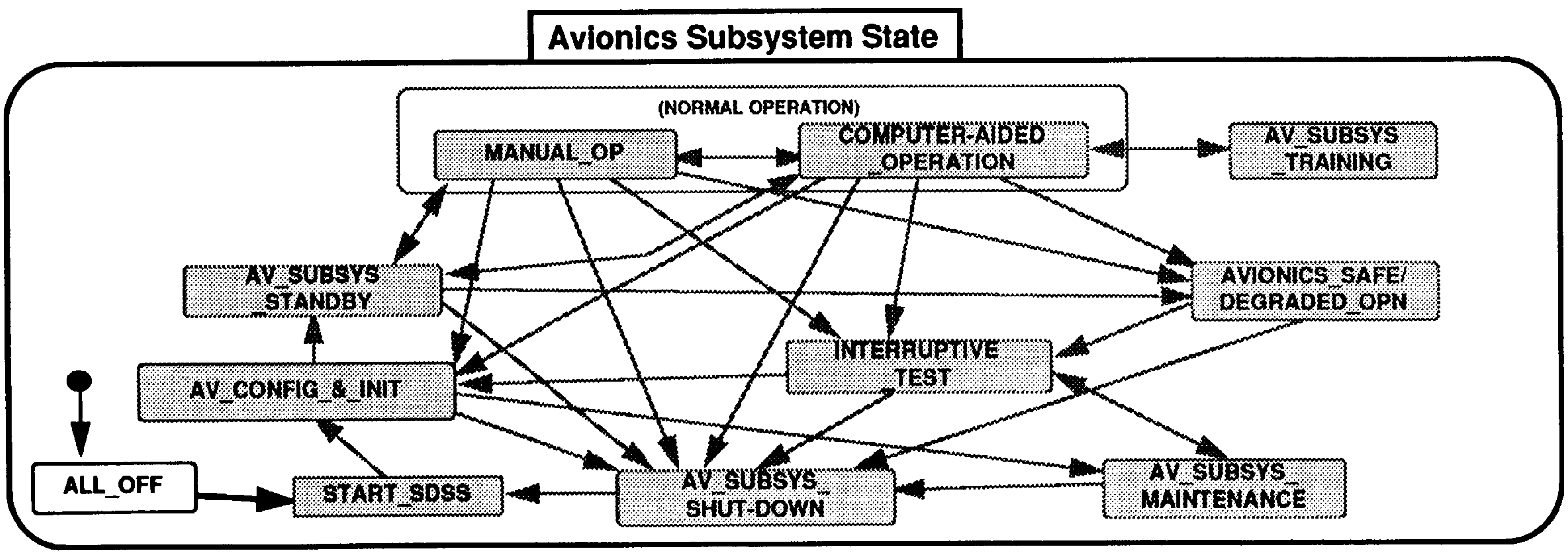
C.1.2.1 States for Vehicle Off Vehicle Mode

When the Vehicle Off Vehicle Mode is in effect, the only applicable avionics state is ALL_OFF, as shown in Figure C-4. The entry and exit conditions for this state are described below.

- ALL_OFF Avionics Subsystem State Exit. In this state, no power is applied to any avionics subsystem while in the Pre-Launch Mission Mode. External power or special battery operated non-avionics capability (such as a timer or external command operated switch) is needed to take the vehicle out of the Vehicle Off Vehicle Mode. When such power is applied (with the power on command), the vehicle mode changes, thus allowing the avionics state to change. When the



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-4. Avionics Subsystem States Allowable in Vehicle Off Vehicle Mode

Vehicle Off Vehicle Mode changes to the Vehicle Initialization Vehicle Mode, additional avionics states are allowed as described below.

- ALL_OFF Avionics Subsystem State Entry. Entry into this state cannot be achieved by the avionics commanding themselves to totally shut-down and power off. After all non-SDSS avionics are shut-down, then a transition to the Vehicle Off Vehicle Mode can be externally achieved, however. In such a Vehicle Mode transition while in START_SDSS, an external power off command signal can be activated, causing the spacecraft to be fully powered down. The lack of an arrow representing a transition into ALL_OFF indicates this can only be achieved by external control, not system control. While in this state (if in the Vehicle Off Vehicle Mode) in the Pre-Launch Mission Mode, all avionics are cold, with no power applied at all.

C.1.2.2 States for Vehicle Initialization Vehicle Mode

When the Vehicle Initialization Vehicle Mode is in effect, the avionics subsystem states shown in Figure C-5 (in black and white) may be entered in the Pre-Launch Mission Mode. These states are described below.

- ALL_OFF Avionics Subsystem State. When the spacecraft first switches from the Vehicle Off to Vehicle Initialization Vehicle Modes, it starts off in the ALL_OFF Avionics Subsystem State. The power on command is applied with external or other power (as noted above) to cause the vehicle mode to switch and the ALL_OFF state to be exited.

- START_SDSS Avionics Subsystem State. The first activity that takes place after powering up the avionics is for the START_SDSS Avionics State to be entered to boot up the avionics processing capabilities. This state causes the data system boot loader to execute, which starts up the data system services, the command processor and the external avionics and their associated software. This state includes the power-on self test (POST) required for the SDSS to load and function. This state also allows for return after the avionics have been shut down, with just the SDSS running and ready to re-configure or re-initialize the avionics. Note that the SDSS is inhibited from transitioning itself to the ALL_OFF avionics state, as a safety precaution. Only an external power line or other external-to-SDSS power switch (similar to the ALL_OFF exit signal) can cause the SDSS to power down.

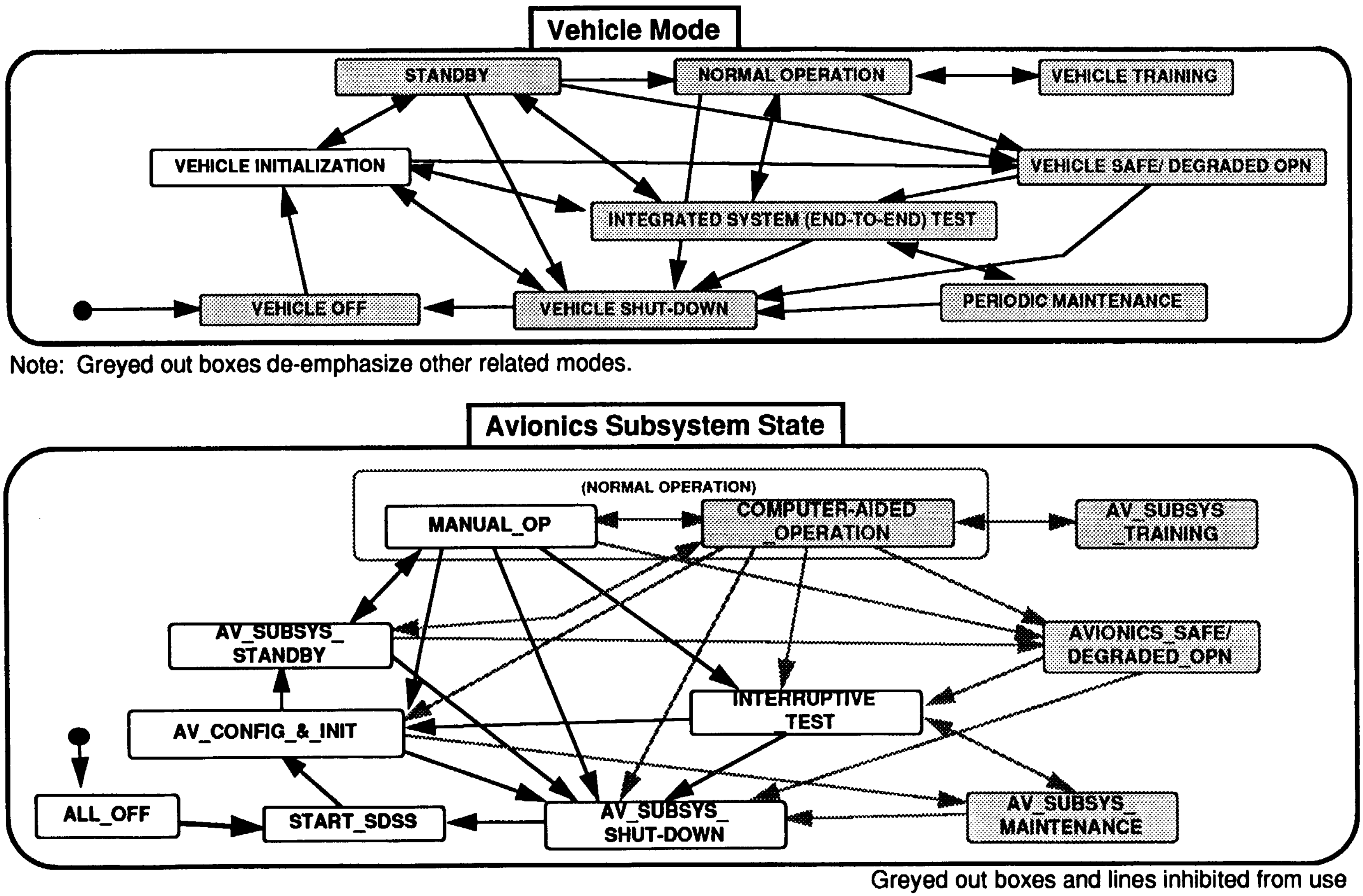


Figure C-5. Avionics Subsystem States Allowable in Vehicle Initialization Vehicle Mode

- AV CONFIG & INIT Avionics Subsystem State. After the avionics are started, then the AV_CONFIG_&_INIT Avionics State is entered to setup the avionics for operation. This state both establishes the configuration of components, priorities, services, information and operating parameters needed for the avionics to function. It then initializes the avionics with their startup data needed for operation. Startup errors are processed and both pre-stored and real-time user setup commands are implemented. This state includes the POST required for the other avionics to load and function.

- AV SUBSYS STANDBY Avionics Subsystem State. After the avionics have initialized and are ready for operation, they must enter the AV_SUBSYS_STANDBY state to ensure that all subsystems data and timing are synchronized, and stay so after any subsystem changes which may be subsequently directed. This state is a holding state while other major state changes are contemplated. While in this state, no general avionics activities may be carried out that are not needed, so the system can remain quiescent and ready to implement subsequent mode commands. This state includes the continuous built-in test (CBIT) and fault detection, isolation and recovery (FDIR) needed to ensure the avionics are functioning sufficiently to carry out any mode commands which may be received.

- MANUAL OP Avionics Subsystem State. When the crew or GSS so command, manual parameters and switches may be set by crew or GSS members. If so, then the MANUAL_OP state ensures that automatic processes do not work against the actions being manually carried out, and that the system monitors manual actions to maintain cognizance of their state and results. Manual control actions always have priority over other system functions. Potentially hazardous manual actions will cause an alert or caution to the crew and GSS.

- INTERRUPTIVE TEST Avionics Subsystem State. While the vehicle is initializing, if it is necessary to resolve errors or problems with testing which is more extensive than POST, then interruptive test may be directed. This state causes tests to be performed on the system or subsystem elements which can interfere with their normal functioning. For instance, special input data that produces known results with normal system operation may be inserted and the actual results and predefined (known) results compared to verify normal system operation. Special test diagnostics may also be executed which make the element unavailable for normal processing until tests are completed. After interruptive testing is completed, it is necessary to either return to AV_INIT_&_CONFIG for re-initialization, or to AV_SHUT-DOWN for termination of processing and avionics operation.

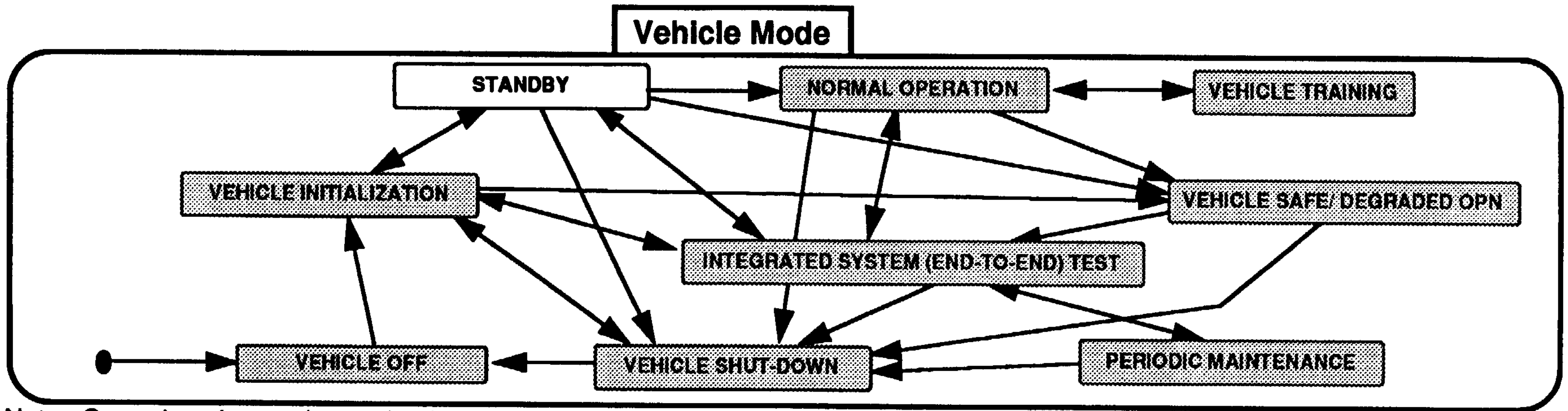
- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. When this state is entered by a command to shut-down the avionics, avionics system elements will be shut down and power removed in an orderly manner to preserve all data, ensure processes do not execute uncontrollably, and that external avionics power is also terminated in the proper manner with controlling software. When this state is entered by a command to shut-down a specific avionics subsystem, then just those elements will be powered down, with the exception of the SDSS. The SDSS can be cold re-started as long as the power line to re-start it remains on; it cannot be powered down from within the system as a safety precaution as noted above. From this state, the only state that can follow is the START_SDSS state in which the data system continues operating and ready to re-configure or re-initialize the avionics if necessary.

C.1.2.3 States for Standby Vehicle Mode

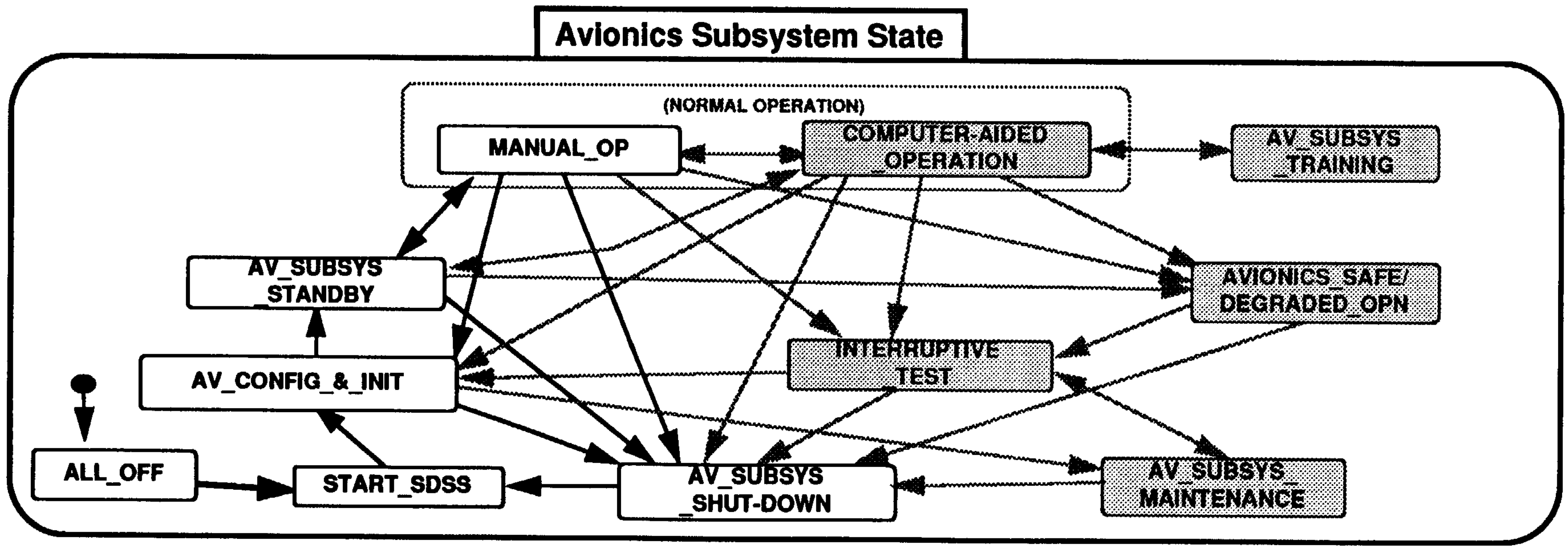
When the Standby Vehicle Mode is in effect, avionics states as shown in Figure C-6 may be entered in the Pre-Launch Mission Mode. These states are described below.

- ALL_OFF Avionics Subsystem State. Although the vehicle is in the Standby Vehicle Mode, there may be some avionics subsystems which are still powered down (for instance backup or spare processing units). Thus, the potential usage of avionics subsystem states starts with the ALL_OFF state. The exit transition in this case would be caused by the SDSS or other avionics function generating a power on command to the component or subsystem which needs to be activated.

- START_SDSS Avionics Subsystem State. When a processing resource is added to the roster of operating SDSS components while the vehicle is in the Standby Vehicle Mode, the START_SDSS state ensures the component boots up with the appropriate service changes to enable its use. This includes performing a POST on the component, downloading the software needed for the component, setting up the appropriate communications and access services, etc. While the START_SDSS generally cannot transition to an ALL_OFF state, specific components that have been powered down can be rebooted (for instance to perform a "cold" start) to improve system operability.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-6. Avionics Subsystem States Allowable in Standby Vehicle Mode

- AV CONFIG & INIT Avionics Subsystem State. After a new processing resource has been started, then this state is re-entered for that component to configure and initialize it as was previously done for the Vehicle Initialization Mode in Section C.1.2.2. If external components are being brought on-line to support a SDSS component, and they require a POST, then this state would ensure it was performed with acceptable results.

- AV SUBSYS STANDBY Avionics Subsystem State. This state is the normal state for most components while the Standby Vehicle Mode is in effect. CBIT, FDIR and routine housekeeping SDSS processes will operate normally as noted in Section C.1.2.2. Communications; guidance navigation and control; and command processing subsystems may operate intermittently for station-keeping or as required by mission parameters.

- MANUAL OP Avionics Subsystem State. While the avionics are generally in a holding state, manual control of the system is always capable of being executed by the crew or GSS.

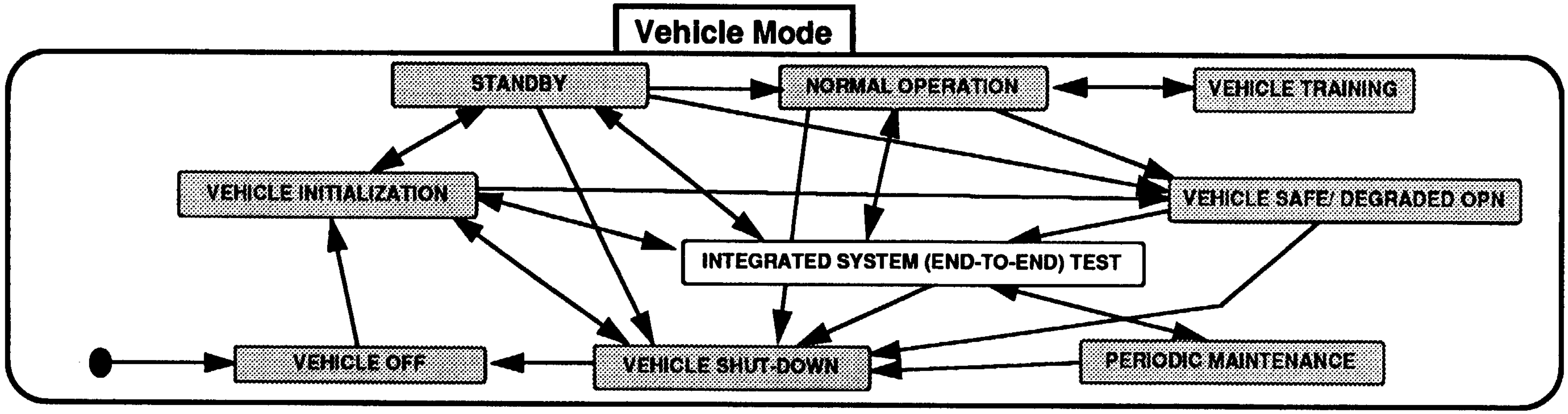
- AV SUBSYS SHUTDOWN Avionics Subsystem State. This state may be entered by a power off command for a specific component while in the Standby Vehicle Mode, either to turn it off (for instance to save power) or to force a re-start on the component (for instance to recover a failed or "confused" subsystem).

C.1.2.4 States for Integrated System Test Vehicle Mode

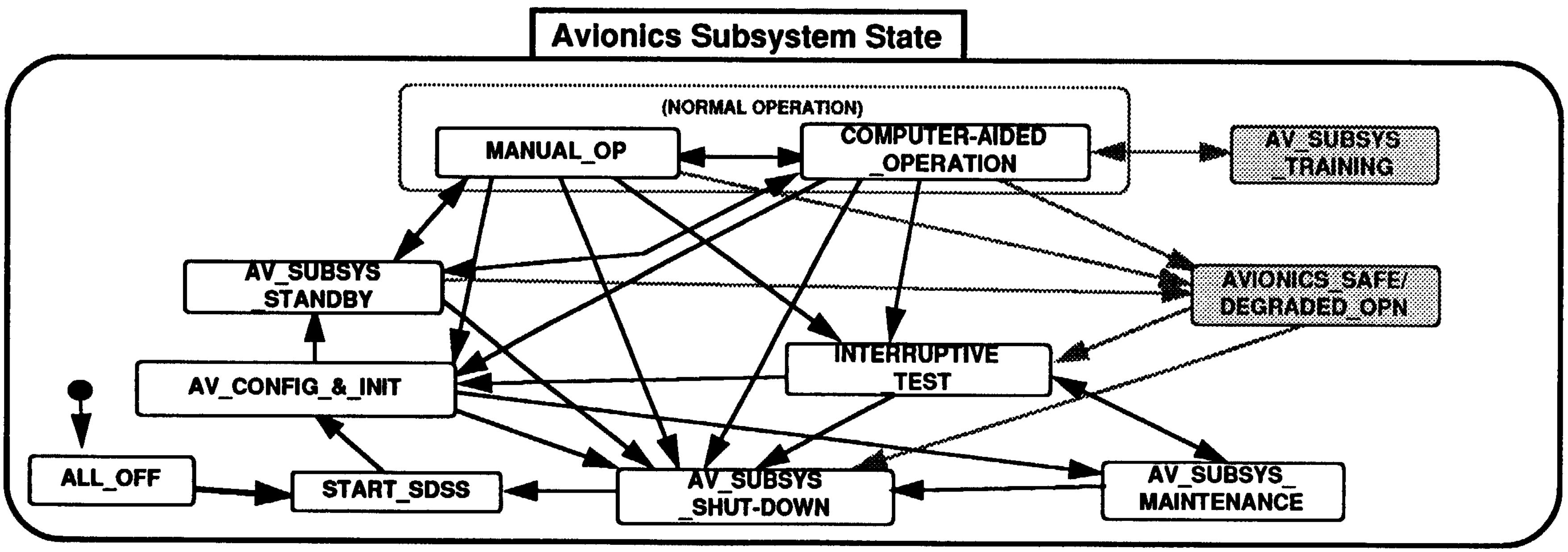
When the Integrated System (End-to-End) Test Vehicle Mode is in effect, the avionics subsystem states shown in Figure C-7 (in black and white) may be entered in the Pre-Launch Mission Mode. These states are described below.

- ALL OFF Avionics Subsystem State. When the vehicle enters into the Integrated System Test Vehicle Mode, activation of specific test equipment may be needed. Entry into this vehicle mode will be accompanied by a test equipment power on command which identifies any special test equipment which is needed. That equipment would be powered on and cause a transition to the START_SDSS state.

- START SDSS Avionics Subsystem State. In this state in this vehicle mode, the test equipment newly powered on will perform a POST of processing components to be used, any special test software needed will be downloaded, and



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-7. Avionics Subsystem States Allowable in Integrated System Test Vehicle Mode other special communications needed for test processing will be made available. Specific test equipment or processors which may need to be re-started can also pass through this state to improve system operability.

- AV_CONFIG_&_INIT Avionics Subsystem State. This state causes the external test equipment to be powered on, POST is performed on them, test applications are downloaded, the test subsystems are configured and initialized for operation (as described for this state in C.1.2.2. Special test-instrumented versions of applications or services may be commanded to be loaded, configured and initialized as needed to meet test requirements.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state causes the test subsystems to become quiescent until explicitly commanded to carry out specific directed actions, similar to this states activities in C.1.2.2.

- MANUAL_OP Avionics Subsystem State. Manually controlled test instrumentation and system under test are commanded in this state. Test cases and procedures can be manually implemented. Test data can be manually injected into the system and tracked.

- COMPUTER-AIDED_OPERATION Avionics Subsystem State. Entry of this state is normally from the MANUAL_OP or AV_SUBSYS_STANDBY states. Upon entry, fully automatic operation of the test systems and the avionics systems are executed. Automatic test operations cease when either commanded, time-out is reached, or specific exit conditions are encountered.

- INTERRUPTIVE_TEST Avionics Subsystem State. This state sets up the specific tests to be executed and data to be recorded for the Integrated System Test Vehicle Mode. Any "quick-look" test results needed are identified and commanded to be processed. Any real-time data analysis requirements are identified and commanded to be processed. Special test-instrumentation parameters in applications or services may be accessed, results stored or analyzed, and reports generated.

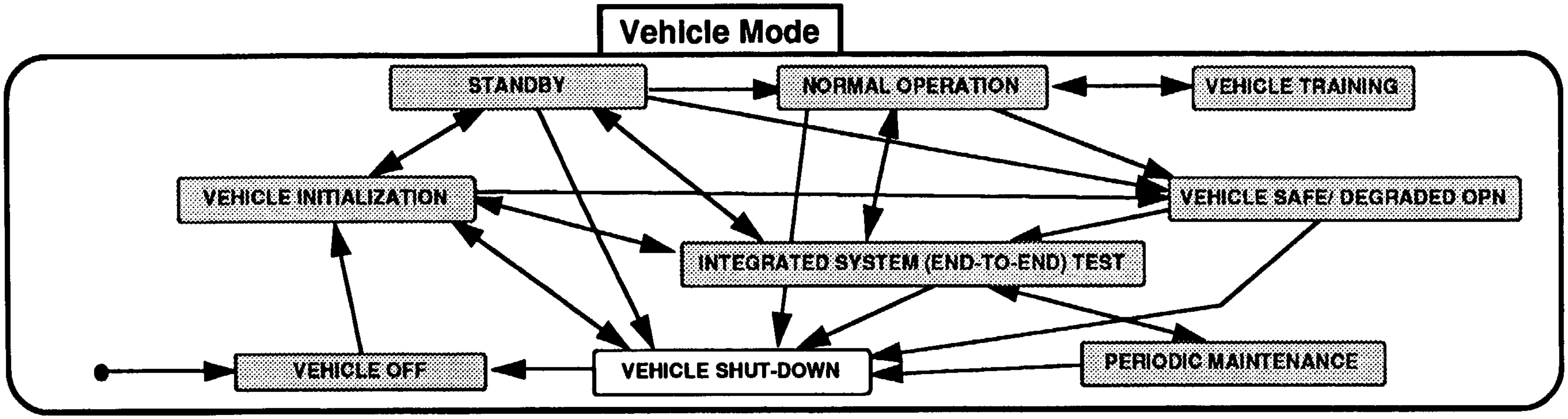
- AV_SUBSYS_MAINTENANCE Avionics Subsystem State. Normal entry into this state is either from the AV_CONFIG_&_INIT or INTERRUPTIVE TEST states. This state allows special maintenance programs to be executed in conjunction with testing to improve test operations, verify test processes, validate test results and aid system repair operations. Exit from this state is upon command or encountering of specific exit conditions. Upon exit, any maintenance capabilities are reset to normal avionics states.

- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state is entered by a command to shut-down the test capability for the system under test, and reset avionics system under test to normal avionics states. Thus the only exit from this state is to re-enter the START_SDSS state, where the systems can be "cold-started" to ensure proper loading, configuration and initialization of the avionics with just the appropriate operational data. All test and maintenance data must be effectively purged from the system.

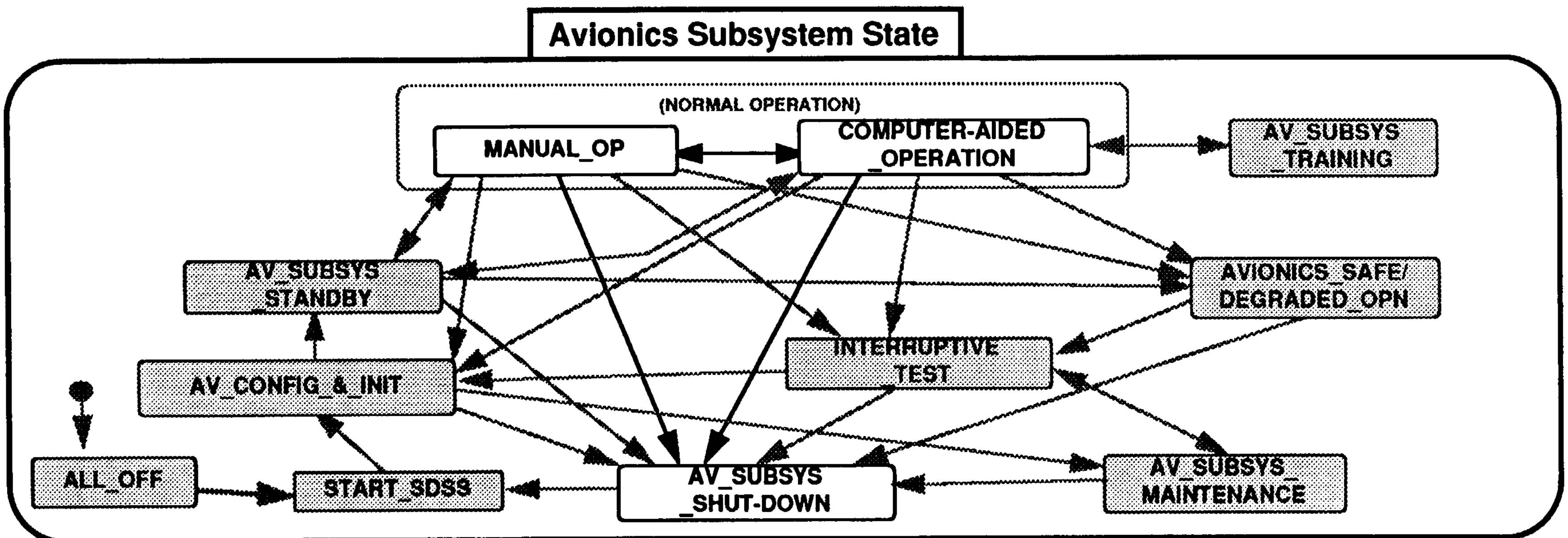
C.1.2.5 States for Vehicle Shut-Down Vehicle Mode

When the Vehicle Shut-Down Vehicle Mode is in effect, the avionics subsystem states shown in Figure C-8 (in black and white) may be entered in the Pre-Launch Mission Mode. Vehicle Shut-Down mode may be preparatory to either turning the vehicle to the Vehicle Off mode or to the Vehicle Initialization mode (for instance, to re-initialize vehicle subsystems). These states are described below.

- MANUAL_OP Avionics Subsystem State. In this state, the vehicle avionics subsystems are manually switched off by sending commands to each subsystem to stop all activity and then sending a power off command to the power subsystem to power down each other subsystem.
- COMPUTER_AIDED_OP Avionics Subsystem State. In this state, a shut-down automated program is executed which turns each subsystem off, commands it be powered down, and powers down itself last. This causes a transition to the AV_SUBSYS_SHUT-DOWN state.
- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. In this state, all avionics except for the SDSS are confirmed to be turned off and powered down. All external hardware subsystems are powered down, and all service peripherals are powered down. The SDSS cannot power itself down as noted above as a safety precaution. In transitioning to the Vehicle Off Mode, an external power off signal can be sent to the power subsystem to remove power from the SDSS and from the power subsystem.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-8. Avionics Subsystem States Allowable in Vehicle Shut-Down Vehicle Mode

C.1.2.6 States for Periodic Maintenance Vehicle Mode

When the Periodic Maintenance Vehicle Mode is in effect, the avionics states shown in Figure C-9 (in black and white) may be entered in the Pre-Launch Mission Mode. Periodic maintenance is required when component anomalies or failures have occurred during test and checkout of the vehicle prior to launch. The states are described below.

- ALL_OFF Avionics Subsystem State. This state provides control over the special maintenance subsystems which start out in the ALL_OFF state. Upon command to enter Periodic Maintenance Vehicle Mode, the SOCS will issue the power on command for the maintenance subsystem and ancillary equipment.

- START_SDSS Avionics Subsystem State. This state provides controls for starting service connections with the maintenance subsystems. This includes performing POST on the maintenance equipment and loading special maintenance software. This state also provides for cold restart of the avionics after maintenance mode if needed to purge maintenance data from the system.

- AV_CONFIG & INIT Avionics Subsystem State. This state provides controls for configuring and initializing (or re-initializing) components being started. Selection of equipment to be used for maintenance or to undergo maintenance is part of the configuration process. It includes setup up controls to ensure the maintenance subsystem can be unambiguously overridden by actual alerts and warnings if needed. It also includes loading and unloading special maintenance versions of operational flight programs if needed.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides controls over the maintenance equipment when it must be placed in a quiescent condition while higher priority tasks interrupt, but termination of the maintenance activities or the current maintenance examination is not desired.

- MANUAL_OP Avionics Subsystem State. This state provides controls to enable the actual avionics systems not in maintenance mode to monitor human actions in maintenance and in non-maintenance operations, keep them separate and to support both sets of actions.

- AV_SUBSYS_MAINTENANCE Avionics Subsystem State. This state provides controls for the maintenance equipment and programs which will be used. It is the normal state for this mode. Maintenance subsystems might include such capabilities as simulations to represent the appearance of mission system

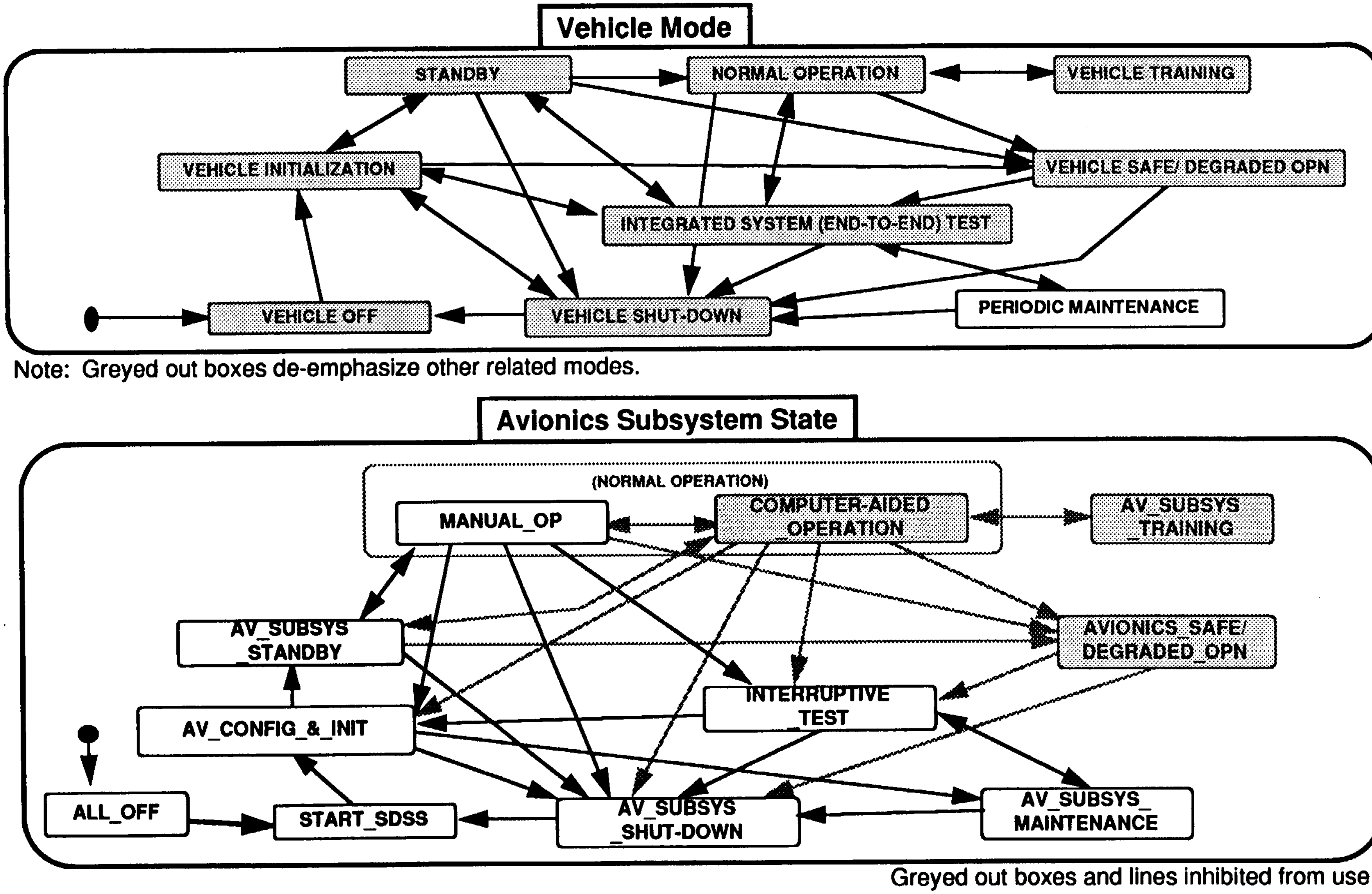


Figure C-9. Avionics Subsystem States Allowable in Periodic Maintenance Vehicle Mode interfaces and their behavior, emulation's of real environmental conditions not currently available to crew operations, and interfaces to real avionics subsystems to enable their use in stimulating avionics being maintained. Entry into this state would be by execution of the Start Periodic Maintenance Mode command. Exit from this state would be caused by the End Maintenance Mode or End AV_SUBSYS_MAINTENANCE State commands, and result in transition to the AV_SUBSYS_SHUT-DOWN state.

- INTERRUPTIVE_TEST Avionics Subsystem State. This state provides controls for special maintenance tests needed. (It is presumed that many of these tests will interfere with normal avionics processing capability, which is acceptable in maintenance mode). It also provides for injection of special maintenance data (e.g., data with known results) into input ports on sensors and other devices.
- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state provides controls to shut-down maintenance subsystems in an orderly manner. It provides for the orderly shut-down (and eventual restart) of avionics which may have been repaired or need to purge confused state conditions.

C.2 FLIGHT MISSION PHASE MODES AND STATES ALLOWED

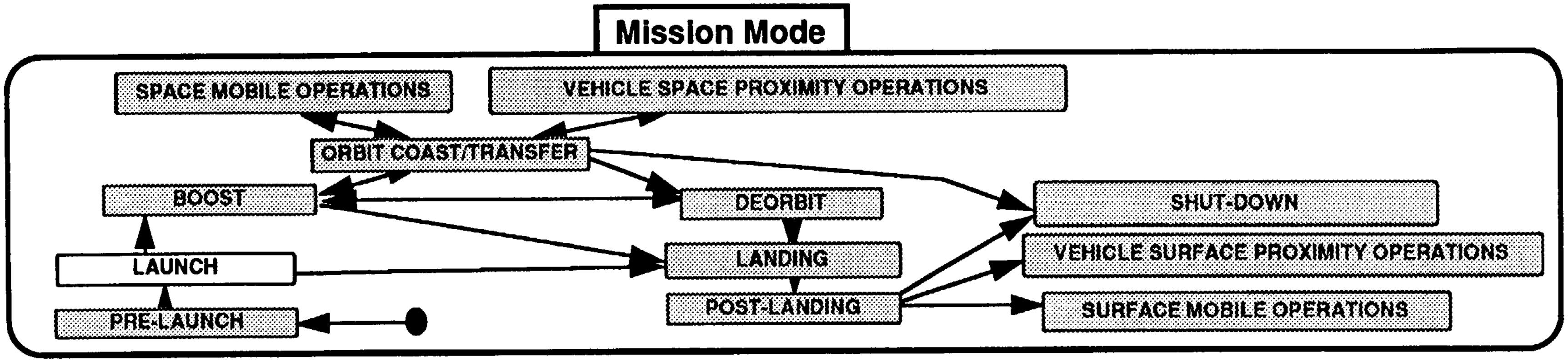
The Flight Mission Phase includes those mission modes where the vehicle is in free space flight, or is still connected to elements of the launch vehicle in free flight and is itself preparing for free flight.

C.2.1 MODES ALLOWED IN THE FLIGHT MISSION PHASE

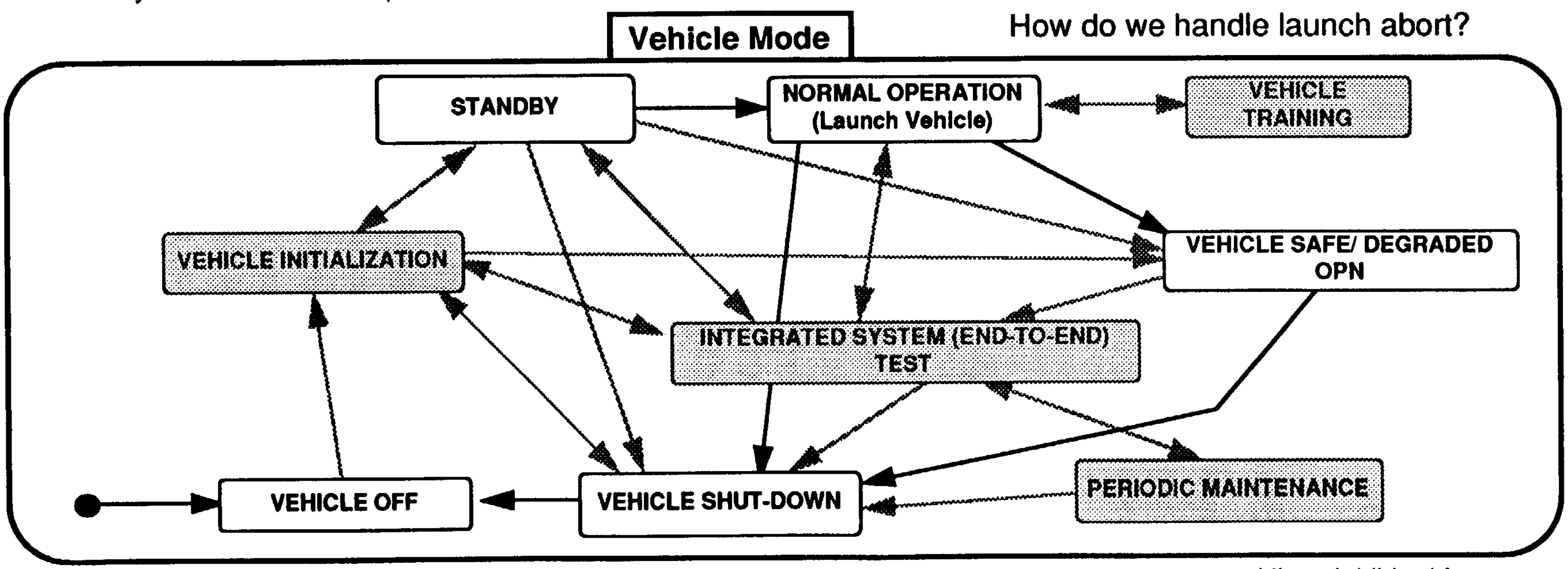
The mission modes in this mission phase are Launch Mission Mode, Boost Mission Mode, Orbit Coast/Transfer Mission Mode (Normal Flight), Deorbit Mission Mode and Landing Mission Mode. During each of these mission modes, the vehicle can be put into the vehicle modes identified below within each mission mode. (The Vehicle Proximity Operations and Space Mobile Operations modes are not addressed in this scenario.)

C.2.1.1 Launch Mission Mode

This mode is shown in Figure C-10 beginning at the end of prelaunch countdown and continuing through translunar injection (TLI). In this mode and prior to launch the vehicle still transmits data to and receive commands from the GSS. All connections to the



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-10. Launch Mission and Vehicle Modes

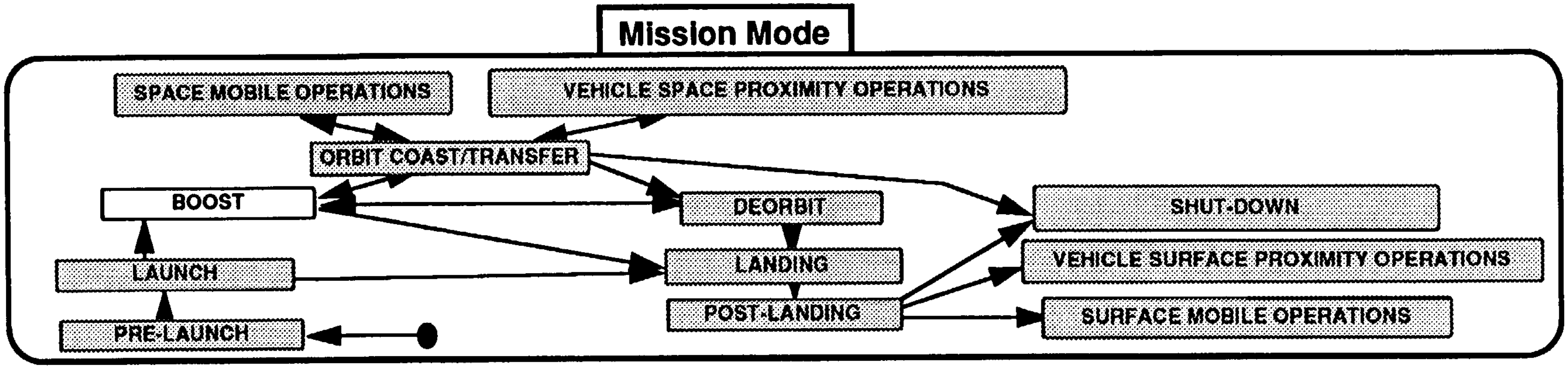
GSS are terminated at launch. This mode can only be entered from the Prelaunch Ready Vehicle Mode. Prior to launch, the vehicle can transition from Launch Mission Mode back into the Prelaunch Mission Mode upon command from the GSS. During launch and boost the vehicle will be in either Vehicle Normal Operation, Safe/Degraded Operation, Shut-down or Off modes.

C.2.1.2 Boost Mission Mode

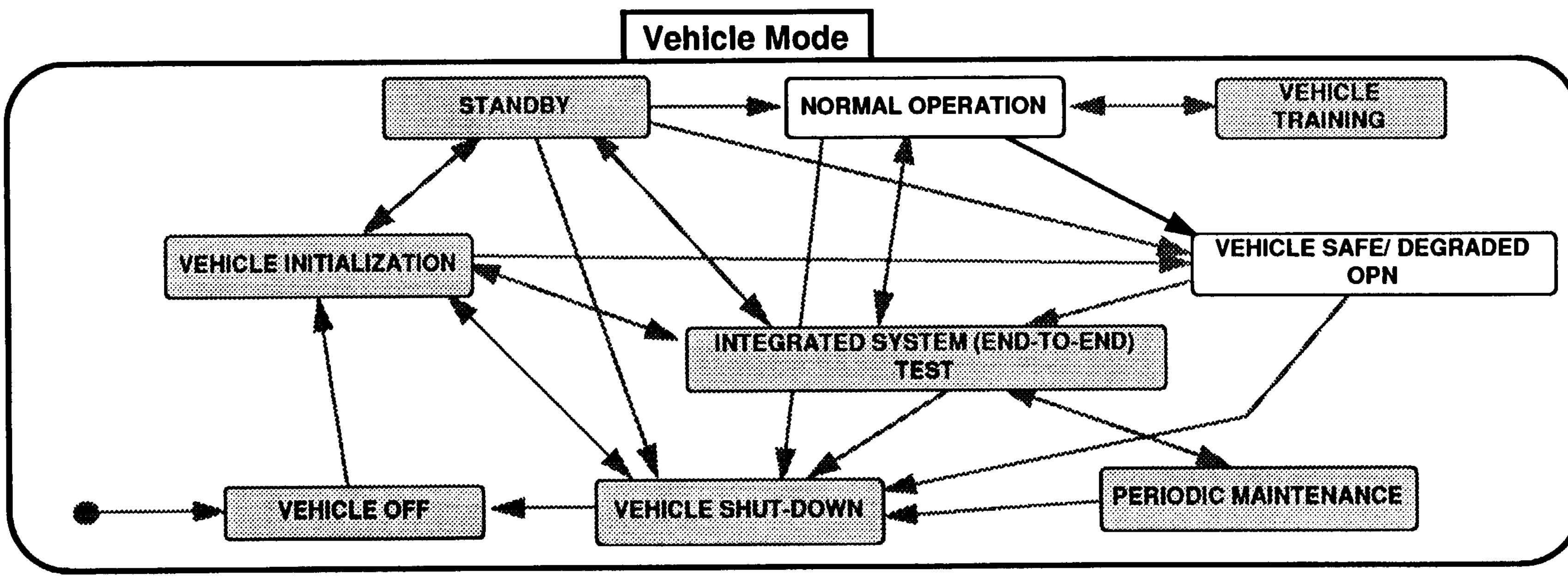
This mode is shown in Figure C-11 and is the mode in which the spacecraft has left the launch pad and is rising under programmed control. This boost mode ends in orbital insertion. After boost mode, the vehicle can enter the Orbit Coast/Transfer, Deorbit or Landing Mission Modes.

C.2.1.3 Orbit Coast/Transfer Mission Mode

This mode is shown in figure C-12 and is the mode in which normal flight operations occur. After boost to orbital insertion, orbital transfer to another orbital trajectory or to translunar injection (TLI) can take place. Prior to TLI, the SOCS will issue commands to enter the TLI configuration which includes activation of the attitude control capability for the combined LVS and launch vehicle third stage, activation of the third stage propulsion system for the TLI burn and leg deployment. Following TLI, the SOCS will issue commands to separate from the launch vehicle and enter the Coast Mode. The vehicle is self-sufficient in this state and will only receive position and velocity state vector updates and emergency commands from the FSS. The SDS will perform all calculations and issue all commands necessary to complete the mission. These SDS issued commands will as a minimum include solar panel and antenna deployment, active ranging, commands to propulsion for thrust and attitude control to maintain the proper trajectory including entering the lunar parking orbit, and communicate telemetry. The FSS monitors and can send override and update commands. If an unrecoverable onboard failure is encountered, the SOCS will put the vehicle in the Vehicle Safe/Degraded Operation Vehicle Mode (Contingency Hold Mode) also shown in Figure C-12 and await commands from the FSS. From the Orbit Cost Mission Mode, the vehicle can only enter the Deorbit and Landing Mission Modes. The SOCS issues the commands necessary to transition into the Deorbit and Landing Mission Mode just prior to the lunar deorbit maneuver.

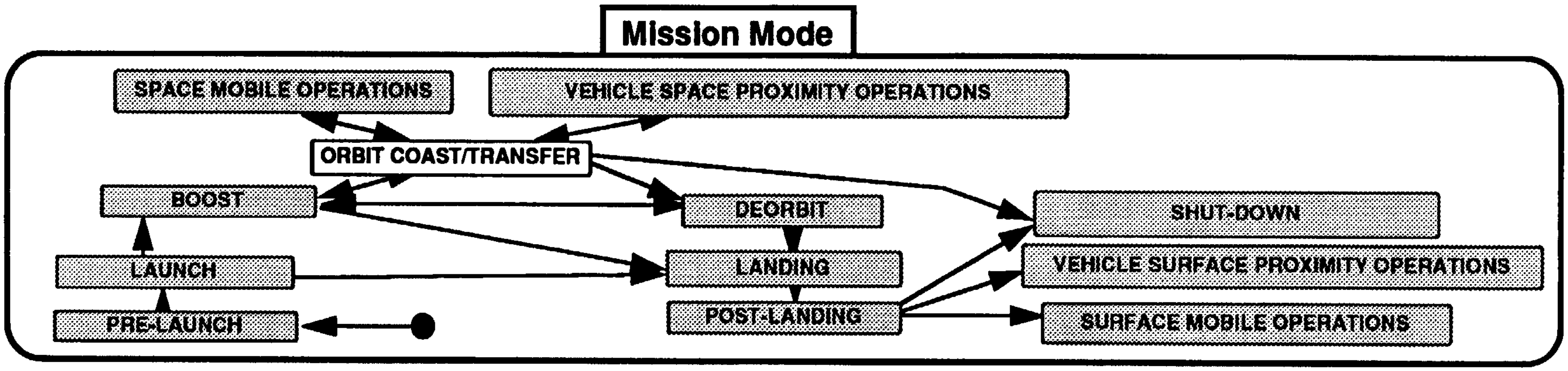


Note: Greyed out boxes de-emphasize other related modes.

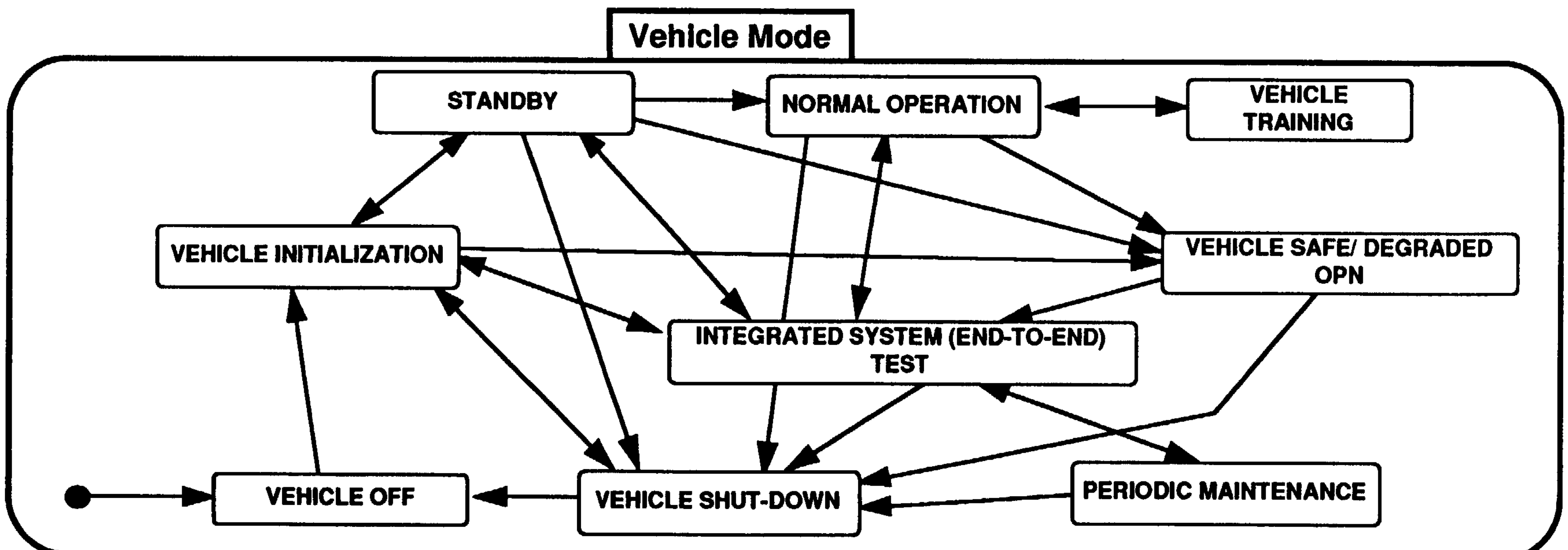


Greyed out boxes and lines inhibited from use

Figure C-11. Boost Mission and Vehicle Modes



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

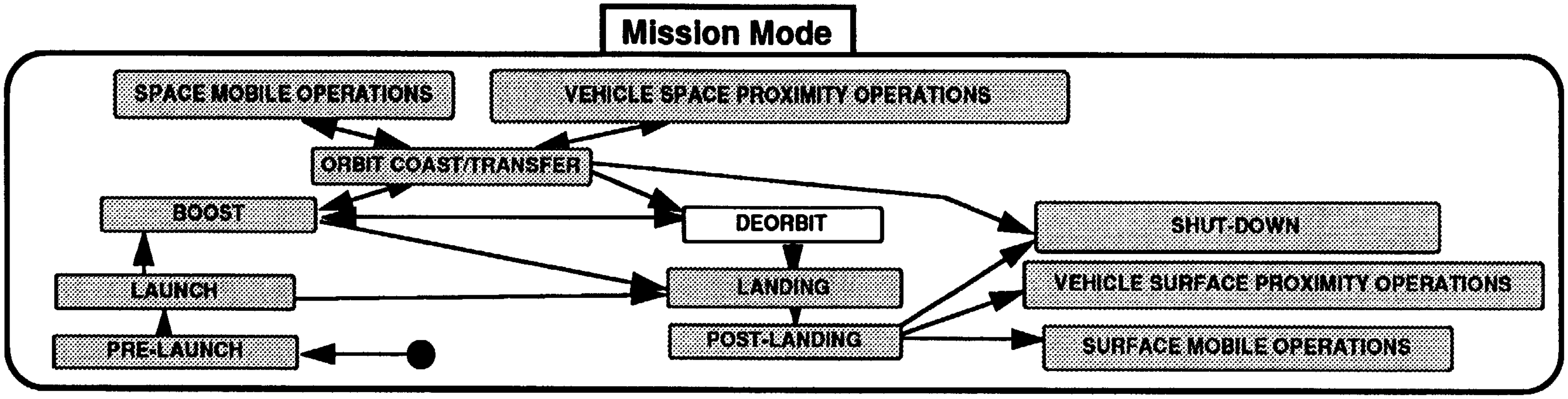
Figure C-12. Orbit Coast/Transfer Mission and Vehicle Modes

C.2.1.4 Deorbit Mission Mode

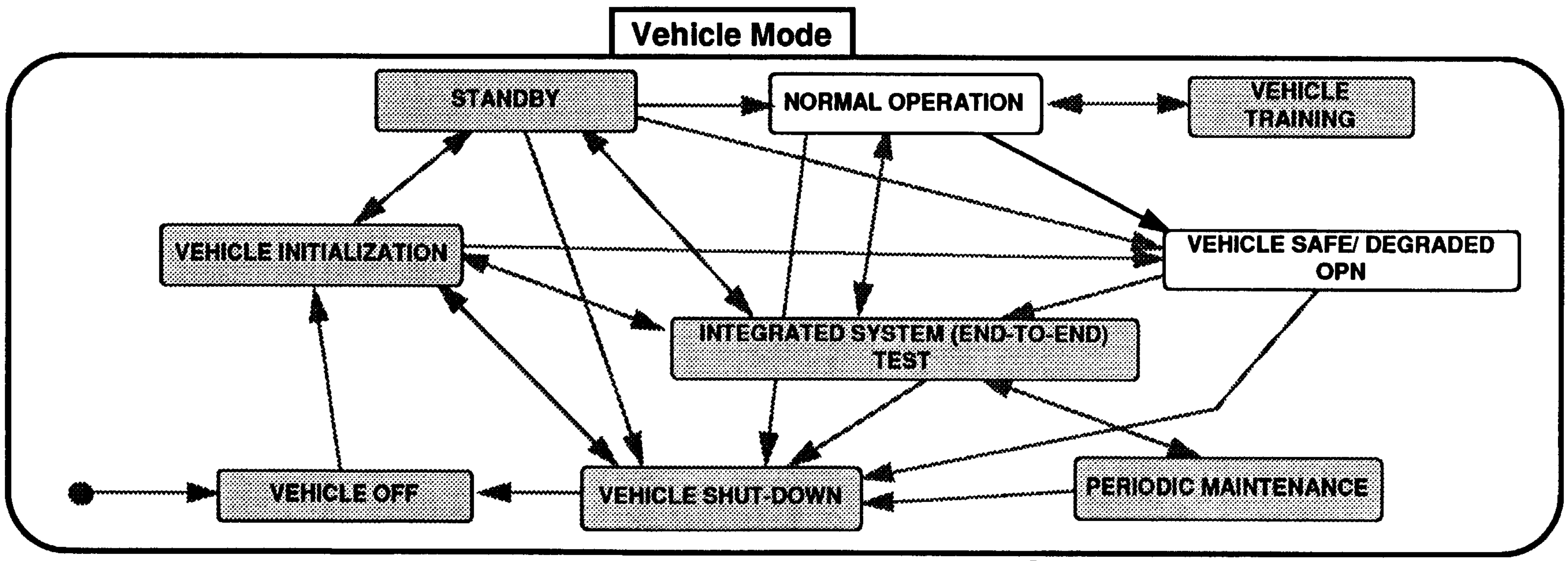
This mode is shown in Figure C-13. This mission mode can be commanded from the modes shown by the arrows in order to effect departure from orbit, with the objective of returning to the surface. Prior to orbit departure, the SOCS will issue commands to insert the spacecraft into a Lunar re-entry trajectory, which includes activation of the appropriate attitude controls, positioning the spacecraft for re-entry, and firing the engines. Following re-entry, the SOCS issues commands to activate landing radar, activates appropriate communications and location signals, and prepares the spacecraft as needed. These commands will as a minimum include solar panel and antenna adjustment/ejection (as needed), active ranging, commands to propulsion for thrust and attitude control to maintain the proper trajectory to reach the terminal area and/or landing site, and communicate telemetry. The FSS monitors and can send override and update commands. If an unrecoverable onboard failure is encountered, the SOCS will put the vehicle in the Vehicle Safe/Degraded Operation Vehicle Mode and execute pre-stored emergency/contingency alternatives. Deorbit mode ends when the spacecraft reaches the terminal area and begins to maneuver and prepare for touchdown. While FSS override can always be executed, there may not be sufficient time during this mode for safe implementation of real-time FSS commands; thus, pre-stored contingency commands must be available in the SOCS.

C.2.1.5 Landing Mission Mode

This mode is shown in Figure C-14. This mission mode can be commanded from the modes shown by the arrows in order to touch down on the surface. Prior to touch down, the SOCS will issue commands to prepare the spacecraft for a safe surface touch down, which includes activation of the appropriate attitude controls, positioning the spacecraft for touch down, and firing the engines. It also includes ranging on the landing site to assure appropriate and safe site terminal guidance can be effected. Following touch down, the SOCS issues commands to turn off and safe the engines, send the touch down telemetry and shut-down the avionics. These commands will as a minimum include solar panel and antenna deployment/adjustment (as needed), active ranging, commands to propulsion for thrust and attitude control to maintain the proper trajectory including touch down on the landing site, and communicate telemetry. The FSS monitors and can send override and update commands. If an unrecoverable onboard failure is encountered, the SOCS will put the vehicle in the Vehicle Safe/Degraded Operation Vehicle Mode and execute pre-stored emergency/contingency alternatives. While FSS override can always be executed, there may

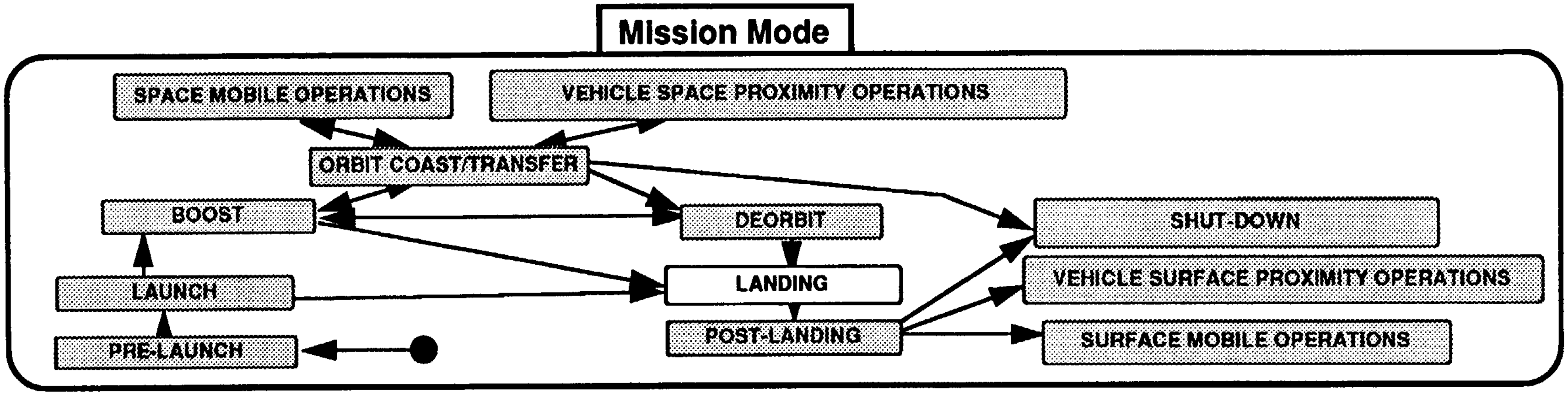


Note: Greyed out boxes de-emphasize other related modes.

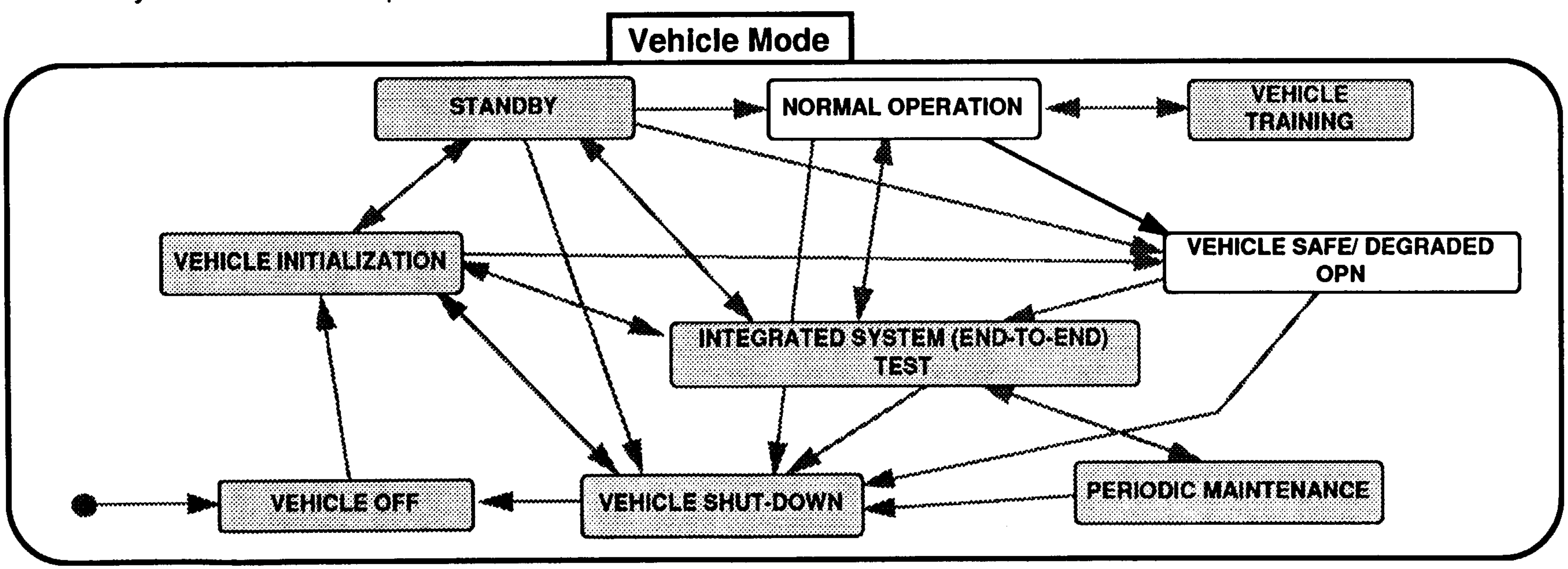


Greyed out boxes and lines inhibited from use

Figure C-13. Deorbit Mission and Vehicle Modes



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-14. Landing Mission and Vehicle Modes not be sufficient time during this mode for safe implementation of real-time FSS commands; thus, pre-stored contingency commands must be available in the SOCS.

C.2.2 STATES ALLOWED IN LAUNCH MISSION MODE

In the Launch Mission Mode, vehicle modes which can be utilized are Normal Operation, Vehicle Safe/Degrade Operation, Vehicle Shut-Down and Vehicle Off, as previously shown in Figure C-10. The other vehicle modes are not available because they could possibly allow hazardous operations to be carried out (for instance by transitioning to shut-down mode during launch after lift-off) or do not make sense (for instance using training mode during the busy launch period). The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

C.2.2.1 States for Standby Vehicle Mode

When the Standby Vehicle Mode is in effect, avionics states as previously shown in Figure C-6 may be entered in the Launch Mission Mode. This mode provides for vehicle behavior during the countdown before the computer systems are activated to control operations. These states are described below.

- ALL_OFF Avionics Subsystem State. Although the vehicle is in the Standby Vehicle Mode, there may be some avionics subsystems which are still powered down awaiting activation. The exit transition in this case would be caused by the SDSS or GSS generating a power on command to the component or subsystem which needs to be activated.

- START_SDSS Avionics Subsystem State. When a processing resource is added to the roster of operating SDSS components during the launch countdown, while the vehicle is in the Standby Vehicle Mode, the START_SDSS state ensures the component boots up as described in Section C.1.2.3.

- AV_CONFIG_&_INIT Avionics Subsystem State. After a new processing resource has been started during the countdown, this state configures and initializes it as was previously done for the Vehicle Initialization Mode in Section C.1.2.2 and described in Section C.1.2.3.

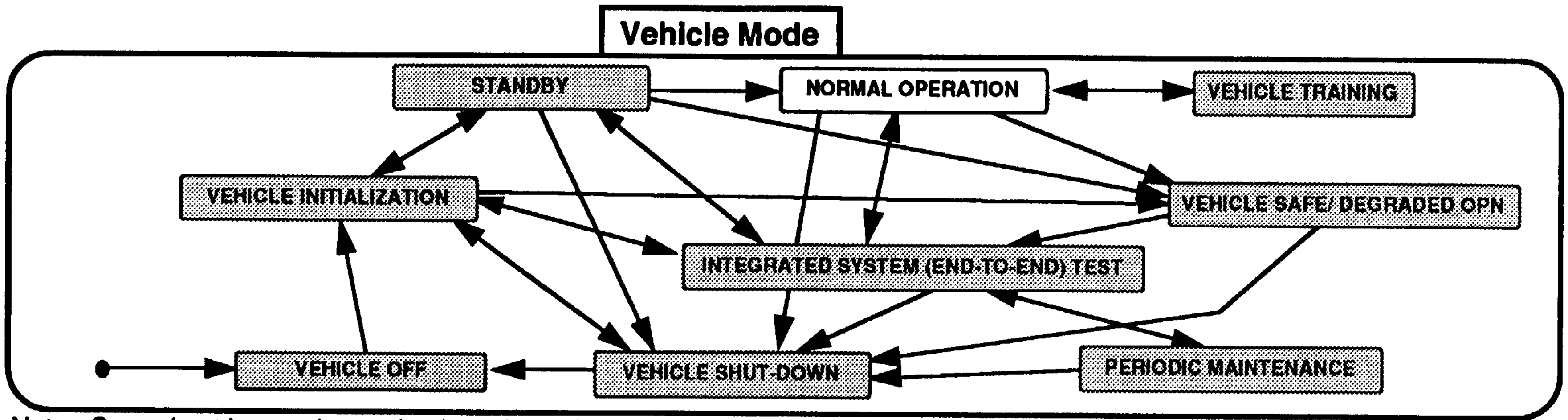
- AV_SUBSYS_STANDBY Avionics Subsystem State. This state is the normal state for most components while the Standby Vehicle Mode is in effect prior to entering the COMPUTER AIDED OPERATION Avionics Subsystem State during the countdown, similar to the description in Section C.1.2.3.

- MANUAL_OP Avionics Subsystem State. While the avionics are generally in a holding state, manual control of the system is always capable of being executed by the crew or GSS.
- AV_SUBSYS_SHUTDOWN Avionics Subsystem State. This state may be entered by a power off command for a specific component while in the Standby Vehicle Mode, either to turn it off (for instance to save power) or to force a re-start on the component (for instance to recover a failed or "confused" subsystem).

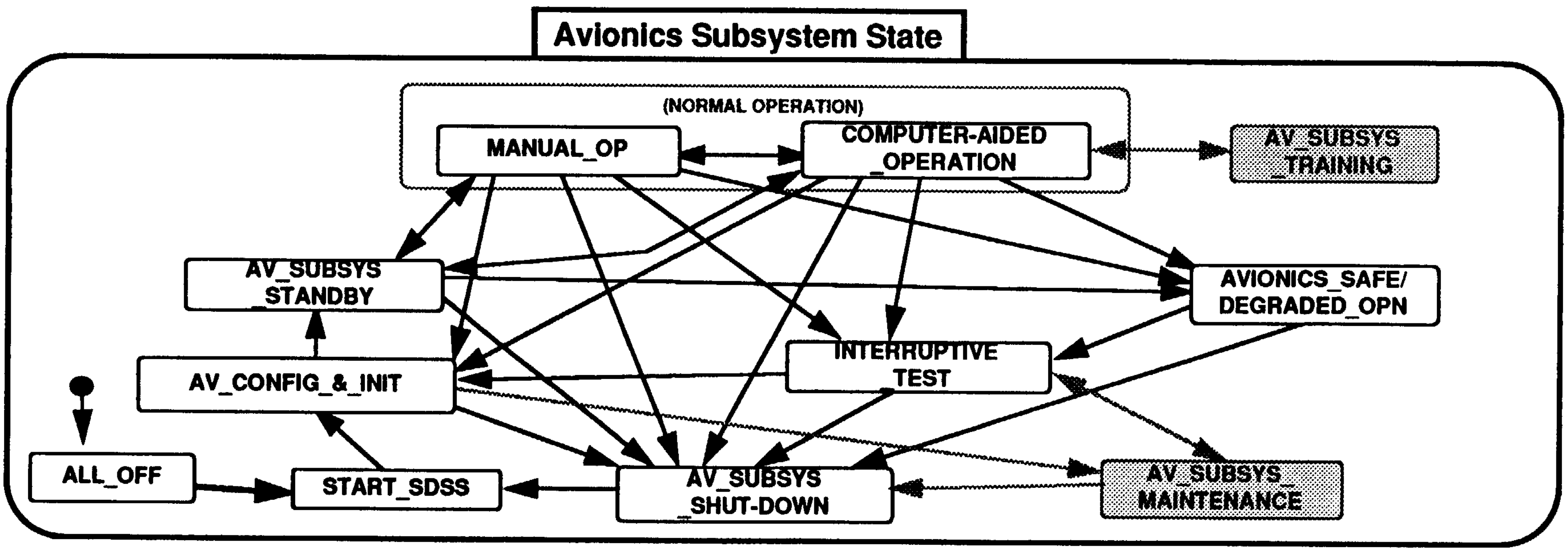
C.2.2.2 States for Normal Operation Vehicle Mode

When the Normal Operation Vehicle Mode is in effect, the avionics states shown in Figure C-15 (in black and white) may be entered in the Launch Mission Mode. These states are described below.

- ALL_OFF Avionics Subsystem State. While in Launch, Normal Operation mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state. Such resources are available if needed for backup and spares purposes. If a hot (i.e., currently running) backup running in standby state were to be selected for primary operation due to a failure, then a cold (i.e., not currently running and off) backup could be needed to be brought on-line to act as a new hot backup.
- START_SDSS Avionics Subsystem State. When a failure of a primary component requires either the hot backup become a primary resource or if there is no hot backup, then activation of cold spares may be needed. Such activation would require the data system to be booted on the processor, and the remaining data system components to be made aware of the "new" existence of such a component. This state includes commanding the power subsystem to apply power to the component, component response to the application of power, the POST of the component as it is powered up, and loading any related component data system software. This state also provides for cold restart after avionics shut-down, with just the SDSS boot routine running to re-boot the SDSS.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-15. Avionics Subsystem States Allowable in Normal Operation Vehicle Mode

- AV CONFIG & INIT Avionics Subsystem State. When new components are brought on-line during launch operations, this state establishes the configuration and initializes (or re-initializes) the components being started. Any external avionics needed to support the newly initialized or re-initialized component are POSTed and errors are handled.

- AV SUBSYS STANDBY Avionics Subsystem State. After new components have been initialized, they transition to standby to await direction for use, or to serve as hot backups as needed. Standby provides for the synchronization of data and timing, with CBIT and FDIR to keep a functional capability.

- MANUAL OP Avionics Subsystem State. In Launch, Normal Operation mode, it is assumed operations are automated. However, if necessary for human intervention, then this state provides for the system to monitor human actions to enable the system to operate in support of such actions.

- COMPUTER-AIDED OPERATION Avionics Subsystem State. This is the normal state for Launch mode operations. Entry takes place upon transition from the Pre-Launch Mission Mode to the Launch Mission Mode; the mission mode transition command, Start Launch Mission Mode, causes entry into the COMPUTER-AIDED_OPERATION state. Upon entry, fully automated launch operations begin and/or are supported from countdown start to through systems checks to engine ignition. (As the mission transitions from Launch Mission Mode to Boost Mission Mode at engine ignition, the avionics state remains in COMPUTER-AIDED_OPERATION.) Exit from this state in Launch Mission Mode occurs when a failure is identified and continuance of the mission is needed, requiring a switch to the AVIONICS_SAFE/DEGRADED_OPN state. Otherwise, the avionics may be commanded to change states to delay the countdown while interruptive tests, shut-down procedures, or re-configuration/re-initialization takes place. Standby may be directed to otherwise delay the countdown for non-avionics concerns. Of course, MANUAL_OP state override is always available.

- AVIONICS SAFE/DEGRADED OPN Avionics Subsystem State. While the vehicle is in the Launch Mission Mode (countdown is running), a failure may occur necessitating a decision on whether to continue to launch with the failure (that is, this usually means one less backup available). If the failure is sufficiently important (either in remaining backup capability, impact or potential consequence), then a safe or degraded operational state may be adopted to maximize remaining capability or the systems shut down. In the SAFE/DEGRADED OPERATIONS State (in the Normal Operation mode), all processing proceeds normally, but there is less backup capability, and the transition from COMPUTER-AIDED_OPERATION to AVIONICS_SAFE/DEGRADED_OPN is transparent to the crew and the mission. (This state is provided to recognize that the risk to the mission and vehicle has increased, but that full mission capability is still available.) The only possible exit from this state is to INTERRUPTIVE_TEST or AV_SUBSYS_SHUT-DOWN to ensure the system has recovered before operations continue.

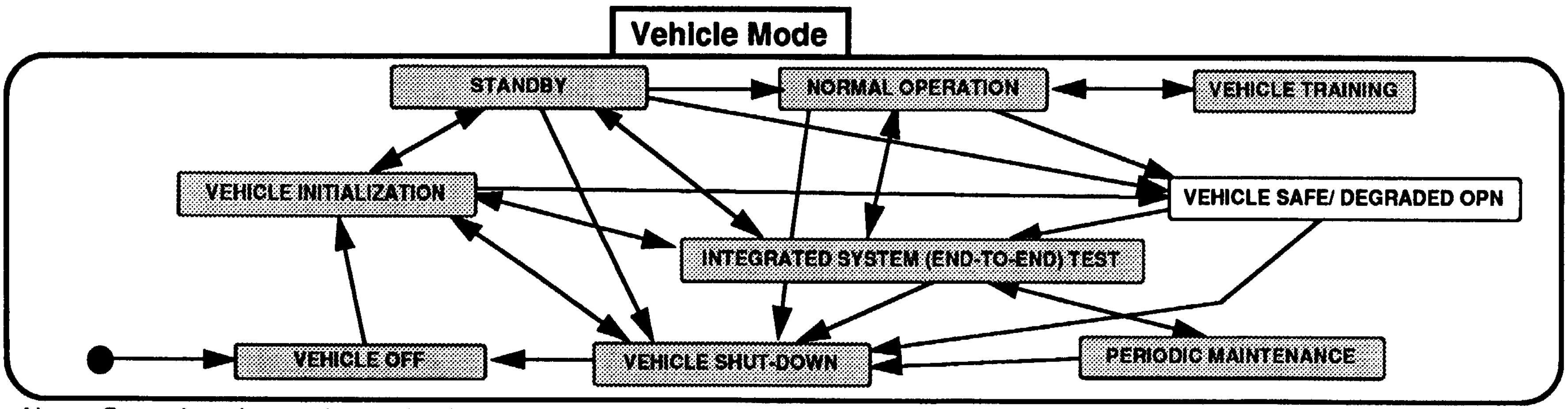
- INTERRUPTIVE_TEST Avionics Subsystem State. This state provides for a delay of the countdown to launch to perform tests which will interfere with normal avionics processing capability, either through the introduction of test data, use of special test programs, recording of special test results, activation of test switches in the flight hardware and/or software, etc. When this state is commanded, the specific test initial conditions to be executed must accompany the command. Exit from this state requires a return to the AV_CONFIG_&_INIT state to ensure all potentially damaging test residues have been cleared from the system, or a shut-down.

- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state is entered in Launch Mission Mode when the launch is aborted and the systems must be shut-down in an orderly manner. This state can also be entered if a cold restart of the avionics is desired to try and correct problems.

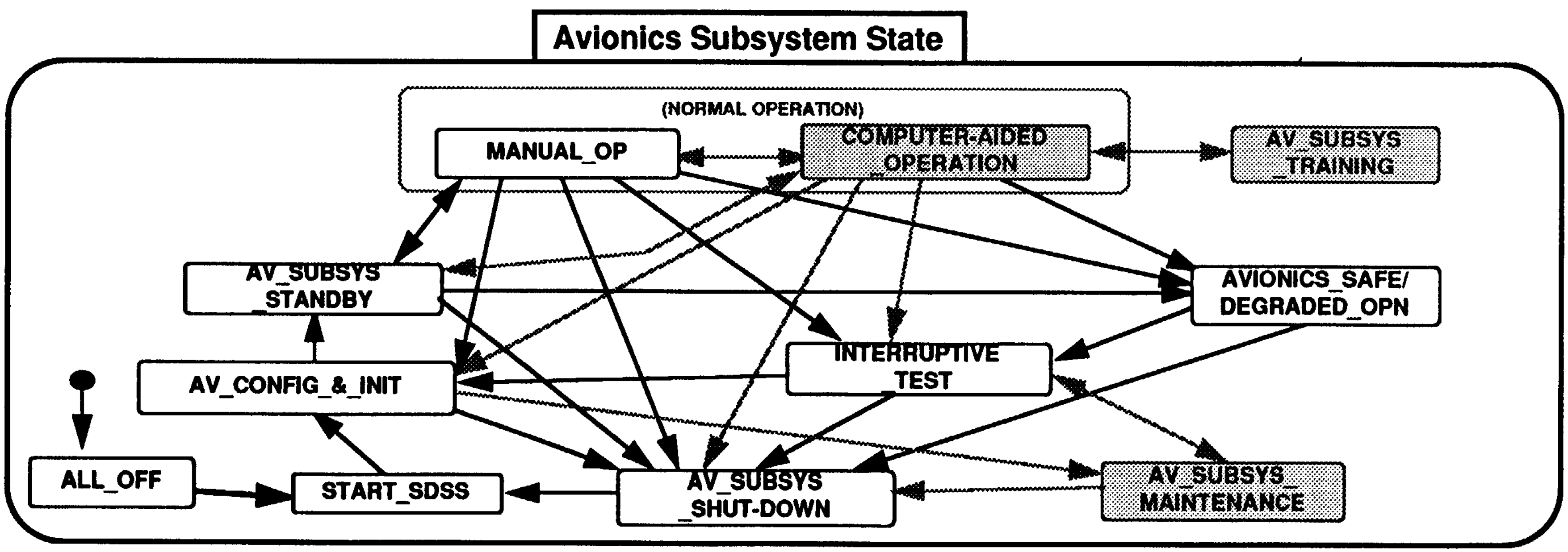
C.2.2.3 States for Vehicle Safe/Degraded Operation Vehicle Mode

When the Vehicle Safe/Degraded Operation Vehicle Mode is in effect during launch, the avionics states shown in Figure C-16 (in black and white) may be entered. It is the mode that the spacecraft will be put into by SOCS command when an anomaly occurs which is sufficiently severe that there may be potential impact on the mission. Such an anomaly cannot be treated by the systems (for instance by use of hot backups) in a manner which is transparent to the crew, FSS and mission operation. Consider a fault tolerant spacecraft data system with three primary computers and one backup computer. An example of such a severe anomaly occurs if the backup mission computer has previously failed, the mission was continued, and now one of the three primary mission computer fails under conditions such that the mission must proceed with no backup and missing one primary computer. In this case, mission safety is not at immediate risk, but continuance of the mission does place the vehicle at significantly increased risk since the ability to mask faults is severely limited with only two computers in the fault tolerant set. The spacecraft is put into this SAFE/DEGRADED OPERATION Mode by a command from the crew, onboard SOCS or the FSS. The spacecraft can only leave this mode by command from the crew or FSS. The only modes the spacecraft can transition to from this mode are the Vehicle Integrated System Test or Shut-down Vehicle Modes. In this Vehicle Safe/Degraded Operation Vehicle Mode, the SOCS command issued as a minimum will include communicate telemetry, attitude control and active ranging. The states are described below.

- ALL OFF Avionics Subsystem State. While in the Launch Mission Mode, some spare components may be made available for use under degraded conditions. This state provides for a power off condition while they are physically made available. Exit from this state occurs when a Power On command is issued for the components made available to the avionics.
- START SDSS Avionics Subsystem State. When a failed component which placed the mission at risk is replaced by spare components, and power is applied, then this state provides for activation of the newly available spares. Such activation will typically require data system booting of the processor and making the other data system components "aware" of the newly available components. This state may provide for issuance of the power on command to activate the new component. It will provide for performance of the component POST, and loading any related component software needed. This state also provides for a cold re-start after avionics shut-down, with just the SDSS boot routine running to re-boot the SDSS.
- AV CONFIG & INIT Avionics Subsystem State. When new components are brought on-line after a safe/degraded operations mode command, this state establishes the configuration and initializes (or re-initializes) the components being started. Any external avionics needed to support the newly initialized or re-initialized component are POSTed and errors are handled.
- AV SUBSYS STANDBY Avionics Subsystem State. After new components have been initialized, they transition to standby to await direction for use, or to serve as hot backups as needed. Standby provides for the synchronization of data and timing, with CBIT and FDIR to keep a functional capability.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-16. Avionics Subsystem States Allowable in Safe/Degraded Opn Vehicle Mode

- MANUAL_OP Avionics Subsystem State. In Launch, Safe/Degraded mode, it is assumed special launch procedures will be required and used. These will probably be human-intensive requiring extensive manual operation of switches. Some system monitoring of the human proceedings, and manual activation of selected automated routines will require close coordination and cooperation between systems and humans in FSS.
- AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State. In the Avionics Safe/Degraded Opn Vehicle Mode, this state is the normal state of operation. Special routines which may require more human support, but less processing resources, and special practices to maximize launch safety may be in place to enable the launch to take place despite significantly higher risks from insufficient backup devices or software. Special flight or mission critical system bypasses may be in effect and processing precedence will probably have been adjusted.
- INTERRUPTIVE_TEST Avionics Subsystem State. This state provides for special testing during a launch delay with severely degraded systems. After this testing which interrupts launch operations and system processing, the return path goes through either shut-down or reinitialization, which if successful means the mission controllers can take the vehicle out of the Vehicle Safe/Degraded Opn Vehicle Mode. Otherwise they must either fly in a degraded condition or abort the mission.
- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state is entered in the Launch Mission Mode when the launch is delayed to try a restart to clear a problem, or the launch is to be aborted.

C.2.2.4 States for Vehicle Shut-Down Vehicle Mode

When the Vehicle Shut-Down Vehicle Mode is in effect, the avionics subsystem states shown previously in Figure C-8 (in black and white) may be entered in the Launch Mission Mode. Vehicle Shut-Down mode may be preparatory to either turning the vehicle to the Vehicle Off mode or to the Vehicle Initialization mode (for instance, to re-initialize vehicle subsystems). Avionics subsystem states which may be entered include MANUAL_OP, COMPUTER-AIDED_OPERATION, AND AV_SUBSYS_SHUT-DOWN states, as described in Section C.1.2.5.

C.2.2.5 States for Vehicle Off Vehicle Mode

When the Vehicle Off Vehicle Mode is in effect, the only applicable avionics state is ALL_OFF, as previously shown in Figure C-4. In the Launch Mission Mode, this vehicle mode and state are entered when a decision is made to terminate the mission countdown and abort the launch. An external power off command signal must be issued by the GSS to fully power down the spacecraft. This transition cannot be created by the spacecraft SDSS (as noted by the lack of an arrow from shut-down to off modes), and described in Section C.1.2.1.

C.2.3 STATES ALLOWED IN BOOST MISSION MODE

In the Boost Mission Mode, vehicle modes which can be utilized are Normal Operation and Vehicle Safe/Degrade Operation, as previously shown in Figure C-11. The other vehicle modes are not available because they could possible allow hazardous conditions to be carried out (for instance by transitioning to shut-down mode during boost) or do not make sense (for instance using training mode during the program controlled boost period). The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

C.2.3.1 States for Normal Operation Vehicle Mode

When the Normal Operation Vehicle Mode is in effect, the avionics states previously shown in Figure C-15 (in black and white) may be entered in the Boost Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.2.

- ALL_OFF Avionics Subsystem State. While boosting in Normal Operation mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.
- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource, activation of spare units for use, or cold restart of avionics elements after an avionics shut-down.
- AV_CONFIG_&_INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during boost operations.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.

- MANUAL_OP Avionics Subsystem State. During boost Normal Operation mode, it is assumed operations are automated. However, if necessary for human intervention, then this state provides for the system to monitor human actions to enable the system to operate in support of such actions.

- COMPUTER-AIDED_OPERATION Avionics Subsystem State. This is the normal state for Boost Mode operations. Entry takes place upon transition from the Launch Mission Mode to the Boost Mission Mode; the mission mode transition command, Start Boost Mission Mode, causes entry into the COMPUTER-AIDED_OPERATION state. Upon entry, fully automated boost operations begin from engine ignition until orbital insertion. Exit from this state in Boost Mission Mode occurs when a failure is identified and continuance of the mission is needed, requiring a switch to the AVIONICS_SAFE/DEGRADED_OPN state. Otherwise, the avionics may not be commanded to change states under normal boost conditions. Of course, MANUAL_OP state override is always available to crew or FSS.

- AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State. While the vehicle is in the Boost Mission Mode (subsequent to engine ignition and liftoff), if a failure occurs, then a safe or degraded operational state must be adopted to maximize remaining capability. This state lasts in Normal Operation Vehicle Mode until either safe orbit is achieved or a decision (and subsequent actions) to abort is completed. In this state (in the Normal Operation mode), all processing proceeds normally, but there is less backup capability, and the transition from COMPUTER-AIDED_OPERATION to AVIONICS_SAFE/DEGRADED_OPN is transparent to the crew and the mission. (This state is provided to recognize that the risk to the mission and vehicle has increased, but that full mission capability is still available.) The only possible exit from this state is to INTERRUPTIVE_TEST or AV_SUBSYS_SHUT-DOWN to ensure the system has recovered before operations continue.

- INTERRUPTIVE_TEST Avionics Subsystem State. This state is a high risk alternative which may only be used during boost if high risk failures occur which require immediate resolution despite potential impact on boost operations. (It is assumed if the mission has already become very risky, but time is available to test problems, then the additional risk to perform tests which will interfere with normal avionics processing capability is not very significant. Such additional risk can possible reduce the mission risk if problems can be identified and resolved in real-time.) Exit from this state requires a return to the AV_CONFIG_&_INIT state to ensure all potentially damaging test residues have been cleared from the system, or a shut-down. Use of this state in boost should be accompanied by clear warnings about specific hazards which may be caused by its use.

- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state is entered in Boost Mission Mode when specific failed avionics must be powered down or cold restarted to try and correct problems. Use of this state may be hazardous, and should be hedged with cautions and double checks to ensure only components are shut-down which would be more hazardous if left operating.

C.2.3.2 States for Vehicle Safe/Degraded Vehicle Mode

When the Vehicle Safe/Degraded Operation Vehicle Mode is in effect during Boost Operation Mission Mode, the avionics states previously shown in Figure C-16 (in black and white) may be entered. It is the mode that the spacecraft will be put into by the onboard SOCS, crew or FSS command when an anomaly occurs which is sufficiently severe that there may be potential impact on the mission. Such an anomaly cannot be treated by the systems (for instance by use of hot backups) in a manner which is transparent to the crew, FSS and mission operation. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.3.

- ALL_OFF Avionics Subsystem State. While in the Boost Mission Mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.

- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource, activation of spare units for use, or cold restart of avionics elements after an avionics shut-down.

- AV_CONFIG_&_INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during boost operations.

- AV SUBSYS STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.
- MANUAL OP Avionics Subsystem State. While boost in Normal Operation mode is assumed to be automated, if sufficiently severe anomalies occur to force the onboard SOCS, crew or FSS to place the vehicle into Vehicle Safe/Degraded Opn Vehicle Mode, then manual control if a crew is onboard can be used to try and recover the mission. Thus, this state provides for the system to monitor human actions to enable the system to operate in support of such actions. The human actions may also command specific automated routines/programs to execute even though the avionics are not under full automated control.
- AVIONICS SAFE/DEGRADED OPN Avionics Subsystem State. In the Avionics Safe/Degraded Opn Vehicle Mode, this state is the normal state of operation. Special routines which may require more human support, but less processing resources, and special practices to maximize crew safety (if a crew is on board) may be in place to enable the boost to continue or to implement approved abort procedures.
- INTERRUPTIVE TEST Avionics Subsystem State. This state provides for special testing during a boost with severely degraded systems to determine how to protect the crew or mission. Use of this state in Boost Mission Mode and Vehicle Safe/Degraded Vehicle Mode will probably have significant impact on vehicle safety.
- AV SUBSYS SHUT-DOWN Avionics Subsystem State. This state is entered in the Boost Mission Mode when specific avionics are determined to be a cause of the problem, and it is determined that shutting down selected avionics is safer than allowing them to continue operating.

C.2.4 STATES ALLOWED IN ORBIT COAST/TRANSFER MISSION MODE

In the Orbit Coast/Transfer Mission Mode, all vehicle modes are available for use, as previously shown in Figure C-11. The following subsections identify the avionics subsystem states allowable in each vehicle mode.

C.2.4.1 States for Vehicle Off Vehicle Mode

When the Vehicle Off Vehicle Mode is in effect during orbit coast/transfer, the only applicable avionics state is ALL_OFF, as previously shown in Figure C-4. In Orbit Coast/Transfer Mission Mode, this vehicle mode and state are provided to enable FSS, onboard SOCS or the crew to turn off subsystems not needed for current mission operations. This mode may also be used to turn off all subsystems on the primary vehicle (completely) if needed for some purpose, although such action would apparently increase the risk to crew (if any) safety. Such subsystems may also need to be turned back on at a later time. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.1.2.1.

- ALL_OFF Avionics Subsystem State Entry. Entry into this state requires an external power off command signal to be activated by either crew or FSS to fully power down a spacecraft. As a safety precaution, SDSS and SOCS cannot issue such a command since it causes SDSS to fully shut-down with no power available for re-start (unless externally applied). Fully powering down the primary spacecraft would increase the hazard to crew safety due to the potential risk of being unable to restart the spacecraft, and thus should only be undertaken as an extreme measure.
- ALL_OFF Avionics Subsystem State Exit. Exit from this state requires application of external power, special battery operated non-avionics capability (such as a timer or external command operated switch), or physically switching the avionics on by a crew member. When power is applied, the vehicle mode changes, thus allowing the avionics state to change. When the Vehicle Off Vehicle Mode changes to the Vehicle Initialization Vehicle Mode, additional avionics states are allowed as described below.

C.2.4.2 States for Vehicle Initialization Vehicle Mode

When the Vehicle Initialization Vehicle Mode is used to start or restart a spacecraft, the avionics subsystem states previously shown in Figure C-5 (in black and white) may be entered while in the Orbit Coast/Transfer Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.1.2.2.

- ALL OFF Avionics Subsystem State. When the spacecraft first switches from the Vehicle Off to Vehicle Initialization Vehicle Modes, it starts off in the ALL_OFF Avionics Subsystem State. The power on command is applied with external or otherwise (as noted above) to cause the vehicle mode to switch and the ALL_OFF state to be exited.

- START SDSS Avionics Subsystem State. After applying powering to the avionics, the SDSS must be booted and the initial program load for the data system services, the command processor and the external avionics software must be done.
- AV CONFIG & INIT Avionics Subsystem State. After the avionics are started, then they must be setup for operation and initialized.
- AV SUBSYS STANDBY Avionics Subsystem State. After the avionics have initialized and are ready for operation, they must enter the standby state to ensure all subsystems are properly synchronized. The system remains quiescent and ready to implement subsequent mode commands.
- MANUAL OP Avionics Subsystem State. This state ensures that automatic processes do not work against the actions being manually carried out, and that the system monitors manual actions to maintain cognizance of their state and results. Manual control actions always have priority over other system functions. Potentially hazardous manual actions will cause an alert or caution to the crew and FSS.
- INTERRUPTIVE TEST Avionics Subsystem State. While the vehicle is initializing, interruptive test may be directed if testing more extensive than POST is needed.
- AV SUBSYS SHUT-DOWN Avionics Subsystem State. This state enables an orderly shut-down of avionics system elements.

C.2.4.3 States for Standby Vehicle Mode

When the Standby Vehicle Mode is in effect, avionics states as previously shown in Figure C-6 may be entered while in the Orbit Coast/Transfer Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.1.2.3.

- ALL OFF Avionics Subsystem State. In the Standby Vehicle Mode, this state provides controls over those avionics subsystems which are still powered down.

- START SDSS Avionics Subsystem State. This state provides the controls for component boot up when additional units are added to the system services. It also provides for rebooted or cold starting SDSS elements to improve system operability.
- AV CONFIG & INIT Avionics Subsystem State. After a new processing resource has been started, then this state provides controls to configure and initialize them.
- AV SUBSYS STANDBY Avionics Subsystem State. This state is the normal state for most components while the Standby Vehicle Mode is in effect. CBIT, FDIR and routine housekeeping SDSS processes will operate normally.
- MANUAL OP Avionics Subsystem State. While the avionics are generally in a holding state, manual control of the system is always capable of being executed by the crew or FSS.
- AV SUBSYS SHUTDOWN Avionics Subsystem State. This state provides for powering off specific components while in the Standby Vehicle Mode.

C.2.4.4 States for Integrated System Test Vehicle Mode

When the Integrated System (End-to-End) Test Vehicle Mode is in effect, the avionics subsystem states previously shown in Figure C-7 (in black and white) may be entered in the Orbit Coast/Transfer Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.1.2.4.

- ALL OFF Avionics Subsystem State. This state provides for control of specific test equipment as needed in end-to-end testing.
- START SDSS Avionics Subsystem State. This state provides controls for test equipment newly powered on to perform POST and download needed software.
- AV CONFIG & INIT Avionics Subsystem State. This state controls starting external test equipment and software, and configuring and initializing them for operation.
- AV SUBSYS STANDBY Avionics Subsystem State. This state causes the test subsystems to become quiescent until explicitly commanded to carry out specific directed actions.

- MANUAL OP Avionics Subsystem State. This state provides control to support manually operated test instrumentation and systems under test.
- COMPUTER-AIDED OPERATION Avionics Subsystem State. This state provides control for fully automatic operation of the test systems.
- INTERRUPTIVE TEST Avionics Subsystem State. This state provides controls over the specific tests to be executed and data to be recorded and/or analyzed.
- AV SUBSYS MAINTENANCE Avionics Subsystem State. This state provides controls for special maintenance equipment and programs.
- AV SUBSYS SHUT-DOWN Avionics Subsystem State. This state provides control to shut-down the test capability and the system under test, and reset avionics to normal avionics states.

C.2.4.5 States for Normal Operation Vehicle Mode

When the Normal Operation Vehicle Mode is in effect, the avionics states previously shown in Figure C-15 (in black and white) may be entered in the Orbit Coast/Transfer Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.2.

- ALL OFF Avionics Subsystem State. This state provides control over those avionics subsystems which are still in the ALL_OFF state.
- START SDSS Avionics Subsystem State. This state provides controls for starting or re-starting avionics while in orbit or transferring to another orbit.
- AV CONFIG & INIT Avionics Subsystem State. This state provides controls for configuring and initializing (or re-initializing) components being started.
- AV SUBSYS STANDBY Avionics Subsystem State. This state provides controls over avionics in a quiescent condition while they await direction for use.
- MANUAL OP Avionics Subsystem State. In Orbit Coast/Transfer, Normal Operation mode, this state provides controls to enable the systems to monitor human actions and to operate in support of such actions.
- COMPUTER-AIDED OPERATION Avionics Subsystem State. This is the normal state for orbiting station-keeping and house-keeping operations. It provides the controls to enable the spacecraft to operate safely and consistently

with the mission payload or science operations. It tracks crew activities and monitors critical systems and crew environments to ensure crew, vehicle and mission safety.

- AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State. This state provide control for responding to minor failures which can be handled transparently to the crew and mission (if in accordance with established practices). Normal processing with less backup can be accomplished. (This state is provided to recognize that the risk to the mission and vehicle has increased, but that full mission capability is still available.)
- INTERRUPTIVE_TEST Avionics Subsystem State. This state provides controls for tests which will interfere with normal avionics processing capability.
- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state provides controls to shut-down avionics systems in an orderly manner while in orbit or transferring orbital planes.

C.2.4.6 States for Vehicle Training Vehicle Mode

When the Vehicle Training Vehicle Mode is in effect, the avionics states shown in Figure C-17 (in black and white) may be entered in the Orbit Coast/Transfer Mission Mode. Training mode may only be used while in orbit coast (and not in orbit transfer) as a safety precaution. It is assumed a key part of the training system, will be simulations to enable crew members to refresh themselves on how subsystems work when not actually being used, and to try out alternative procedures for equipment to address new problems or conditions as directed by FSS. These states are described below.

- ALL_OFF Avionics Subsystem State. This state provides control over the training subsystems which start out in the ALL_OFF state. Upon command to enter Vehicle Training Vehicle Mode, the SOCS will issue the power on command for the training subsystem and ancillary equipment.
- START_SDSS Avionics Subsystem State. This state provides controls for starting service connections with the training subsystems and the SDSS while in orbit. This includes performing POST on the training equipment and loading special training software. This state also provides for cold restart of the avionics after training mode if needed to purge training data from the system.

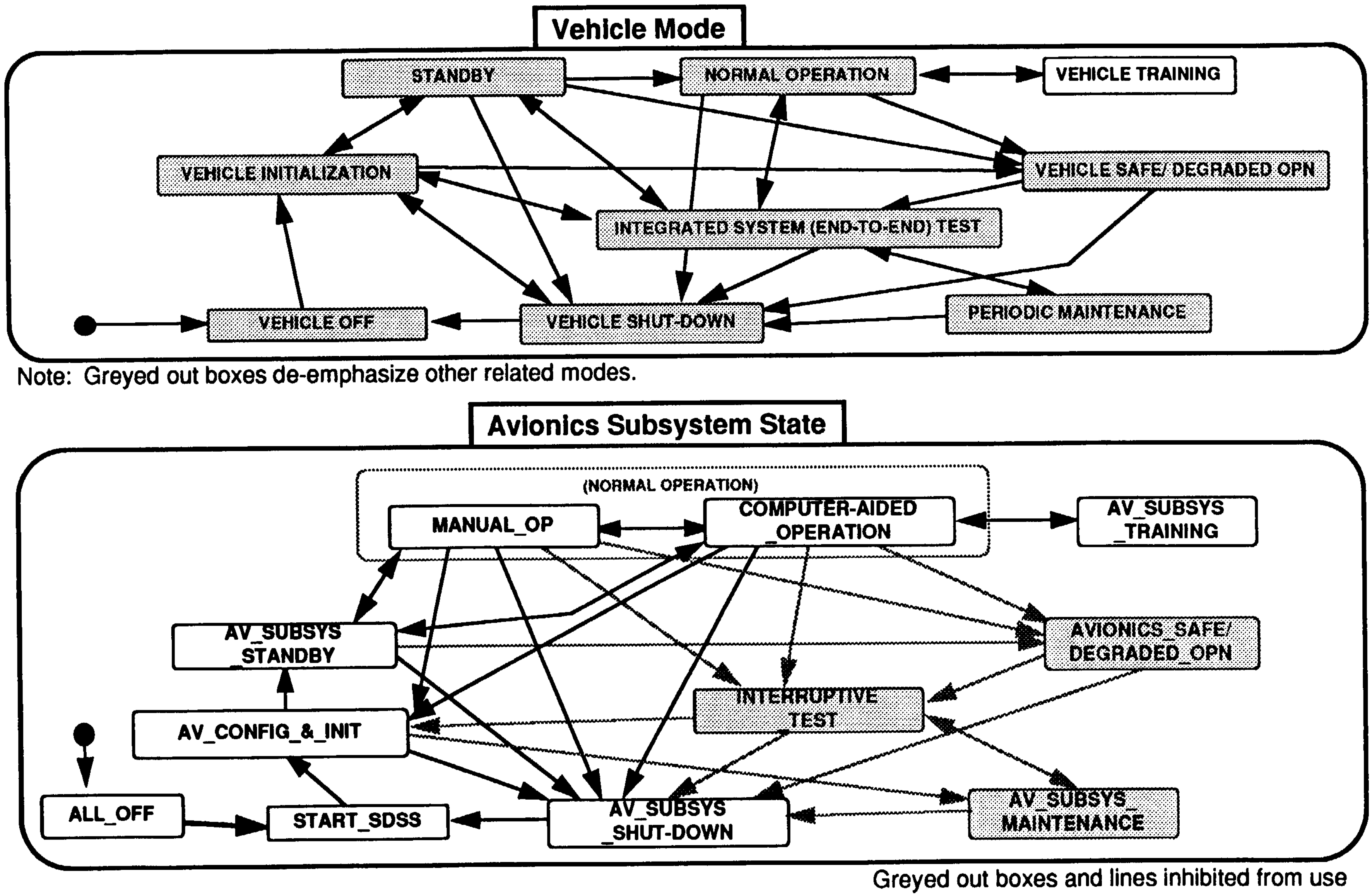


Figure C-17. Avionics Subsystem States Allowable in Vehicle Training Vehicle Mode

- AV_CONFIG & INIT Avionics Subsystem State. This state provides controls for configuring and initializing training components and software being started. Selection of equipment to be used for training is part of the configuration process. It includes setup up controls to ensure the training system can be unambiguously overridden by actual alerts and warnings if needed.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides controls over the training system when it must be placed in a quiescent condition while higher priority tasks interrupt, but termination of the training activities or the current training scenario is not desired.

- MANUAL_OP Avionics Subsystem State. In Orbit Coast/Transfer, Normal Operation mode, this state provides controls to enable the actual avionics systems to monitor human actions in training and in non-training operations, keep them separate and to support of both sets of actions.

- COMPUTER-AIDED_OPERATION Avionics Subsystem State. This provides the controls to enable all interfacing real avionics subsystems and the specialized training systems (controlled by AV_SUBSYS_TRAINING as described in the next paragraph) to interoperate. One essential capability in this state is for the controls to track and differentiate between "real" mission data and training data being used and exchanged with the training system. It provides the controls to enable the spacecraft to operate safely and consistently with the training activities as they (possibly) interact with the mission operational systems. It tracks crew activities and monitors critical systems and crew environments to ensure crew, vehicle and mission safety. This state also ensures that all training data, conditions, scenario residuals, and other avionics equipment are returned to an operational condition after the end of training.

- AV_SUBSYS_TRAINING Avionics Subsystem State. This state provides controls for the training equipment and programs which will be used. Training subsystems might include such capabilities as simulations to represent the appearance of mission system interfaces and their behavior, emulation's of real environmental conditions not currently available to crew operations, and interfaces to real avionics subsystems to enable their use for training (i.e., with much greater allowances for error, and recognition that the results are training data not to be confused with real mission operational data). Special training "instructor" programs, scoring programs, computer-aided instructional programs and pre-canned scenarios for learning special condition simulated experiences might be available. Entry into this state would be by execution of the Start Training Mode command. Exit from this state would be by the End Training State or End Training Mode commands. As shown in the diagram, this state must be ended to return to COMPUTER-AIDED_OPERATION before the system may actually be powered down.

- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state provides controls to shut-down the training system in an orderly manner while in orbit. A prerequisite to training power off is that COMPUTER-AIDED_OPERATION state has successfully purged all training residuals from the operational systems.

C.2.4.7 States for Vehicle Safe/Degraded Vehicle Mode

When the Vehicle Safe/Degraded Operation Vehicle Mode is in effect during Orbit Coast/Transfer Mission Mode, the avionics states previously shown in Figure C-16 (in black and white) may be entered. It is the mode that the spacecraft will be put into by the onboard SOCS, crew or FSS command when an anomaly occurs which is sufficiently severe that there may be potential impact on the mission. Such an anomaly cannot be treated by the systems (for instance by use of hot backups) in a manner which is transparent to the crew, FSS and mission operation. The states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.3.

- ALL_OFF Avionics Subsystem State. While in the Orbit Coast/Transfer Mission Mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.

- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource, activation of spare units for use, or cold restart of avionics elements after an avionics shut-down.

- AV_CONFIG_&_INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during orbit or orbital transfer operations.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.

- MANUAL OP Avionics Subsystem State. While orbit and coast operations do not usually endure stressful timelines, orbital transfer operations may have high priority systems operating either semi-automatically or fully-automatically. If sufficiently severe anomalies occur to force the onboard SOCS, crew or FSS to place the vehicle into Vehicle Safe/Degraded Opn Vehicle Mode, then manual control if a crew is present can be used to try and recover the mission. Thus, this state provides for the system to monitor human actions to enable the system to operate in support of such actions. The human actions may also command specific automated routines/programs to execute even though the avionics are not under full automated control.
- AVIONICS SAFE/DEGRADED OPN Avionics Subsystem State. In the Avionics Safe/Degraded Opn Vehicle Mode, this state is the normal state of operation. Special routines which may require more human support, but less processing resources, and special practices to maximize crew safety may be in place to enable the safe orbit or orbital transfer operations to continue or to implement approved abort procedures.
- INTERRUPTIVE TEST Avionics Subsystem State. This state provides for special testing during orbit or orbital transfer operations with severely degraded systems to determine how to protect the crew or mission. Use of this state in orbital transfer mission mode while in Vehicle Safe/Degraded Vehicle Mode will probably have significant impact on vehicle safety.
- AV SUBSYS SHUT-DOWN Avionics Subsystem State. This state is entered in the Orbit Coast/Transfer Mission Mode when specific avionics are determined to be a cause of the problem, and it is determined that shutting down selected avionics is safer than allowing them to continue operating.

C.2.4.8 States for Periodic Maintenance Vehicle Mode

When the Periodic Maintenance Vehicle Mode is in effect, the avionics states shown in Figure C-9 (in black and white) may be entered in the Orbit Coast/Transfer Mission Mode. Periodic maintenance is required when component anomalies or failures have occurred, or sufficient time has passed that equipment needs to be checked, and there is sufficient time in the mission schedule to pull and examine equipment. Note that although parts of the vehicle are undergoing periodic maintenance, since the mission is still underway in space, actual mission avionics activity for critical tasks such as life support and ground communications must continue. The states are described below.

- ALL_OFF Avionics Subsystem State. This state provides control over the special maintenance subsystems which start out in the ALL_OFF state. Upon command to enter Periodic Maintenance Vehicle Mode, the SOCS will issue the power on command for the maintenance subsystem and ancillary equipment.

- START_SDSS Avionics Subsystem State. This state provides controls for starting service connections with the maintenance subsystems and the SDSS while in orbit. If the mission mode in one of transferring to another orbit, periodic maintenance will be delayed until orbit coast is re-established. This includes performing POST on the maintenance equipment and loading special maintenance software. This state also provides for cold restart of the avionics after maintenance mode if needed to purge maintenance data from the system.

- AV_CONFIG_&_INIT Avionics Subsystem State. This state provides controls for configuring and initializing (or re-initializing) components being started. Selection of equipment to be used for maintenance or to undergo maintenance is part of the configuration process. It includes setup up controls to ensure the maintenance subsystem can be unambiguously overridden by actual alerts and warnings if needed. It also includes loading and unloading special maintenance versions of operational flight programs if needed.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides controls over the maintenance equipment when it must be placed in a quiescent condition while higher priority tasks interrupt, but termination of the maintenance activities or the current maintenance examination is not desired.

- MANUAL_OP Avionics Subsystem State. In Orbit Coast/Transfer, Normal Operation mode, this state provides controls to enable the actual avionics systems not in maintenance mode to monitor human actions in maintenance and in non-maintenance operations, keep them separate and to support both sets of actions.

- AV_SUBSYS_MAINTENANCE Avionics Subsystem State. This state provides controls for the maintenance equipment and programs which will be used. It is the normal state for this mode. Maintenance subsystems might include such capabilities as simulations to represent the appearance of mission system interfaces and their behavior, emulation's of real environmental conditions not currently available to crew operations, and interfaces to real avionics subsystems to enable their use in stimulating avionics being maintained. Entry into this state would be by execution of the Start Periodic Maintenance Mode command. Exit from this state would be caused by the End Maintenance Mode or End AV_SUBSYS_MAINTENANCE State commands, and result in transition to the AV_SUBSYS_SHUT-DOWN state.

- INTERRUPTIVE_TEST Avionics Subsystem State. This state provides controls for special maintenance tests needed. (It is presumed that many of these tests will interfere with normal avionics processing capability, which is acceptable in maintenance mode). It also provides for injection of special maintenance data (e.g., data with known results) into input ports on sensors and other devices.
- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state provides controls to shut-down maintenance subsystems in an orderly manner while in orbit. It provides for the orderly shut-down (and eventual restart) of avionics which may need to be removed for repair or have been repaired or need to be shut-down and restarted to purge confused state conditions.

C.2.4.9 States for Vehicle Shut-Down Vehicle Mode

When the Vehicle Shut-Down Vehicle Mode is in effect, the avionics subsystem states shown previously in Figure C-8 (in black and white) may be entered in the Orbit Coast/Transfer Mission Mode. Vehicle Shut-Down mode may be preparatory to either turning the vehicle to the Vehicle Off mode (if it is being placed in long term hibernation or storage) or to the Vehicle Initialization mode (for instance, to re-initialize vehicle subsystems on ancillary spacecraft). Avionics subsystem states which may be entered include MANUAL_OP, COMPUTER-AIDED_OPERATION, AND AV_SUBSYS_SHUT-DOWN states, as described in Section C.1.2.5.

C.2.5 STATES ALLOWED IN DEORBIT MISSION MODE

In the Deorbit Mission Mode, vehicle modes which can be utilized are Normal Operation and Vehicle Safe/Degrade Operation, as previously shown in Figure C-13. The other vehicle modes are not available because they could possible allow hazardous conditions to be carried out (for instance by transitioning to shut-down mode during engine firing or thrusting during deorbit) or do not make sense (for instance using training mode during the program controlled deorbit period). During the Deorbit Mission Mode, the SOCS (may be in response to crew inputs if a crew is onboard) or FSS will issue the command to maneuver, reconfigure for landing, jettison unneeded equipment (for example solar panels and spacecraft elements to remain in orbit), do deorbit burn and perform final preparations for powered descent. SOCS will issue the commands to control the spacecraft during powered descent. The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

C.2.5.1 States for Normal Operation Vehicle Mode

When the Normal Operation Vehicle Mode is in effect, the avionics states previously shown in Figure C-15 (in black and white) may be entered in the Deorbit Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.2.

- ALL_OFF Avionics Subsystem State. While thrusting in Normal Operation mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.
- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource, activation of spare units for use, or cold restart of avionics elements after an avionics shut-down.
- AV_CONFIG_&_INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during deorbit operations.
- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.
- MANUAL_OP Avionics Subsystem State. During deorbit Normal Operation mode, it is assumed operations are automated. However, if necessary for human intervention, then this state provides for the system to monitor human actions to enable the system to operate in support of such actions.
- COMPUTER-AIDED_OPERATION Avionics Subsystem State. This is the normal state for Deorbit Mode operations. Entry takes place upon transition from the Orbit Coast/Transfer or direct from Boost Mission Modes to the Deorbit Mission Mode; the mission mode transition command, Start Deorbit Mission

Mode, causes entry into the COMPUTER-AIDED_OPERATION state. Upon entry, fully automated deorbit operations begin from engine ignition until the spacecraft is ready to begin terminal area maneuvering (if any) or touchdown (whichever occurs sooner). Exit from this state in Deorbit Mission Mode occurs when a failure is identified and continuance of the mission is needed, requiring a switch to the AVIONICS_SAFE/DEGRADED_OPN state. Otherwise, the avionics may be not commanded to change states under normal deorbit conditions. Of course, MANUAL_OP state override is always available to crew or FSS.

- <u>AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State</u>. While the vehicle is in the Deorbit Mission and Normal Operation Vehicle Modes, if a failure occurs, then a safe or degraded operational state must be adopted to maximize remaining capability. This state lasts until either safe landing is achieved or a decision (and subsequent actions) to abort the deorbit (if possible) is completed. In this state (in the Normal Operation mode), all processing proceeds normally, but there is less backup capability, and the transition from COMPUTER-AIDED_OPERATION to AVIONICS_SAFE/DEGRADED_OPN is transparent to the crew and the mission. (This state is provided to recognize that the risk to the mission and vehicle has increased, but that full mission capability is still available.) The only possible exit from this state is to INTERRUPTIVE_TEST or AV_SUBSYS_SHUT-DOWN to ensure the system has recovered before operations continue.

- <u>INTERRUPTIVE_TEST Avionics Subsystem State</u>. This state is a high risk alternative which may only be used during deorbit if high risk failures occur which require immediate resolution despite potential impact on deorbit operations. (It is assumed if the mission has already become very risky, but time is available to test problems, then the additional risk to perform tests which will interfere with normal avionics processing capability is not very significant. Such additional risk can possible reduce the mission risk if problems can be identified and resolved in real-time.) Exit from this state requires a return to the AV_CONFIG_&_INIT state to ensure all potentially damaging test residues have been cleared from the system, or a shut-down. Use of this state in deorbit should be accompanied by clear warnings about <u>specific</u> hazards which may be caused by its use.

- AV_SUBSYS SHUT-DOWN Avionics Subsystem State. This state is entered in Deorbit Mission Mode when specific failed avionics must be powered down or cold restarted to try and correct problems. Use of this state may be hazardous, and should be hedged with cautions and double checks to ensure only components are shut-down which would be more hazardous if left operating.

C.2.5.2 States for Vehicle Safe/Degraded Vehicle Mode

When the Vehicle Safe/Degraded Operation Vehicle Mode is in effect during Deorbit Mission Mode, the avionics states previously shown in Figure C-16 (in black and white) may be entered. It is the mode that the spacecraft will be put into by the onboard SOCS, crew or FSS command when an anomaly occurs which is sufficiently severe that there may be potential impact on the mission. Such an anomaly cannot be treated by the systems (for instance by use of hot backups) in a manner which is transparent to the crew, FSS and mission operation. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.3.

- ALL_OFF Avionics Subsystem State. While in the Deorbit Mission Mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.
- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource, activation of spare units for use, or cold restart of avionics elements after an avionics shut-down.
- AV_CONFIG & INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during deorbit operations.
- AV_SUBSYS STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.
- MANUAL_OP Avionics Subsystem State. While deorbit in Normal Operation mode is assumed to be automated, if sufficiently severe anomalies occur to force the crew or FSS to place the vehicle into Vehicle Safe/Degraded Opn Vehicle Mode, then it is assumed only manual control can be used to try and recover the mission. Thus, this state provides for the system to monitor human actions to enable the system to operate in support of such actions. The human actions may

also command specific automated routines/programs to execute even though the avionics are not under full automated control.

- AVIONICS SAFE/DEGRADED OPN Avionics Subsystem State. In the Avionics Safe/Degraded Opn Vehicle Mode, this state is the normal state of operation. Special routines which may require more human support, but less processing resources, and special practices to maximize crew safety may be in place to enable the deorbit to continue or to implement approved abort procedures.

- INTERRUPTIVE TEST Avionics Subsystem State. This state provides for special testing during a deorbit with severely degraded systems to determine how to protect the crew or mission. Use of this state in Deorbit Mission Mode and Vehicle Safe/Degraded Vehicle Mode will probably have significant impact on vehicle safety.

- AV SUBSYS SHUT-DOWN Avionics Subsystem State. This state is entered in the Deorbit Mission Mode when specific avionics are determined to be a cause of the problem, and it is determined that shutting down selected avionics is safer than allowing them to continue operating.

C.2.6 STATES ALLOWED IN LANDING MISSION MODE

In the Landing Mission Mode, vehicle modes which can be utilized are Normal Operation and Vehicle Safe/Degrade Operation, as previously shown in Figure C-14. The other vehicle modes are not available because they could possible allow hazardous conditions to be carried out (for instance by transitioning to shut-down mode during engine firing during touchdown) or do not make sense (for instance using training mode during the program controlled touchdown period). On sensing the touchdown, the SOCS will issue commands to terminate thrust and transition into the Post Landing Mission Mode.

The following three phase landing scenario sequence was extracted from [KIL92].

- Phase 1 Braking: GN&C issues commands for full throttle from all eight engines and pitch of -15 degrees.

- Phase 2 Begin Pitchup and Thrust Reduction: GN&C issues commands for a 60 degree pitchup to vertical attitude at a 1.2 degrees per second rate, and reduces throttle by issuing commands to shut down pairs of engines very 20 seconds until only two engines are running for 25% of throttle.

- Phase 3 Final Vertical Descent Phase: The LVS is in a vertical attitude and the throttle is at 25%.

The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

C.2.6.1 States for Normal Operation Vehicle Mode

When the Normal Operation Vehicle Mode is in effect, the avionics states previously shown in Figure C-15 (in black and white) may be entered in the Landing Mission Mode. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.2.

- ALL_OFF Avionics Subsystem State. When landing in Normal Operation mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.

- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource during landing.

- AV_CONFIG_&_INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during landing operations.

- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.

- MANUAL_OP Avionics Subsystem State. During landing Normal Operation mode, it is assumed operations are automated. However, if necessary for human intervention, then this state provides for the system to monitor human actions to enable the system to operate in support of such actions.

- COMPUTER-AIDED_OPERATION Avionics Subsystem State. This is the normal state for Landing Mode operations. Entry takes place upon transition from the Deorbit or direct from Boost Mission Modes to the Landing Mission Mode; the mission mode transition command, Start Landing Mission Mode, causes entry into the COMPUTER-AIDED_OPERATION state. Upon entry, fully automated landing operations begin with terminal area maneuvering (if any) or touchdown (whichever occurs sooner) and end with completion of touchdown and systems safing. Exit from this state in Landing Mission Mode occurs when a failure is identified and continuance of the mission is needed, requiring a switch to the AVIONICS_SAFE/DEGRADED_OPN state. Otherwise, the avionics may be not commanded to change states under normal deorbit conditions. Of course, MANUAL_OP state override is always available to crew or FSS.

- AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State. While the vehicle is in the Landing Mission and Normal Operation Vehicle Modes, if a failure occurs, then a safe or degraded operational state must be adopted to maximize remaining capability. This state lasts until safe touchdown is completed. In this state (in the Normal Operation mode), all processing proceeds normally, but there is less backup capability, and the transition from COMPUTER-AIDED_OPERATION to AVIONICS_SAFE/DEGRADED_OPN is transparent to the crew and the mission. (This state is provided to recognize that the risk to the mission and vehicle has increased, but that full mission capability is still available.) The only possible exit from this state is to INTERRUPTIVE_TEST or AV_SUBSYS_SHUT-DOWN to ensure the system has recovered before operations continue.

- INTERRUPTIVE_TEST Avionics Subsystem State. This state is a high risk alternative which may only be used during landing if high risk failures occur which require immediate resolution despite potential impact on landing operations. (It is assumed if the mission has already become very risky, but time is available to test problems, then the additional risk to perform tests which will interfere with normal avionics processing capability is not very significant. Such additional risk can possible reduce the mission risk if problems can be identified and resolved in real-time.) Exit from this state requires a return to the AV_CONFIG_&_INIT state to ensure all potentially damaging test residues have been cleared from the system, or a shut-down. Use of this state in landing should be accompanied by clear warnings about specific hazards which may be caused by its use.

- AV_SUBSYS_SHUT-DOWN Avionics Subsystem State. This state is entered in Landing Mission Mode when specific failed avionics must be powered down or the mission has ended and touchdown has been completed. Use of this state may be hazardous, and should be hedged with cautions and double checks to ensure only components are shut-down which would be more hazardous if left operating.

C.2.6.2 States for Vehicle Safe/Degraded Vehicle Mode

When the Vehicle Safe/Degraded Operation Vehicle Mode is in effect during Landing Mission Mode, the avionics states previously shown in Figure C-16 (in black and white) may be entered. It is the mode that the spacecraft will be put into by the onboard SOCS, crew or FSS command when an anomaly occurs which is sufficiently severe that there may be potential impact on the mission. Such an anomaly cannot be treated by the systems (for instance by use of hot backups) in a manner which is transparent to the crew, FSS and mission operation. These states are addressed below. Detailed descriptions of the following states were previously provided in Section C.2.2.3.

- ALL_OFF Avionics Subsystem State. While in the Landing Mission Mode, some of the avionics subsystems not immediately needed may be in the ALL_OFF state.
- START_SDSS Avionics Subsystem State. This state provides for converting a hot backup into a primary resource, activation of spare units for use, or cold restart of avionics elements after an avionics shut-down.
- AV_CONFIG_&_INIT Avionics Subsystem State. This state enables the configuration and initialization (or re-initialization) of components being started during landing operations.
- AV_SUBSYS_STANDBY Avionics Subsystem State. This state provides for operating components to remain in a quiescent condition utilizing minimum power until they need to transition to active use.
- MANUAL_OP Avionics Subsystem State. While landing in Normal Operation mode is assumed to be automated, if sufficiently severe anomalies occur to force the onboard SOCS, crew or FSS to place the vehicle into Vehicle Safe/Degraded Opn Vehicle Mode, manual control can be used to try and recover the mission. Thus, this state provides for the system to monitor human actions to enable the system to operate in support of such actions. The human actions may also command specific automated routines/programs to execute even though the avionics are not under full automated control.

- AVIONICS SAFE/DEGRADED OPN Avionics Subsystem State. In the Avionics Safe/Degraded Opn Vehicle Mode, this state is the normal state of operation. Special routines which may require more human support, but less processing resources, and special practices to maximize crew safety may be in place to enable the landing to continue.
- INTERRUPTIVE TEST Avionics Subsystem State. This state provides for special testing during a landing with severely degraded systems to determine how to protect the crew or mission. Use of this state in Landing Mission Mode and Vehicle Safe/Degraded Vehicle Mode will probably have significant impact on vehicle safety.
- AV SUBSYS SHUT-DOWN Avionics Subsystem State. This state is entered in the Landing Mission Mode when specific avionics are determined to be a cause of the problem, and it is determined that shutting down selected avionics is safer than allowing them to continue operating or touchdown has been completed.

C.3 TERMINAL MISSION PHASE MODES AND STATES ALLOWED

The Terminal Mission Phase consists of those vehicle modes in which the spacecraft has landed and the crew are conducting mission, science or payload operations on the surface after a successful landing (presumably on the moon or another planet).

C.3.1 MODES ALLOWED IN THE TERMINAL MISSION PHASE

The mission modes in this phase are the Post-Landing and Shut-Down Mission Modes. During each of these mission modes, the vehicle can be put into the vehicle modes identified below within each mission mode. (The Vehicle Surface Proximity Operations and Surface Mobile Operations modes are not addressed in this scenario.)

C.3.1.1 Post Landing Mission Mode

This mode is shown in Figure C-18. It begins after touchdown and spacecraft safing. In this mode, the SOCS, crew, FSS and spacecraft systems prepare the spacecraft to be able to support science and payload operations to the extent consistent with mission requirements. This mode can only be entered from the Landing Mission Mode. While a spacecraft on another planetary body may be able to return to Earth, the activities leading to Earth return

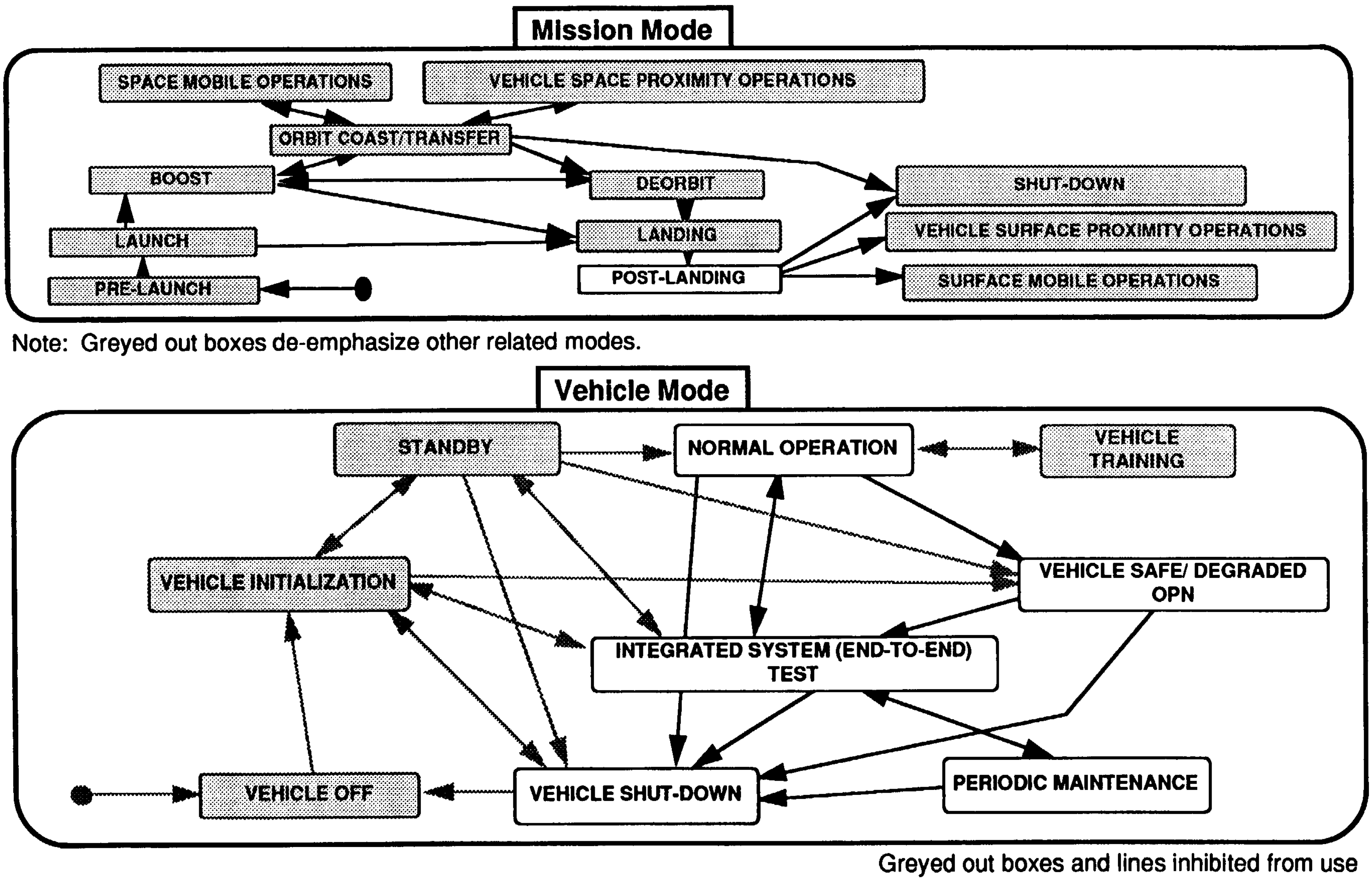


Figure C-18. Post-Landing Mission and Vehicle Modes are treated (for the purposes of this paper) as another mission with a full pre-launch to landing cycle of its own.

C.3.1.2 Shut-Down Mission Mode

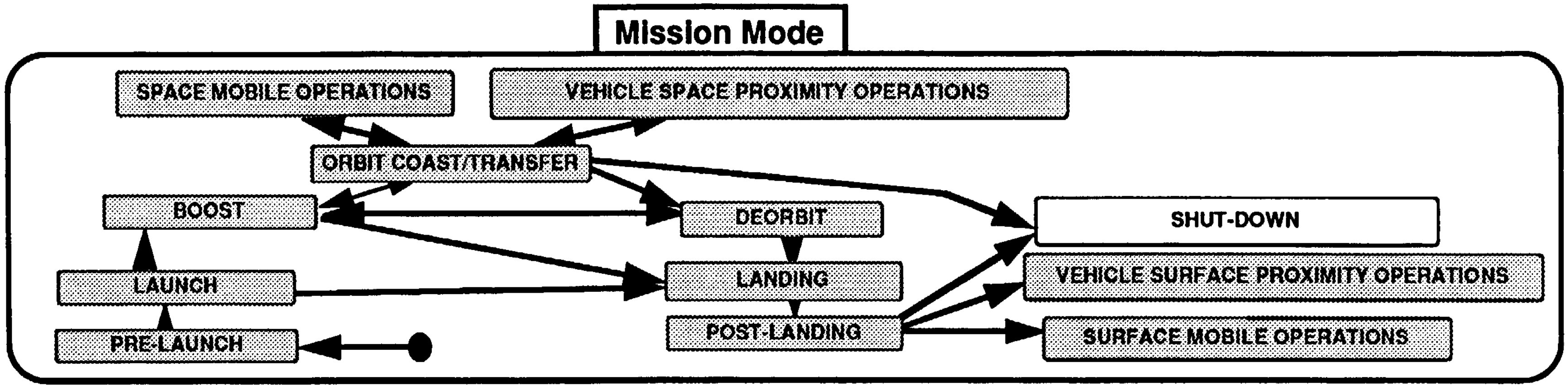
This mode is shown in Figure C-19. It begins after the spacecraft has been prepared or configured for science and payload operations. For missions which have landed on other planetary bodies, this mode shuts down the spacecraft systems not needed to perform crew life support and mission support for science and payload operations. (It is assumed for this paper's scenario and required for the Artemis scenario that systems support for such operations are handled by independent systems not integrated into the spacecraft systems.) This mode ends when the Pre-Launch Mode cycle starts to prepare the mission for return to Earth. For a mission which has returned to Earth, the Shut-Down Mission mode provides the controls to safely end spacecraft avionics processing, download data and materials to FSS, and enable the crew to depart the spacecraft safely.

C.3.2 STATES ALLOWED IN POST-LANDING MISSION MODE

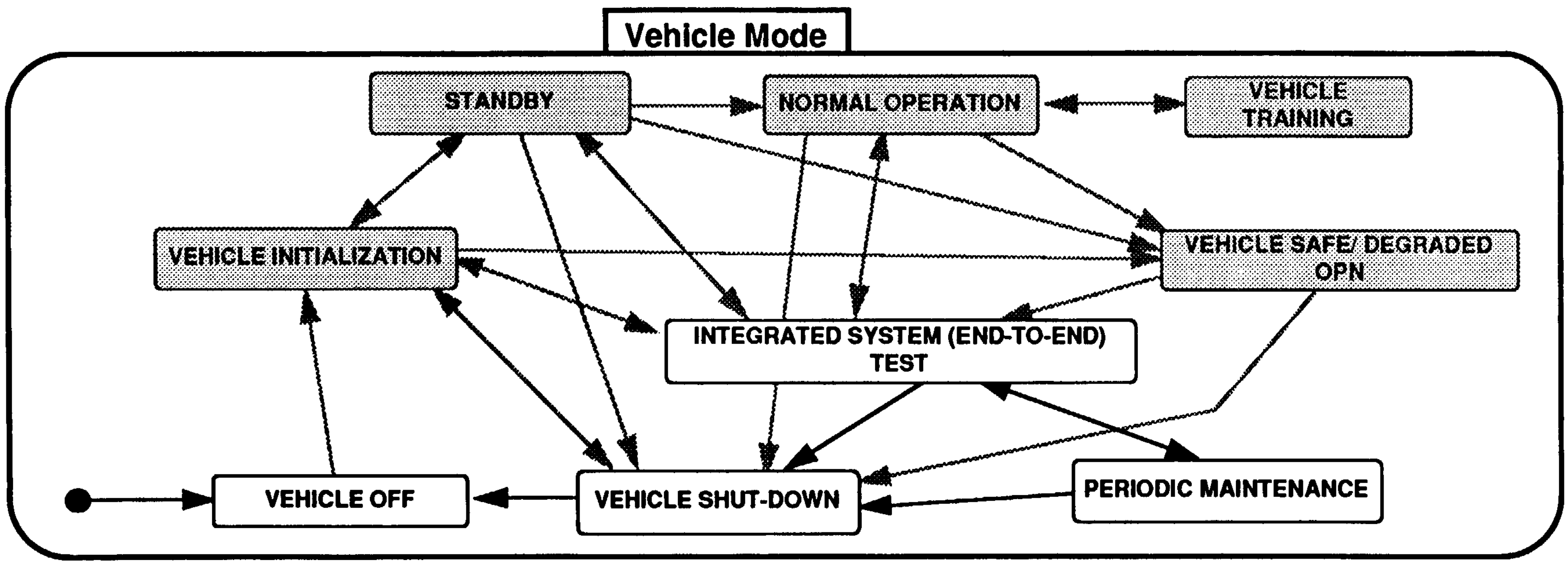
In the Post-Landing Mission Mode, vehicle modes which can be utilized are Normal Operation, Vehicle Safe/Degraded Operation, Integrated System Test, Periodic Maintenance, and Vehicle Shut-Down, as previously shown in Figure C-18. When the Post-Landing Mission Mode is entered, it must transition from either the Normal Operation or Vehicle Safe/Degraded Operation Vehicle modes, since only these modes are available from the Landing Mission Mode. Exit from the Post-Landing Mission mode is as shown in Figure C-18. While landed on another planetary body, exit from the Post-Landing Mission Mode would probably not allow a transition to the Shut-Down Mission Mode, but would include a return to the Pre-Launch Mission Mode (not shown in Figure C-18) to return to the Earth. The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

C.3.2.1 States for Normal Operation Vehicle Mode

When the Normal Operation Vehicle Mode is in use, the avionics states previously shown in Figure C-15 (in black and white) may be entered in the Post-Landing Mission Mode. These states were previously described in Section C.2.2.2. Normal operation is concerned with providing the post-landing support needed on another planetary body to enable the crew to survive and/or to support the mission's science and payload processing systems.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-19. Shut-Down Mission and Vehicle Modes

On Earth, normal operation is concerned with enabling the vehicle to returned to its post-mission processing facility. This vehicle mode is entered from the Landing Mission Mode's Normal Operation Vehicle Mode and exited as shown in Figure C-15.

C.3.2.2 States for Vehicle Safe/Degraded Operation Vehicle Mode

When the Vehicle Safe/Degraded Operation Vehicle Mode is in effect during post-landing, the avionics states previously shown in Figure C-16 (in black and white) may be entered. These states were previously described in Section C.2.2.3. This mode is also concerned with providing the post-landing support needed on another planetary body to enable the crew to survive and support the mission's science and payload processing systems after a severe anomaly has occurred. On Earth, vehicle safe/degraded operation is concerned with enabling the vehicle to returned to its post-mission processing facility despite the severe anomaly. (Recall that an anomaly which requires the onboard SOCS, crew or FSS to place the entire vehicle into Vehicle Safe/Degraded Operation Vehicle mode is caused by a problem beyond the capacity of the avionics to respond in a manner transparent to vehicle operation.) This vehicle mode is entered either from the Landing Mission Mode's Vehicle Safe/Degraded Operation Vehicle Mode or from the Post-Landing Mission Mode's Normal Operation Vehicle Mode if the severe anomaly occurs after touchdown. It is exited as shown in Figure C-15.

C.3.2.3 States for Integrated System Test Vehicle Mode

When the Integrated System (End-to-End) Test Vehicle Mode is in effect, the avionics subsystem states previously shown in Figure C-7 (in black and white) may be entered in the Post-Landing Mission Mode. These states were previously described in Section C.1.2.4. This mode is concerned with supporting any extensive testing that may be desired by crew or FSS after touchdown to identify and resolve any anomalies that cannot wait for identification and resolution in the Kennedy Space Flight Center's (KSFC) operations analysis after the mission's return to KSFC. This mode is entered and exited as shown in Figure C-7.

C.3.2.4 States for Periodic Maintenance Vehicle Mode

When the Periodic Maintenance Vehicle Mode is in effect, the avionics subsystem states previously shown in Figure C-9 (in black and white) may be entered in the Post-Landing Mission Mode. These states were previously described in Sections C.1.2.6 and C.2.4.8. This mode is concerned with providing the controls to support the crew or FSS as they work on identifying and resolving accumulated anomalies (primarily while landed on other planetary bodies). Since the vehicle is assumed to be landed on another planetary body for this periodic maintenance, critical tasks such as life support or communications to payloads for science mission support must continue. This mode is entered and exited as shown in Figure C-9.

C.3.2.5 States for Vehicle Shut-Down Vehicle Mode

When the Vehicle Shut-Down Vehicle Mode is in effect, the avionics subsystem states shown previously in Figure C-8 (in black and white) may be entered in the Post-Landing Mission Mode. These states were previously described in Section C.1.2.5. This mode is concerned with providing the controls to safely shut-down the avionics not needed for critical crew or FSS support tasks, and not needed to support payload and science operations processing while landed on another planetary body. On Earth, this mode provides for controls to minimally operate avionics needed (for example to download mission tapes and maintenance data logs) until FSS is ready to order avionics to be fully shut-down.

C.3.3 STATES ALLOWED IN SHUT-DOWN MISSION MODE

In the Shut-Down Mission Mode, vehicle modes which can be utilized are Integrated System Test, Periodic Maintenance, Vehicle Shut-Down and Vehicle off, as previously shown in Figure C-19. This mode would probably only be available to a spacecraft landed on Earth and the crew are preparing to depart from the vehicle, a spacecraft that will remain on another planetary body and its mission is complete, or a spacecraft in Orbit Coast Mission Mode that has completed its mission. The following subsections identify the avionics subsystem states allowable in each of these vehicle modes.

C.3.3.1 States for Integrated System Test Vehicle Mode

When the Integrated System (End-to-End) Test Vehicle Mode is in effect, the avionics subsystem states previously shown in Figure C-7 (in black and white) may be entered in the Shut-Down Mission Mode. These states were previously described in Section C.1.2.4. This mode is concerned with continuing Post-Landing testing or supporting any other extensive testing that may be desired by crew or FSS prior to turning the vehicle off. While this mode can be used on Earth to identify and resolve any anomalies in the KSFC operations analysis after the mission's return to KSFC, it is assumed this is not a primary purpose of this mode. It is entered and exited as shown in Figure C-7.

C.3.3.2 States for Periodic Maintenance Vehicle Mode

When the Periodic Maintenance Vehicle Mode is in effect, the avionics subsystem states previously shown in Figure C-9 (in black and white) may be entered in the Shut-Down Mission Mode. These states were previously described in Sections C.1.2.6 and C.2.4.8. This mode is concerned with providing the controls to support the crew or FSS as they work on identifying and resolving accumulated anomalies (primarily while landed on other planetary bodies). Since the vehicle is assumed to be landed on another planetary body for this periodic maintenance, critical tasks such as life support or communications to payloads for science mission support must continue. This mode is entered and exited as shown in Figure C-9.

C.3.3.3 States for Vehicle Shut-Down Vehicle Mode

When the Vehicle Shut-Down Vehicle Mode is in effect, the avionics subsystem states shown previously in Figure C-8 (in black and white) may be entered in the Shut-Down Mission Mode. These states were previously described in Section C.1.2.5. This mode is concerned with providing the controls to safely shut-down the avionics after the vehicle has returned to Earth. It provides for controls to minimally operate avionics needed (for example to download mission tapes and maintenance data logs) until FSS is ready to order avionics to be fully powered down.

C.3.3.4 States for Vehicle Off Vehicle Mode

When the Vehicle Off Vehicle Mode is in effect, the only applicable avionics state is ALL_OFF, as previously shown in Figure C-4. In the Shut-Down Mission Mode, this vehicle mode and state are entered when a decision is made to terminate the mission and no further avionics processing is needed. An external power off command signal must be issued by the FSS to fully power down the spacecraft. This transition cannot be created by the spacecraft SDSS (as noted by the lack of an arrow from shut-down to off modes), and is described in Section C.1.2.1.

C.5 AVIONICS SUBSYSTEM STATES AND SDSS FUNCTION STATES ALLOWED

Function states describe the control of the major functional service entities within an avionics subsystem. Only the SDSS avionics subsystem functional service entities are addressed in this document in accordance with the objectives of this modeling effort.

However, the analysis is expandable to address service functions for other avionics subsystems. As previously shown in figure B-2 and as described in paragraph B.1, the SDSS functional service entities are the DSM, NSM, OS, DBM and the IOSM. Regardless of the mission mode, vehicle mode, or avionics state, any interaction within the system in other than OFF modes or states will require support from the SDSS service functional entities.

Each SDSS functional state defines a boundary of allowable SDSS functional behavior. Each state encompasses the set of commands, controls, events, conditions and procedures needed to safely operate the SDS in a stable manner. The transitions from one state to another establish how the SDSS functional entities transition from one stable set of processes and table look up tables to another. For instance, "Full Service Operation" state establishes the allowable conditions for normal calls to services such as Data Base Write, while a state such as "Scheduled Testing" calls up the controls needed for specific built-in tests such as memory self-test to be run.

The availability of each SDSS functional state depends upon the Avionics Subsystem States in effect, since the avionics states control the behavior of the SDSS as it support external activities. Note that the action of any specific state may vary depending upon which mission and vehicle modes are in effect at the time the state is entered. The following subsections identify all the combinations of allowable avionics and SDSS functional states.

C.5.1 SDSS FUNCTION STATES ALLOWED IN ALL_OFF AVIONICS SUBSYSTEM STATE

In the ALL_OFF Avionics Subsystem State, SDSS Functional States which can be utilized are none, as shown in Figure C-20. If the avionics are off, as previously described in Section C.1.2.1, then the SDSS has no applicable states because it takes an external power signal or command to start the bootup process. The default entry into an operable SDSS is the SDSS_LOADED state which occurs after a vehicle mode change out of the Vehicle Off Vehicle Mode as described in Section C.1.2.1.

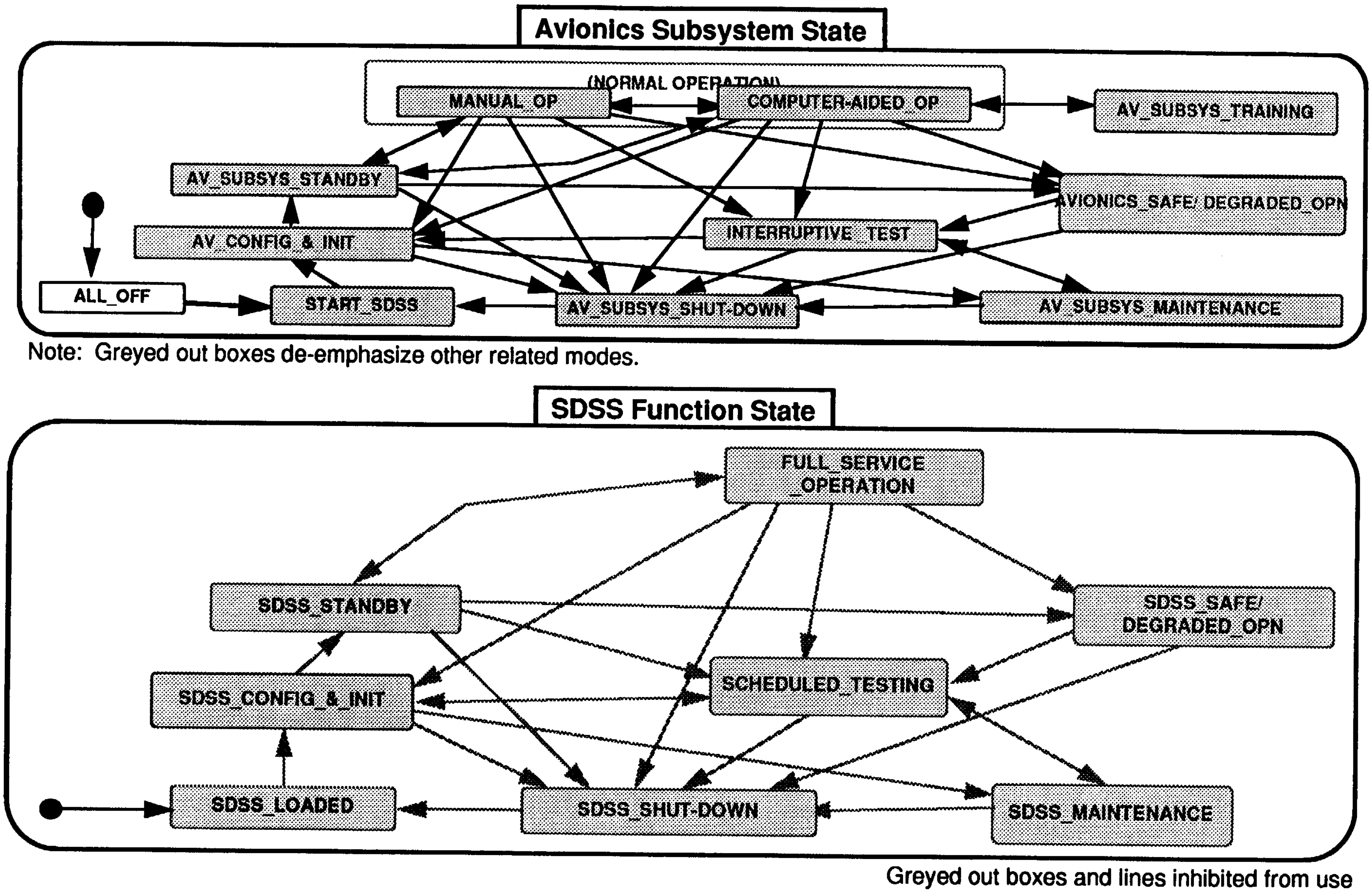


Figure C-20. SDSS Function States Allowable in ALL_OFF Avionics Subsystem State

C.5.2 SDSS FUNCTION STATES ALLOWED IN START_SDSS AVIONICS SUBSYSTEM STATE

In the START_SDSS Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-21. The default entry into an operable SDSS is the SDSS_LOADED state which occurs after a vehicle mode change out of the Vehicle Off Vehicle Mode as described in Section C.1.2.2. The SDSS Functional States are described below.

- SDSS LOADED SDSS Functional State. When the mission mode changes to cause the START_SDSS Avionics Subsystem State to execute, this executes the power-up process by booting the SDSS loader, loading the SDSS initial program code, and executing the SDSS startup program. The SDSS_LOADED state is in effect while the SDSS is booting and loading, performing the POST for the SDSS processors, and ensures that all SDSS linkages are working. This includes capabilities to cold start (start from an initial services power off condition but boot program still loaded) and warm start (start services by reloading the services except for the OS which continues to execute). This state is exited when the SDSS indicates that it is loaded and ready for configuration to the mission and vehicle.

- SDSS CONFIG & INIT SDSS Functional State. While in the START_SDSS Avionics Subsystem State, after the SDSS has successfully loaded, it must be tailored to the mission and vehicle to be supported. This state provides that the SDSS configuration data will be loaded (or re-loaded in a restart condition). For instance, the applications to be run, the priorities to be used, the crew/GSS/FSS/SOCS commands and controls to govern processing execution unless overridden, and linkages of allowable communications and calls upon services to be accepted must be set up. Then the initial operating condition data is installed and the SDSS confirms the services have been properly initialized (or re-initialized in a restart condition).

- SDSS STANDBY SDSS Functional State. After the SDSS has loaded, been configured and initialized for the vehicle, then it enters the SDSS_STANDBY state where it awaits commands to execute or requests for services. It exits this state each time such a command or request is received. In the START_SDSS avionics state, this is the normal state for SDSS to wait in since no applications execution may take place until after the applications are loaded. The SDSS is fully loaded and ready to operate.

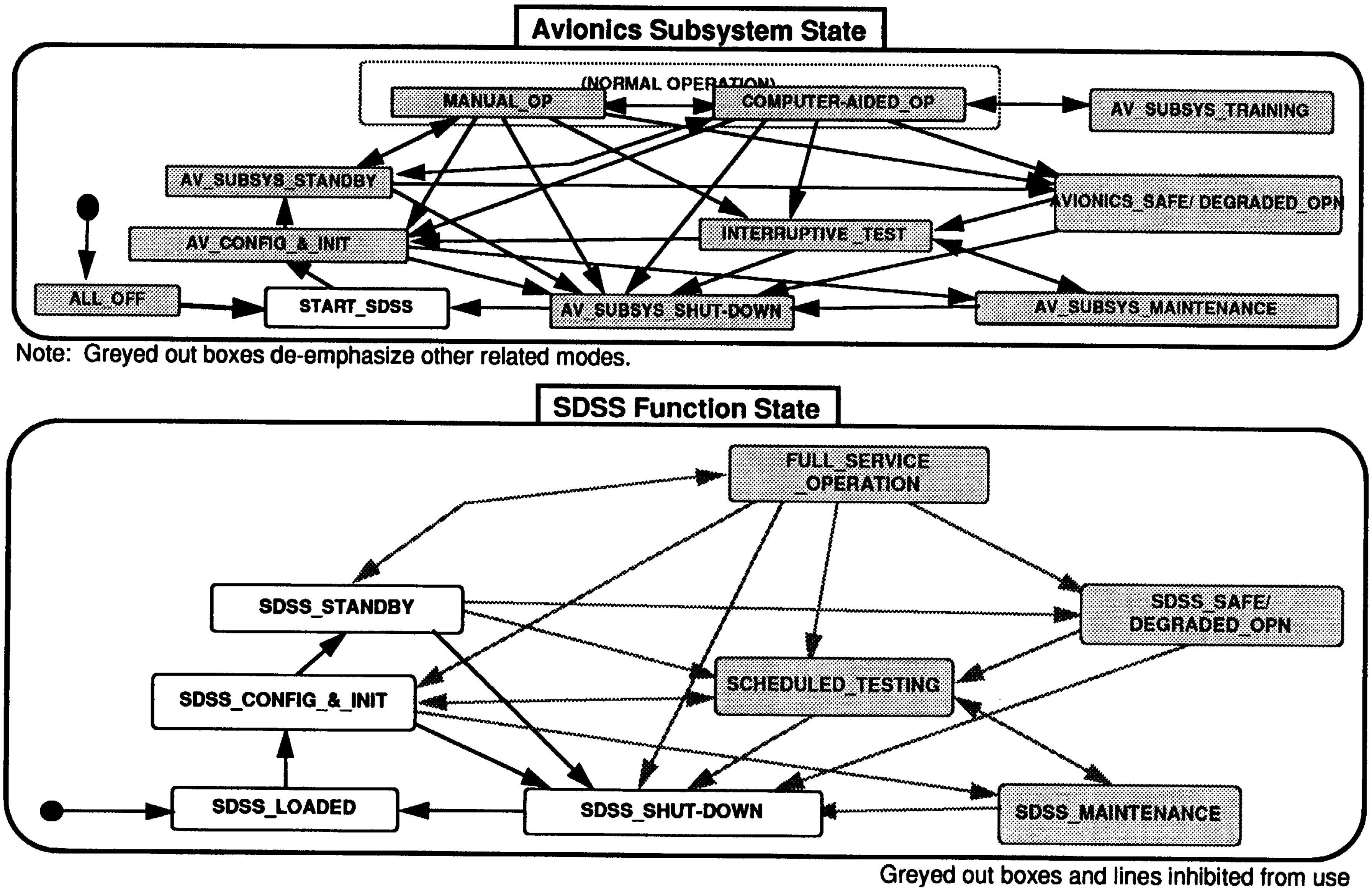


Figure C-21. SDSS Function States Allowed in START_SDSS Avionics Subsystem States

- SDSS_SHUT-DOWN SDSS Functional State. If necessary, the SDSS_SHUT-DOWN state may be entered to turnoff power to all elements of the SDSS except for the boot processing capability. SDSS cannot turn itself fully off as a safety precaution. This state provides for the orderly saving of state data and the subsequent shut-down of SDSS capabilities.

C.5.3 SDSS FUNCTION STATES ALLOWED IN AV_CONFIG_&_INIT AVIONICS SUBSYSTEM STATE

In the AV_CONFIG_&_INIT Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-22. The normal entry into an operable SDSS is the SDSS_STANDBY state which occurs after the SDSS has been loaded. (The AV_CONFIG_&_INIT Avionics Subsystem State was described in Section C.1.2.2.) The SDSS Functional States are described below.

- SDSS_LOADED SDSS Functional State. When the avionics are being loaded, configured and initialized, there may be a need to re-load the SDSS services. If so, this state provides the controls to enable the re-load of the SDSS, except for the boot program.
- SDSS_CONFIG_&_INIT SDSS Functional State. If the SDSS does get re-loaded, then this state provides for re-configuring and re-initializing the SDSS.
- SDSS_STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution.
- FULL_SERVICE_OPERATION SDSS Functional State. This state provides the controls to respond to onboard SOCS, FSS, GSS or crew commands to load application software, configure and initialize the avionics selected for use. It executes the command or request involved in such activities and places the applications into standby when their initialization is completed.
- SCHEDULED_TESTING SDSS Functional State. During AV_CONFIG_&_INIT, if it is necessary to execute tests either in response to POST results, or to fault detection capabilities, then this state provides the controls needed for scheduling the test, controlling the related test resources, capturing the resulting data and providing a report on results. This state knows the tests available and conditions needed for execution. It does not necessarily do extensive checking to determine

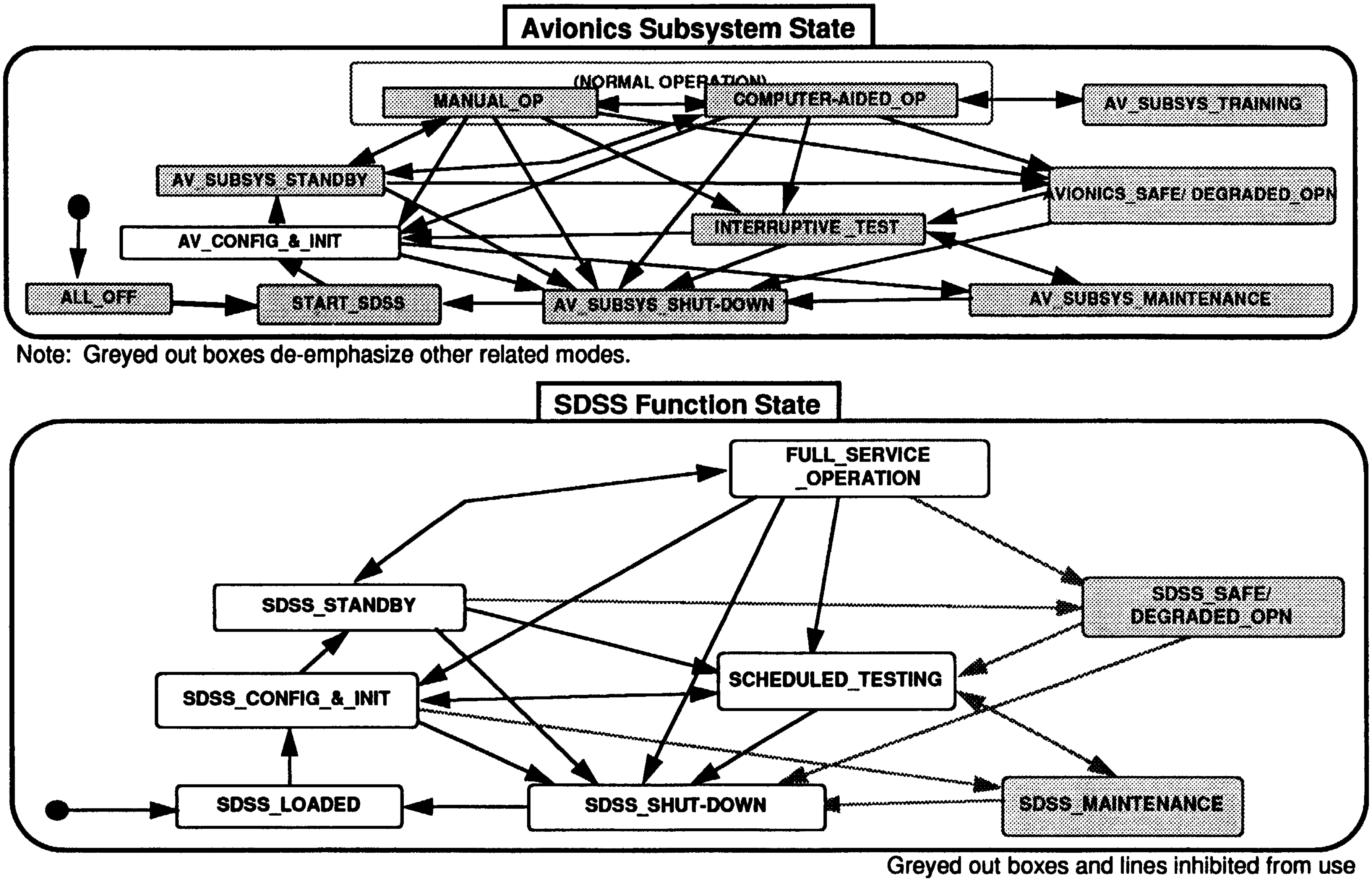


Figure C-22. SDSS Function States Allowed in AV_CONFIG_&_INIT Avionics Subsystem State that the test called for is appropriate to the avionics state, vehicle mode or mission mode; such context checking must be performed elsewhere.

- SDSS SHUT-DOWN SDSS Functional State. If the AV_CONFIG_&_INIT is unsuccessful or is terminated without successful completion for other reasons, then this state provides the controls to properly shut-down the SDSS. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

C.5.4 SDSS FUNCTION STATES ALLOWED IN AV_SUBSYS_STANDBY AVIONICS SUBSYSTEM STATE

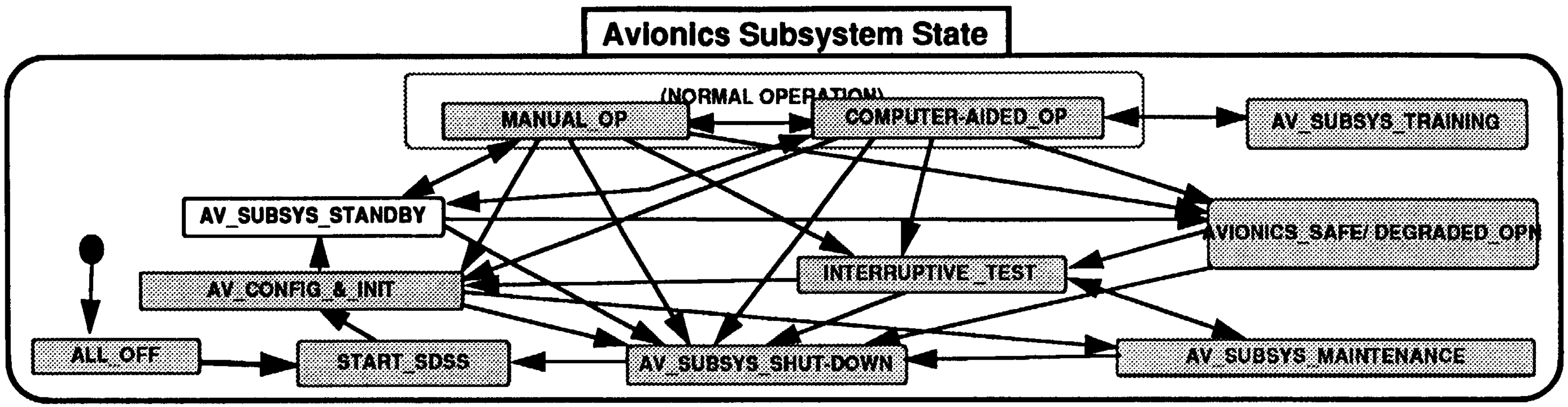
In the AV_SUBSYS_STANDBY Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-23. The normal entry into an operable SDSS is the SDSS_STANDBY state which occurs after the SDSS has been loaded, configured and initialized. (The AV_SUBSYS_STANDBY Avionics Subsystem State was described in Section C.1.2.2.) The SDSS Functional States are described below.

- SDSS LOADED SDSS Functional State. When the avionics are in standby and undergoing CBIT, there may be a need to re-load the SDSS services to respond to possible failures. If so, this state provides the controls to enable the re-load of the SDSS, except for the boot program.

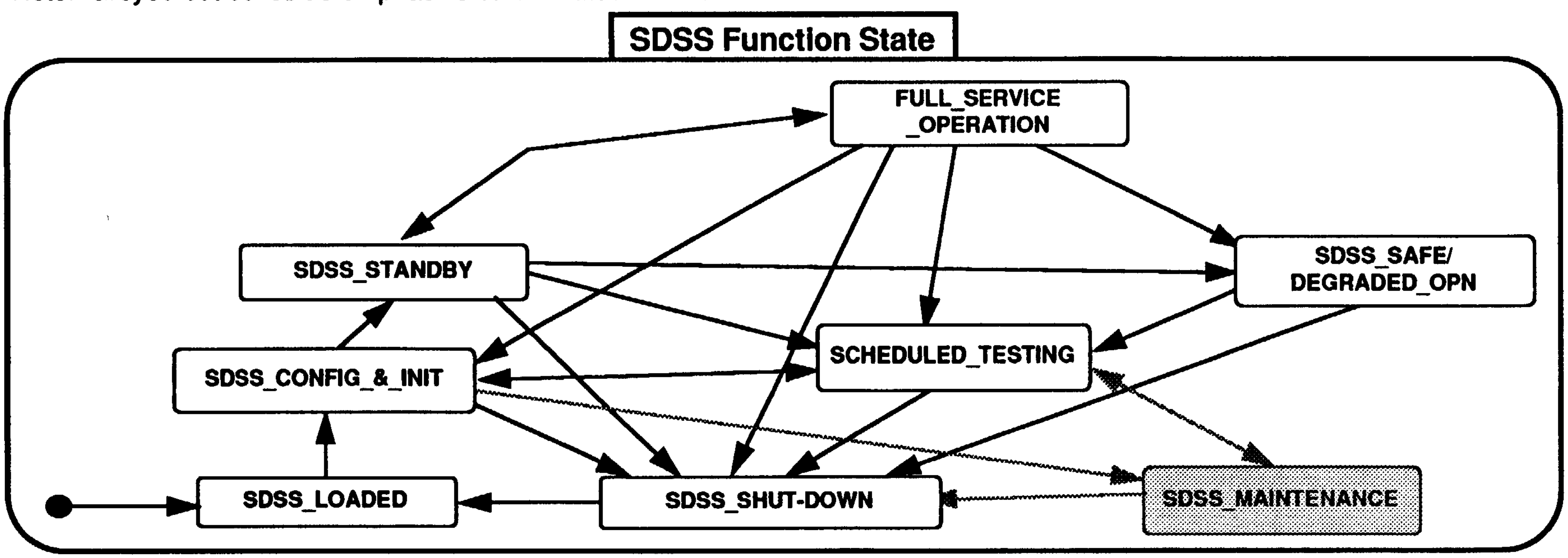
- SDSS CONFIG & INIT SDSS Functional State. If the SDSS does get re-loaded, then this state provides for re-configuring and re-initializing the SDSS.

- SDSS STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution. When the avionics are also in standby, few commands or requests may be encountered other than status maintenance types of services, such as to support CBIT.

- FULL SERVICE OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for services in association with responding to possible failures or other standby service requests. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-23. SDSS Function States Allowed in AV_SUBSYS_STANDBY Avionics Subsystem State

- SDSS_SAFE/DEGRADED_OPN SDSS Functional State. This state provides the SDSS fall back capability if failures interfere with the ability of the SDSS to provide full service operation. If the applications will still need to be supported, and restarts fail to restore full service capability, then this state provides less capable service operation.
- SCHEDULED_TESTING SDSS Functional State. During AV_SUBSYS_STANDBY, SDSS will respond to requests for services to support fault detection capabilities. This state provides the controls needed for handling the CBIT or other service requests for tests.
- SDSS_SHUT-DOWN SDSS Functional State. While the avionics are in standby, if it becomes necessary to shut-down the SDSS (except for the boot program) to either reboot or to stop processing, then this state provides the controls to do so properly. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

C.5.5 SDSS FUNCTION STATES ALLOWED IN MANUAL_OP AVIONICS SUBSYSTEM STATE

In the MANUAL_OP Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-24. In manual avionics operations, all the SDSS capabilities must be available to respond to any manual inputs provided by the FSS or crew. (The MANUAL_OP Avionics Subsystem State was described in Section C.1.2.2.) The SDSS Functional States are described below.

- SDSS_LOADED SDSS Functional State. When the avionics are under manual control, the FSS, GSS or crew may direct a re-load of the SDSS services. If so, this state provides the controls to enable the re-load of the SDSS, except for the boot program.
- SDSS_CONFIG_&_INIT SDSS Functional State. If the SDSS does get re-loaded, then this state provides for re-configuring and re-initializing the SDSS.
- SDSS_STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution.

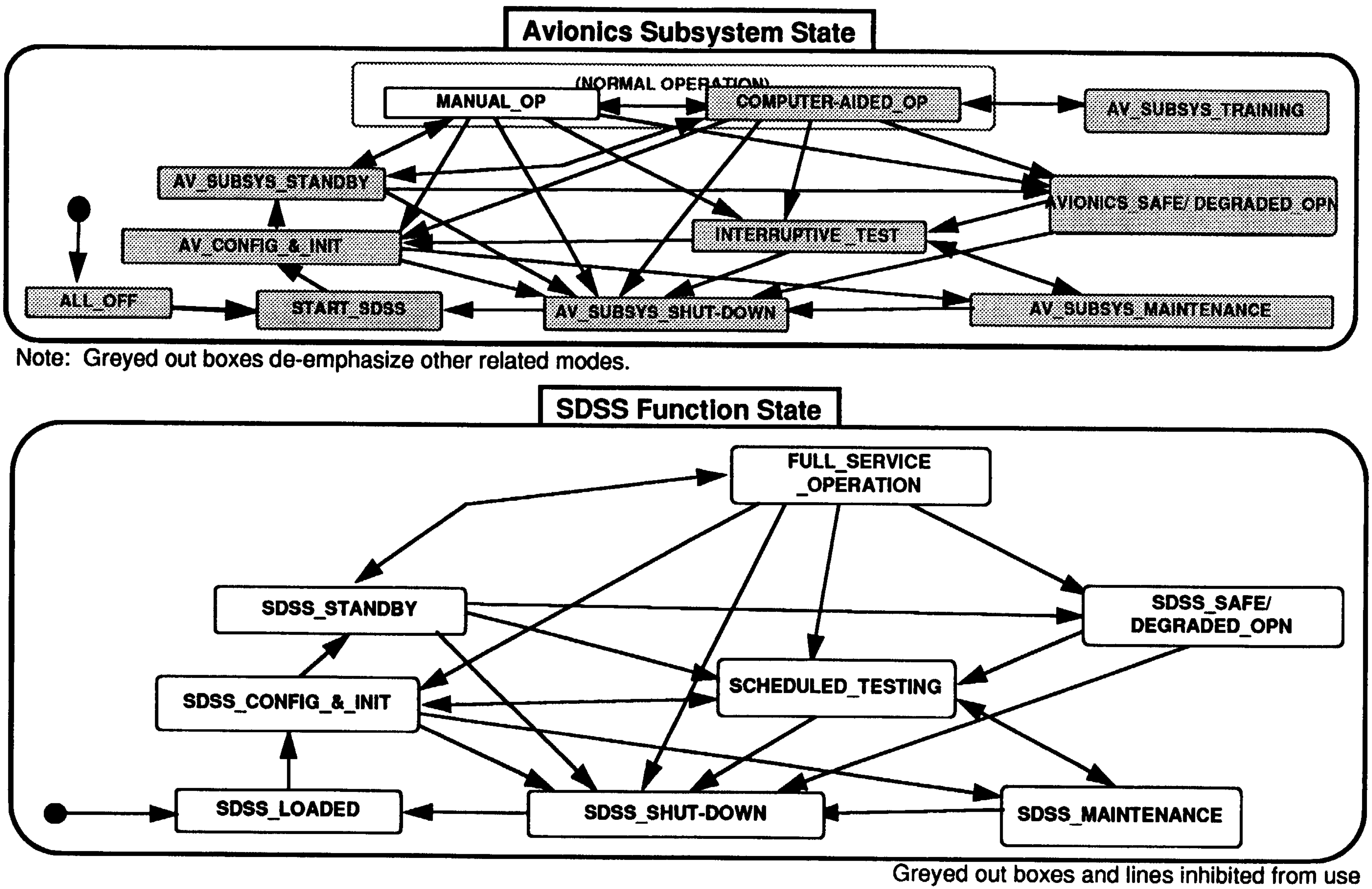


Figure C-24. SDSS Funcitonal States Allowed in MANUAL_OP Avionics Subsystem State

- FULL SERVICE OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for services in association with responding to FSS, GSS or crew service directions. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed.
- SDSS SAFE/DEGRADED OPN SDSS Functional State. This state provides the SDSS fall back capability if failures interfere with the ability of the SDSS to provide full service operation. If the FSS, GSS or crew still need to be supported, and restarts fail to restore full service capability, then this state provides less capable service operation.
- SDSS MAINTENANCE SDSS Functional State. This state provides the crew, FSS or GSS capability to operate the SDSS under maintenance conditions, with special maintenance states, programs and equipment to resolve critical anomalies.
- SCHEDULED TESTING SDSS Functional State. During manual control, SDSS will respond to requests for services to test any capabilities. This state provides the controls needed for handling any service requests for tests.
- SDSS SHUT-DOWN SDSS Functional State. While the avionics are under manual control, if it becomes necessary to shut-down the SDSS (except for the boot program) to either reboot or to stop processing, then this state provides the controls to do so properly. Only the SDSS boot program cannot be shut-down in this state (by SDSS); such action requires an external power off signal. Even under manual control, safety overrides would have to be bypassed by the crew, FSS or GSS to fully power down the SDSS by external power off signal since no processing support, reboot support, life support or other critical services would be available during such a power off condition, and the ability of the spacecraft to restart might not be assumable.

C.5.6 SDSS FUNCTION STATES ALLOWED IN COMPUTER-AIDED_OP AVIONICS SUBSYSTEM STATE

In the COMPUTER-AIDED_OP Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-25. (The COMPUTER-AIDED_OP Avionics Subsystem State was described in Section C.2.4.5.) The SDSS Functional States are described below.

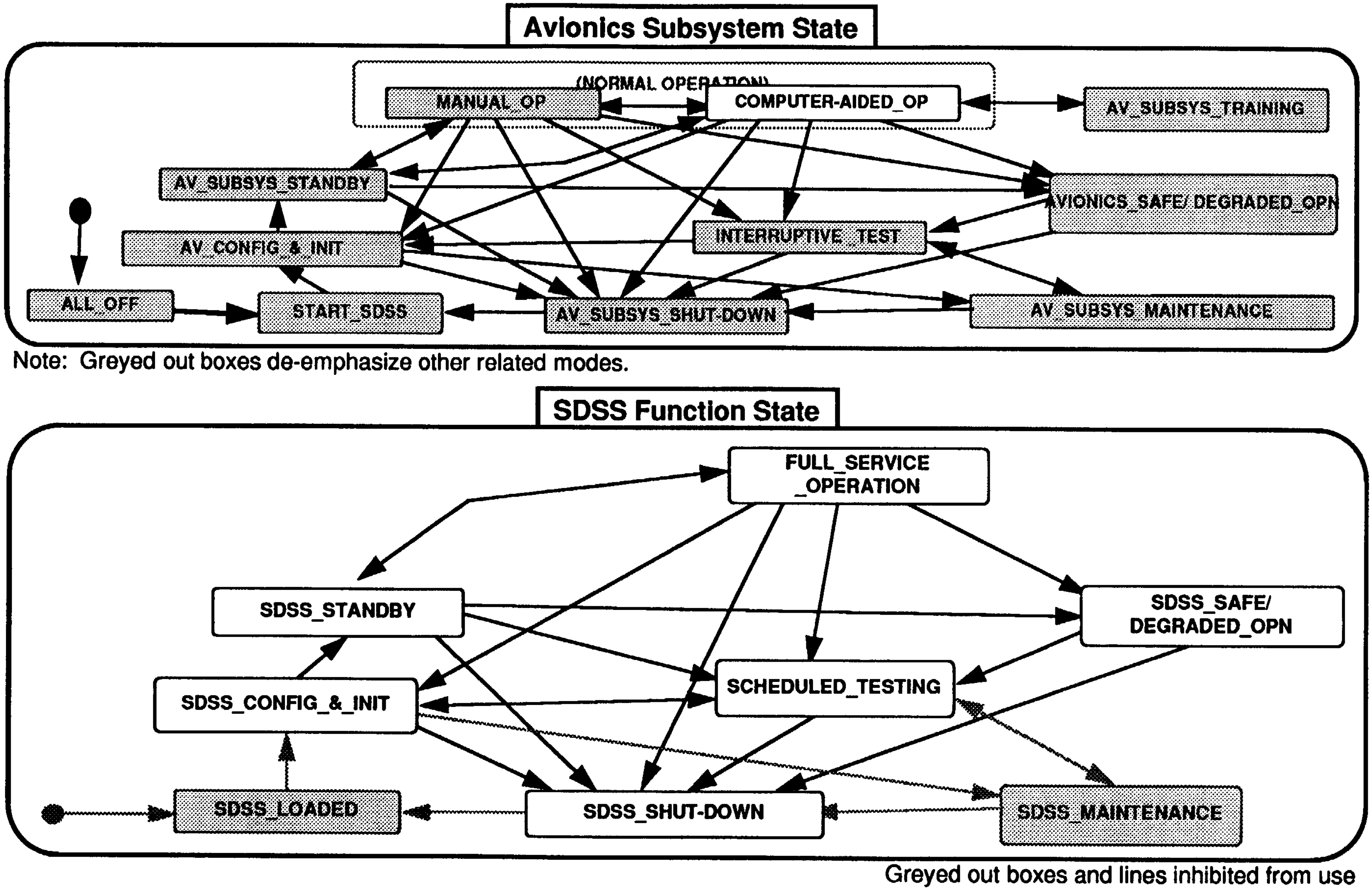
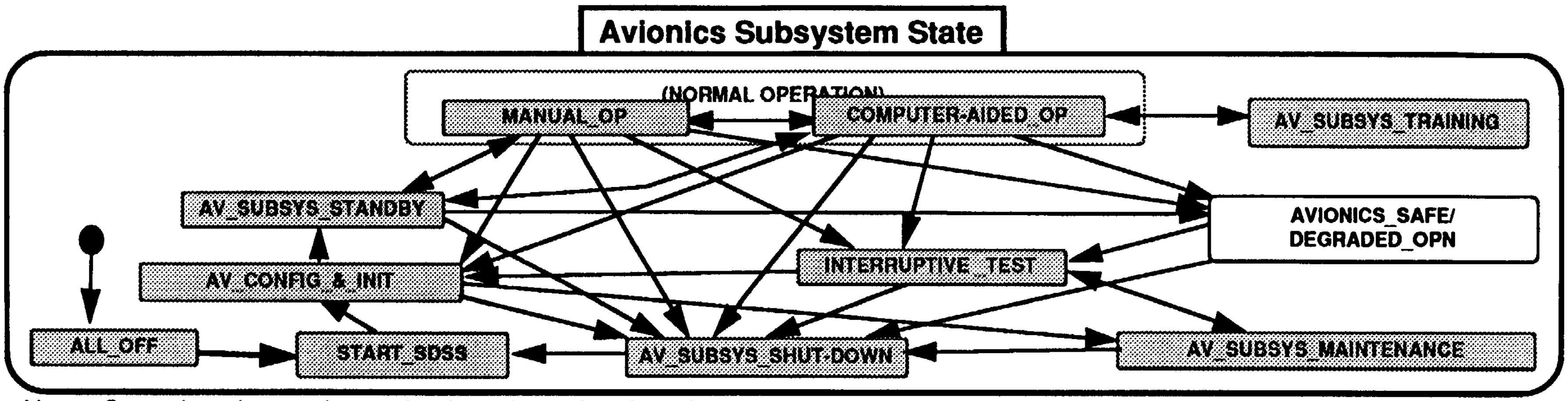


Figure C-25. SDSS Functional States Allowed in COMPUTER-AIDED_OP Avionics Subsystem State

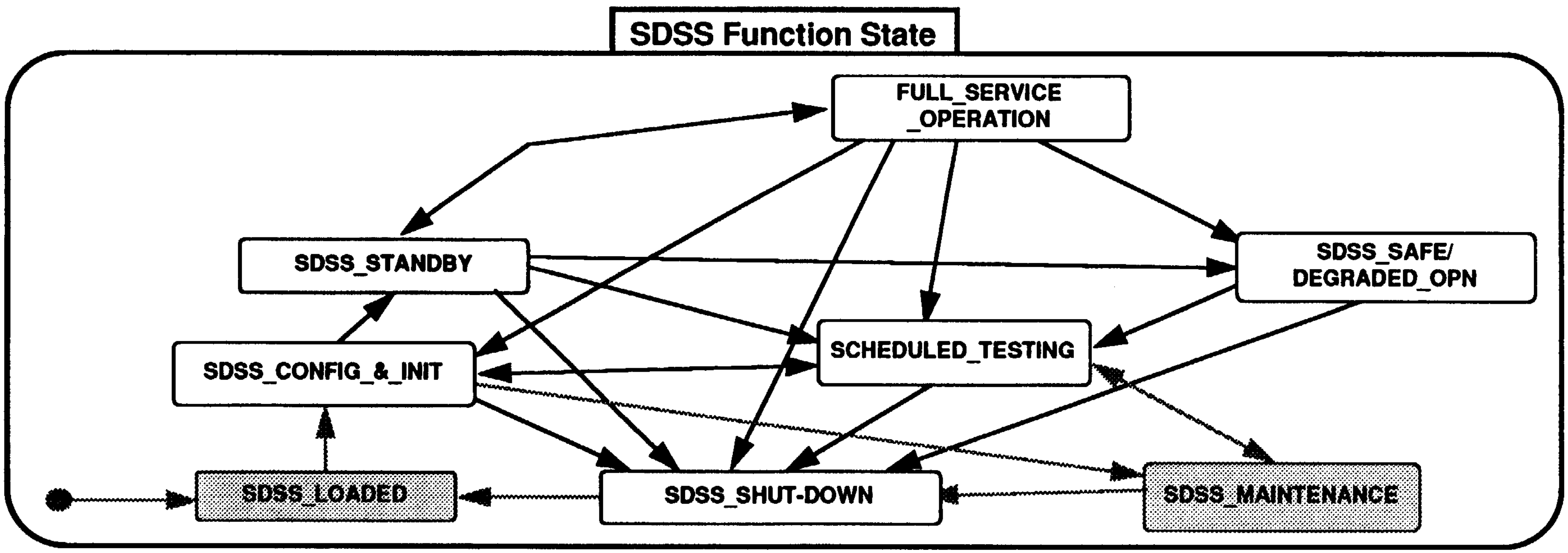
- SDSS_CONFIG_&_INIT SDSS Functional State. When the avionics are in COMPUTER-AIDED_OP, there may be a need to re-configure and re-initialize the SDSS tò accommodate different planned applications processing requirements.
- SDSS_STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution.
- FULL_SERVICE_OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for services. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed.
- SDSS_SAFE/DEGRADED_OPN SDSS Functional State. This state provides the SDSS fall back capability if failures interfere with the ability of the SDSS to provide full service operation. If the applications still need to be supported, and restarts fail to restore full service capability, then this state provides less capable service operation.
- SCHEDULED_TESTING SDSS Functional State. During normal avionics operation, SDSS will respond to requests for services to handle CBIT or other service requests for tests.
- SDSS_SHUT-DOWN SDSS Functional State. While the avionics are normal operation, if it becomes necessary to shut-down the SDSS (except for the boot program) to either reboot or to stop processing, then this state provides the controls to do so properly. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

C.5.7 SDSS FUNCTION STATES ALLOWED IN AVIONICS_SAFE/DEGRADED_OPN AVIONICS SUBSYSTEM STATE

In the AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-26. (The AVIONICS_SAFE /DEGRADED_OPN Avionics Subsystem State was described in Section C.2.4.5.) The SDSS Functional States are described below.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-26. SDSS Functional States Allowed in AVIONICS_SAFE/DEGRADED_OPN Avionics Subsystem State

- SDSS CONFIG & INIT SDSS Functional State. When the avionics are operating in a state of safe or degraded operations, it may be necessary for the SDSS to be reconfigured. This state provides for re-configuring and then re-initializing the SDSS.

- SDSS STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution.

- FULL SERVICE OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for services. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed.

- SDSS SAFE/DEGRADED OPN SDSS Functional State. This state provides the SDSS fall back capability if failures interfere with the ability of the SDSS to provide full service operation. If the applications will still need to be supported, and restarts fail to restore full service capability, then this state provides less capable service operation.

- SCHEDULED TESTING SDSS Functional State. During AVIONICS_SAFE /DEGRADED_OPN, SDSS will respond to requests for services to continue attempting to resolve the anomaly which holding the avionics in a safe or degraded condition. This state provides the controls needed for handling the CBIT or other service requests for tests.

- SDSS SHUT-DOWN SDSS Functional State. While the avionics are in safe or degraded operating conditions, if it becomes necessary to shut-down the SDSS (except for the boot program) to either reboot or to stop processing, then this state provides the controls to do so properly. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

C.5.8 SDSS FUNCTION STATES ALLOWED IN AV_SUBSYS_TRAINING AVIONICS SUBSYSTEM STATE

In the AV_SUBSYS_TRAINING Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-27. (The AV_SUBSYS_TRAINING Avionics Subsystem State was described in Section C.2.4.6.) The SDSS Functional States are described below.

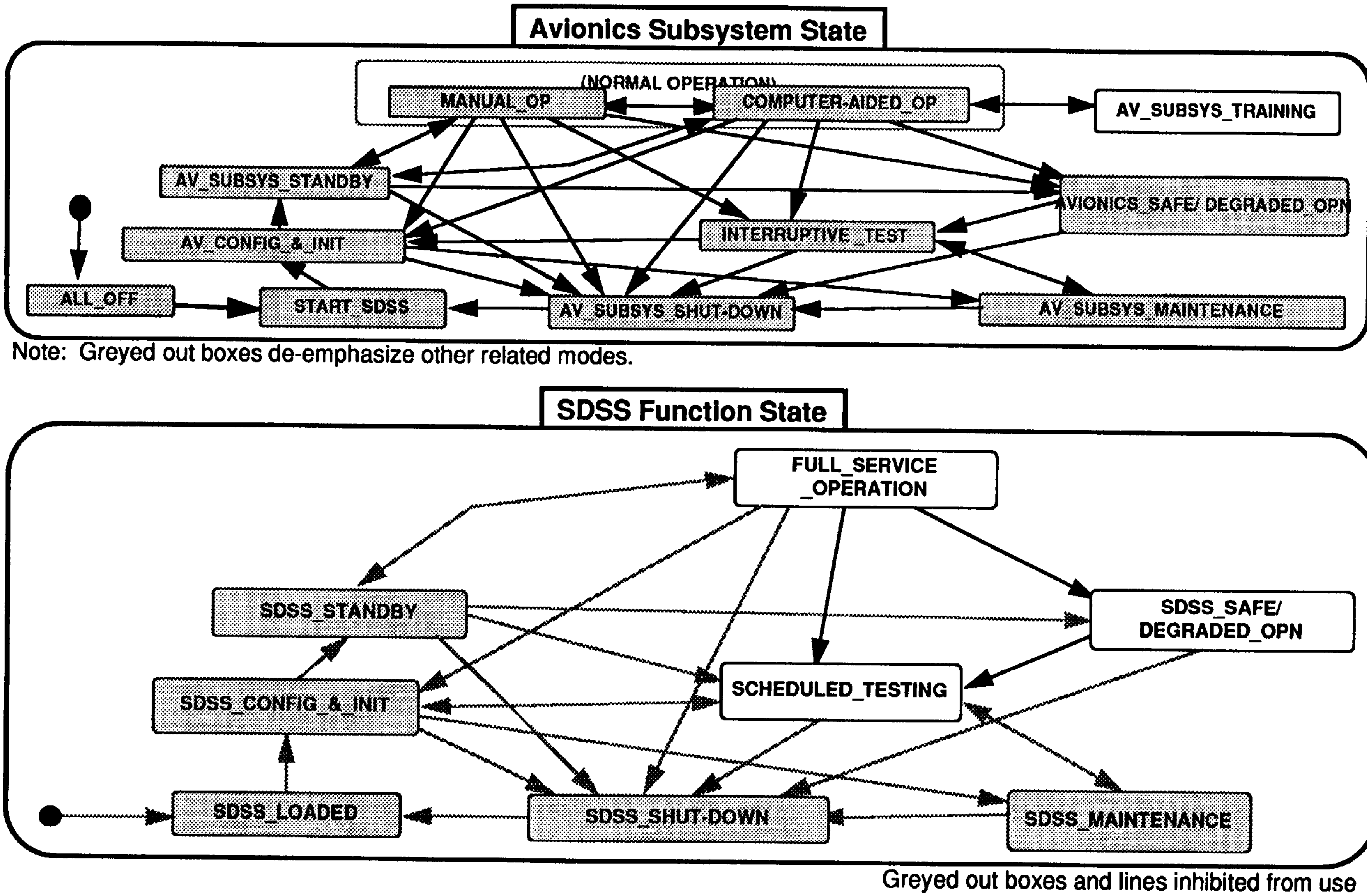


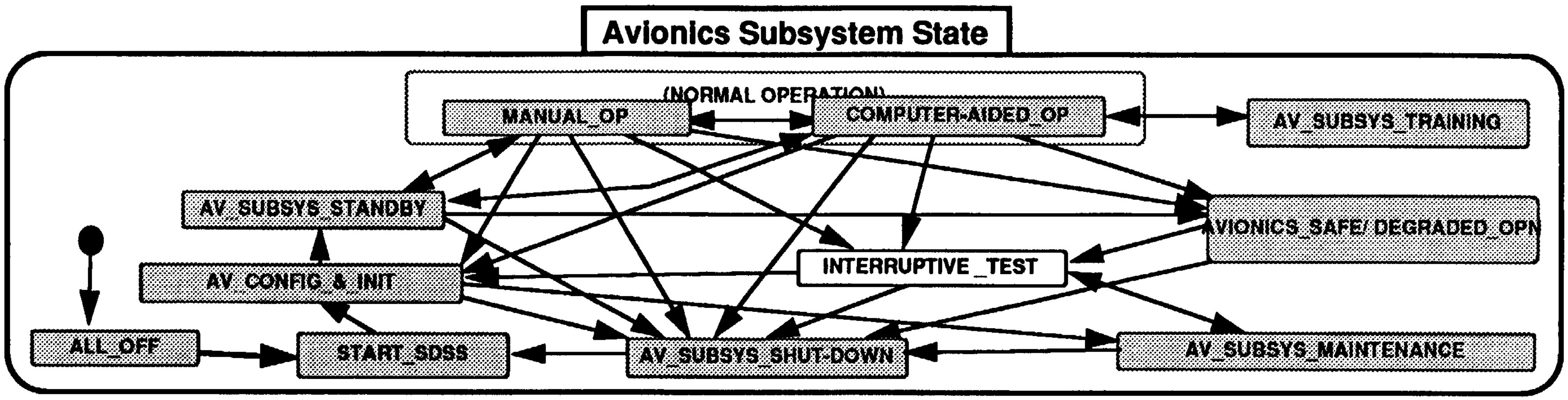
Figure C-27. SDSS Functional States Allowed in AV_SUBSYS_TRAINING Avionics Subsystem State

- FULL SERVICE OPERATION SDSS Functional State. This state provides the controls to respond to avionics simulation or other training program state requests for services in association with providing training to the crew. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed. The SDSS tracks all training data to ensure no possible cross-over or contamination between training data and real operational mission data. The SDSS recognizes real operational mission alerts and warnings and provides overrides to the training subsystem to clearly indicate non-training information which is critical in nature.
- SDSS SAFE/DEGRADED OPN SDSS Functional State. During training operations, this state provides the SDSS interlock capability to protect critical and other vehicle capabilities from responding to training subsystem direction as if it were real direction. (The SDSS ensures system safety by tracking and controlling training data and control commands.) The FULL_SERVICE_OPERATION is inhibited from responding to overrides while in training mode; such actions require special SAFE state handling for safety and security protection, although such actions must still be responded to immediately.
- SCHEDULED TESTING SDSS Functional State. During AV_SUBSYS_TRAINING, SDSS will respond to requests for services to support fault detection capabilities. This state is independent of the training activities to ensure the training and other systems actually function properly. This state provides the controls needed for handling the CBIT or other service requests for tests.

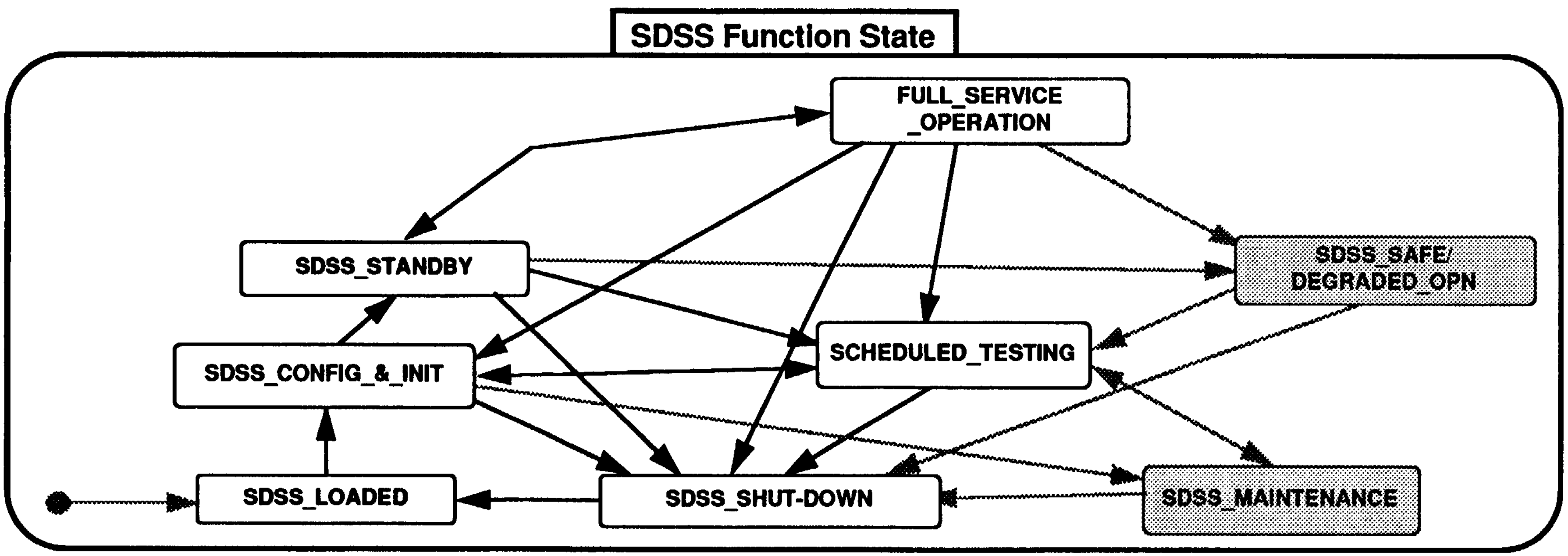
C.5.9 SDSS FUNCTION STATES ALLOWED IN INTERRUPTIVE_TEST AVIONICS SUBSYSTEM STATE

In the INTERRUPTIVE_TEST Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-28. (The INTERRUPTIVE_TEST Avionics Subsystem State was described in Section C.1.2.2.) The SDSS Functional States are described below.

- SDSS LOADED SDSS Functional State. After the avionics undergo tests which interrupt normal processing capability, there may be a need to re-load the SDSS services to restore the capability to respond normally. If so, this state provides the controls to enable the re-load of the SDSS, except for the boot program.



Note: Greyed out boxes de-emphasize other related modes.



Greyed out boxes and lines inhibited from use

Figure C-28. SDSS Functional States Allowed in INTERRUPTIVE_TEST Avionics Subsystem State

- SDSS_CONFIG_&_INIT SDSS Functional State. If the SDSS does get re-loaded, then this state provides for re-configuring and re-initializing the SDSS.

- SDSS_STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution.

- FULL_SERVICE_OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for test services. It executes the test command or request involved and schedules the specific tests to be conducted.

- SCHEDULED_TESTING SDSS Functional State. After tests are scheduled in the FULL_SERVICE_OPERATION state, this state performs the actual tests, and handles the results. The normal exit from this state is through SDSS_CONFIG_&_INIT to ensure that all test data has been properly purged from memory and state conditions are reset to normal processing.

- SDSS_SHUT-DOWN SDSS Functional State. An alternative exit from SDSS Function States supporting interruptive testing is through a complete shut-down of the SDSS (except for the boot program). This may be to either reboot or to stop processing; this state provides the controls to do so properly. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

C.5.10 SDSS FUNCTION STATES ALLOWED IN AV_SUBSYS_MAINTENANCE AVIONICS SUBSYSTEM STATE

In the AV_SUBSYS_MAINTENANCE Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-29. (The AV_SUBSYS_MAINTENANCE Avionics Subsystem State was described in Section C.1.2.4.) The SDSS Functional States are described below.

- SDSS_LOADED SDSS Functional State. When the avionics are undergoing maintenance, there may be a need to either load special maintenance enabled versions of SDSS programs, or to re-load the SDSS normal services. If so, this state provides the controls to load or re-load the SDSS, except for the boot program.

- SDSS_CONFIG_&_INIT SDSS Functional State. If the SDSS does get loaded or re-loaded, then this state provides for re-configuring and re-initializing the SDSS.

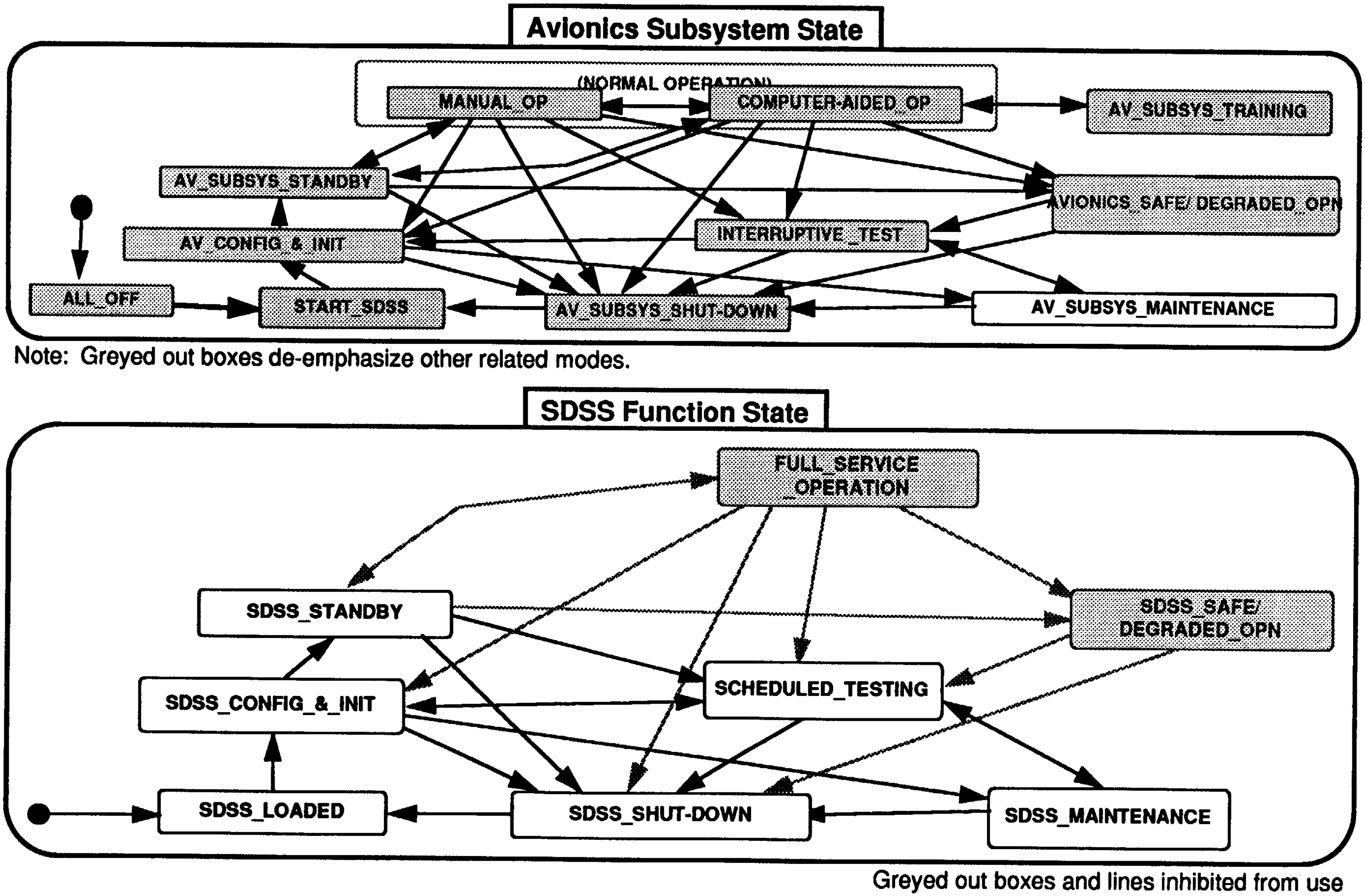


Figure C-29. SDSS Functional States Allowed in AV_SUBSYS_MAINTENANCE Avionics Subsystem State

- SDSS_STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution.

- FULL_SERVICE_OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for services in association with maintenance of the system. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed.

- SDSS_MAINTENANCE SDSS Functional State. This state provides the crew, FSS or GSS capability to operate special maintenance programs and maintenance versions of the SDSS, with special maintenance states, programs and equipment to resolve anomalies.

- SCHEDULED_TESTING SDSS Functional State. During AV_SUBSYS_MAINTENANCE, SDSS will respond to requests for test services to support maintenance capabilities. This state provides the controls needed for handling the special service requests for tests.

- SDSS_SHUT-DOWN SDSS Functional State. When maintenance is completed, the normal exit will to the SDSS_SHUT-DOWN state to ensure that all maintenance data and programs are purged from memory. This state provides the controls to properly shut-down the SDSS (except for the boot program) to either reboot or to stop processing. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

C.5.11 SDSS FUNCTION STATES ALLOWED IN AV_SUBSYS_SHUT-DOWN AVIONICS SUBSYSTEM STATE

In the AV_SUBSYS_SHUTDOWN Avionics Subsystem State, SDSS Functional States which can be utilized are shown in Figure C-30. (The AV_SUBSYS_SHUT-DOWN Avionics Subsystem State was described in Section C.1.2.2.) The SDSS Functional States are described below.

- SDSS_STANDBY SDSS Functional State. This state is the normal SDSS state while awaiting commands or requests for service. Exit from this state occurs when a command or request is received and approved by SDSS for execution. When the avionics are shutting down, the shut-down request will cause a transition to the SDSS_SHUT-DOWN state, rather than the

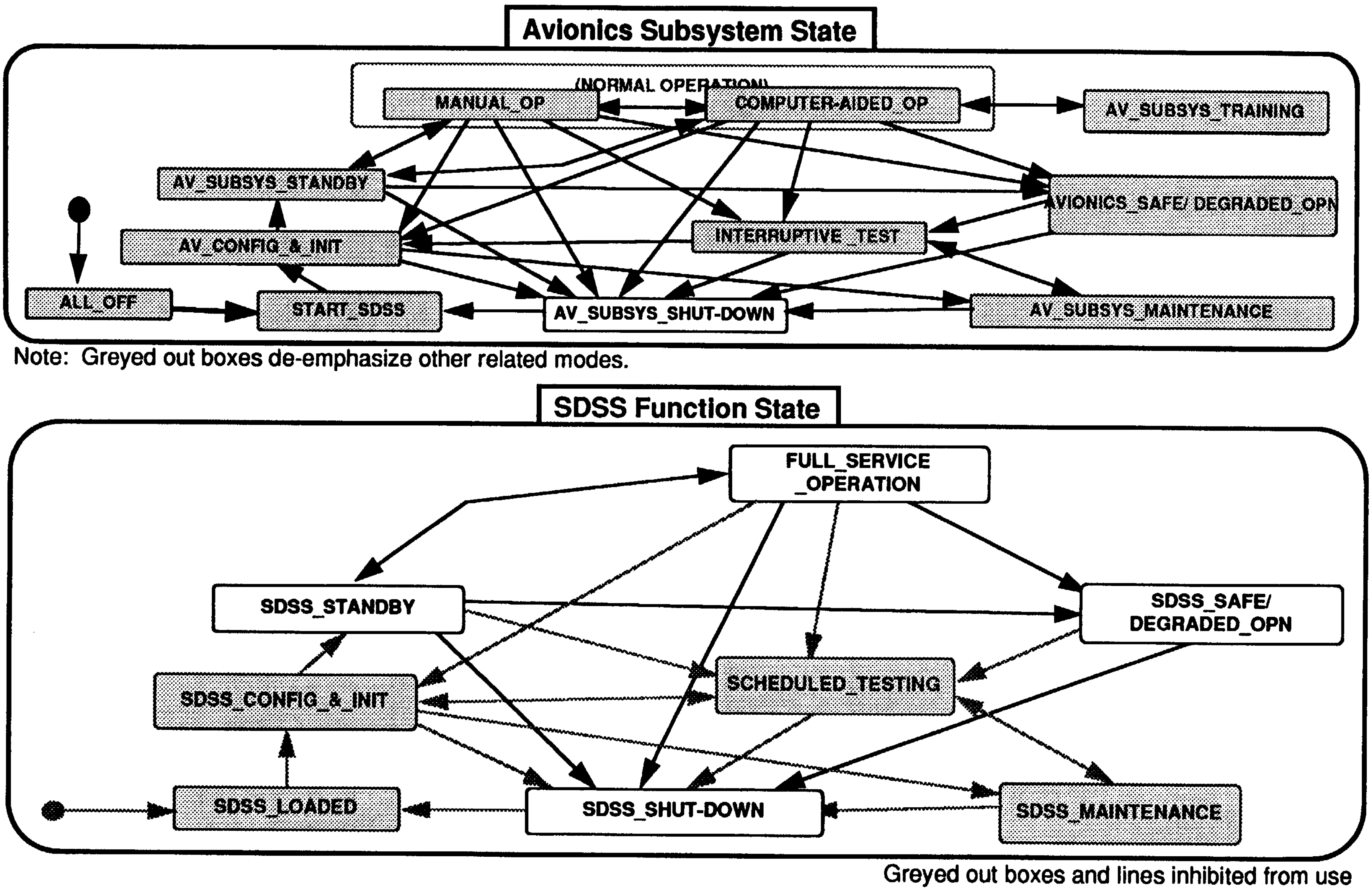


Figure C-30. SDSS Functional States Allowed in AV_SUBSYS_SHUT-DOWN Avionics Subsystem State

FULL_SERVICE_OPERATION state, after the avionics applications and external systems have been powered off.

- FULL_SERVICE_OPERATION SDSS Functional State. This state provides the controls to respond to avionics state requests for services in association with responding to avionics applications and related systems shut-down service requests. It executes the command or request involved in such activities then returns to SDSS_STANDBY when completed.
- SDSS_SAFE/DEGRADED_OPN SDSS Functional State. This state provides the SDSS fall back capability if failures interfere with the ability of the SDSS to provide full service operation. If the applications will still need to be shut-down, and restarts fail to restore full SDSS service capability, then this state provides less capable service operation for SDSS shut-down.
- SDSS_SHUT-DOWN SDSS Functional State. After the avionics have been shut-down, this state provides the capability and controls to shut-down the SDSS (except for the boot program) to either reboot or to stop processing. Only the SDSS boot program cannot be shut-down in this state; such action requires an external power off signal.

APPENDIX D
SGOAA SIMULATION PHASE 1

APPENDIX D
SGOAA SIMULATION PHASE 1

This appendix describes the Phase 1 results in the development of a dynamic architecture simulation model using the Statemate CASE tool for validation of the SGOAA. The Statemate CASE Tool is a development of the i-Logic Corporation and a copy is installed in the NASA JSC Real Time Systems Engineering Laboratory (RSEL). A complete set of documentation for this tool is also available in the RSEL. The following paragraphs provide a short overview of the tool and how it was applied to the SGOAA. The simulation model developed for the SGOAA resides as an application in the data base of the Statemate CASE Tool installed in the RSEL.

D.1 MODELING LANGUAGES OF STATEMATE

Statemate has four modeling languages - Activity-charts, Statecharts, Module-charts and Forms. These languages are completely described in the document entitled "The Modeling Languages of Statemate" located in the RSEL. For ease in interpreting this appendix a short description of each of these languages is provided here. The following Statemate language descriptions enclosed in parenthesis are extracted from the i-Logic Marketing Brochure entitled "The STATEMATE Approach to Complex Systems".

D.1.1 ACTIVITY CHARTS

"Functional issues are treated in Statemate using activities that represent the processing capabilities of the system. Dealing with a customer's confirmation request in an airline reservation system is an example of an activity, as is updating the aircraft's position in an avionics system. Activities can be nested, forming a hierarchy that constitutes a functional decomposition of the system. Items of information such as the distance to a target or the customer's name, will typically flow between activities, and might also be kept in data stores. This functional view of a system is captured with the language of Activity-charts, which are similar to conventional flow diagrams." Activity-charts show the possible data and control flows for the system.

Figure D-1 is the top level Activity-chart created for the SGOAA simulation. The structure associated with this Activity-chart is shown in Figure D-2. The data dictionary is shown in Table D-1.

D.1.2 STATECHARTS

"Statecharts describe the dynamics of a systems behavior, and identify the conditions and events causing transitions between states. Unlike conventional state transition diagrams, Statecharts feature hierarchy (encapsulated states), concurrency, and broadcasting."

"Dynamic behavioral issues, commonly referred to as control aspects, are treated in Statemate using the Statecharts language. Here, states (or modes) can be nested or linked in a number of ways to represent sequential of concurrent behavior. An avionics mission computer, for example, could be in one of three states, air-to-air, air-to-ground, or navigation. At the same time, it must be in the state of either automatic or flight control. Transition between states are typically triggered by events, which may be qualified by conditions. Flipping a certain switch on the throttle, for example, is an event that will cause a transition from the navigate state to the air-to-ground state, but only on the condition that the aircraft has air-to-ground ammunition available."

Figure D-3 is a Statechart generated to describe avionics control for the SGOAA simulation scenario. The structure associated with this Statechart is shown in Figure D-4. The data dictionary is shown in Table D-2.

D.1.3 MODULE CHARTS

"Module-charts allow activities to be associated with the physical components of the system. They identify the system modules used in the implementation, the external elements, and the information and control channels between these components. This structural view provides the basis for the transition to design."

Figure B-1 in Appendix B is a Module type chart for the Artemis CLL vehicle including the allocation of functions to the various modules.

D.1.4 FORMS

"Certain non graphical parts of the modeling process, such as specifying the connections between Module charts and Activity-charts or defining the structure of compound data items, are carried out in the forms language of Statemate."

Statemate distinguishes between graphical elements, which are depicted graphically, and textural elements which are not depicted graphically, but may appear as part of labels in the charts. Graphical elements include states, activities, data-stores, modules, transitions, connectors and flow-lines. There are two types of flow-lines: data flow-lines, drawn as solid lines, and control flow-lines, drawn as dashed lines. Typically, control flow-lines carry information or signals that are used in making control decisions, while data flow-lines carry information that is used in computations and data-processing operations. Textual elements include events, conditions, data-items, information-flows, and actions. Both types of elements have forms that may contain further information, though among the graphical elements only box elements (i.e., states, activities, data-stores and modules) have forms. All five textual elements have forms, which contain the type and structure of data-items, the decomposition of information-flows and also serve as the mechanism for defining compound events, conditions, data-items and actions.

D.2 INTEGRATING ACTIVITY-CHARTS AND STATECHARTS

Associated with each Activity-chart will usually be a Statechart, called a control activity, whose role is to control the activities and data flows for the Activity-chart. An example of a control activity for an Activity-chart is @AVIONICS_CTRL_REV2 in Figure D-1. Figure D-3 is the Statechart for that control activity.

D.3 DATA DICTIONARIES

A data dictionary is provided for each Activity-chart and for each Statechart. This data dictionary defines the external activities associated with the charts and all of the flows associated with the chart including those flows defined in lower level charts.

D.4 THE SGOAA MODEL

The Activity-charts, Statecharts and supporting forms developed during the build of the SGOAA simulation are discussed in the following paragraphs and provided in the associated figures and tables.

D.4.1 SGOAA ACTIVITY-CHART

The highest level SGOAA Activity-chart is shown in Figure D-1. This chart defines all of the system elements, both internal and external, and the data and command flows between these elements for the SGOAA as applied to the CLL. The AVIONICS activity is the large solid line box. The solid lines exiting the AVIONICS activity are the external interfaces. Figure D-2 is the SGOAA Activity-chart structure diagram showing each of the defined elements down to their lowest defined level and also identifies by figure number the lower level detailed Activity-charts and/or Statecharts in the data base. For example, the SPACE_DATA_SYS_SERVICES Activity-chart is Figure D-6 and the INIT_AV_CONFIG Activity-chart is Figure D-11.

In the figure, AVIONICS_APPS contains all of the avionics application software. The data flow interfaces from the applications to external elements are shown as solid lines such as the interfaces from the GN&C application to the guidance system hardware (GUIDANCE_HW) and propulsion system hardware (PROPULSION_HW). AVIONICS_APPS has control flow interfaces to @AVIONICS_CTRL_REV2 expanded as a Statechart in Figure D-3. @AVIONICS_CTRL_REV2 has control flow interfaces to @SPACE_DATA_SYS_SERVICES expanded as a lower level Activity-chart in Figure D-6 and to the external activity GROUND_SPT_SYS.
Table D-1 is the SGOAA Activity-chart dictionary.

D.4.2 AVIONICS_CTRL_REV2 STATECHART

The AVIONICS_CTRL_REV2 Statechart was shown in Figure D-3. It's role is to control the activities and data flows of the activity in which it is contained. In this instance, it controls the activities and data flows of the SGOAA Avionics activity and defines those states the Avionics activity can assume from startup to shutdown. Figure D-4 is a state structure diagram showing each of the AVIONICS_CTRL Statechart defined states down to their lowest level and also identifies by figure number lower level detailed Statecharts in the data base. For example, the START_SDSS Statechart is Figure D-7 and the AV_CONFIG_INIT Statechart is Figure D-12.

Table D-2 is the AVIONICS_CTRL_REV2 Statechart dictionary.

D.4.3 PUP_AND_LOAD ACTIVITY-CHART

The PUP_AND_LOAD Activity-chart is shown in Figure D-5. It defines the activities associated with the power up of the Avionics System, loading of SDSS system software and the activation of the SDSS for performing its mission functions. Figure D-7 is the Statechart for @Start_SDSS. Table D-3 is the Activity-chart dictionary for PUP_AND_LOAD.

D.4.4 SPACE_DATA_SYS_SERVICES ACTIVITY-CHART

Figure D-6 defines all of the SPACE_DATA_SYS_SERVICES elements, both internal and external, and the data and command flows between these elements. The data dictionary in Table D-4 defines the contents of these flows. Figure D-9 is the lower level @SDDS_CTRL_REV1 Statechart. The functions of the SPACE_DATA_SYS_SERVICES internal elements are defined in the SGOAA Standard.

D.4.5 START_SDSS STATECHART

Figure D-7 is the Statechart for the @START_SDSS activity contained in Figure D-5, the Powerup and Load Activity Chart. This chart defines those states the SDSS is put into in getting all of the system processors up and running, loading of the system software and handling any failures that might occur in the start up process. Table D-5 is the Statechart dictionary for START_SDSS. Figure D-8 is the state structure diagram for START_SDSS.

D.4.6 SDSS_CTRL_REV1 STATECHART

Figure D-9 is the Statechart for the @SDSS_CTRL_REV1 control activity shown in Figure D-6, the SDSS Activity-chart. This chart defines the SDSS operating and reset system software states. Table D-6 is the SDSS_CTRL_REV1 Statechart dictionary and Figure D-10 is the Statechart structure.

D.4.7 INIT_AV_CONFIG ACTIVITY-CHART

Figure D-1 defined an activity called @INIT_AV_CONFIG. Figure D-11 is the Activity-chart for that activity and defines all of those activities involved in the initial configuration of the Avionics System. As defined in Figure D-3, the Avionics Control Statechart, the activities defined in this figure occur following the SDSS activation. The external data flow PON_SIGS contains power on commands for the Avionic Systems external to the SDSS. PON_RESP is the data flow that reports the results of the power on commands. Table D-7 is the INIT_AV_CONFIG Activity-chart dictionary.

D.4.8 AV_CONFIG_INIT STATECHART

Figure D-12 is the Statechart for @AV_CONFIG_INIT. It defines the dynamic system behavior involved in bringing all of the Avionics on-line and operational in a predefined configuration, the handling of failures to power on and failures to load application software. Retries and application of watchdog timers (time outs) is also defined. Table D-8 is the AV_CONFIG_INIT Statechart dictionary and Figure D-13 is the Statechart structure.

D.4.9 INTERRUPTIVE_TEST STATECHART

Figure D-3, the Statechart for Avionics Control defined an INTERRUPTIVE_TEST state. Figure D-14 describes the states for INTERRUPTIVE_TEST. It is the lower level Statechart for that defined state and defines the dynamic system behavior to be exhibited by the system during interruptive testing. The dictionary is shown in Table D-9 and the state structure in Figure D-15.

D.4.10 SGOAA SCENARIO SIMULATION PANEL

This is the control panel for running the SGOAA scenario simulation. This panel is displayed on the workstation monitor. Selection of a button, for example, POWER_ON_AV causes that dynamic activity command to be made true in the statechart in which it is defined. In this case POWER_ON_AV is defined in Figure D-3, the Avionics Control Statechart. Table D-10 contains the script for the simulation. The GO ADVANCE 1.000000 in the script steps through the statechart one step at a time until all state changes that are a direct result of the issued command have been executed allowing the system's response to be viewed graphically, using the interactive simulation feature of the analyzer package. The active elements in the charts (states that the system is in at that moment and activities that are active) are highlighted graphically. The execution can also be made to simulate the system running in real time and to keep track of the time dependent information. At any point during the execution, the status of non graphical elements such as the value of a variable or a condition can also be viewed.

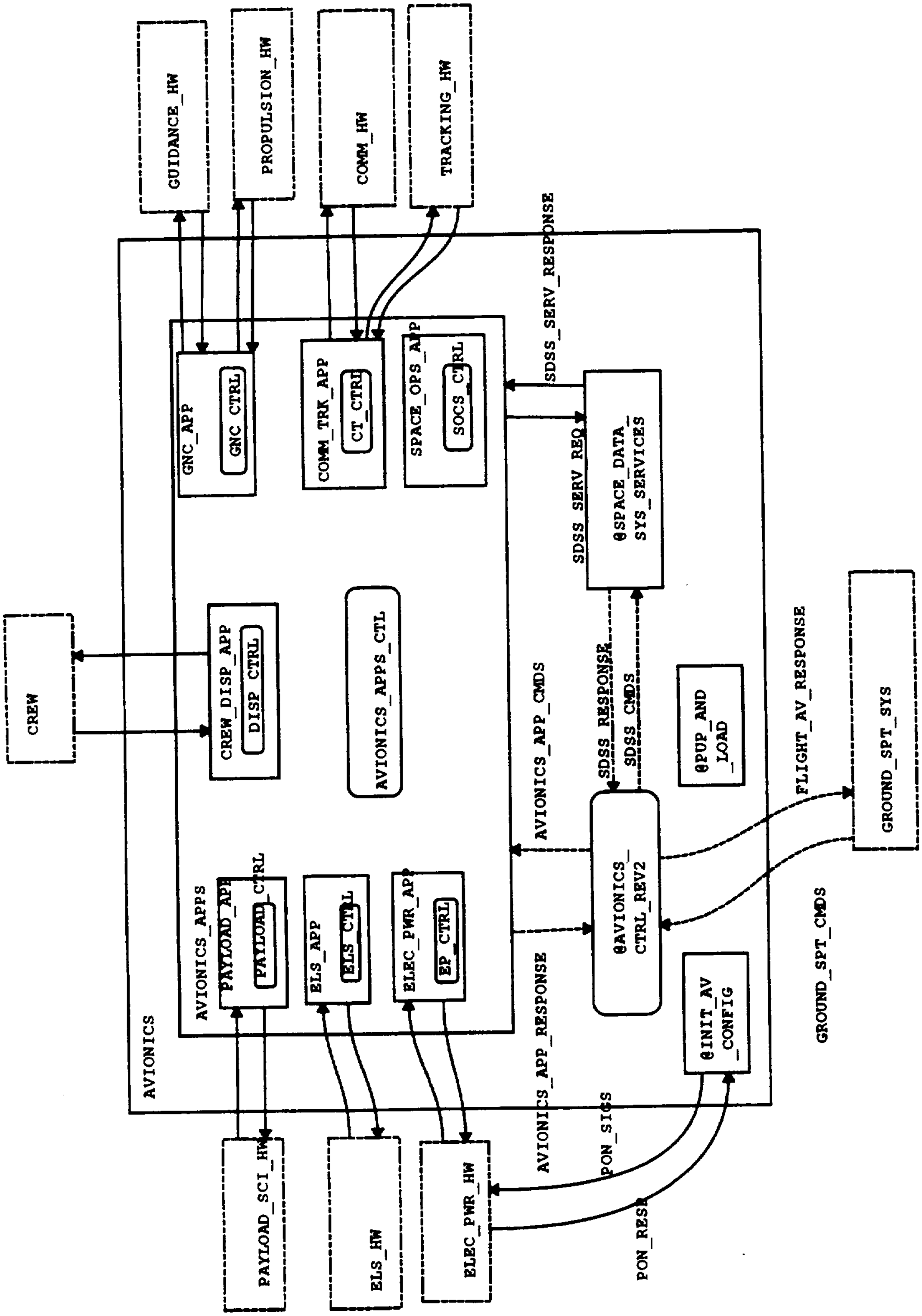


Figure D-1. SGOAA Activity Chart

```
STRUCTURE FOR SGA0:
===================

                                        --------------
                                        |            |
                                        |   SGA0:    |
                                        |            |
                                        -----D-1------
                                              |
                                              |
              -------------------------------------------------------------
              |                  |                  |                   |
        --------------     --------------     --------------     --------------
        |            |     |            |     |PROPULSION_H|     |            |
        |  AVIONICS  |     |ELEC_PWR_HW |     |W           |     |GUIDANCE_HW |
        |            |     |            |     |            |     |            |
        --------------     --------------     --------------     --------------
CONTINUE...
              -------------------------------------------------------------
              |                  |                  |                   |
        --------------     --------------     --------------     --------------
        |GROUND_SPT_S|     |PAYLOAD_SCI_|     |            |     |            |
        |YS          |     |HW          |     |   ELS_HW   |     |TRACKING_HW |
        |            |     |            |     |            |     |            |
        --------------     --------------     --------------     --------------
CONTINUE...
              --------------------------------
              |                  |
        --------------     --------------
        |            |     |            |
        |  COMM_HW   |     |    CREW    |
        |            |     |            |
        --------------     --------------
```

Figure D-2. SGOAA Activity Structure

```
LEVEL     2
                                   ---------------
                                   |             |
                                   |  AVIONICS   |
                                   |             |
                                   ---------------
                                          |
                                          |
              -----------------------------------------------------------------------------
              |                     |                     |                     |
        ---------------       ---------------       ---------------       ---------------
        |SPACE_DATA_S|        |INIT_AV_CONF|        |            |        |AVIONICS_APP|
        |YS_SERVICES |        |IG          |        |PUP_AND_LOAD|        |S           |
        |            |        |            |        |            |        |            |
        -----D-6------        -----D-11-----        -----D-5------        ---------------
CONTINUE...
              -----------------------------------------
              |
        ---------------
        |AVIONICS_CTR|
        |L_REV2      |
        |            |
        -----D-3------

LEVEL     3
                                   ---------------
                                   |SPACE_DATA_S|
                                   |YS_SERVICES |
                                   |            |
                                   -----D-6------
                                          |
                                          |
              ------------------------------------------------------
              |                     |                     |
        ---------------       ---------------       ---------------
        |SPACE_DATA_S|        |AVIONICS_CTR|        |AVIONICS_APP|
        |YS_SERVICES |        |L_REV2      |        |S           |
        |            |        |            |        |            |
        -----D-6------        -----D-3------        ---------------

                                   ---------------
                                   |INIT_AV_CONF|
                                   |IG          |
                                   |            |
                                   -----D-11-----
                                          |
                                          |
              -------------------------------------
              |                     |
        ---------------       ---------------
        |INIT_AV_CONF|        |            |
        |IG          |        |ELEC_PWR_HW |
        |            |        |            |
        -----D-11-----        ---------------
```

Figure D-2. SGOAA Activity Structure - continued

```
                          --------------
                          |            |
                          |PUP_AND_LOAD|
                          |            |
                          -----D-5------
                                 |
                                 |
          ---------------------------
          |
--------------
|            |
|PUP_AND_LOAD|
|            |
--------------

                          --------------
                          |AVIONICS_APP|
                          |S           |
                          |            |
                          --------------
                                 |
                                 |
          ----------------------------------------------------
          |                |                 |                 |
--------------    --------------    --------------    --------------
|            |    |AVIONICS_APP|    |CREW_DISP_AP|    |SPACE_OPS_AP|
|PAYLOAD_APP |    |S_CTL       |    |P           |    |P           |
|            |    |            |    |            |    |            |
--------------    --------------    --------------    --------------
CONTINUE...
          ----------------------------------------------------
          |                |                 |                 |
--------------    --------------    --------------    --------------
|            |    |            |    |            |    |            |
|COMM_TRK_APP|    |  GNC_APP   |    |ELEC_PWR_APP|    |  ELS_APP   |
|            |    |            |    |            |    |            |
--------------    --------------    --------------    --------------
```

Figure D-2. SGOAA Activity Structure - continued

```
LEVEL      4
                                   --------------
                                   |SPACE_DATA_S|
                                   |YS_SERVICES |
                                   |    D-6     |
                                   --------------
                                         |
                                         |
             ------------------------------------------------------------
             |                 |                  |                   |
      --------------    --------------    --------------    --------------
      |IO_DATA_SERV|    |            |    |SDSS_CTRL_RE|    |            |
      |_MGR        |    |OP_SYS_SERV |    |V1          |    |DATA_SYS_MGR|
      |            |    |            |    |    D-9     |    |            |
      --------------    --------------    --------------    --------------
CONTINUE...
             -------------------------------
             |                 |
      --------------    --------------
      |NETWORK_SERV|    |DATA_BASE_MG|
      |_MGR        |    |R           |
      |            |    |            |
      --------------    --------------

                                   --------------
                                   |INIT_AV_CONF|
                                   |IG          |
                                   |    D-11    |
                                   --------------
                                         |
                                         |
             ------------------------------------------------------------
             |                 |                  |                   |
      --------------    --------------    --------------    --------------
      |AV_CONFIG_IN|    |            |    |            |    |            |
      |IT          |    |  DO_INIT   |    | DO_CONFIG  |    | LOAD_CT_SW |
      |    D-12    |    |            |    |            |    |            |
      --------------    --------------    --------------    --------------
CONTINUE...
             ----------------------------------------
             |                 |                  |
      --------------    --------------    --------------
      |            |    |            |    |            |
      |LOAD_GNC_SW |    |LOAD_ELS_SW |    |LOAD_SOCS_SW|
      |            |    |            |    |            |
      --------------    --------------    --------------
```

Figure D-2. SGOAA Activity Structure - continued

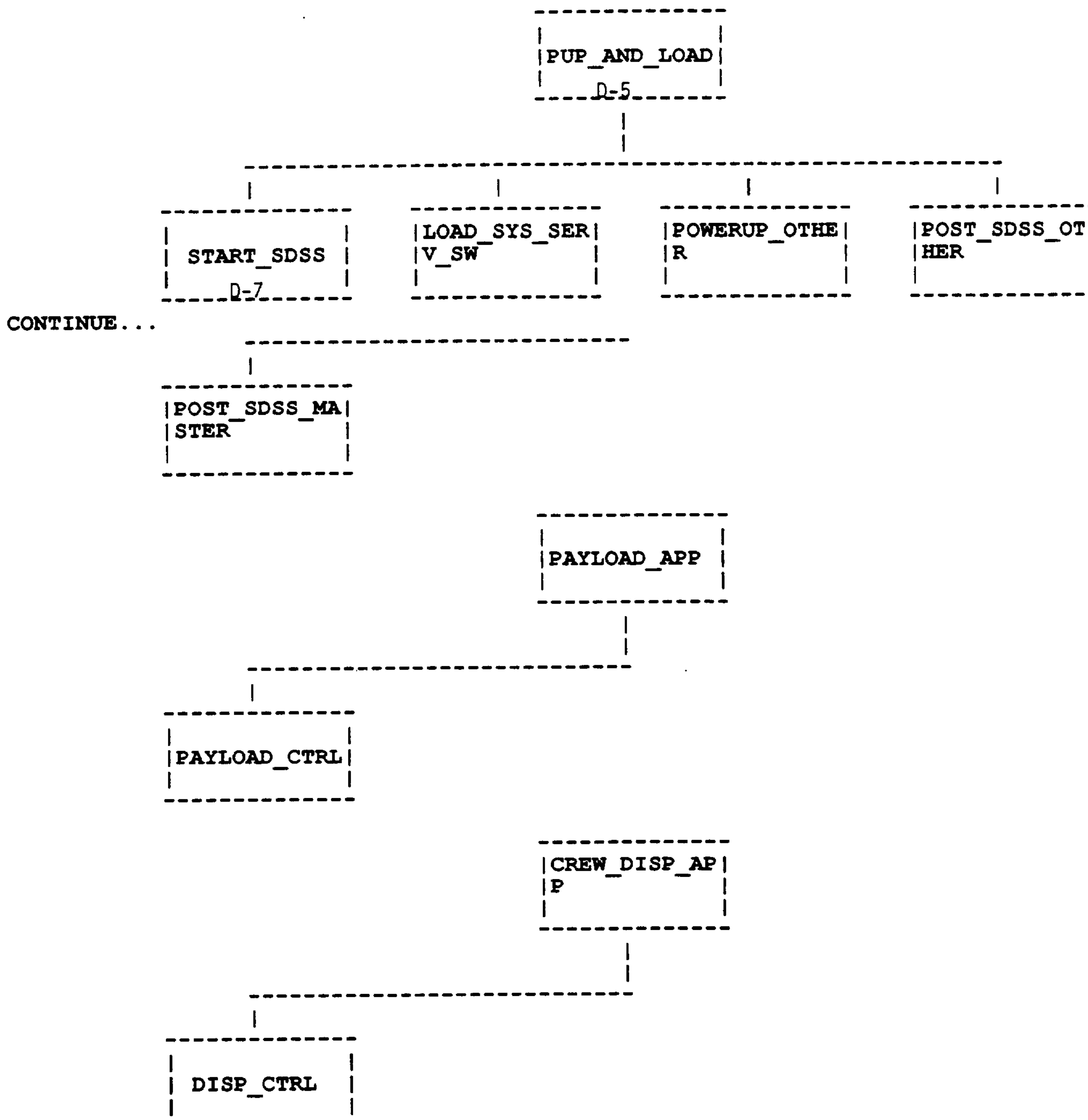


Figure D-2. SGOAA Activity Structure - continued

```
                                    ---------------
                                    |SPACE_OPS_AP|
                                    |P           |
                                    |            |
                                    ---------------
                                           |
                                           |
                 -----------------------------
                 |
          ---------------
          |             |
          | SOCS_CTRL   |
          |             |
          ---------------

                                    ---------------
                                    |             |
                                    |COMM_TRK_APP |
                                    |             |
                                    ---------------
                                           |
                                           |
                 -----------------------------
                 |
          ---------------
          |             |
          |  CT_CTRL    |
          |             |
          ---------------

                                    ---------------
                                    |             |
                                    |   GNC_APP   |
                                    |             |
                                    ---------------
                                           |
                                           |
                 -----------------------------
                 |
          ---------------
          |             |
          |  GNC_CTRL   |
          |             |
          ---------------
```

Figure D-2. SGOAA Activity Structure - continued

```
                                            ---------------
                                            |             |
                                            |ELEC_PWR_APP |
                                            |             |
                                            ---------------
                                                  |
                                                  |
                  ---------------------------------
                  |
             ---------------
             |             |
             |  EP_CTRL    |
             |             |
             ---------------

                                            ---------------
                                            |             |
                                            |   ELS_APP   |
                                            |             |
                                            ---------------
                                                  |
                                                  |
                  ---------------------------------
                  |
             ---------------
             |             |
             |  ELS_CTRL   |
             |             |
             ---------------
```

Figure D-2. SGOAA Activity Structure - concluded

Table D-1. SGOAA Activity Chart Dictionary

Dictionary for chart SGA0

External Activities

COMM_HW
external activity in chart SGA0

CREW
external activity in chart SGA0

ELEC_PWR_HW
external activity in chart SGA0

ELS_HW
external activity in chart SGA0

GROUND_SPT_SYS
external activity in chart SGA0

GUIDANCE_HW
external activity in chart SGA0

PAYLOAD_SCI_HW
external activity in chart SGA0

PROPULSION_HW
external activity in chart SGA0

TRACKING_HW
external activity in chart SGA0

Elements defined and/or used in chart SGA0

ALL_SOFT_RESET (information-flow); unresolved in chart: SGA0

ALTIMETER_PON (condition); unresolved in chart: SGA0

AVIONICS_APP_CMDS (information-flow); unresolved in chart: SGA0

AVIONICS_APP_RESPONSE (information-flow); defined in chart: SGA0
Contains: MAJOR_FAILURE

DO_MANUAL_OP (information-flow); unresolved in chart: SGA0

DATA_BASE_SOFT_RESET (event); defined in chart: SGA0

DATA_SYS_SOFT_RESET (event); defined in chart: SGA0

DATA_SYS_SOFT_RESET_INFO (information-flow); defined in chart: SGA0
Contains: IO_DATA_SOFT_RESET
DATA_BASE_SOFT_RESET
OP_SYS_SOFT_RESET
NETWORK_SERV_SOFT_RESET
DATA_SYS_SOFT_RESET
ALL_SOFT_RESET

DEGRADE_MODE (condition); unresolved in chart: SGA0

DO_ALTIMETER_PWR (event); unresolved in chart: SGA0

DO_AVIONICS_TEST (information-flow); unresolved in chart: SGA0

DO_HARD_RESET (information-flow); unresolved in chart: SGA0

DO_IMU_PWR (event); unresolved in chart: SGA0

DO_POSITION_SYS_PWR (event); unresolved in chart: SGA0

DO_PROCESSOR_SELF_TEST (information-flow); unresolved in chart: SGA0

DO_RADAR_PWR (event); unresolved in chart: SGA0

DO_SOFT_RESET (information-flow); unresolved in chart: SGA0

DO_SUBSYSTEM_TEST (information-flow); unresolved in chart: SGA0

DO_TRANSMITTER_PWR (event); unresolved in chart: SGA0

FLIGHT_AV_RESPONSE (information-flow); defined in chart: SGA0
Contains: POWER_OFF_AV_MSG
VEHICLE_INITIALIZED_MSG
PROCESSOR_SELF_TESTED_MSG
SUBSYS_TESTED_MSG
HARD_RESET_DONE
SOFT_RESET_DONE

GROUND_SPT_CMDS (information-flow); defined in chart: SGA0
Contains: POWER_ON_AV
INITIALIZE_VEHICLE
DO_PROCESSOR_SELF_TEST
DO_SUBSYSTEM_TEST
DO_AVIONICS_TEST
DO_HARD_RESET
DO_SOFT_RESET
POWER_OFF_AV
DEGRADE_MODE
OPN_DONE
DO_MANUAL_OP

HARD_RESET_DONE (information-flow); unresolved in chart: SGA0

IMU_PON (condition); unresolved in chart: SGA0

INITIALIZE_VEHICLE (information-flow); unresolved in chart: SGA0

IO_DATA_SOFT_RESET (event); defined in chart: SGA0

MAJOR_FAILURE (condition); unresolved in chart: SGA0

NETWORK_SERV_SOFT_RESET (event); defined in chart: SGA0

OPN_DONE (event); unresolved in chart: SGA0

OP_SYS_SOFT_RESET (event); defined in chart: SGA0

Table D-1. SGOAA Activity Chart Dictionary - concluded

```
POW_RESP (information-flow); defined in chart: SGA0
Contains: RADAR_PON
          ALTIMETER_PON
          TRANSMITTER_PON
          POSITION_SYS_PON
          IMU_PON

POW_SIGS (information-flow); defined in chart: SGA0
Contains: DO_RADAR_PWR
          DO_POSITION_SYS_PWR
          DO_IMU_PWR
          DO_TRANSMITTER_PWR
          DO_ALTIMETER_PWR

POSITION_SYS_PON (condition); unresolved in chart: SGA0

POWER_OFF_AV (event); unresolved in chart: SGA0

POWER_OFF_AV_MSG (information-flow); unresolved in chart: SGA0

POWER_ON_AV (event); unresolved in chart: SGA0

PROCESSOR_SELF_TESTED_MSG (information-flow); unresolved in
chart: SGA0

RADAR_PON (condition); unresolved in chart: SGA0

SDSS_CMDS (information-flow); defined in chart: SGA0
Contains: DATA_SYS_SOFT_RESET_INFO

SDSS_RESPONSE (information-flow); defined in chart: SGA0
Contains: MAJOR_FAILURE

SDSS_SERV_REQ (information-flow); unresolved in chart: SGA0

SDSS_SERV_RESPONSE (information-flow); unresolved in chart:
SGA0

SOFT_RESET_DONE (information-flow); unresolved in chart: SGA0

SUBSYS_TESTED_MSG (information-flow); unresolved in chart:
SGA0

TRANSMITTER_PON (condition); unresolved in chart: SGA0

VEHICLE_INITIALIZED_MSG (information-flow); unresolved in
chart: SGA0
```

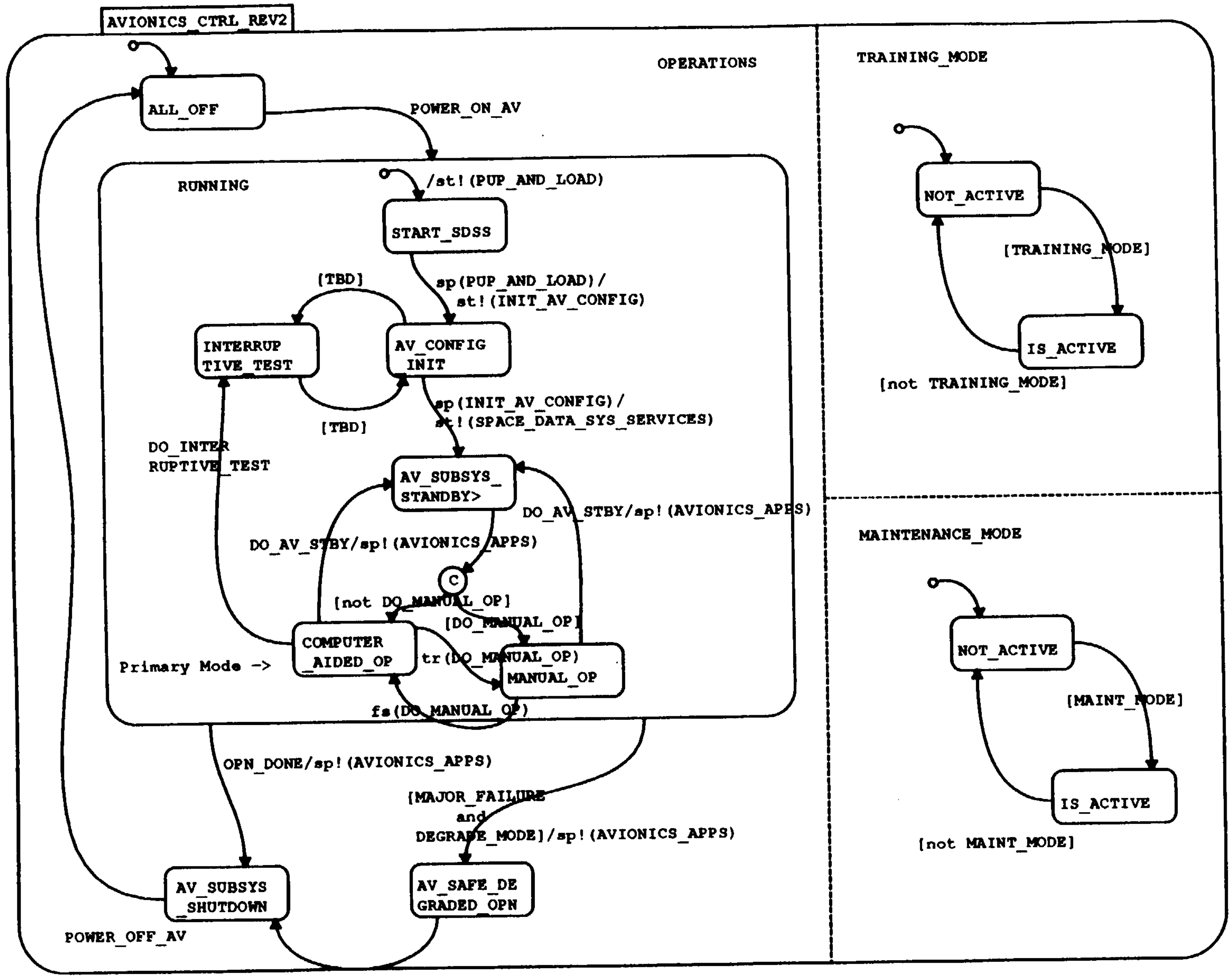


Figure D-3. Avionics Control Statechart

```
STRUCTURE FOR AVIONICS_CTRL_REV2:
=================================

                                          --------------
                                          |AVIONICS_CTR|
                                          |L_REV2:     |
                                          |            |
                                          -----D-3------
                                                |
                                                |
                     ----------------------------
                     |
                --------------
                |AVIONICS_CTR|
                |L_REV2      |
                |            |
                -----D-3------

LEVEL     2
                                          --------------
                                          |AVIONICS_CTR|
                                          |L_REV2      |
                                          |            |
                                          -----D-3------
                                                |
                                                |
                     ------------------------------------
                     |                 |                |
                --------------   --------------   --------------
                |TRAINING_MOD|   |MAINTENANCE_|   |            |
                |E           |   |MODE        |   | OPERATIONS |
                |            |   |            |   |            |
                --------------   --------------   --------------

LEVEL     3
                                          --------------
                                          |TRAINING_MOD|
                                          |E           |
                                          |            |
                                          --------------
                                                |
                                                |
                     ----------------------------
                     |                 |
                --------------   --------------
                |            |   |            |
                | NOT_ACTIVE |   | IS_ACTIVE  |
                |            |   |            |
                --------------   --------------
```

Figure D-4. Avionics Control State Structure

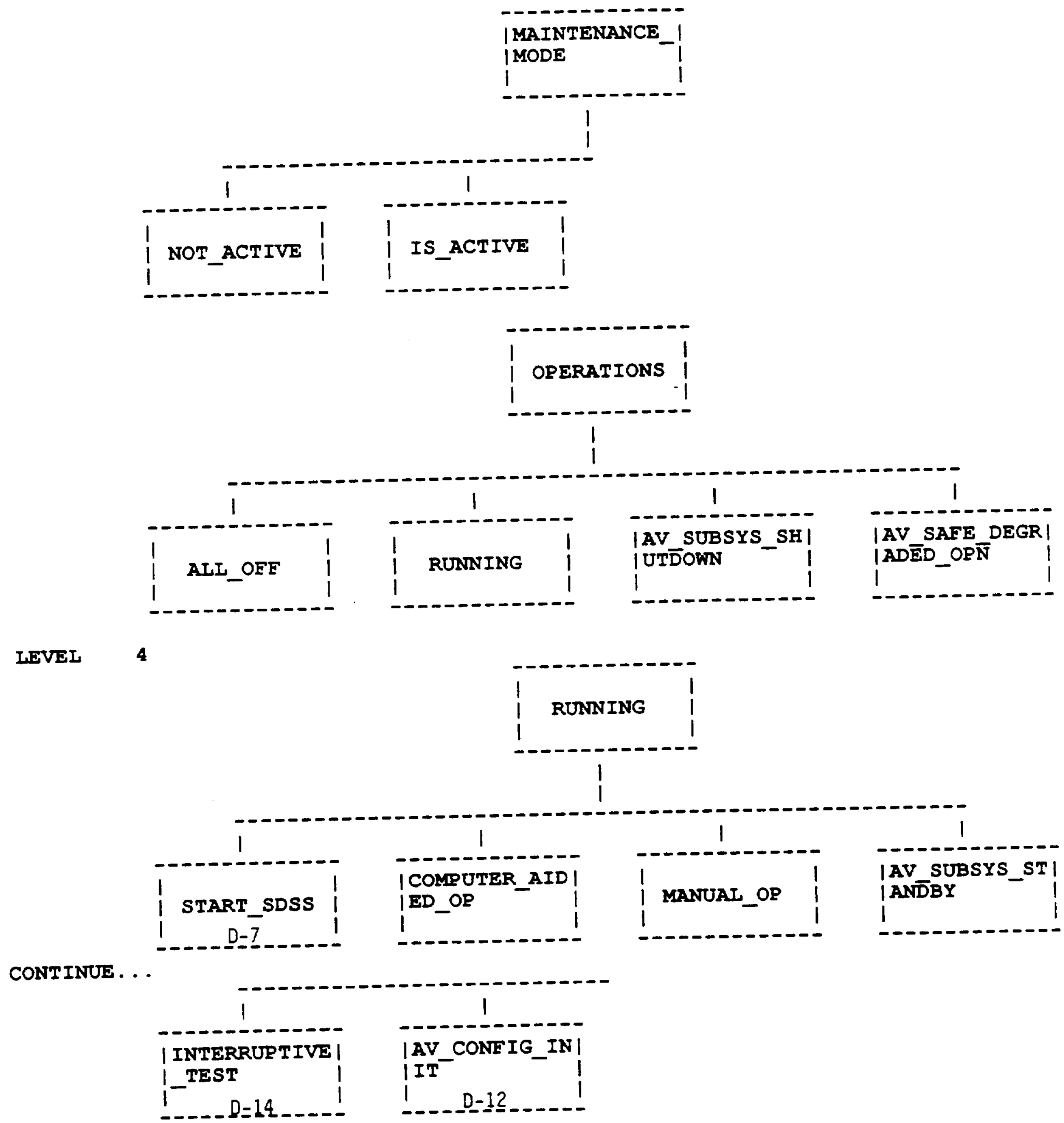


Figure D-4. Avionics Control State Structure - concluded

Table D-2. Avionics Control Statechart Dictionary

Dictionary for chart AVIONICS_CTRL_REV2

States with Static Reactions and Activities Throughout/Within

AV_SUBSYS_STANDBY
Type: BASIC
Reactions: exiting/st!(AVIONICS_APPS)

Elements defined and/or used in chart AVIONICS_CTRL_REV2

AVIONICS_APPS (activity); defined in chart: SGA0

DEGRADE_MODE (condition); unresolved in chart: SGA0

DO_AV_STBY (event); unresolved in chart: AVIONICS_CTRL_REV2

DO_INTERRUPTIVE_TEST (event); unresolved in chart: AVIONICS_CTRL_REV2

DO_MANUAL_OP (condition); unresolved in chart: AVIONICS_CTRL_REV2

INIT_AV_CONFIG (activity); defined in chart: SGA0

MAINT_MODE (condition); unresolved in chart: AVIONICS_CTRL_REV2

MAJOR_FAILURE (condition); unresolved in chart: SGA0

OPN_DONE (event); unresolved in chart: SGA0

POWER_OFF_AV (event); unresolved in chart: SGA0

POWER_ON_AV (event); unresolved in chart: SGA0

PUP_AND_LOAD (activity); defined in chart: SGA0

SPACE_DATA_SYS_SERVICES (activity); defined in chart: SGA0

TBD (condition); unresolved in chart: AVIONICS_CTRL_REV2

TRAINING_MODE (condition); unresolved in chart: AVIONICS_CTRL_REV2

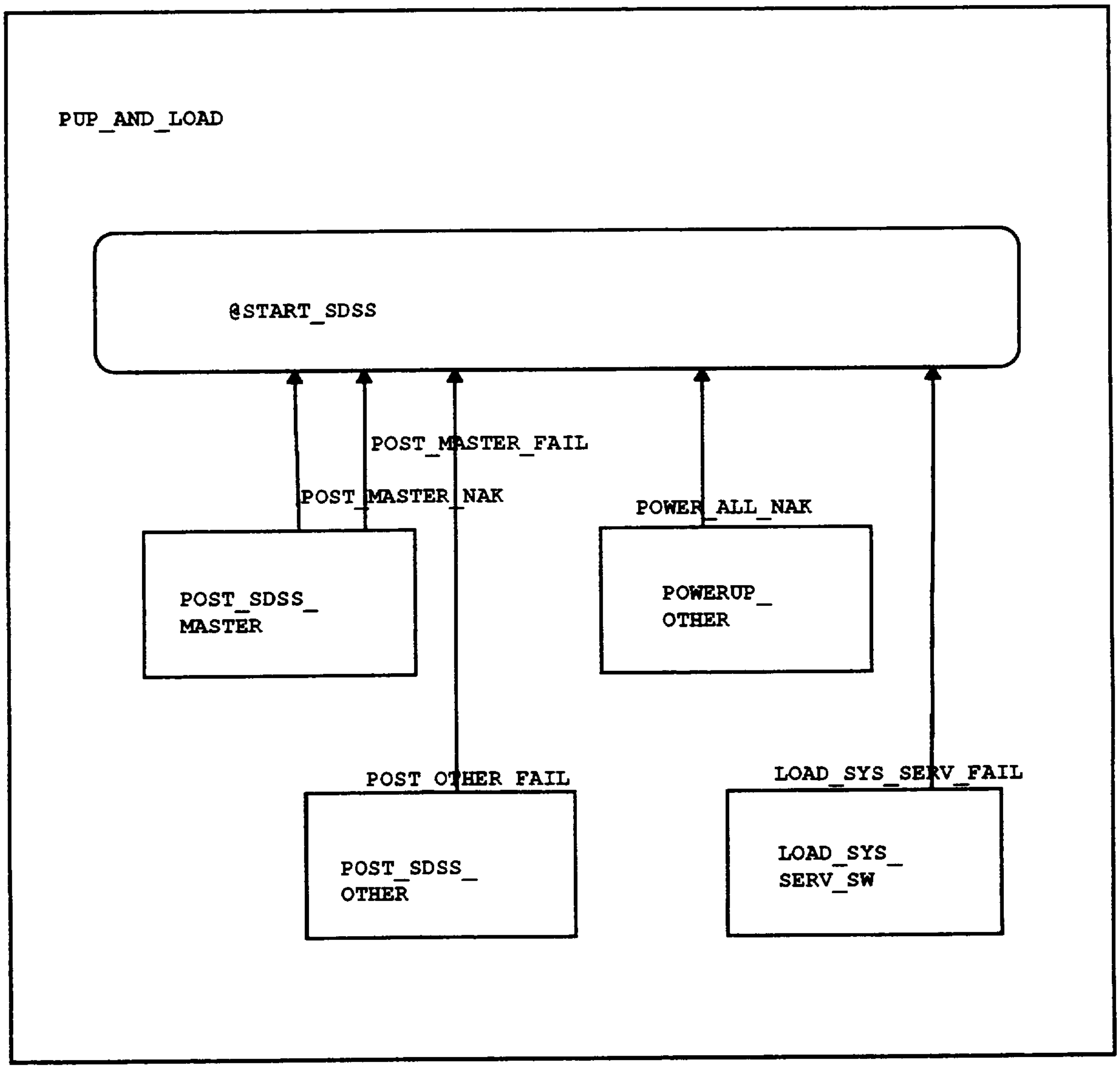


Figure D-5. Powerup and Load Activity Chart

Table D-3. Powerup and Load Activity Chart Dictionary

Dictionary for chart PUP_AND_LOAD

Elements defined and/or used in chart PUP_AND_LOAD

LOAD_SYS_SERV_FAIL (condition); unresolved in chart: PUP_AND_LOAD

POST_MASTER_FAIL (condition); unresolved in chart: PUP_AND_LOAD

POST_MASTER_NAK (condition); unresolved in chart: PUP_AND_LOAD

POST_OTHER_FAIL (condition); unresolved in chart: PUP_AND_LOAD

POWER_ALL_NAK (condition); unresolved in chart: PUP_AND_LOAD

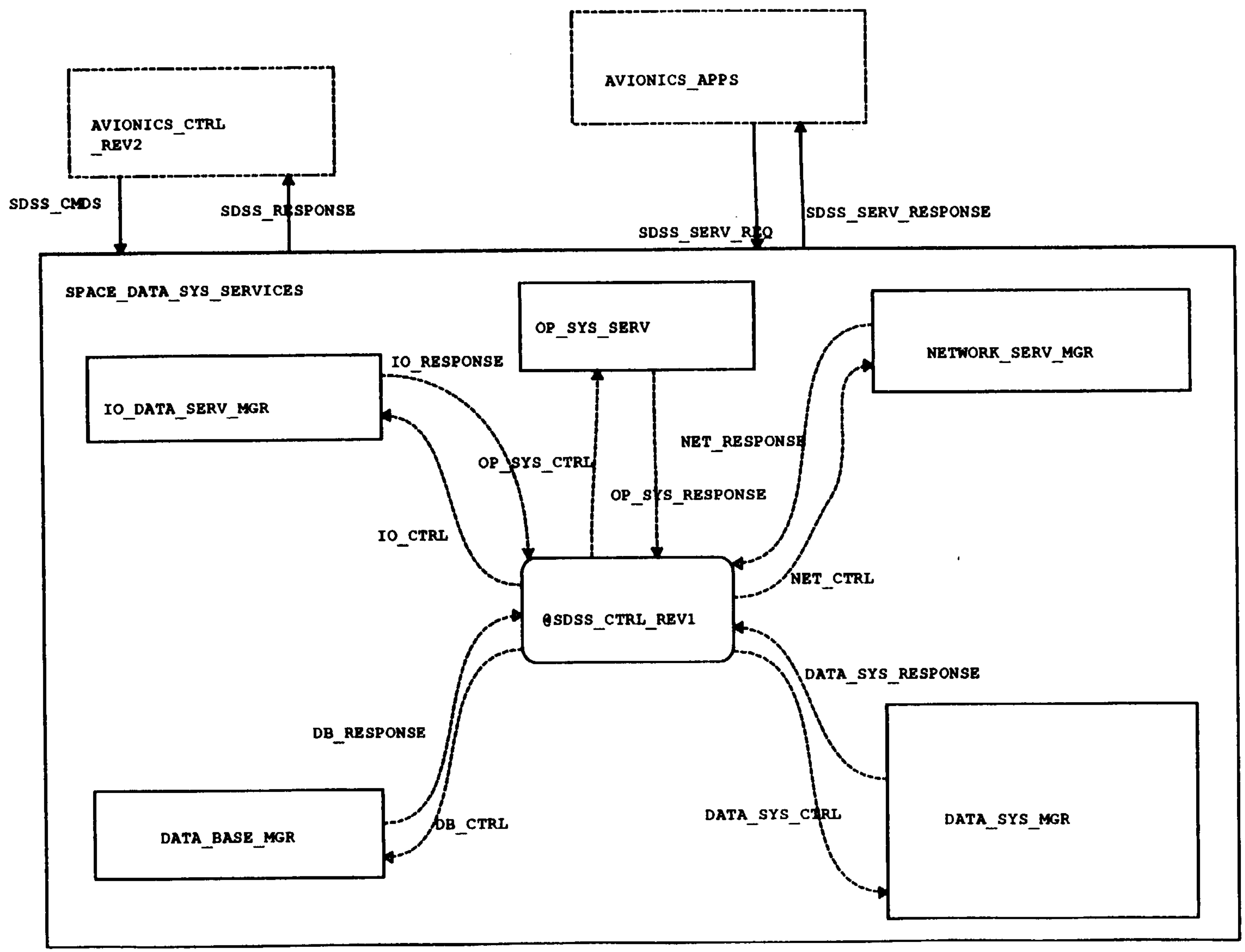


Figure D-6. Space-Data System Services Activity Chart

Table D-4. Space-Data System Services Activity Chart Directory

Dictionary for chart SPACE_DATA_SYS_SERVICES

External Activities

AVIONICS_APPS
activity in chart SGA0

AVIONICS_CTRL_REV2
control activity in chart SGA0

Elements defined and/or used in chart SPACE_DATA_SYS_SERVICES

DATA_SYS_CTRL (information-flow); unresolved in chart: SPACE_DATA_SYS_SERVICES

DATA_SYS_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

DATA_SYS_RESPONSE (information-flow); defined in chart: SPACE_DATA_SYS_SERVICES
Contains: DATA_SYS_RELOADED

DB_CTRL (information-flow); unresolved in chart: SPACE_DATA_SYS_SERVICES

DB_RESPONSE (information-flow); unresolved in chart: SPACE_DATA_SYS_SERVICES

IO_CTRL (information-flow); unresolved in chart: SPACE_DATA_SYS_SERVICES

IO_DATA_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

IO_RESPONSE (information-flow); defined in chart: SPACE_DATA_SYS_SERVICES
Contains: IO_DATA_RELOADED

NETWORK_SERV_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

NET_CTRL (information-flow); unresolved in chart: SPACE_DATA_SYS_SERVICES

NET_RESPONSE (information-flow); defined in chart: SPACE_DATA_SYS_SERVICES
Contains: NETWORK_SERV_RELOADED

OP_SYS_CTRL (information-flow); unresolved in chart: SPACE_DATA_SYS_SERVICES

OP_SYS_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

OP_SYS_RESPONSE (information-flow); defined in chart: SPACE_DATA_SYS_SERVICES
Contains: OP_SYS_RELOADED

SDSS_CMDS (information-flow); defined in chart: SGA0
Contains: DATA_SYS_SOFT_RESET_INFO

SDSS_RESPONSE (information-flow); defined in chart: SGA0
Contains: MAJOR_FAILURE

SDSS_SERV_REQ (information-flow); unresolved in chart: SGA0

SDSS_SERV_RESPONSE (information-flow); unresolved in chart: SGA0

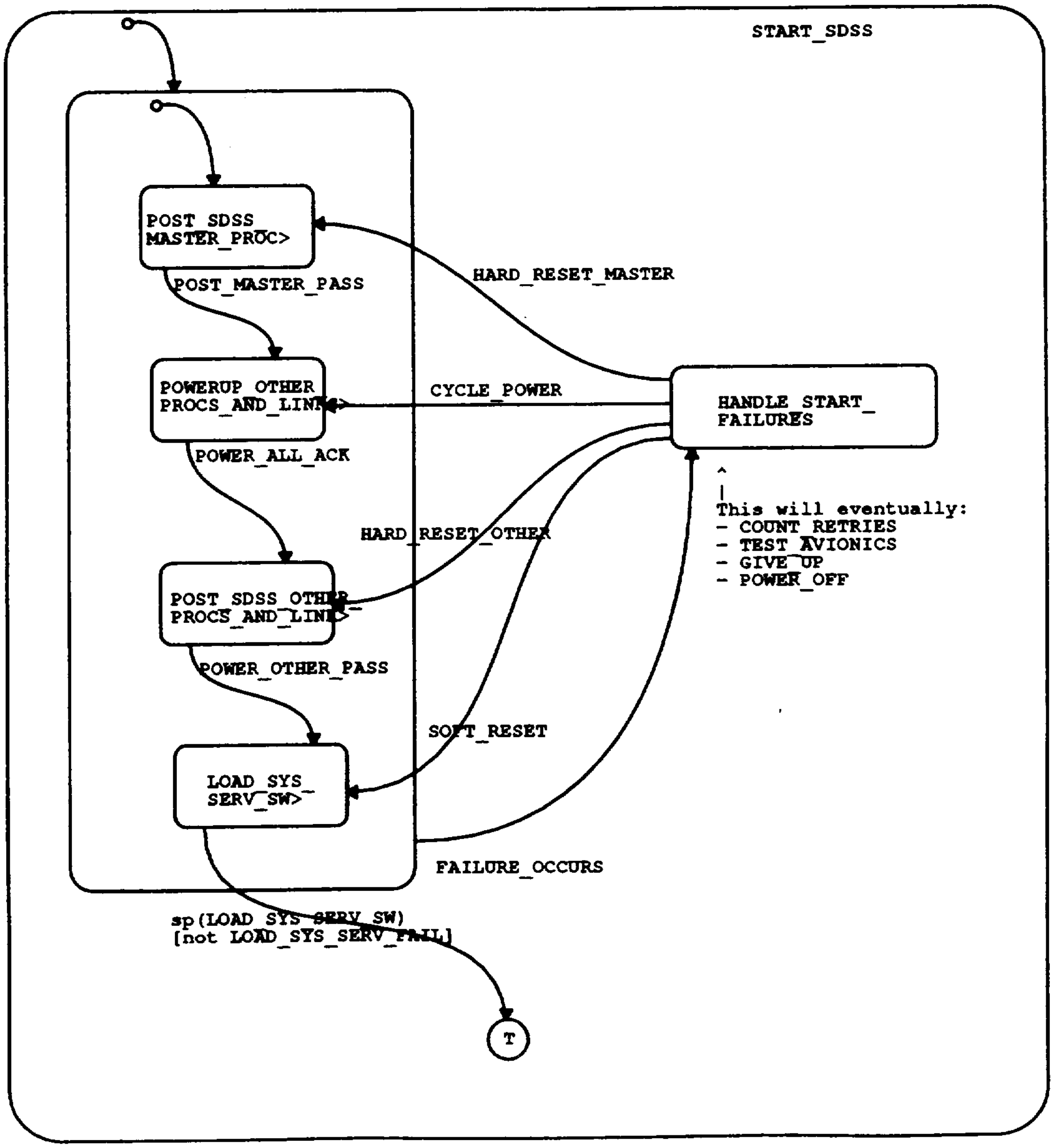


Figure D-7. Start SDSS Statechart

Table D-5. Start SDSS Statechart Dictionary

```
Dictionary for chart START_SDSS
-------------------------------

States with Static Reactions and Activities Throughout/Within
-------------------------------------------------------------
LOAD_SYS_SERV_SW
Type: BASIC
Reactions: entering/st!(LOAD_SYS_SERV_SW)

POST_SDSS_MASTER_PROC
Type: BASIC
Reactions: entering/st!(POST_SDSS_MASTER)

POST_SDSS_OTHER_PROCS_AND_LINK
Type: BASIC
Reactions: entering/st!(POST_SDSS_OTHER)

POWERUP_OTHER_PROCS_AND_LINKS
Type: BASIC
Reactions: entering/st!(POWERUP_OTHER)

Elements defined and/or used in chart START_SDSS
------------------------------------------------
CYCLE_POWER (event); unresolved in chart: START_SDSS

FAILURE_OCCURS (event); defined in chart: START_SDSS
Definition: sp(POST_SDSS_MASTER)[POST_MASTER_NAK or POST_MASTER_
            FAIL] or
            sp(POWERUP_OTHER)[POWER_ALL_NAK] or
            sp(POST_SDSS_OTHER)[POST_OTHER_FAIL] or
            sp(LOAD_SYS_SERV_SW)[LOAD_SYS_SERV_FAIL]

HARD_RESET_MASTER (event); unresolved in chart: START_SDSS

HARD_RESET_OTHER (event); unresolved in chart: START_SDSS

LOAD_SYS_SERV_FAIL (condition); unresolved in chart: PUP_AND_
LOAD

LOAD_SYS_SERV_SW (activity); defined in chart: PUP_AND_LOAD

POST_MASTER_FAIL (condition); unresolved in chart: PUP_AND_
LOAD

POST_MASTER_NAK (condition); unresolved in chart: PUP_AND_LOAD

POST_MASTER_PASS (event); defined in chart: START_SDSS
Definition: sp(POST_SDSS_MASTER)[not (POST_MASTER_NAK or POST_
            MASTER_FAIL)]

POST_OTHER_FAIL (condition); unresolved in chart: PUP_AND_LOAD

POST_SDSS_MASTER (activity); defined in chart: PUP_AND_LOAD

POST_SDSS_OTHER (activity); defined in chart: PUP_AND_LOAD

POWERUP_OTHER (activity); defined in chart: PUP_AND_LOAD

POWER_ALL_ACK (event); defined in chart: START_SDSS
Definition: sp(POWERUP_OTHER)[not POWER_ALL_NAK]

POWER_ALL_NAK (condition); unresolved in chart: PUP_AND_LOAD

POWER_OTHER_PASS (event); defined in chart: START_SDSS
Definition: sp(POST_SDSS_OTHER)[not POST_OTHER_FAIL]

SOFT_RESET (event); unresolved in chart: START_SDSS
```

```
STRUCTURE FOR START_SDSS:
=========================

                                   --------------
                                   |            |
                                   |START_SDSS: |
                                   |            |
                                   -----D-7------
                                         |
                                         |
                  ------------------------
                  |
               --------------
               |            |
               | START_SDSS |
               |            |
               -----D-7------

LEVEL     2
                                   --------------
                                   |            |
                                   | START_SDSS |
                                   |            |
                                   -----D-7------
                                         |
                                         |
                  ------------------------
                  |                  |
               --------------     --------------
               |HANDLE_START|     |            |
               |_FAILURES   |     |  STATE#19  |
               |            |     |            |
               --------------     --------------

LEVEL     3
                                   --------------
                                   |            |
                                   |  STATE#19  |
                                   |            |
                                   --------------
                                         |
                                         |
                  ------------------------------------------------------
                  |                  |                  |                  |
               --------------     --------------     --------------     --------------
               |POST_SDSS_MA|     |LOAD_SYS_SER|     |POST_SDSS_OT|     |POWERUP_OTHE|
               |STER_PROC   |     |V_SW        |     |HER_PROCS_AN|     |R_PROCS_AND_|
               |            |     |            |     |D_LINK      |     |LINKS       |
               --------------     --------------     --------------     --------------
```

Figure D-8. Start_SDSS State Structure

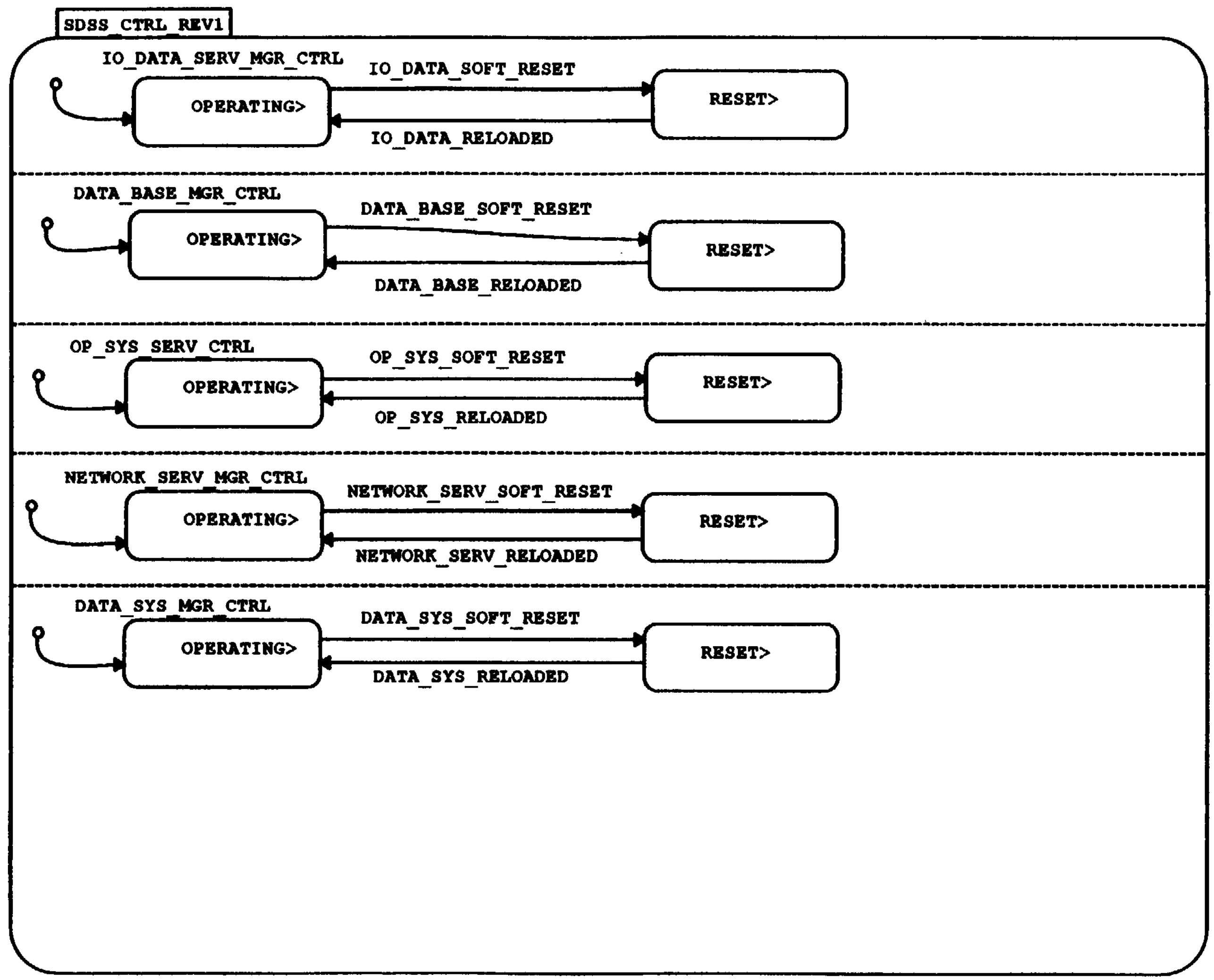


Figure D-9. SDSS Control Statechart

Table D-6. SDSS Control Statechart Dictionary

Dictionary for chart SDSS_CTRL_REV1

States with Static Reactions and Activities Throughout/Within

OPERATING
Type: BASIC
Unique name: IO_DATA_SERV_MGR_CTRL.OPERATING
Reactions: entering/st!(IO_DATA_SERV_MGR)

OPERATING
Type: BASIC
Unique name: DATA_SYS_MGR_CTRL.OPERATING
Reactions: entering/st!(DATA_SYS_MGR)

OPERATING
Type: BASIC
Unique name: NETWORK_SERV_MGR_CTRL.OPERATING
Reactions: entering/st!(NETWORK_SERV_MGR)

OPERATING
Type: BASIC
Unique name: OP_SYS_SERV_CTRL.OPERATING
Reactions: entering/st!(OP_SYS_SERV)

OPERATING
Type: BASIC
Unique name: DATA_BASE_MGR_CTRL.OPERATING
Reactions: entering/st!(DATA_BASE_MGR)

RESET
Type: BASIC
Unique name: IO_DATA_SERV_MGR_CTRL.RESET
Reactions: entering/sp!(IO_DATA_SERV_MGR)

RESET
Type: BASIC
Unique name: DATA_SYS_MGR_CTRL.RESET
Reactions: entering/sp!(DATA_SYS_MGR)

RESET
Type: BASIC
Unique name: NETWORK_SERV_MGR_CTRL.RESET
Reactions: entering/sp!(NETWORK_SERV_MGR)

RESET
Type: BASIC
Unique name: OP_SYS_SERV_CTRL.RESET
Reactions: entering/sp!(OP_SYS_SERV)

RESET
Type: BASIC
Unique name: DATA_BASE_MGR_CTRL.RESET
Reactions: entering/sp!(DATA_BASE_MGR)

Elements defined and/or used in chart SDSS_CTRL_REV1

DATA_BASE_MGR (activity); defined in chart: SPACE_DATA_SYS_SERVICES

DATA_BASE_RELOADED (event); defined in chart: SDSS_CTRL_REV1

DATA_BASE_SOFT_RESET (event); defined in chart: SGA0

DATA_SYS_MGR (activity); defined in chart: SPACE_DATA_SYS_SERVICES

DATA_SYS_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

DATA_SYS_SOFT_RESET (event); defined in chart: SGA0

IO_DATA_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

IO_DATA_SERV_MGR (activity); defined in chart: SPACE_DATA_SYS_SERVICES

IO_DATA_SOFT_RESET (event); defined in chart: SGA0

NETWORK_SERV_MGR (activity); defined in chart: SPACE_DATA_SYS_SERVICES

NETWORK_SERV_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

NETWORK_SERV_SOFT_RESET (event); defined in chart: SGA0

OP_SYS_RELOADED (event); defined in chart: SPACE_DATA_SYS_SERVICES

OP_SYS_SERV (activity); defined in chart: SPACE_DATA_SYS_SERVICES

OP_SYS_SOFT_RESET (event); defined in chart: SGA0

STRUCTURE FOR SDSS_CTRL_REV1:

```
                              -------------
                             |SDSS_CTRL_RE|
                             |V1:         |
                             |    D-9     |
                              -------------
                                   |
                                   |
            ------------------------
            |
 -------------
|SDSS_CTRL_RE|
|V1          |
|    D-9     |
 -------------
```

Figure D-10. SDSS_CNTRL_REV1 State Structure

```
LEVEL     2
                              --------------
                              |SDSS_CTRL_RE|
                              |V1          |
                              |     D-9    |
                              --------------
                                    |
                                    |
      -----------------------------------------------------------------
      |                  |                  |                  |
--------------     --------------     --------------     --------------
|IO_DATA_SERV|     |DATA_SYS_MGR|     |NETWORK_SERV|     |OP_SYS_SERV_|
|_MGR_CTRL   |     |_CTRL       |     |_MGR_CTRL   |     |CTRL        |
|            |     |            |     |            |     |            |
--------------     --------------     --------------     --------------
CONTINUE...
      ---------------------------
      |
--------------
|DATA_BASE_MG|
|R_CTRL      |
|            |
--------------

LEVEL     3
                              --------------
                              |IO_DATA_SERV|
                              |_MGR_CTRL   |
                              |            |
                              --------------
                                    |
                                    |
      -------------------------------
      |                  |
--------------     --------------
|            |     |            |
| OPERATING  |     |   RESET    |
|            |     |            |
--------------     --------------

                              --------------
                              |DATA_SYS_MGR|
                              |_CTRL       |
                              |            |
                              --------------
                                    |
                                    |
      -------------------------------
      |                  |
--------------     --------------
|            |     |            |
| OPERATING  |     |   RESET    |
|            |     |            |
--------------     --------------
```

Figure D-10. SDSS_CNTRL_REV1 State Structure - continued

```
                                      --------------
                                      |NETWORK_SERV|
                                      |_MGR_CTRL   |
                                      |            |
                                      --------------
                                             |
                                             |
                 ----------------------------
                 |                  |
    --------------     --------------
    |            |     |            |
    | OPERATING  |     |   RESET    |
    |            |     |            |
    --------------     --------------

                                      --------------
                                      |OP_SYS_SERV_|
                                      |CTRL        |
                                      |            |
                                      --------------
                                             |
                                             |
                 ----------------------------
                 |                  |
    --------------     --------------
    |            |     |            |
    | OPERATING  |     |   RESET    |
    |            |     |            |
    --------------     --------------

                                      --------------
                                      |DATA_BASE_MG|
                                      |R_CTRL      |
                                      |            |
                                      --------------
                                             |
                                             |
                 ----------------------------
                 |                  |
    --------------     --------------
    |            |     |            |
    | OPERATING  |     |   RESET    |
    |            |     |            |
    --------------     --------------
```

Figure D-10. SDSS_CNTRL_REV1 State Structure - concluded

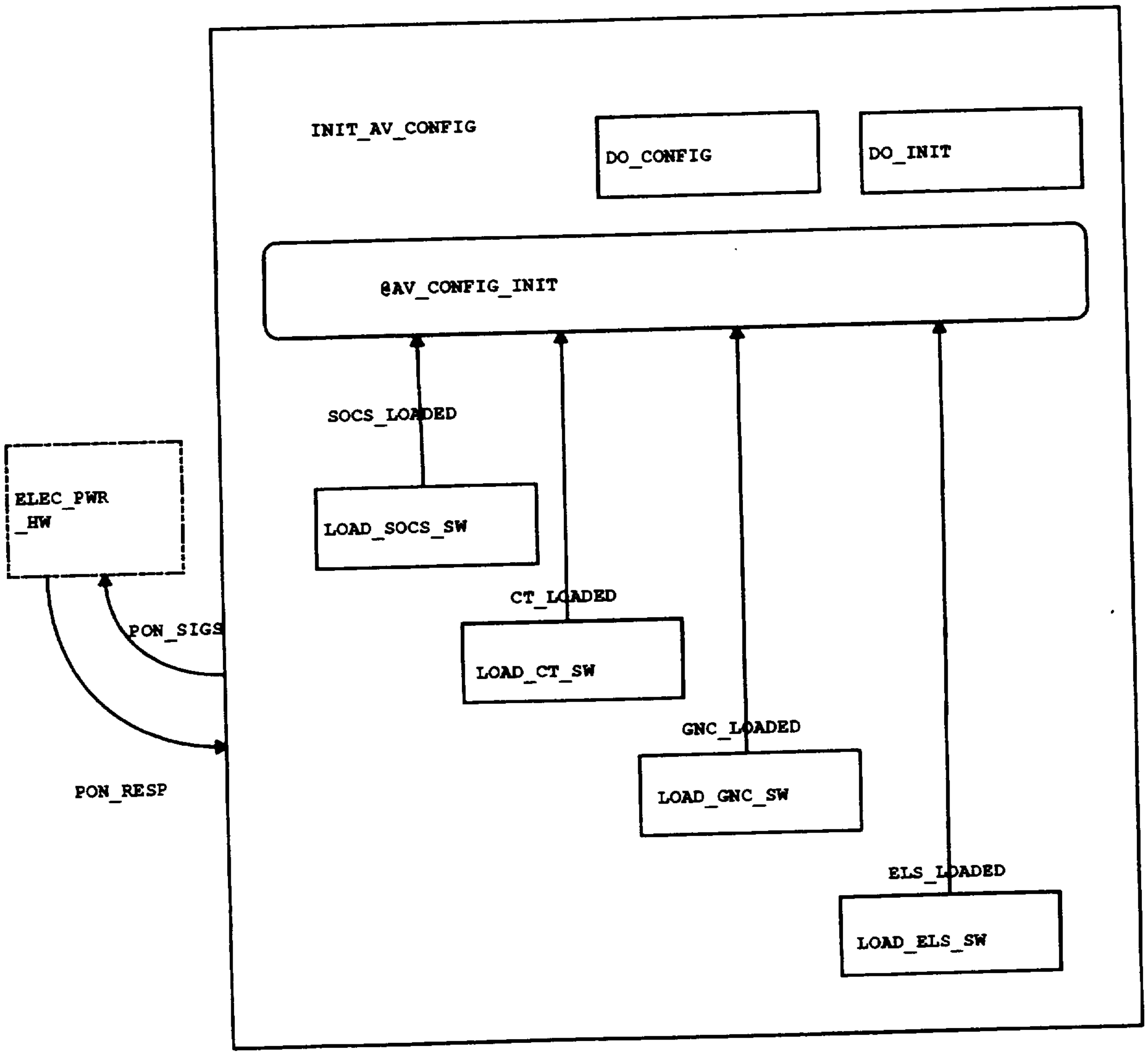


Figure D-11. Initial Avionics Configure Activity Chart

Table D-7. Initial Avionics Configure Activity Chart Dictionary

Dictionary for chart INIT_AV_CONFIG

External Activities

ELEC_PWR_HW
external activity in chart SGA0

Elements defined and/or used in chart INIT_AV_CONFIG

CT_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

ELS_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

GNC_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

PON_RESP (information-flow); defined in chart: SGA0
Contains: RADAR_PON
ALTIMETER_PON
TRANSMITTER_PON
POSITION_SYS_PON
IMU_PON

PON_SIGS (information-flow); defined in chart: SGA0
Contains: DO_RADAR_PWR
DO_POSITION_SYS_PWR
DO_IMU_PWR
DO_TRANSMITTER_PWR
DO_ALTIMETER_PWR

SOCS_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

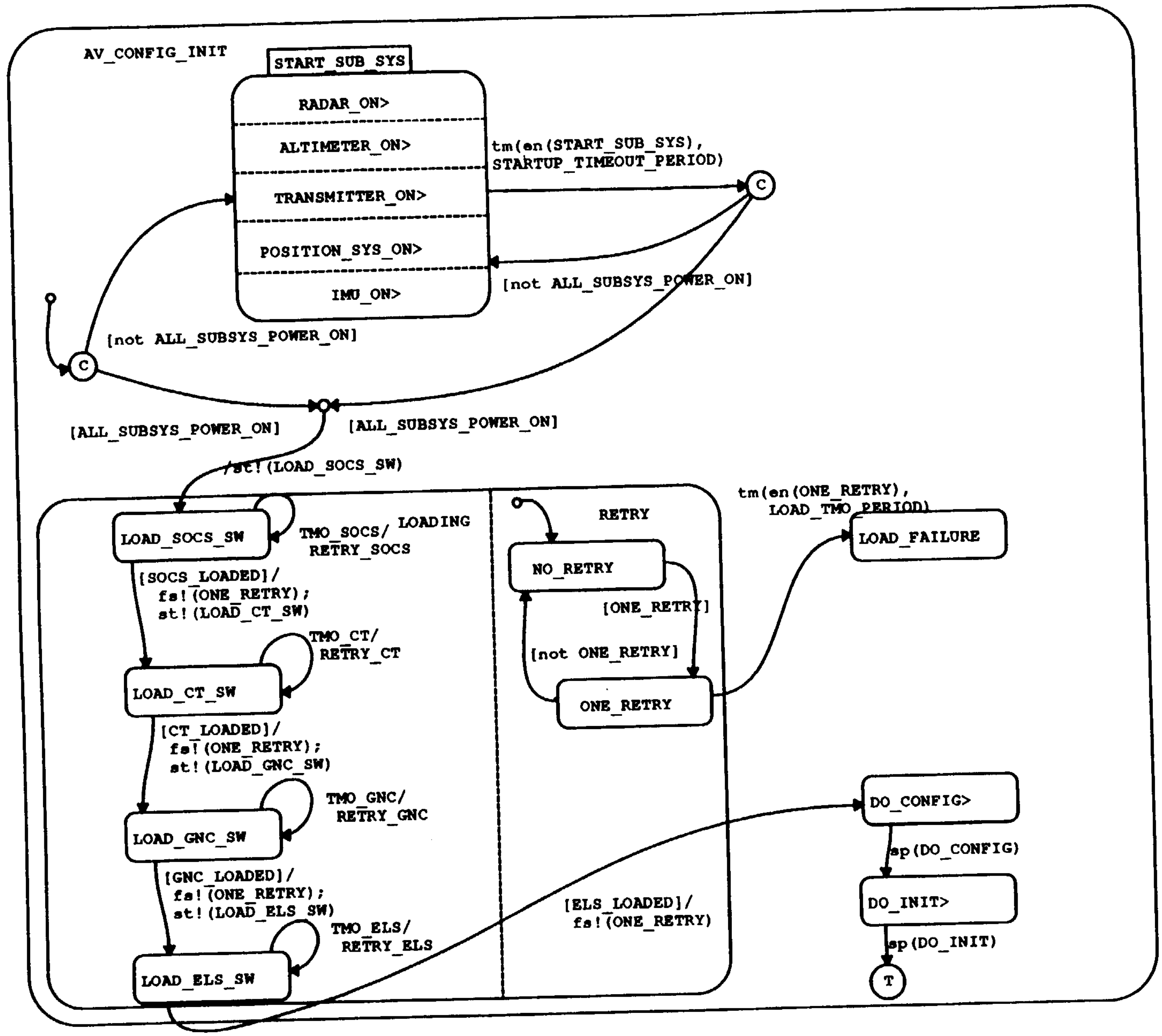


Figure D-12. Avionics Configure Initiate Statechart

Table D-8. Avionics Configure Initiate Statechart Directory

```
Dictionary for chart AV_CONFIG_INIT
-----------------------------------

States with Static Reactions and Activities Throughout/Within
-------------------------------------------------------------
ALTIMETER_ON
Type: COMPONENT BASIC
Reactions: entering/if not ALTIMETER_PON then DO_ALTIMETER_PWR
           end if

DO_CONFIG
Type: BASIC
Reactions: entering/st!(DO_CONFIG)

DO_INIT
Type: BASIC
Reactions: entering/st!(DO_INIT)

IMU_ON
Type: COMPONENT BASIC
Reactions: entering/if not IMU_PON then DO_IMU_PWR end if

POSITION_SYS_ON
Type: COMPONENT BASIC
Reactions: entering/if not POSITION_SYS_PON then DO_POSITION_SYS_
           PWR end if

RADAR_ON
Type: COMPONENT BASIC
Reactions: entering/if not RADAR_PON then DO_RADAR_PWR end if

TRANSMITTER_ON
Type: COMPONENT BASIC
Reactions: entering/if not TRANSMITTER_PON then DO_TRANSMITTER_
           PWR end if

Elements defined and/or used in chart AV_CONFIG_INIT
----------------------------------------------------
ALL_SUBSYS_POWER_ON (condition); defined in chart: AV_CONFIG_
INIT
Definition: RADAR_PON and ALTIMETER_PON and TRANSMITTER_PON and
            POSITION_SYS_PON and IMU_PON

ALTIMETER_PON (condition); unresolved in chart: SGA0

A_LOAD_FAILED (event); defined in chart: AV_CONFIG_INIT
Definition: (TMO_SOCS or TMO_CT or TMO_GNC or TMO_ELS)

CT_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

DO_ALTIMETER_PWR (event); unresolved in chart: SGA0

DO_CONFIG (activity); defined in chart: INIT_AV_CONFIG

DO_IMU_PWR (event); unresolved in chart: SGA0

DO_INIT (activity); defined in chart: INIT_AV_CONFIG

DO_POSITION_SYS_PWR (event); unresolved in chart: SGA0

DO_RADAR_PWR (event); unresolved in chart: SGA0

DO_TRANSMITTER_PWR (event); unresolved in chart: SGA0

ELS_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

GNC_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

IMU_PON (condition); unresolved in chart: SGA0

LOAD_CT_SW (activity); defined in chart: INIT_AV_CONFIG

LOAD_CT_SW (state); defined in chart: AV_CONFIG_INIT

LOAD_ELS_SW (activity); defined in chart: INIT_AV_CONFIG

LOAD_ELS_SW (state); defined in chart: AV_CONFIG_INIT

LOAD_GNC_SW (activity); defined in chart: INIT_AV_CONFIG

LOAD_GNC_SW (state); defined in chart: AV_CONFIG_INIT

LOAD_SOCS_SW (activity); defined in chart: INIT_AV_CONFIG

LOAD_SOCS_SW (state); defined in chart: AV_CONFIG_INIT

LOAD_TMO_PERIOD (data-item); defined in chart: AV_CONFIG_INIT
Definition: 5

ONE_RETRY (condition); unresolved in chart: AV_CONFIG_INIT

ONE_RETRY (state); defined in chart: AV_CONFIG_INIT

POSITION_SYS_PON (condition); unresolved in chart: SGA0

RADAR_PON (condition); unresolved in chart: SGA0

RETRY_CT (action); defined in chart: AV_CONFIG_INIT
Definition: sp!(LOAD_CT_SW);
            tr!(ONE_RETRY);
            sc!(st!(LOAD_CT_SW),1)

RETRY_ELS (action); defined in chart: AV_CONFIG_INIT
Definition: sp!(LOAD_ELS_SW);
            tr!(ONE_RETRY);
            sc!(st!(LOAD_ELS_SW),1)

RETRY_GNC (action); defined in chart: AV_CONFIG_INIT
Definition: sp!(LOAD_GNC_SW);
            tr!(ONE_RETRY);
            sc!(st!(LOAD_GNC_SW),1)

RETRY_SOCS (action); defined in chart: AV_CONFIG_INIT
Definition: sp!(LOAD_SOCS_SW);
            tr!(ONE_RETRY);
            sc!(st!(LOAD_SOCS_SW),1)

SOCS_LOADED (condition); unresolved in chart: INIT_AV_CONFIG

STARTUP_TIMEOUT_PERIOD (data-item); defined in chart: AV_
CONFIG_INIT
Definition: 5
```

Table D-8. Avionics Configure Initiate Statechart Directory - concluded

START_SUB_SYS (state); defined in chart: AV_CONFIG_INIT

TMO_CT (event); defined in chart: AV_CONFIG_INIT
Definition: tm(en(LOAD_CT_SW),LOAD_TMO_PERIOD)[not ONE_RETRY]

TMO_ELS (event); defined in chart: AV_CONFIG_INIT
Definition: tm(en(LOAD_ELS_SW),LOAD_TMO_PERIOD)[not ONE_RETRY]

TMO_GNC (event); defined in chart: AV_CONFIG_INIT
Definition: tm(en(LOAD_GNC_SW),LOAD_TMO_PERIOD)[not ONE_RETRY]

TMO_SOCS (event); defined in chart: AV_CONFIG_INIT
Definition: tm(en(LOAD_SOCS_SW),LOAD_TMO_PERIOD)[not ONE_RETRY]

TRANSMITTER_PON (condition); unresolved in chart: SGA0

```
STRUCTURE FOR AV_CONFIG_INIT:
=============================

                                                  --------------
                                                  |AV_CONFIG_IN|
                                                  |IT:         |
                                                  |    D-12    |
                                                  --------------
                                                        |
                                                        |
                    ------------------------------------
                    |
              --------------
              |AV_CONFIG_IN|
              |IT          |
              |    D-12    |
              --------------

 LEVEL     2
                                                  --------------
                                                  |AV_CONFIG_IN|
                                                  |IT          |
                                                  |    D-12    |
                                                  --------------
                                                        |
                                                        |
                    ------------------------------------------------------------
                    |                    |                    |                    |
              --------------       --------------       --------------       --------------
              |START_SUB_SY|       |            |       |            |       |            |
              |S           |       |  DO_INIT   |       | DO_CONFIG  |       |  STATE#39  |
              |            |       |            |       |            |       |            |
              --------------       --------------       --------------       --------------
CONTINUE...
                    ------------------------------------
                    |
              --------------
              |            |
              |LOAD_FAILURE|
              |            |
              --------------
```

Figure D-13. AV_CONFIG_INIT State Structure

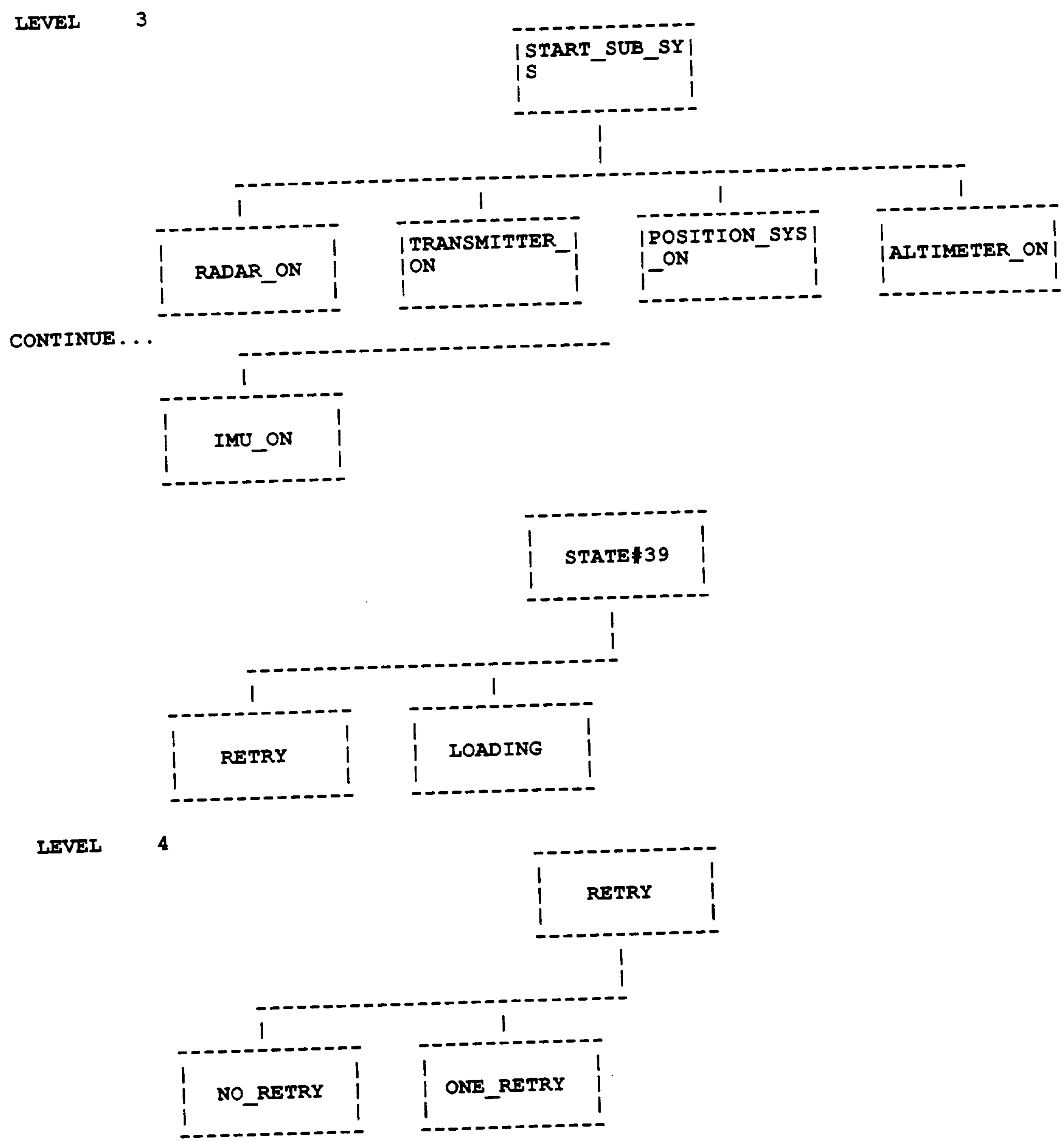


Figure D-13. AV_CONFIG_INIT State Structure - continued

```
                    --------------
                    |            |
                    |  LOADING   |
                    |            |
                    --------------
                          |
                          |
   -------------------------------------------------------
   |                 |                 |                 |
--------------  --------------  --------------  --------------
|            |  |            |  |            |  |            |
|LOAD_SOCS_SW|  |LOAD_ELS_SW |  |LOAD_GNC_SW |  | LOAD_CT_SW |
|            |  |            |  |            |  |            |
--------------  --------------  --------------  --------------
```

Figure D-13. AV_CONFIG_INIT State Structure - concluded

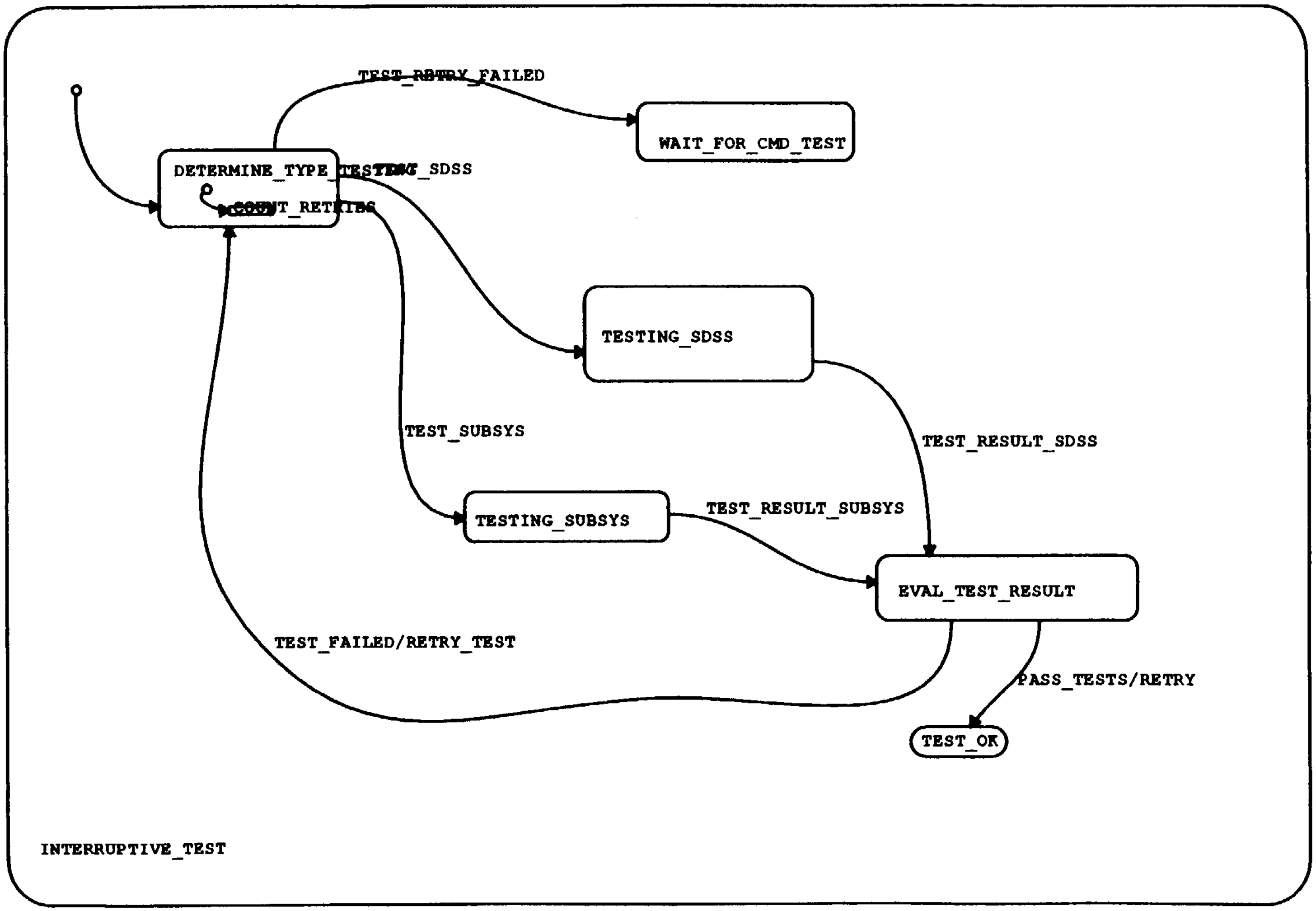


Figure D-14. Interruptive Test Statechart

Table D-9. Interruptive Test Statechart Directory

Dictionary for chart INTERRUPTIVE_TEST

Elements defined and/or used in chart INTERRUPTIVE_TEST

PASS_TESTS (event); unresolved in chart: INTERRUPTIVE_TEST

RETRY (event); unresolved in chart: INTERRUPTIVE_TEST

RETRY_TEST (event); unresolved in chart: INTERRUPTIVE_TEST

TEST_FAILED (event); unresolved in chart: INTERRUPTIVE_TEST

TEST_RESULT_SDSS (event); unresolved in chart: INTERRUPTIVE_TEST

TEST_RESULT_SUBSYS (event); unresolved in chart: INTERRUPTIVE_TEST

TEST_RETRY_FAILED (event); unresolved in chart: INTERRUPTIVE_TEST

TEST_SDSS (event); unresolved in chart: INTERRUPTIVE_TEST

TEST_SUBSYS (event); unresolved in chart: INTERRUPTIVE_TEST

STRUCTURE FOR INTERRUPTIVE_TEST:
================================

```
                                               --------------
                                               |INTERRUPTIVE|
                                               |_TEST:      |
                                               |    D-14    |
                                               --------------
                                                      |
                                                      |
                       --------------------------------
                       |
                --------------
                |INTERRUPTIVE|
                |_TEST       |
                |    D-14    |
                --------------

   LEVEL     2
                                               --------------
                                               |INTERRUPTIVE|
                                               |_TEST       |
                                               |    D-14    |
                                               --------------
                                                      |
                                                      |
                       ---------------------------------------------------------------
                       |                  |                   |                  |
                --------------     --------------     --------------     --------------
                |            |     |WAIT_FOR_CMD|     |EVAL_TEST_RE|     |TESTING_SUBS|
                |TESTING_SDSS|     |_TEST       |     |SULT        |     |YS          |
                |            |     |            |     |            |     |            |
                --------------     --------------     --------------     --------------
  CONTINUE...
                       --------------------------------
                       |
                --------------
                |DETERMINE_TY|
                |PE_TESTING  |
                |            |
                --------------
```

Figure D-15. Interrptive Test State Structure

```
LEVEL      3
                                                  --------------
                                                  |DETERMINE_TY|
                                                  |PE_TESTING  |
                                                  |            |
                                                  --------------
                                                        |
                                                        |
                              ---------------------------
                              |
                        --------------
                        |COUNT_RETRIE|
                        |S           |
                        |            |
                        --------------
```

Figure D-15. Interruptive Test State Structure - concluded

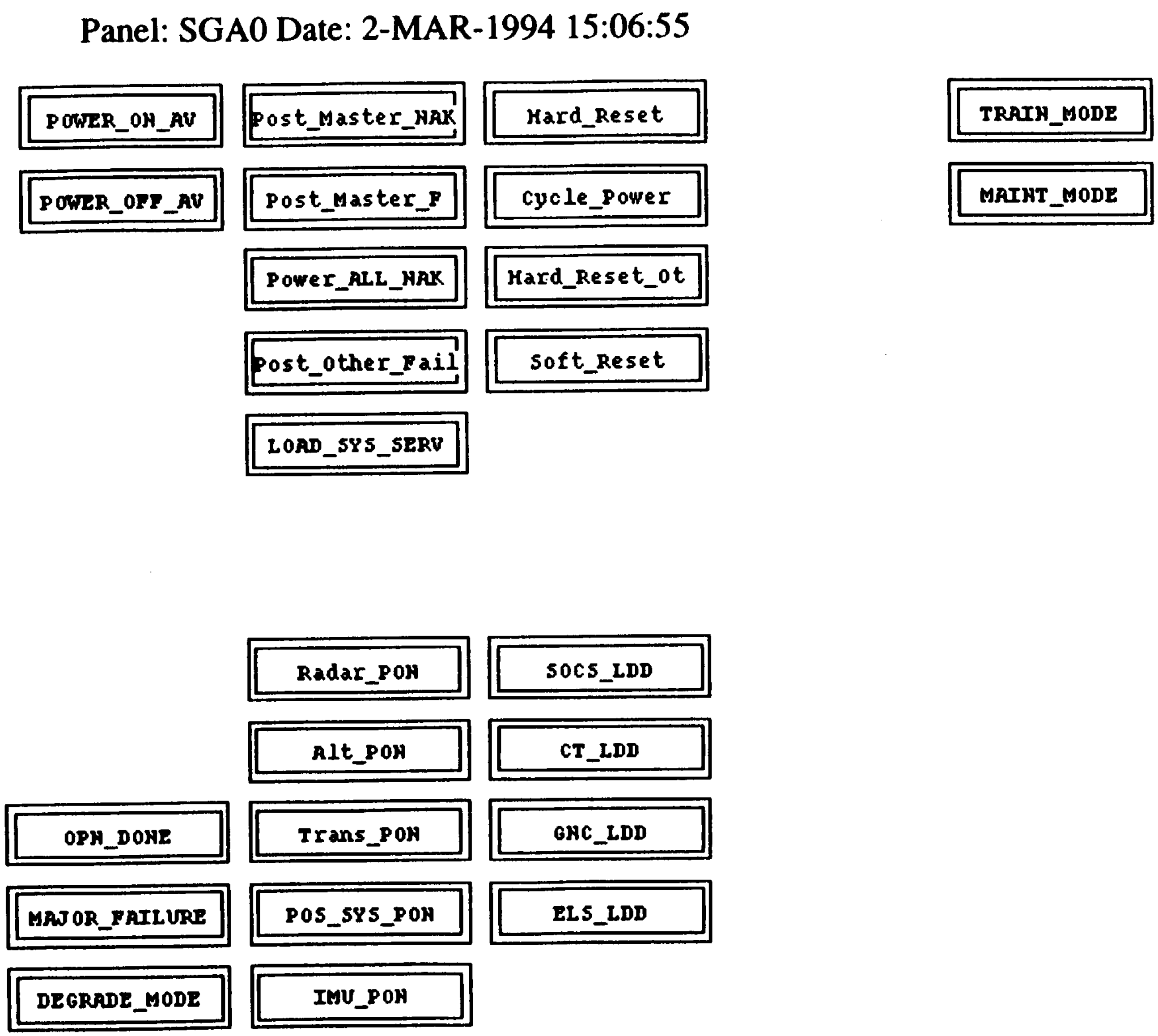


Figure D-16. SGOAA Simulation Panel

C-3.

Table D-10. SCRIPT Simulation Demonstration

```
PROGRAM run2;
VARIABLE
  INTEGER         nondet_no;
  BOOLEAN         step_mode;
  BOOLEAN         notify_mode;
  FLOAT           random_seed;
INIT
  nondet_no := 0 ;
  fs!(notify_mode) ;
  fs!(step_mode) ;
  write('Playback RUN2. \n');

END INIT;

SET BREAKPOINT  [ STEP ] DO
  IF (notify_mode) THEN
    WRITE('PLAYBACK# STEP :',step_number,' TIME  :',cur_clock,'\n\n');
  END IF;
  IF (step_mode) THEN
    WRITE('PLAYBACK# Type cont to continue\n');
    SET INTERACTIVE;
  END IF;
END BREAKPOINT;


BEGIN
  GO STEP;
  GO REPEAT;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;

    WRITE('PLAYBACK# Event POWER_ON_AV generated\n');
    write('Script paused, type "cont" to continue. \n');
    set interactive;

  POWER_ON_AV;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;

    WRITE('PLAYBACK# Activity POST_SDSS_MASTER stopped\n');
    write('Script paused, type "cont" to continue. \n');
    set interactive;

  sp!(POST_SDSS_MASTER);
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
  GO ADVANCE 1.000000;
```

```
  WRITE('PLAYBACK# Condition POWER_ALL_NAK was changed to TRUE\n');
  write('Script paused, type "cont" to continue. \n');
  set interactive;

POWER_ALL_NAK := TRUE;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Activity POWERUP_OTHER stopped\n');
  write('Script paused, type "cont" to continue. \n');
  set interactive;

sp!(POWERUP_OTHER);
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Event CYCLE_POWER generated\n');

CYCLE_POWER;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Condition POWER_ALL_NAK was changed to FALSE\n');

POWER_ALL_NAK := FALSE;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Activity POWERUP_OTHER stopped\n');

sp!(POWERUP_OTHER);
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Activity POST_SDSS_OTHER stopped\n');

sp!(POST_SDSS_OTHER);
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Activity LOAD_SYS_SERV_SW stopped\n');

sp!(LOAD_SYS_SERV_SW);
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Condition RADAR_PON was changed to TRUE\n');

RADAR_PON := TRUE;

  WRITE('PLAYBACK# Condition ALTIMETER_PON was changed to TRUE\n');

ALTIMETER_PON := TRUE;
GO ADVANCE 1.000000;
```

Table D-10. SCRIPT Simulation Demonstration - continued

```
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Condition TRANSMITTER_PON was changed to TRUE\n');

TRANSMITTER_PON := TRUE;

  WRITE('PLAYBACK# Condition POSITION_SYS_PON was changed to TRUE\n');

POSITION_SYS_PON := TRUE;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;
GO ADVANCE 1.000000;

  WRITE('PLAYBACK# Condition IMU_PON was changed to TRUE\n');
  write('Script paused, type "cont" to continue. \n');
  set interactive;

IMU_PON := TRUE;
GO NEXT;
GO STEP;

  WRITE('PLAYBACK# Condition SOCS_LOADED was changed to TRUE\n');

SOCS_LOADED := TRUE;
GO STEP;
GO NEXT;
GO STEP;

  WRITE('PLAYBACK# Condition CT_LOADED was changed to TRUE\n');

CT_LOADED := TRUE;
GO STEP;
GO NEXT;
GO STEP;
GO NEXT;
GO STEP;
GO NEXT;
GO NEXT;
GO STEP;
  write('Script paused, type "cont" to continue. \n');
  set interactive;
GO BACK;

  WRITE('PLAYBACK# Condition GNC_LOADED was changed to TRUE\n');

GNC_LOADED := TRUE;
GO STEP;
GO BACK;
GO BACK;

  WRITE('PLAYBACK# Condition GNC_LOADED was changed to TRUE\n');

GNC_LOADED := TRUE;
GO STEP;
GO STEP;
GO STEP;

  WRITE('PLAYBACK# Condition ELS_LOADED was changed to TRUE\n');

ELS_LOADED := TRUE;
GO STEP;
GO STEP;

  WRITE('PLAYBACK# Activity DO_CONFIG stopped\n');

sp!(DO_CONFIG);
```

Table D-10. SCRIPT Simulation Demonstration - concluded

```
  GO STEP;
    WRITE('PLAYBACK#.Activity DO_INIT stopped\n');
  sp!(DO_INIT);
  GO STEP;
  GO STEP;
END;
END.
```

DISTRIBUTION LIST FOR LESC-31195
AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION
FOR SGOAA - CONTINUED

OTHER LOCKHEED

LAD, P. O. BOX 17100, AUSTIN, TX. 78744-1016
CURTIS WELLS, O/ T2-10, BLDG 30F

LADC, P. O. BOX 250, SUNLAND, CA. 91041
ALEX LOEWENTHAL, DEPT. 25-14, BLDG 311

LAS Ontario, P. O. BOX 33, ONTARIO, CA. 91761-0033
C. R. (BOB) FENTON

LASC, 86 S. COBB ST.,MARRIETTA, GA. 30063
RICK HARWELL, D/73-D2, ZONE 0685
JOHN WEAVER, D/73-D1, ZONE 0685
HUDSON, ROCKY, D/73-D2, ZONE 0685
REED, MIKE, D/73-MA, ZONE 0081
COX, JIM, D/73-MA ZONE 0081

LFWC, P. O. BOX 748, FORT WORTH, TX 76101
PAUL DANIEL, MAIL ZONE 2640

LMSC, 1111 LOCKHEED WAY, SUNNYVALE, CA. 94088-3504
ROY PETIS, O/ 73-12, BLDG 564
JOHN McMORRIS, O/ 81-90, BLDG 157
DUWAYNE DICKSON, O/ 80-06, BLDG 154
MERLIN DORFMAN, O/ 62-80, BLDG 563
CHARLES TADJERAN, O/ 62-31, BLDG 150
RANDY FLEMING, O/ 73-12, BLDG 564
F. L. LORY, O/ 68-15, BLDG 104

LMSC (RD&D), 3251 HANOVER STREET, PALO ALTO, CA 94303-1191
BILL GUYTON, O/ 92-20, BLDG 254E
STEVE SHERMAN, O/ 96-10, BLDG 254E
TOM ARKWRIGHT, ORG 96-10, BLDG 254E
RAY MUZZY, O/ 90-21, BLDG. 254E

LOCKHEED-SANDERS, 95 CANAL ST., NASHUA, NH 03061
RAY GARBOS (NAM5D-5002)
JOHN MILLER (NCA 09-1106)
DAVE AIBEL
ANNETTE LANIGAN
JEFF E. SMITH (PTPZ-B002)
DUNCAN MOORE (MER 24)
WALT ZANDI

LOCKHEED CORP, 4500 PARK GRANADA BLVD, CALABASIS, CA 91399-0310
BART KRAWETZ
MICHAEL CARROLL

LSOC, 1100 LOCKHEED WAY, TITUSVILLE, FL 32780
L. J. (LEWIS) BOYD, O/ 32-40, (Z/LSO-183)
ARTHUR EDWARDS, O/ 11-42, BLDG. B/DX-D, Z/LSO-284)

DISTRIBUTION LIST FOR LESC-31195
AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION
FOR SGOAA - CONTINUED

OTHER GOVERNMENT

NIST/CSL, FRITZ SCHULTZ, BLDG 225, ROOM B266, GATHISBURG, MD. 20899

DoD

AMSEL-RD-C2-TS-I, FT MONMOUTH, NJ 07703
DOUG JOHNSON/ACC #66

ASC/ENAS, WRIGHT-PATTERSON AFB, OH 45433
FRED WILSON

MARTIN FREED, (ASC/ENASC), 5565 BARBANNA LANE, DAYTON, OH 45415

ASC/YFMXT, WRIGHT-PATTERSON AFB, OH 45433-7003
MR. BYRON STEPHENS/JIAWG

HQ USAF/SCS, 1250 AIR FORCE, PENTAGON, WASHINGTON, D. C. 20330-1250
COL ROBERT HANLON

NAVAL AIR WARFARE CENTER, AIRCRAFT DIVISION, WARMINSTER, PA 18974-0591
RICHARD J. PARISEAU/CODE 102A
RICHARD S. MEJZAK/CODE 2021

ROME LABS/OCTS, GRIFFIS AFB, NY 13441-5700
RICHARD WOOD

NAVAIR, (AIR-56M), 1421 JEFFERSON HIGHWAY, ARLINGTON, VA, 22243
CMDR LARRY JAHNKE

SAE/AEROSPACE

SAE/ASD, SAE INTERNATIONAL, 400 COMMONWEALTH AVE, WARRENDALE, PA. 15096
BARBARA ROTH (FILE) RICH VANDAME

BOEING CORP, PO BOX 3999, SEATTLE, WA 98124-2499
RICHARD FLANAGAN
AL COSGROVE

CTA INC. SUITE 310, 18333 EGRET BAY BLVD, HOUSTON, TX 77058
MR DAVID COOPER

DISTRIBUTION LIST FOR LESC-31195
AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION
FOR SGOAA - CONTINUED

COMPUTING DEVICES INTL, 8800 QUEEN AVENUE SOUTH, BLOOMINGTON, MN 55431
JIM JAMES, M/S BLCS1D
DOCK ALLEN, M/S BLCW2S

C.S. DRAPER LABS, 555 TECHNOLOGY SQUARE, CAMBRIDGE, MA 02139
J. BARTON DEWOLFE/MS 61

E-SYSTEMS, P. O. BOX 12248, ST. PETERSBURG, FL. 33733-2248
JIM BRADY/MS29

E-SYSTEMS, P.O. BOX 660023, DALLAS, TX 75266-0023
TIM SMITH/MC 4-47310

EER SYSTEMS INC., 3027 MARINA BAY DR., SUITE 105,
LEAGUE CITY, TX 77573
RAY HARTENSTEIN

FAIRCHILD SPACE, 20301 CENTURY BLVD., GERMANTOWN, MD. 20874
JOHN SCHNEIDER, FLIGHT DATA SYSTEMS

GE. CORPORATE RESEARCH & DEVELOPMENT, PO BOX 8, SCHENECTADY, NY 12301
DAVID W. OLIVER/BLDG K-1, RM 3C3

GOODRICH AEROSPACE, SIMMONDS PRECISION PRODUCTS INC., AIRCRAFT SYSTEMS, PANTON ROAD, VERGENNES, VT 05491
JOHN D. BLAIR

HONEYWELL INC, 3660 TECHNOLOGY DR, MINNEAPOLIS, MN 55418
MR RON FRAZZINI

HUGHES AIRCRAFT, PO BOX 92426, LOS ANGELES, CA 90009-2426
JOHN GRIFFITH, RE/RI/B500

MCDONNELL DOUGLAS CORPORATION, 1801 E. ST ANDREW PLACE, SANTA ANA, CA 92705
TERRY RASSET/MS A208

MITRE CORPORATION, 202 BURLINGTON ROAD, BEDFORD, MA 01730-1420
WILLIAM T. BRANDOM/D-96
JACK SHAY/DIRECTOR OF SYSTEMS DEVELOPMENT

DISTRIBUTION LIST FOR LESC-31195
AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION
FOR SGOAA - CONTINUED

NAVMAR APPLIED SCIENCES CORP, 65 WEST STREET, SUITE C200, WARMINSTER, PA 18974
MR. DOUG D'AVINO

NORTHROP B-2 DIVISION, 8900 E. WASHINGTON BLVD., PICO RIVERA, CA 90660
JIM NELSON/DEPT T216/GB

PARAMAX SYSTEMS CORP, PO BOX 64525, ST PAUL, MN 55164-0525
MR DARYLE HAMLIN/MS U1F15

RESEARCH ANALYSIS AND MAINTENANCE INC., 512 AUDOBON ST., LEAGUE CITY, TX 77573
ROGER EVANS

ROCKWELL INT'L CORP.- SPACE TRANSPORTATION SYSTEMS DIV., 12214 LAKEWOOD BLVD., DOWNEY, CA. 90241
BURTON SMITH, M/S FA20

ROCKWELL INTL CORP.- ROCKETDYNE DIV., 6633 CANOGA AVE, P. O. BOX 7922, CANOGA PARK, CA. 91309-7922
ANTHONY THOMPSON, D1055-LB33

SBS ENGINEERING, 5550 MIDWAY PARK PLACE, NE, ALBUQUERQUE, NM 87109
MR. DEREK HEAD

SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA 15213
B. CRAIG MEYERS

TEXAS INSTRUMENTS, 6550 CHASE OAKS BLVD, PO BOX 869305, PLANO, TX 75086
DR. CHUCK ROARK/MS 8481

TRW, HOUSTON, TX 77058
DOUG RUE (NASA MAIL)

WESTAR CORP. 6808 ACADEMY PKWY EAST, NE, BLDG C, SUITE 3, ALBUQUERQUE, NM 87109
CHRIS DE LONG

DISTRIBUTION LIST FOR LESC-31195
AN AVIONICS SCENARIO AND COMMAND MODEL DESCRIPTION FOR SGOAA - CONCLUDED

UNIVERSITIES & OTHERS

UHCL, UNIVERSITY OF HOUSTON - CLEAR LAKE, 2700 BAY AREA BLVD. - BOX 444, HOUSTON, TEXAS 77058
CHARLES HARDWICH

UNIVERSITY OF TEXAS AT AUSTIN, PO BOX 8029, 10000 BURNET ROAD, AUSTIN, TX 78713-8029
GRANVILLE OTT/APPLIED RESEARCH LABORATORIES

NCOSE TGCC, 1907 BELLMEADE, HOUSTON, TX 77019
ED SMITH