NSTS 16979
Part I
Revision C

Shuttle Orbiter Failure Modes and Fault Tolerances for Interface Services

July 1991

National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas

DESCRIPTION OF CHANGES TO

SHUTTLE ORBITER FAILURE MODES AND FAULT TOLERANCES

FOR INTERFACE SERVICES

CHANGE NO.	DESCRIPTION/AUTHORITY	DATE	PAGES AFFECTED
--	Baseline issue/R16979-PT1-001	06/80	All
REV A	Update Fault Tolerances/ R16797-PT1-002	09/88	All
REV B	Two Fault Tolerance Equiva- lence for Toggle Switches/ R16979-PT1-003	11/03/89	All
REV C	General revision/R16979- PT1-004;-005A;-006	07/02/91	All
1	Update section 4.0/R16979- PT1-007C	04/28/93	18,18A,18B
2	Update table of contents, section 4.0, table 5-11, and add figure 5-11a/R16979-PT1- 008;-009	02/08/94	vi,17,17A, 66,67,67A, 68A
3	Update section 4.0 and tables 5-10 and 5-11/R16979-PT-0010	11/07/95	16,17,17A, 22,63,64, 66,67,67A, 67B
4	Update section 4.0 and table 5-4/R16979-PT1-0012	09/01/98	10,11,22A,43

Note: Dates reflect latest approval date of CR's received by PILS.

NSTS 16979 REV. B - PART 1

STS 80-0012A

SHUTTLE ORBITER FAILURE MODES AND FAULT TOLERANCES FOR INTERFACE SERVICES

(Defined in ICD 2-19001)

November 3, 1989

CONTRACT NAS9-14000
IRD RA-267C
WBS 21.2.14

Rockwell International

NASA/JSC 5-18-88

Rockwell International 5/15/88

NASA/JSC 5/31/88

CONTENTS

TABLES

FIGURES

1.0 INTRODUCTION

This document identifies the possible failure conditions and tolerances at the Orbiter/payload interfaces. The possible failure conditions are related to the failure modes of the associated Orbiter subsystems. A matrix is provided of the payload service versus Orbiter subsystem Failure Mode Effects Analysis (FMEA's).

The Shuttle Orbiter/cargo interfaces analyzed herein are defined in ICD 2-19001, Shuttle Orbiter/Cargo Standard Interfaces.

1.1 PURPOSE

These interface failure modes analyses and fault tolerances are related to the Space Shuttle Program (SSP)-provided core and optional payload services.

This document is intended to provide failure mode/fault tolerance information to SSP customers to aid in the development and design of their payloads and the required documentation.

1.2 SCOPE

These analyses are limited to the Orbiter/payload physical interfaces. The effects of Orbiter failures in subsystems that do not directly serve cargo functions are not included. While every effort has been made to identify all of the failure modes that may affect payloads, the analyses have been conducted without reference to the particular requirements of any specific user. The level of detail is limited by the intent to produce a usable and compact document. When clarification or further information is needed, users may consult the SSP at National Aeronautics and Space Administration (NASA) Lyndon B. Johnson Space Center (JSC) Customer Services Office.

1.3 MIXED USERS ALLOCATIONS AND REDUNDANCY

The SSP has established a policy of allocating cargo interfaces, particularly multiple avionics services, in four equal standard sections (NSTS 07700, Volume XIV) (see figure 1-1). One or more sections may be assigned to a user to support their requirements based on their load factor and redundancy requirements. For dedicated flights, all four sections are at the disposal of the user. Where appropriate in this analysis, a distinction is made for failure tolerance of multiple section interfaces. If the user has only one-quarter of the services allocated, special consideration must be given to redundancy requirements. This document addresses failure tolerances for services of a single section user.

1.4 SAFETY CRITICAL FUNCTION INTERFACES

The use of any of the Orbiter/payload interfaces to control safety-critical payload operations will be identified by the SSP user during the Orbiter/payload Interface Control Document (ICD) development phase.

The SSP user will also provide features of the payload design that permit test verification of critical electrical/fluid interfaces postmate including all redundancy.

These critical interface and design features will be identified in the Orbiter/payload ICD and STS User Payload Hazard Report. In addition, hazardous commands shall be identified in the payload-unique Payload Integration Plan (PIP) Annex 4, Command and Data Annex.

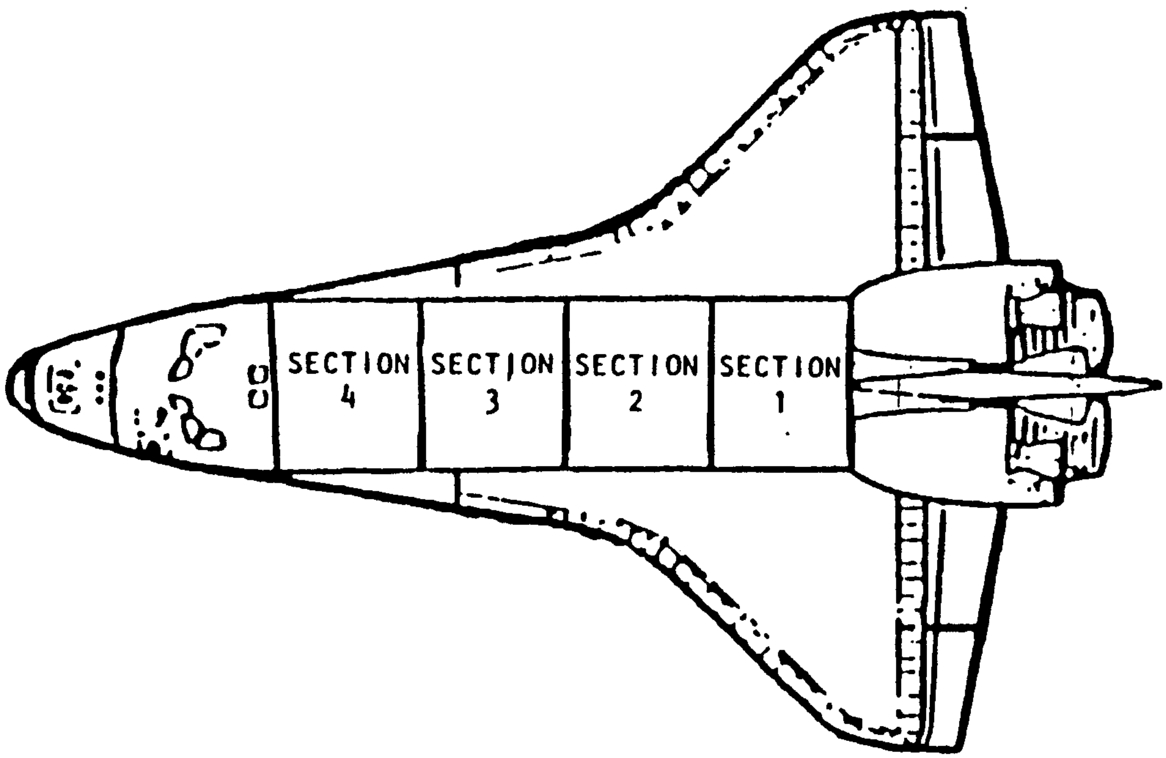


Figure 1-1.- Cargo bay sections for mixed user missions.

2.0 GROUND RULES AND CRITERIA

1. Because Orbiter software failure modes were not considered credible, they were not included in the analysis.

2. The failure modes presented are consistent with individual harness failures of open or short to structure. While such failures of Space Shuttle wiring and connectors are credible, the risk is managed to an acceptably low level due to manufacture, testing, and inspection controls, which include dielectric testing of all Space Shuttle harnesses before installation and electrical verification of all wiring paths before payload installation. In addition, payload interface verification testing provides further harness integrity verification, as well as verification of critical circuits after final connector mate. On-orbit testing of connector signal paths provides data to justify the elimination of on-orbit connector separation as a credible failure mode.

3. Failure mode identification for hardware associated with redundant functional paths was limited to like components; e.g., fuse in each functional path fails open. Multiple combinations of failures for unlike components were not considered; e.g., fuse fails open in one path and a switch (remote power controller) fails to transfer power in the other functional path.

4. Ground servicing equipment interfacing with the payload through the vehicle's launch umbilical was not included in the analysis.

5. Payload-associated crew control switch failure modes consisting of failure to transfer and inadvertent open or closed applied to all control switches. These failure modes were considered credible only when switch actuations were being performed or, during vehicle ascent to orbit, when the vehicle vibration environment was applied.

6. All switches, except single-pole switches, had structural failure modes that could cause shorts between contacts or shorts to ground.

7. In section II of this document, failure modes and fault tolerances are discussed only for the first level of Orbiter avionics service (e.g., Multiplexer/Demultiplexer (MDM), Payload Signal Processor (PSP), etc.). Further failure mode and effects analysis specifications for these units, as well

as related Orbiter avionics units, are discussed in separate documents. Table 2-1 is a cross-reference listing of the Orbiter subsystems providing the payload services and the FMEA associated with that Orbiter subsystem.

8. In order to provide a generic discussion at payload interface services, section 5, Orbiter/Cargo Interface Analysis, was divided into two sections. Section I details the power services provided to the payload: main 28 V dc in the cargo bay, payload station distribution panel, on-orbit station distribution panel and mission station distribution panel; auxiliary 28 V dc; and 115 V ac three phase power. The rest of the avionics services are detailed in section II.

9. Where applicable the interface analysis identified failure modes and effects per one-quarter Standard Mixed Cargo Harness (SMCH) interface (i.e., a single payload). However, certain failure modes and effects did not readily format into a single payload approach and are so identified.

10. Removal of power to Orbiter main dc, ac, or essential buses is not an allowable condition to enhance payload redundancy.

Table 2-1.- PAYLOAD SERVICE VERSUS ORBITER SUBSYSTEM FMEA

Orbiter subsystem	Part number	FMEA
1. Master Timing	MC456-0051	05-4-221200 STS 82-0031
2. Timing Buffer	MC456-0060	05-4-221400 STS 82-0031
3. Multiplexer/Demultiplexer	MC615-0004	STS 82-0032
4. S-band Payload Interrogator	MC478-0105	05-2J-21300 STS 82-0029
5. Payload Signal Processor	MC476-0318	05-2J-21600 STS 82-0029
6. Ku-band Signal Processor	MC409-0025	05-2R-5100 05-2R-5200 05-2R-5300 05-2R-5400 STS 82-0029
7. Deployment/Pointing Panel	SED 3101223-301	STS 82-0033 STS 82-0020
8. Payload Data Interleaver	MC476-0136	05-4-221300 STS 82-0031
9. Caution and Warning Electronics	MC409-0012	05-3-12309 STS 82-0030
10. FM Signal Processor	MC478-0106	05-2G-21000 05-2G-21100 05-2G-21200 STS 82-0029
11. Pulse Coded Modulation Master Unit	MC476-0130	05-4-320400 STS 82-0031
12. Electrical Power Distribution and Control		STS 82-0033

3.0 REFERENCE DOCUMENTS

Document number	Title
NSTS 07700 Vol. XIV	Space Shuttle System Payload Accommodations
NSTS 139751	Standard Payload Display and Control Interface Specification
ICD-2-05301	Shuttle Vehicle/Spacelab Avionics Interfaces
ICD 2-19001	Shuttle Orbiter/Cargo Standard Interfaces
ICD 3-0021-01	Payload Recorder Interface Control Documents
ICD 3-0050-01	Video Switching Unit and Remote Control Unit Interface Control Document
VS70-760302 (0V102 only) VS70-760309 (0V103 and subs)	Main dc Power Distribution Subsystem Schematic Diagram
VS70-760402 (0V102 only) VS70-760409 (0V103 and subs)	AC Power Distribution Subsystem Schematic Diagram
VS70-760809	Payload Subsystem Interface Schematic Diagrams
STS82-0020	Payload Retention, Manipulator Positioning, and Retention Mechanisms FMEA
STS82-0032	Data Processing and Software and Computers FMEA
STS82-0033	Electric Power Distribution and Control FMEA
STS82-0028	Guidance, Navigation, and Control FMEA
STS82-0029	Communication and Tracking FMEA
STS82-0031	Instrumentation FMEA

MJ073-0001-1A	Standard End Item Specification for Orbiter Payload Integration Hardware
STS87-0047	Failure Modes and Effects Analyses for STS Payload Optional Service Kit Hardware
NSTS 18798	Interpretations of Payload Safety Requirements

4.0 ORBITER/CARGO INTERFACES

This section establishes for reference the standard shared cargo services and optional electrical and avionic payload interfaces, and their associated controls and locations in the crew compartment. Where applicable, SMCH's are identified for each service that interfaces with the payloads (see figures 4-1 through 4-7).

The following paragraphs summarize the Orbiter power, command, and monitoring services and their applicable fault tolerances. These data can be used in conjunction with the safety critical function interface requirements as discussed in section 1.4. More detailed analyses to support the fault tolerance summaries are provided in section 5, Orbiter/Cargo Interface Analysis.

SUMMARY OF ORBITER POWER SERVICES

Standard

1. Payload dc bus (SMCH 0 AWG Feeder)
2. Cabin dc bus (Standard Switch Panel power - four powered switches)
3. T-0 payload GSE interface

Optional

1. Auxiliary power
2. Aft dc bus
3. Cabin dc bus (Standard Switch Panel circuit breakers)
4. AC power (AFD and payload bay)
5. Starboard T-0 interface

FAILURE TOLERANCE SUMMARY FOR ORBITER POWER SERVICES

0 AWG Feeder

1. Equivalent to one fault tolerant under specific conditions (see note 1 on page 12).

2. Additional use of any other source (including use of second 0 AWG Feeder) provides the equivalent of two fault tolerance if the conditions required for one fault equivalence are met (see 1 above).

3. Fault tolerance is the same for loss of power/nominal restoration of power.

Standard Switch Panel Powered Switches

1. Powered from cabin payload buses 1 or 3.

2. Standard Switch Panel switches that are internally wired to Orbiter power are zero fault tolerant in this application.

3. 0 fault tolerant as a group (up to four switches) when wired to a single cabin payload bus. Can be considered equivalent to 1 fault tolerant under certain conditions when using more than one cabin payload bus as a power source (see section 4, note 5).

4. Payload short removes power from 1 section only.

5. Power source is independent of other Orbiter power sources.

T-0 Payload Interface

1. Each payload T-0 wire pair (except for EMI considerations) totally independent of any other wiring (including other T-0 wire pairs)

AUX Power

1. Aux A or aux B is 0 fault tolerant.

2. The use of both aux A and aux B provides one fault tolerant power if either of the following is true:

   a. Circuit redundancy is maintained by the payload and Extravehicular Activity (EVA) is not required for two fault tolerance, or

   b. Circuit redundancy is maintained by the payload and both buses can be verified on the payload side of the interface prior to the start of hazardous operations and with no further aux power switch (S29) cycling. For this case, the payload PIP, table 5.1, must reflect the specific requirement for verification of redundant buses (by the payload) and procedural assurance of no switch cycling (S29) until completion of hazardous functions.

3. Aux buses A and B are independent of other power sources, and the Remote Power Controllers (RPC's) powering these buses are resettable if the fault is cleared, but note that both aux buses must be powered off momentarily in order to reset the RPC.

Aft dc Bus

1. Aft bus B or aft bus C is 0 fault tolerant.

2. Aft buses B and C are independent of each other and other power sources.

Cabin Payload Bus

1. Standard Switch Panel circuit breakers are powered by cabin bus 2.

2. All three cabin buses are usable as outputs of Standard Switch Panel no. 2 (or in lieu of Standard Switch Panels).

3. Cabin payload buses 1, 2, and 3 are 0 fault tolerant separately. Use of more than one cabin payload bus can be considered equivalent to 1 fault tolerant under certain conditions (see section 4, note 5).

4. The cabin payload bus is independent of other power sources.

AC Power

1. AC bus 2 or ac bus 3 is 0 fault tolerant.

2. AC bus 2 and ac bus 3 is 1 fault tolerant.

3. Phases (A, B, and C) are 0 fault tolerant, separately and collectively.

4. AC bus 2 and/or ac bus 3 is routed to the payload bay when ac power, other than latch loads, is required there.

5. Payload Release/Latch Actuator (PRLA) ac buses 1 and 2 (which are controlled by the A6A1 panel) are available in the payload bay for latch-type loads. PRLA ac bus 2 is the same ac bus 2 mentioned in 1 and 2 above.

Starboard T-0 Interface

1. Each payload T-0 wire pair (except for EMI considerations) totally independent of any other wiring (including other T-0 wire pairs)

Note 1: The power distribution within a cargo bay payload that uses a single 0 AWG Orbiter primary power feeder is considered to be the equivalent of one fault tolerant if all of the following conditions are met:

1. The input power on the payload side of the interface is immediately split into redundant power distribution circuits.

2. The payload power wiring from the Orbiter-to-payload interface to the point where it splits into redundant circuits is protected physically; e.g., using chafe guards and/or wire trays.

3. Each branch of the payload power distribution contains circuit protection devices such that no fault in one redundant branch can cause the loss of the primary power source to the other branch or branches. The method for determining this is as follows:

   a. For one of the typical payload mission configurations, select one of the payload power distribution branches and assume a fault current is flowing through the circuit protection device that is nearest the Orbiter equal to the maximum trip or blow value of that device. [The maximum trip or blow value of a circuit protection device is the lowest continuous current that the device manufacturer guarantees will open the device.] Note that this step applies to all power distribution branches and circuit protection devices, whether normally powered or not during this assumed mission configuration.

   b. Assume that all other circuits have a current flow equal to their maximum possible levels that they could have during normal operation in that mission configuration.

   c. The sum of the currents determined in a and b does not exceed the rating of the 200 ampere fuse in the 0 AWG feeder; i.e., 200 amperes.

d. Repeat this procedure for each power distribution branch for the assumed mission configuration.

e. Repeat this process for all payload mission configurations.

f. The payload organization is responsible for review of flight procedures to insure that powered branches are restricted to those used in this analysis.

The power distribution within a cargo bay payload that uses a single 0 AWG power feeder to provide power through Orbiter-provided integration hardware to the payload is considered to be the equivalent of one fault tolerant if all of the following conditions are met:

1. Orbiter-provided integration hardware used between the 0 AWG feeder and the payload is solely for the use of this payload, and is so identified in the PIP, unique payload ICD, and payload hazard reports.

2. Multiple feeds from the Orbiter-provided integration hardware may be maintained by the payload as separate, redundant power distribution circuits, or they may be combined to form a single power bus which must immediately be split into redundant power distribution circuits. In either case, their separation as redundant power branches, either of which can be used to control or operate the payload hazardous functions, shall be maintained.

3. The payload interface wiring from the Orbiter-to-payload interface to the point where it splits into redundant circuits is protected physically; e.g., using chafe guards and/or wire trays.

4. Each branch of the payload power distribution contains circuit protection devices such that no fault in one redundant branch can cause the loss of the primary power source to the other branch or branches. The method for determining this is as follows:

   a. For one of the typical payload mission configurations, select one of the payload power distribution branches and assume a fault current is flowing through the circuit protection device that is nearest the Orbiter power source equal to the maximum trip or blow value of that device. [The maximum trip or blow value of a circuit protection device is the lowest continuous current that the device manufacturer guarantees will open the device.] Note that this step applies to all power distribution branches and circuit protection devices, whether normally powered or not during this assumed mission configuration.

b. Assume that all other circuits have a current flow equal to their maximum possible levels that they could have during normal operation in that mission configuration.

c. The sum of the currents determined in a and b does not exceed the rating of the 200 ampere fuse in the 0 AWG feeder; i.e., 200 amperes, nor does it exceed the rating of the wiring contained in the Orbiter-provided integration hardware used between the 0 AWG feeder and the payload. If the ratings of circuit protection devices contained in Orbiter-provided integration hardware used between the 0 AWG feeder and the payload are exceeded under these fault conditions, their loss does not cause the loss of the Orbiter-provided power source to the payload redundant power distribution branch or branches.

d. Repeat this process for each power distribution branch for the assumed mission configuration.

e. Repeat this process for all payload mission configurations.

f. The payload organization is responsible for review of flight procedures to insure that powered branches are restricted to those used in this analysis.

SUMMARY OF ORBITER COMMAND SERVICES

Standard

1. Standard Switch Panel switches

2. PSP

3. MDM DOL

4. MDM DOH

5. GPC data bus (for payload BTU)

6. Payload Interrogator

7. T-0 payload GSE interface

Optional

1. DPP switches

2. Flight deck safing switches

3. SPASP switches

4. A6A1 panel (retention system) in payload unique application

5. MDM DOL

6. MDM DOH

7. MDM SIO

8. Ku-band 128 kbps channel

FAILURE TOLERANCE SUMMARY FOR ORBITER COMMAND SERVICES

Standard Switch Panel Switches

1. Standard Switch Panel switches that are internally wired to Orbiter power are zero fault tolerant for this application.

2. Nonpowered switches are independent of all other Standard Switch Panel switches, powered and nonpowered, as well as any other Orbiter command service.

3. All Standard Switch Panel switches can be considered equivalent to one fault tolerant for must-work operations (see note 2 on page 18).

4. The use of two switches can be considered equivalent to two fault tolerant in certain specific applications (see note 3 on page 19).

PSP*

1. PSP no. 1 or PSP no. 2 is 0 fault tolerant.

2. PSP no. 1 and PSP no. 2 are 1 fault tolerant.

MDM DOL*

1. 0 fault tolerant individually

2. 0 fault tolerant as a group, one or more sections

MDM DOH*

1. 0 fault tolerant individually

2. 0 fault tolerant as a group, one or more sections

GPC Data Bus*

1. 0 fault tolerant individually.

2. If implemented properly by payload, data bus no. 1 and data bus no. 2 are 1 fault tolerant.

Payload Interrogator*

1. PI no. 1 or PI no. 2 is 0 fault tolerant.

2. PI no. 1 and PI no. 2 are 1 fault tolerant.

T-0 Payload Interface

1. Each payload T-0 wire pair (except for EMI considerations) is totally independent of any other wiring (including other T-0 wire pairs).

DPP Switches (Deployment Part)

1. Select, arm, and deploy switches are hooked up in daisy-chain fashion, with the electrical path(s) being electrically redundant, if cabled up to be so.

2. In a must fire case, the panel is one fault tolerant (see general notes 2 and 4).

3. In an inhibit mode, the panel can be considered 1 fault tolerant (the switching arrangement does not open the return line).

4. DPP switches are independent of all other command modes.

Flight Deck Safing Switches

1. Each safing switch is independent of other safing switches as well as all other command modes.

2. Safing switches can be considered equivalent to one fault tolerant in certain specific applications (see note 2 on page 18).

3. The use of two switches can be considered equivalent to two fault tolerant in certain specific applications (see note 3 on page 19).

SPASP Switches

1. 0 fault tolerant individually.

2. Each SPASP switch is independent of other SPASP switches as well as all other command modes.

Payload Retention/Latch Assembly System (A6A1)

1. Individual latch/release switches are independent of each other.

2. The Orbiter portion of the Payload Retention/Latch Assembly System avionics and power services (whether or not Orbiter latches are utilized) is considered one fault tolerant for must work operations if the following conditions are met:

   - At least one fault tolerance as defined in NSTS 1700.7B is maintained on the payload side of the interface.

   - Failure of the redundant Orbiter services does not result in an immediate hazard.

3. The Orbiter portion of the Payload Retention/Latch Assembly System avionics and power services (not including latches) may be used as a system wherein two fault tolerance is required if the following conditions are met:

   - At least two fault tolerance as defined in NSTS 1700.7B is maintained on the payload side of the interface (refer to Figure 5-11a for Orbiter side implementation).

- Payload must verify the end-to-end performance of all paths of all electrical and mechanical functions in flight immediately prior to exposure to a potentially hazardous condition.

- Complete failure of Orbiter redundant services does not result in a hazard if failures occur prior to exposure to a potentially hazardous condition.

- Time exposure to a potentially hazardous condition can be limited to 10 minutes, nominally.

- Failure of the redundant Orbiter services within the 10-minute period does not result in an immediate hazard.

4. Latch/release switches are considered zero fault tolerant to inadvertent operations during other PRLA operations if the latch of concern is on the same Payload Select (S37) switch position. Latch/release switches are considered two fault tolerant to inadvertent operations during other PRLA operations if the latch of concern is not on the same Payload Select switch position.

MDM DOL (Non-SMCH)*

1. 0 fault tolerant individually.

2. DOL's of MDM PF2 are independent of DOL's of MDM PF1.

MDM DOH (Non-SMCH)*

1. 0 fault tolerant individually.

2. DOH's of MDM PF2 are independent of DOH's of MDM PF1.

MDM SI0*

1. 0 fault tolerant individually.

2. SIO's of MDM PF2 are independent of SIO's of MDM PF1.

*This capability will be lost for a brief period of time if the GPC that is processing payload data fails. In this event one of the remaining four GPC's will be configured to perform the payload command/monitor task. The reconfiguration process can take on the order of 15 min. Other than this specific situation, each interface type is independent of all other types.

The Orbiter GPC may be used to store and control multiple inhibits to a payload catastrophic hazardous function under certain specific restrictions and constraints. These restrictions and constraints are listed below. The organization responsible for implementing each constraint is also given.

1. The GPC command interface shall be through the Payload Signal Processor. (Implemented by payload organization via Payload Integration Plan (PIP) input.)

2. No single command shall remove more than one inhibit. (Implemented by the payload organization via PIP Annex 4 input.)

3. Each GPC stored command shall be initiated by a separate Orbiter cargo control spec item entry and be defined using the cargo control indexing capability. (Implemented by the Mission Operations Directorate (MOD) at JSC after payload organization defines hazardous commands in PIP Annex 4.)

4. Inhibit monitoring requirements (per NSTS 1700.7 current issue) shall apply while the command link is available. (Implemented by the payload organization by defining inhibit monitors in a hazard report and by defining requirement in the PIP for interface service to provide monitoring capability.)

5. The Orbiter Payload Control Supervisor (PCS) shall be limited to removing only one inhibit to a payload catastrophic hazard. (Implemented by the MOD.)

6. While the hazard potential exists, the Orbiter Time Execute Command buffer will not be loaded with any hazardous commands. (Implemented by the MOD.)

7. When the GPC is used to store and issue commands via the PSP to more than one payload, any of which having hazardous functions controlled by the GPC, the command data formats must be evaluated by the SSP to ensure against cross-commanding. Operational constraints may be used to prevent cross-commanding in lieu of detailed format evaluation. (Implemented by the SSP (Level II) and MOD after the payload organization defines hazardous commands in PIP Annex 4.)

8. If the combination of two or more inhibit commands are less than 64 halfwords in length, the command format requirements must be defined in such a way that the commands will be spaced in the Orbiter flight software table so that one operation cannot result in multiple commands being moved into the GPC 64 halfword output buffer. (Implemented by the SSP (Level II) and MOD after the payload organization defines hazardous commands in PIP Annex 4.)

9. All payload command inputs to the Payload Integration Plan Annex 4, determined as nonhazardous, will be verified by the payload organization to be nonhazardous. (Implemented by the payload organization.)

10. While the hazard potential exists, at least one non-GPC (independent) control is required. (Implemented by the payload organization by design and defined in hazard report through the normal safety process.)

Note 2: For the control of payload hazardous functions, certain Orbiter switches can be considered equivalent to one fault tolerant under the following specific conditions:

1. The switches are Orbiter-type, multipole toggle switches (Orbiter Project Parts List (OPPL) parts), with two poles wired to provide redundant electrical circuits, and powered from separate services.

2. The third control, if required to complete the provisioning of two fault tolerant hazard control, must be provided via hardware (not EVA).

3. All circuits used in this application, including redundancy, must be verified preflight.

4. This applies only to the use of switches in Must Work To Be Safe functions and does not apply when switches are used as safety inhibits (three inhibits are required regardless of type).

5. Payload circuit design must provide for two electrical inputs, either of which will complete the must-work function.

Note 3: For the control of payload hazardous functions, two Orbiter switch panel switches can be considered the equivalent of 2 fault tolerant under the following specific conditions:

1. The switches are Orbiter-type, multipole toggle switches (Orbiter Project Parts List (OPPL) parts), with two poles of all switches wired to provide electrical redundancy for both switch paths as well as at least 2 fault tolerant power.

2. All circuits used in this application, including redundancy, must be verified preflight.

3. This applies only to the use of switches in Must Work To Be Safe functions and does not apply when switches are used as safety inhibits (three inhibits are required regardless of type).

4. Payload circuit design must provide four electrical inputs, any one of which will complete the must-work function.

SUMMARY OF ORBITER MONITORING SERVICES

Standard

1. Standard Switch Panel talkbacks
2. PDI
3. MDM DIL
4. MDM AID
5. GPC data bus (payload BTU)
6. Payload Interrogator
7. T-0 payload GSE interface

Optional

1. SPASP talkbacks

2. A6A1 panel (retention system) in payload-unique application

3. MDM DIL

4. MDM DIH

5. MDM AID

6. MDM SIO

7. Ku-band

8. S-band FM

FAILURE TOLERANCE SUMMARY FOR ORBITER MONITORING SERVICES

Standard Switch Panel Talkbacks

1. 0 fault tolerant individually

2. Independent of other talkbacks and any other Orbiter monitor mode

PDI*

1. 0 fault tolerant individually, or as a group of inputs

MDM DIL*

1. 0 fault tolerant individually

2. 0 fault tolerant as a group, one or more sections

MDM AID*

1. 0 fault tolerant individually

2. 0 fault tolerant as a group, one or more sections

GPC Data Bus*

1. 0 fault tolerant individually

2. If implemented properly by payload, data bus no. 1 and data bus no. 2 are 1 fault tolerant

Payload Interrogator*

1. 0 fault tolerant with one or both PI's used (PDI input)

T-0 Payload Interface

1. Each payload T-0 wire pair (except for EMI considerations) is totally independent of any other wiring (including other T-0 wire pairs).

SPASP Talkbacks

1. 0 fault tolerant individually.
2. Each SPASP talkback is independent of other SPASP talkbacks as well as all other monitor modes.

Payload Release/Latch Actuator System (A6A1)

1. Individual release/latch talkbacks are 0 fault tolerant and are considered independent of each other.

MDM DIL (Non-SMCH)*

1. 0 fault tolerant individually.
2. DIL's of MDM PF2 are independent of DIL's of MDM PF1.

MDM AID (Non-SMCH)*

1. 0 fault tolerant individually.
2. AID'S of MDM PF2 are independent of AID'S of MDM PF1.

MDM DIH*

1. 0 fault tolerant individually.
2. DIH's of MDM PF2 are independent of DIH's of MDM PF1.

MDM SIO*

1. 0 fault tolerant individually.
2. SIO's of MDM PF2 are independent of SIO's of MDM PF1.

Ku-band

1. 0 fault tolerant in any configuration

2. Independent of other Orbiter monitor modes

S-band FM

1. 1 fault tolerant

*This capability will be lost for a brief period of time if the GPC that is processing payload data fails. In this event one of the remaining four GPC's will be configured to perform the payload command/monitor task. The reconfiguration process can take on the order of 15 min. Other than this specific situation, each interface type is independent of all other types.

Note: Transmission of Orbiter/payload data via Orbiter PCMMU to the ground is 1 fault tolerant.

Note 4: For the control of payload hazardous functions, certain Orbiter rotary switches can be considered equivalent to one fault tolerant under the following specific conditions:

1. The switches are Orbiter-type, multipole rotary switches (Orbiter Project Parts List (OPPL) parts), with at least two poles wired to provide redundant electrical circuits, and powered from separate services.

2. The third control, if required to complete the provisioning of two fault tolerant hazard control, must be provided via hardware, unless a contingency EVA is planned for this function.

3. All circuits used in this application, including redundancy, must be verified preflight.

4. This applies only to the use of switches in Must-Work-To-Be-Safe functions and does not apply when switches are used as safety inhibits (three inhibits are required regardless of type).

5. Payload circuit design must provide for two electrical inputs, either of which will complete the must-work function.

Note 5: Use of more than one cabin payload bus is equivalent to 1 fault tolerant for Must Work functions if the following conditions are met:

1. Circuit redundancy is maintained by the Orbiter integration wiring and payload wiring for the function(s) involved,

2. 1 fault tolerant power is required only for a limited time (e.g., control of pyro firing functions, etc.), and this power will not also be used for control of functions that are the additional means required to achieve 2 fault tolerance (e.g., jettison).

3. Existence of Cabin Payload Bus 1, 2 or 3 power can be verified without subsequent cycling of the Orbiter S25 panel switch until completion of the potentially hazardous operation.

4. Failure of the redundant Orbiter Cabin payload buses during the hazardous operations does not result in an immediate catastrophic hazard.

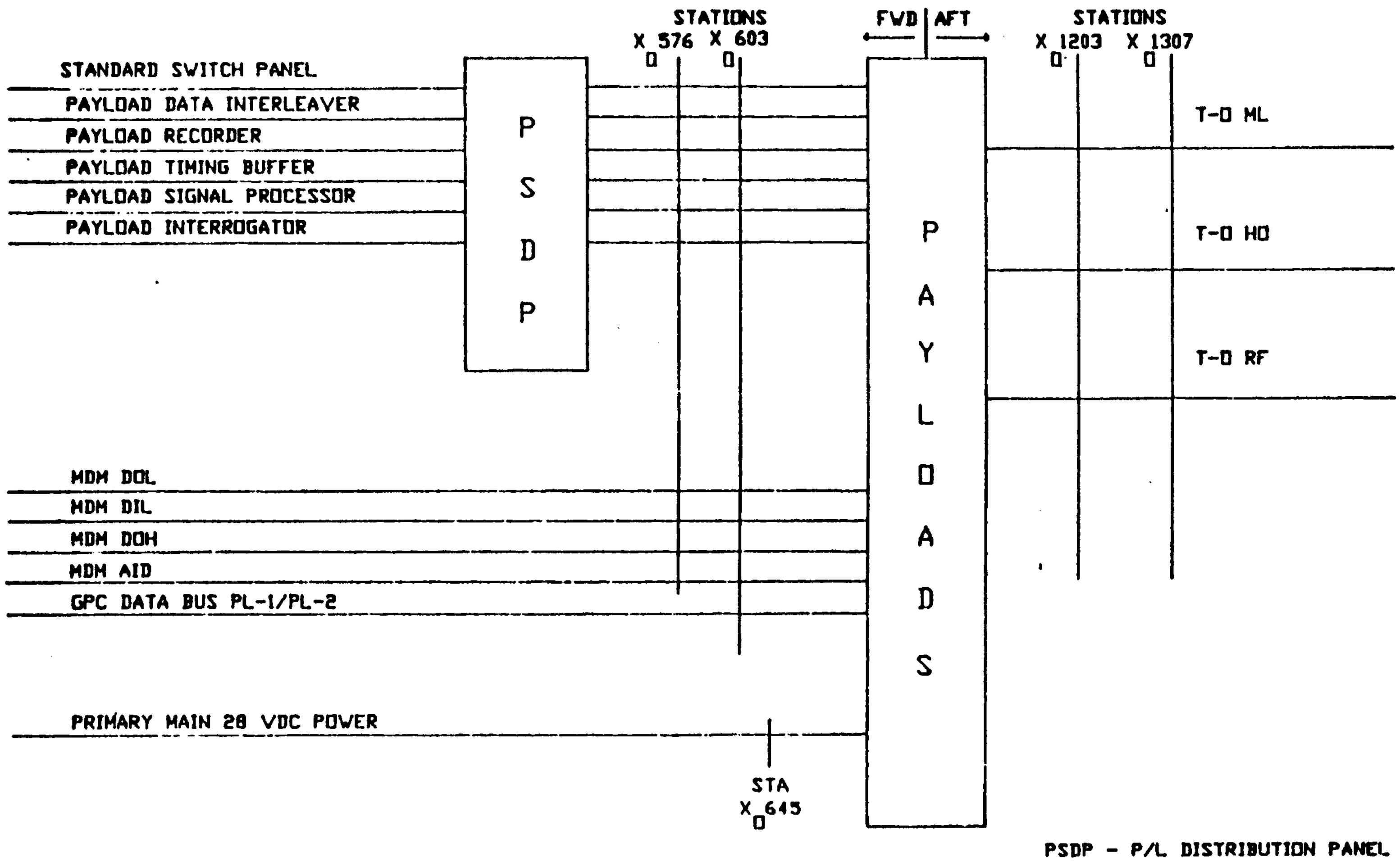


Figure 4-1. - Standard payload accommodations.

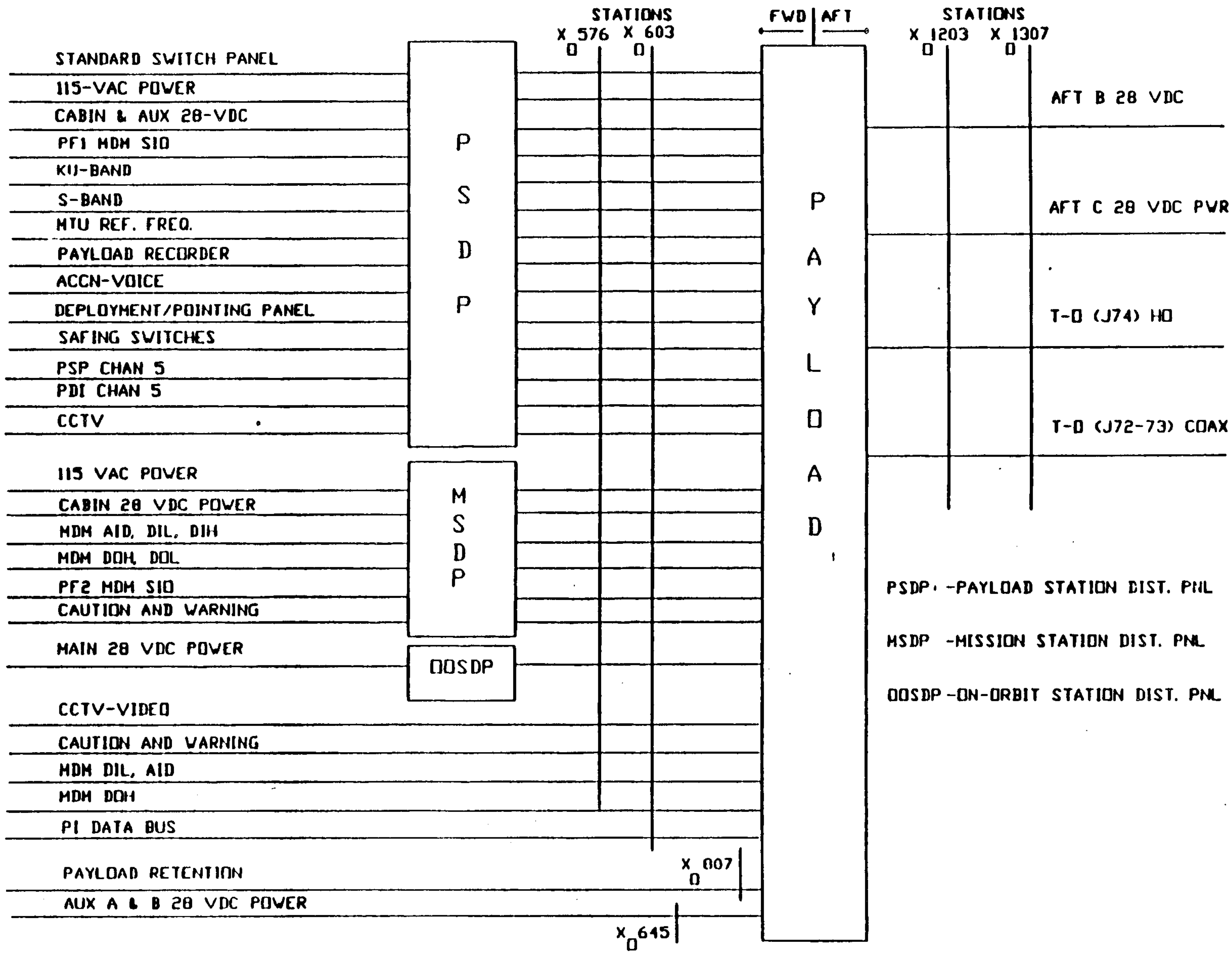


Figure 4-2.- Optional payload accommodations.

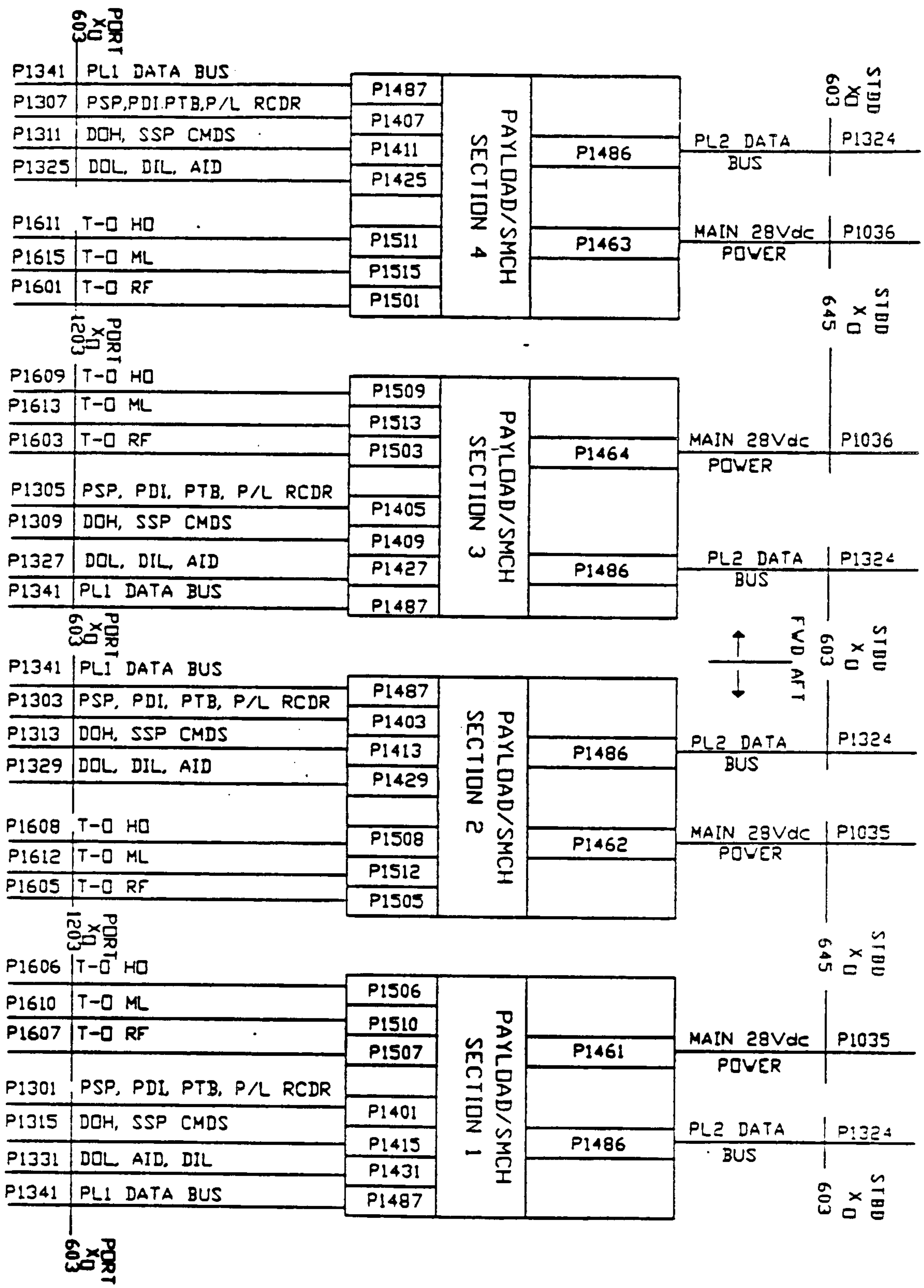
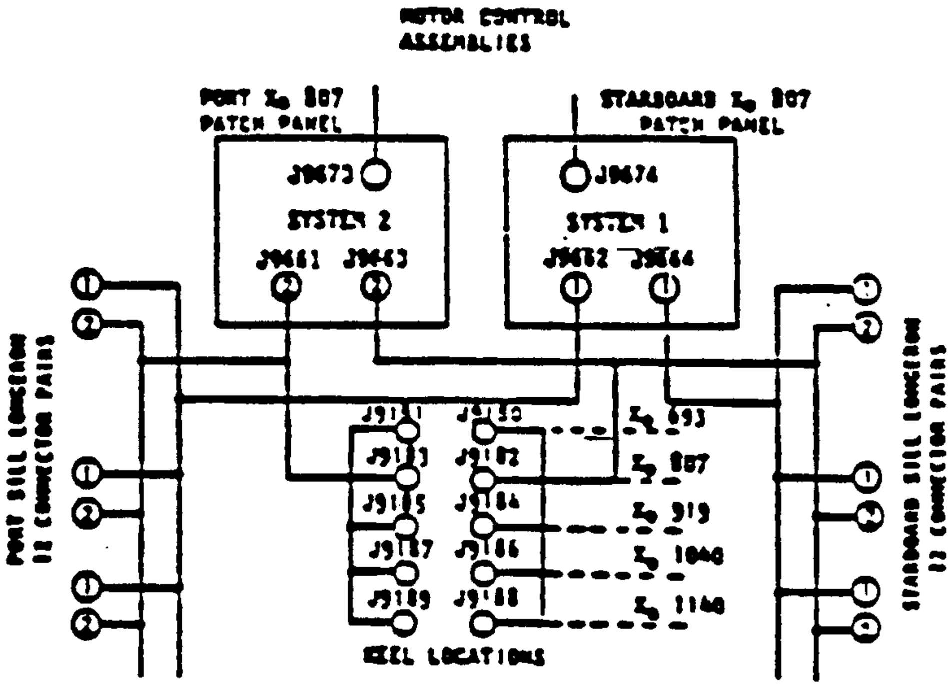


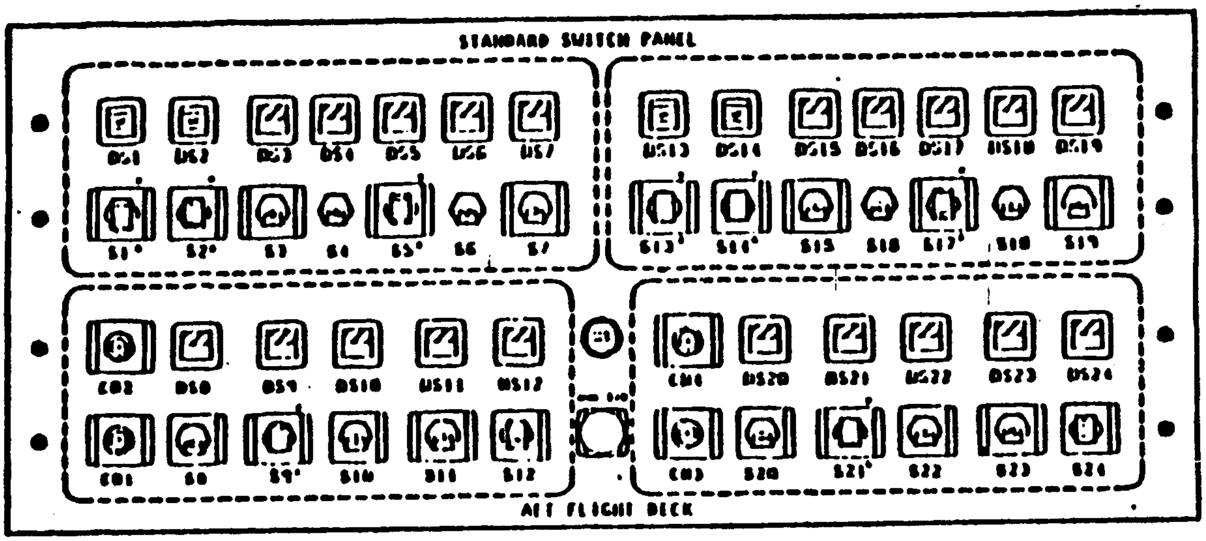
Figure 4-3.- Standard Mixed Cargo Harness (SMCH)
Orbiter-to-payload signals.



SILL LONGERON
POWER CONNECTOR LOCATIONS

X_o	PORT (Y_o-94, Z_o410)		STARBOARD (Y_o94, Z_o410)	
	SYSTEM 1	SYSTEM 2	SYSTEM 1	SYSTEM 2
631	J9017	J9019	J9022	J9024
647	J9021	J9023	J9026	J9028
712	J9049	J9051	J9048	J9052
747	J9061	J9063	J9064	J9066
815	J9073	J9075	J9078	J9082
[illegible]	J9085	J9087	J9094	J9096
929	J9097	J9099	J9108	J9112
1008	J9101	J9103	J9114	J9116
1053	J9111	J9113	J9126	J9128
1111	J9121	J9123	J9138	J9142
1145	J9133	J9135	J9154	J9156
1233	J9143	J9145	J9166	J9168

Figure 4-4.- Retention system power interfaces.



DS - ANNUNCIATOR
S - TOGGLE SWITCH
CB - CIRCUIT BREAKER

Figure 4-5.- Standard Switch Panel controls.

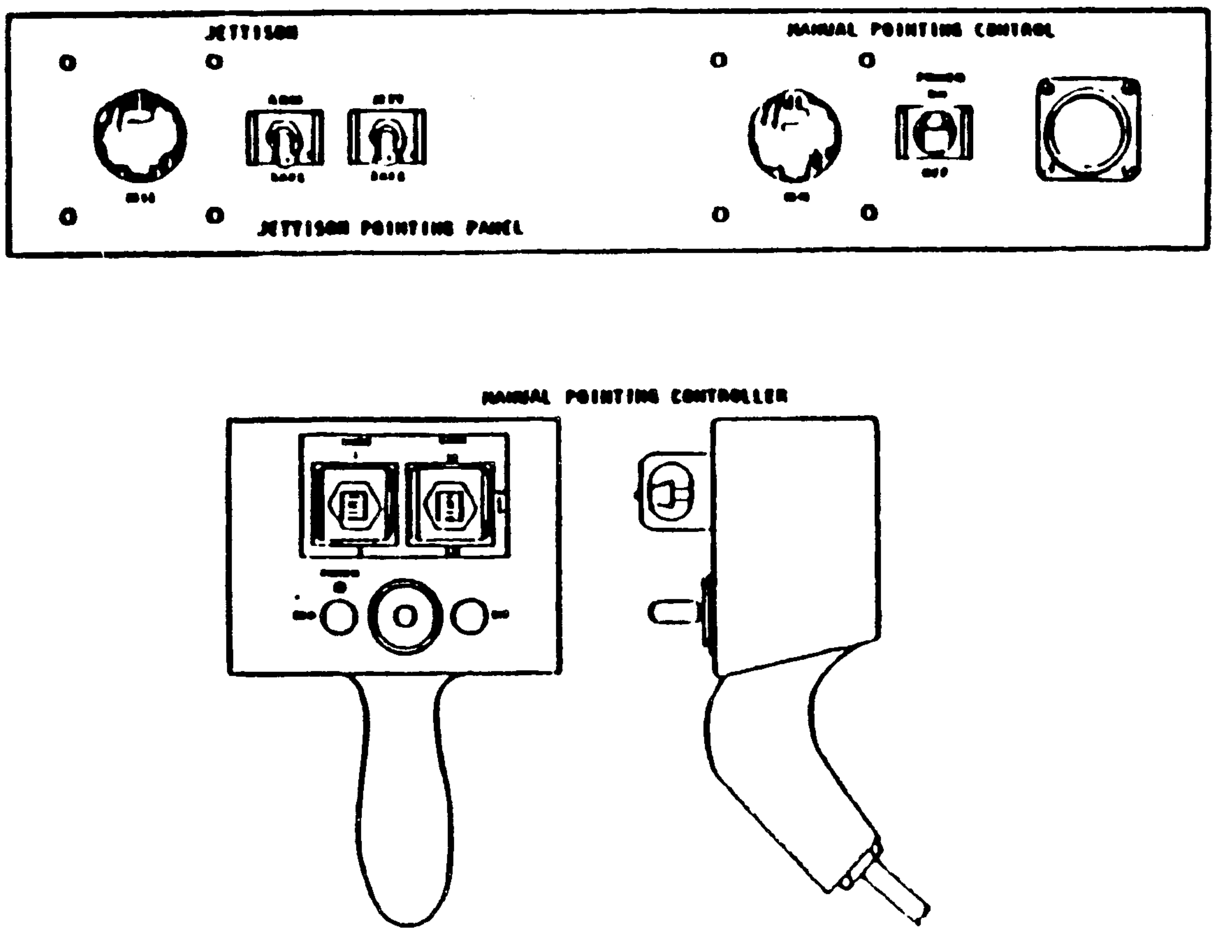


Figure 4-6.- Jettison pointing panel/manual pointing controls
(Aft Flight Deck).

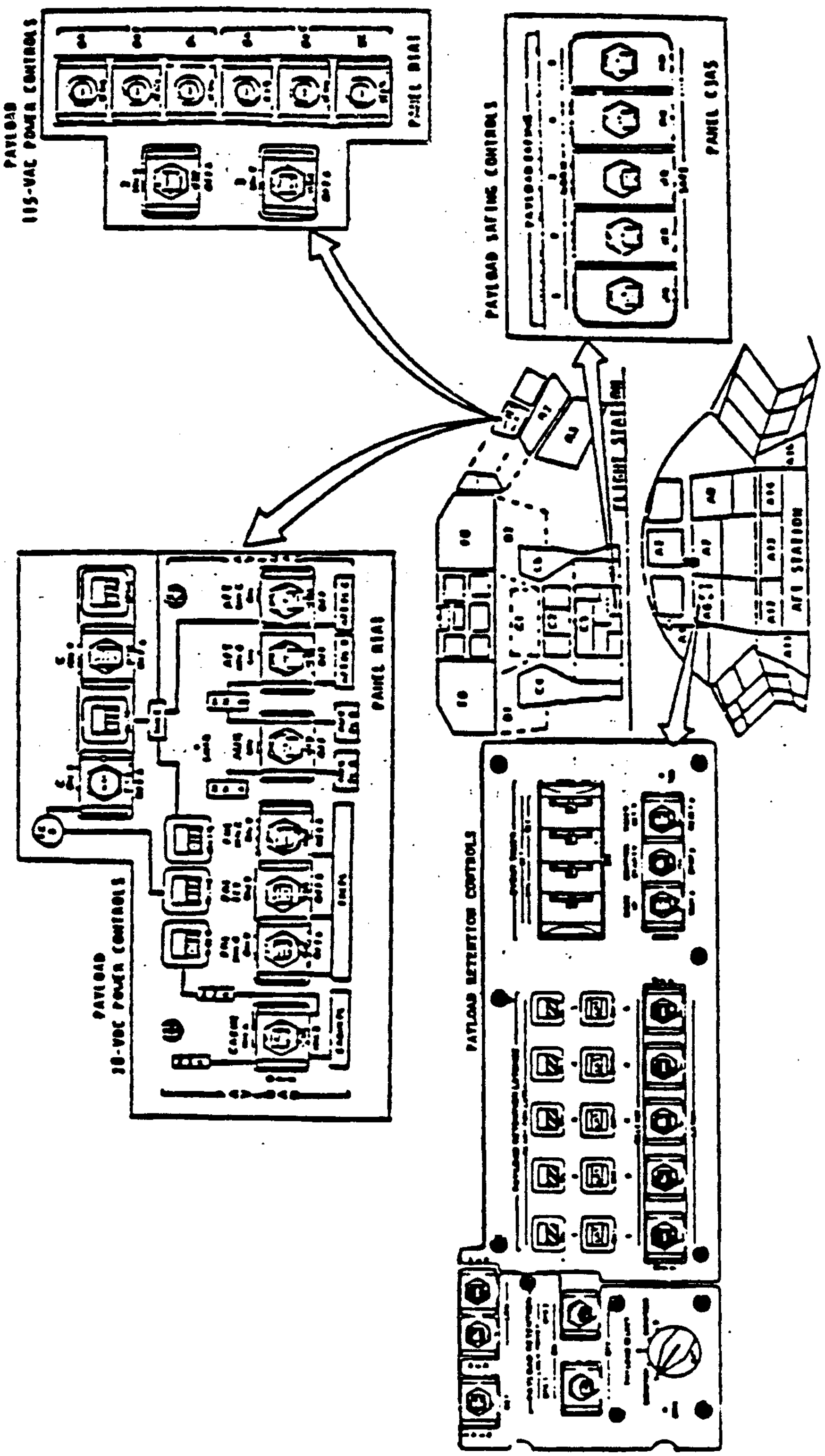


Figure 4-7.- Payload power, retention, and safing controls.

5.0 ORBITER/CARGO INTERFACE ANALYSIS

This section contains the analysis for the Orbiter-to-payload interfaces. The analysis identifies each interface and postulates credible failure conditions that can occur at the interface. These interface failure conditions are then related to the number and type of failure modes that would have to occur in the associated Orbiter subsystems or hardware to produce the interface failure condition.

Table 5-1 describes the general content of the analysis sheets used in the analysis. Each analysis chart (tables 5-2 through 5-24) is accompanied by a functional schematic (figure 5-2 through 5-24) depicting the interface and associated Orbiter equipment, crew control provisions, and (where applicable) identification of SMCH's.

The failure tolerance definition shown in the tables in this section is based on the number of failures that can be tolerated and still retain functional capability at the Orbiter/payload interface. The definition assumes that, based on the SSP mixed user's allocation policy, the payload accommodation user has access to one of the four equal standard sections. The user must therefore analyze the payload effects to determine if access to additional standard sections are needed to meet redundancy and load factor requirements.

The failure tolerance definition for the payload main 28 V dc power is shown in tables 5-2 and 5-3 for circuit elements up to the single fuse that is supplying the payload and for the particular user interface point on the other side of the fuse. The user must consider the potential his circuit has for blowing this fuse in the determination of his redundancy requirements.

Table 5-4 has been annotated with number as shown in tables 5-4 x 1 and 5-4 x 2 for use in explaining how to read the failure mode, column 2, and effects, column 1, to arrive at the associated failure tolerance, column 4 and 5.

The various combinations of failure mode and effect that lead to the failure tolerance for the two examples are as follows:

	Failure effects column 1	Failure mode column 2	Failed component column 3	Failure tolerance column 4 and 5
Example 1	10	13	6	8 and 9
	10	14	7	11 and 12
	10	14	8	11 and 12
	10	14	9	11 and 12
Example 2	19	24	13	20 and 22
	19	25	14	20 and 22
	19	25	15	20 and 22
	19	25	16	20 and 22
	19	25	17	21 and 23
	19	25	18	21 and 23

Table 5-1.- PAYLOAD SERVICE PROVIDED: IDENTIFICATION OF PAYLOAD INTERFACE FUNCTION UNDER ANALYSIS

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Describe failure effects at the Orbiter-to-payload interface.	Identify failure modes that could cause the noted interface failure effect	Identify the system component causing the failure effect	Number of failures that can be tolerated and still retain functional capability at interface Describe levels of redundancy that achieve this tolerance		Describe any crew actions or equipment availability that may be used to maintain functional capability
(Same)	(Describe all additional failure modes until all are analyzed)	(Same)	(Same)	(Same)	

Table 5-4 X 1.- FAILURE TOLERANCE EXPLANATION - EXAMPLE 1

Failure effects 1	Failure mode 2	Failed component 3	Failure tolerance: w/o crew action 4	Failure tolerance: with crew action 5	Rationale/ remarks
10 Total power loss of all 28 V commands of Standard Switch Panel 1 and 2 to 1/4 SMCH, sections 1-4. (Payload connectors P1409, P1411, P1413, P1415.)	Open 13	6 1 payload cabin main power (crew) control switch (S25)	8 Zero Switch S25 functionally inoperative	9 One	
	No output 14	7 2 main (A and B) buses	11 Zero	12 One	
		8 Essential buses (1BC and 2CA)			
		9 Fuel cells (1 and 2) power generators			

Table 5-4 X 2.- FAILURE TOLERANCE EXPLANATION - EXAMPLE 2

Failure effects 1	Failure mode 2	Failed component 3	Failure tolerance: w/o crew action 4	Failure tolerance: with crew action 5	Rationale/ remarks
19 Interruption of 28 V commands to all 1/4 SMCH, sections 1-4 (Standard Switch Panel 1A, 1B, 2A and 2B) (Payload interface connectors P1409, P1411, P1413 and P1415	Open 24	13 1 main crew control switch (25, panel R1A1)	20 One	22 One	**Fuel cell undervoltage output will result in a crew-activated shutdown of that fuel cell.
			Crew can switch to redundant string.		
	No output 25	14 1 main (A or B) bus			
		15 1 essential (1BC or 2CA) bus			
		16 1 fuel cell power generator (1 or 2) **			

Table 5-4 X 2.- FAILURE TOLERANCE EXPLANATION - EXAMPLE 2 (Concluded)

Failure effects 1	Failure mode 2	Failed component 3	Failure tolerance w/o crew action 4	Failure tolerance with crew action 5	Rationale/ remarks
		17 2 active diodes (a and d or c and d)	21 One	32 One	
		18 2 active RPC's (c and f or g and h)			

SECTION I: POWER SERVICES

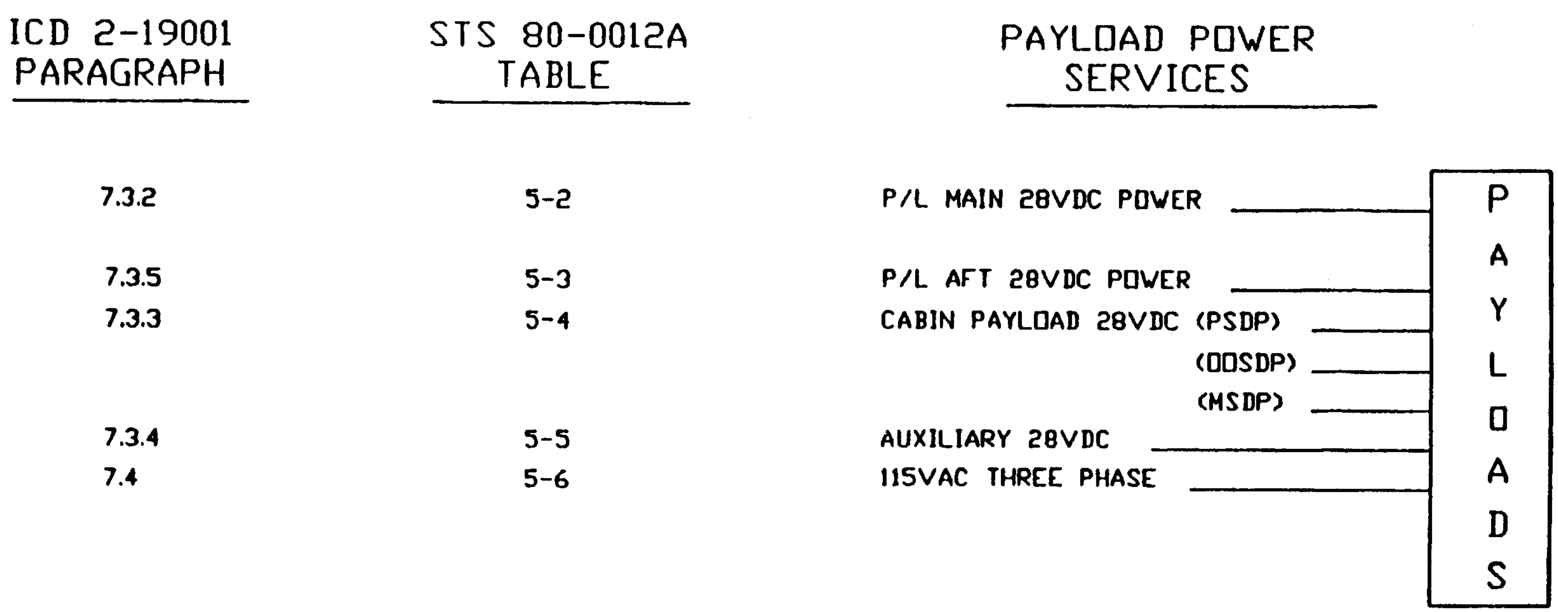


Figure I.- Payload power accommodations (overview).

Table 5-2.- POWER SERVICES: PAYLOAD MAIN 28 V DC POWER
(Figure 5-2)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of primary power (after power applied) (based on single 0 gauge feeder)	Open	200 amp fuse	Zero	Zero	See note 1 on page 12
		Crew control switches S12 or S28		One	Interruption of 28 V dc power to payload. Main bus B provides a backup for main C. (Main C is primary payload 28 V dc bus.)
		Motor control switches S2 or S5 of MDA-3			
	No output	Fuel cell			
		Main bus			
	Output high	Kill power RPC in mid PCA-2			Dedicated fuel cell mode must be used to supply payload power.
	Input high	Kill power RPC in mid PCA-2 and PCA-3			

Table 5-2.- POWER SERVICES: PAYLOAD MAIN 28 V DC POWER (Concluded)
(Figure 5-2)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Unable to re- 28 V dc power from payload	Open	S28		Zero	
	No output	ESS bus 3AB and 2CA	One	One	Orbiter es- sential buses are continuously powered from 2 Orbiter- main buses.

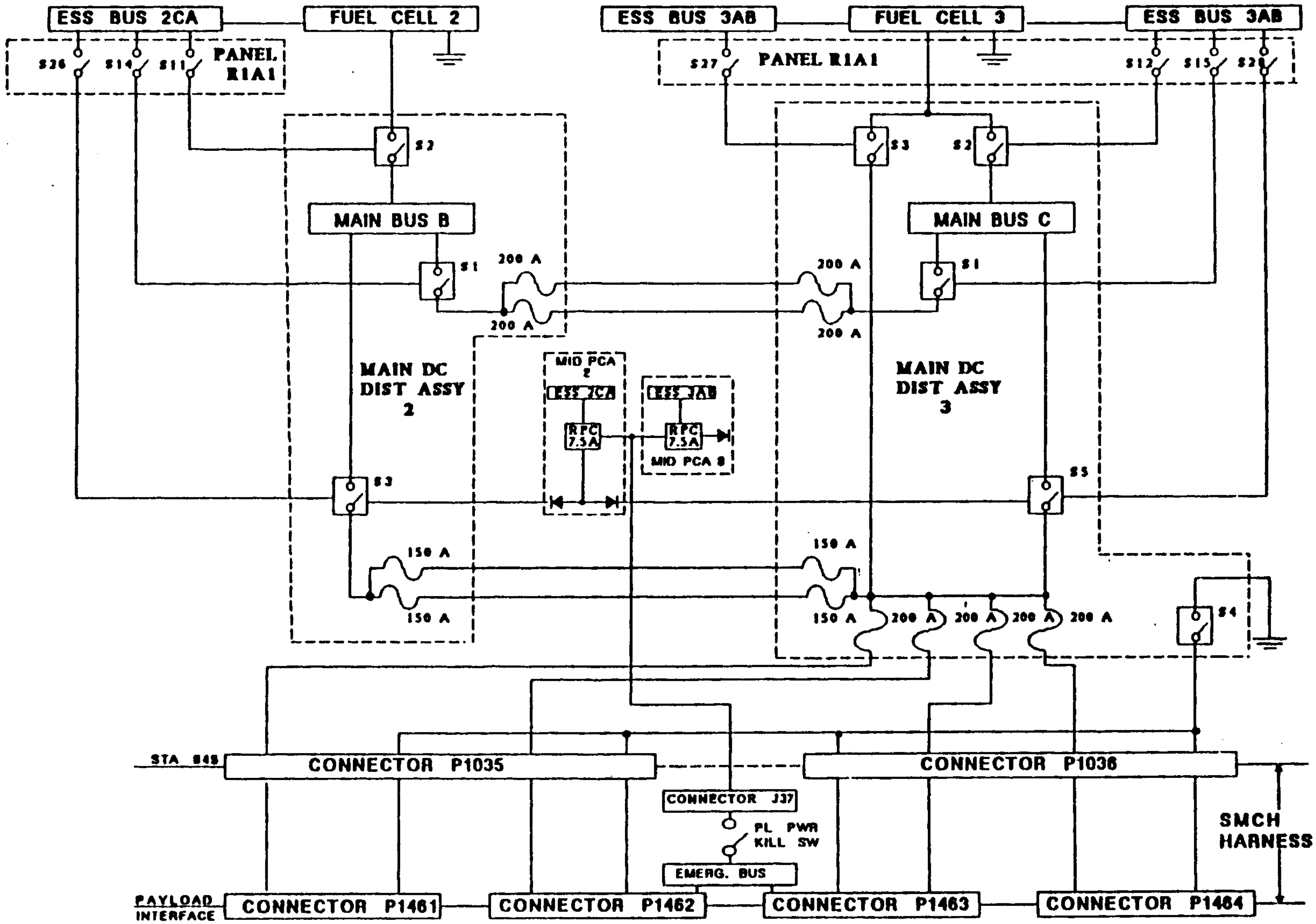


Figure 5-2.- Main 28 V dc power.

Table 5-3.- POWER SERVICES: AFT BUS
(Figure 5-3)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of power from either bus (with power ap- plied)	Open	Latching relay	Zero	Zero	
		80 amp fuse			
		150 amp fuse			
		200 amp fuse			
		Motor switch		One	
	No output	Main bus			
		Fuel cell			
Inability to apply power (with power off)	Open	S30 (S31)		Zero	
		ESS bus			
		Latching relay			
		80 amp fuse			
		150 amp fuse			
		200 amp fuse			
		Motor switch		One	
	No output	Main bus			
		Fuel cell			
Inability to remove power (with power applied)	Open	ESS bus	One		
		S30 (S31)	Zero	Zero	
	Short to +28	Latch relay			

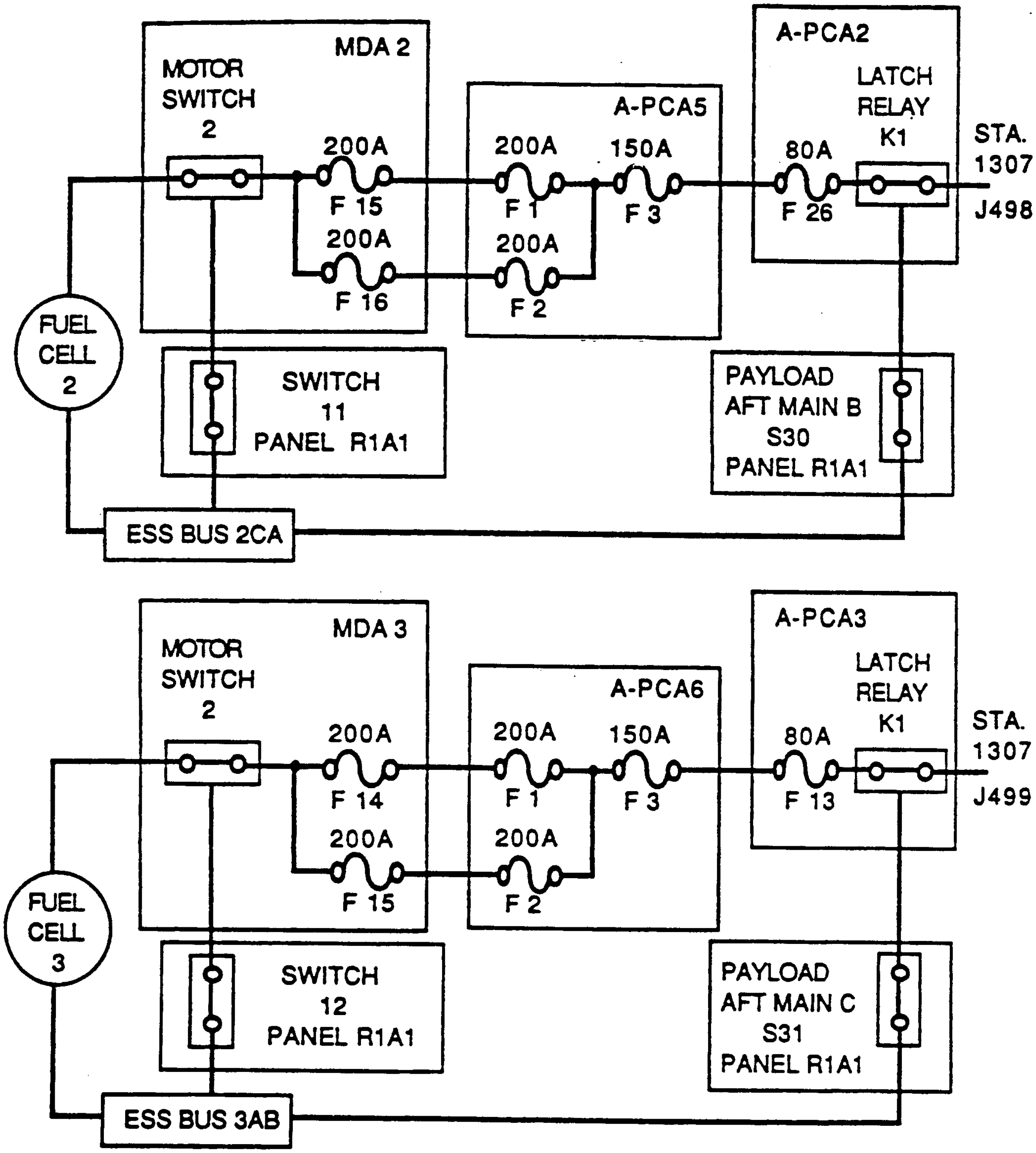


Figure 5-3.- Main 28 V dc power (aft buses B and C).

Table 5-4.- POWER SERVICES: CABIN PAYLOAD BUS
(Figure 5-4)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of 28 V dc on cabin payload bus (with power ap- plied)	Open	Switch S25	Zero*	Zero	*Use of more than one Cabin Payload Bus can be equivalent to 1 fault tol- erant (see section 4, note 5)
		1.2 K resistor		One	
		Diode			
		RPC			
		Motor switch			
	Short to case	Diode		Zero	
	No output	ESS bus	One	One	
		Main bus	Zero		
		Fuel cell			
Inability to remove power	Short	RPC			
	Closed	Switch S25		Zero	

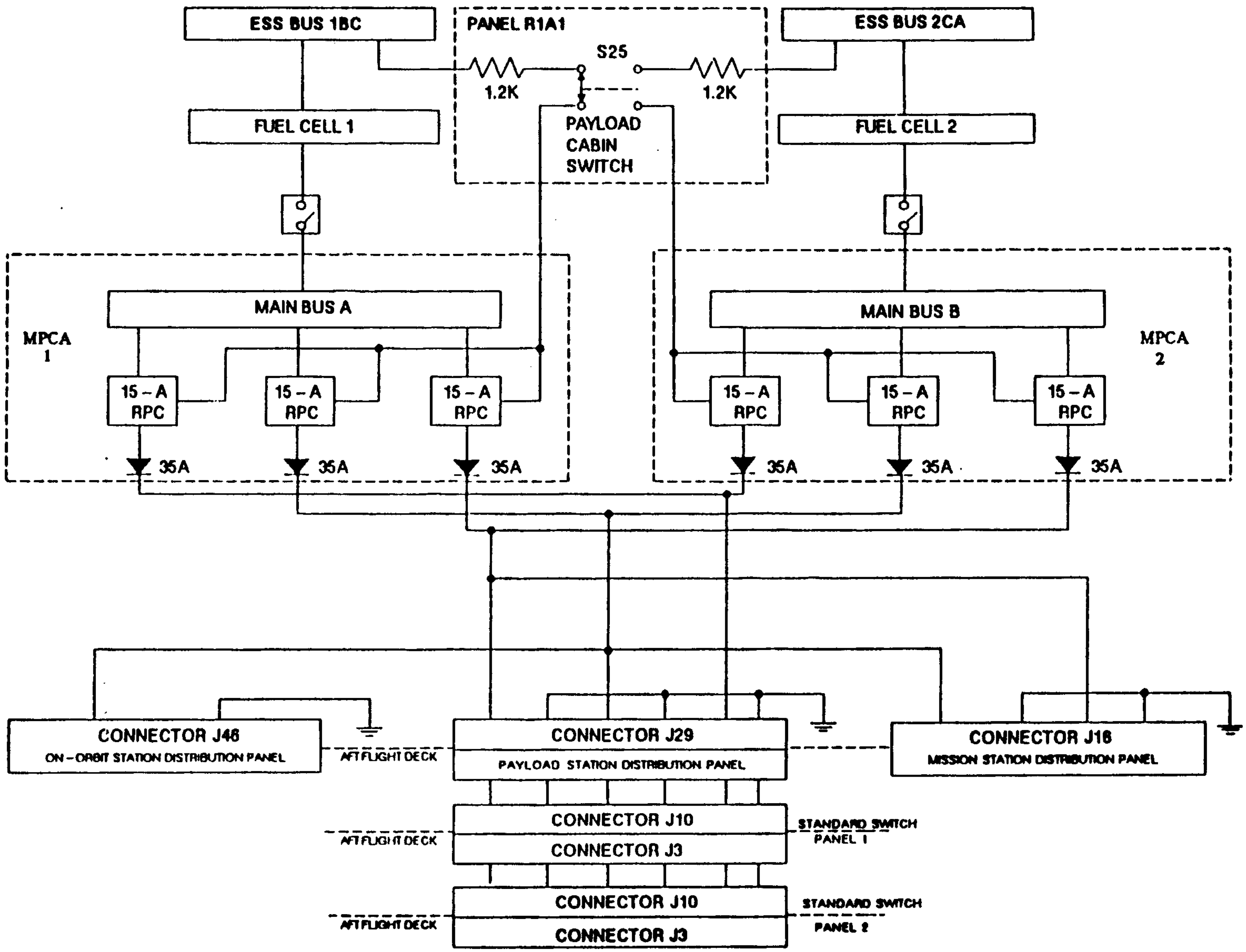


Figure 5-4.- Cabin payload bus 28 V dc.

Table 5-5.- POWER SERVICES: AUXILIARY 28 V DC POWER
(Figure 5-5)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of 28 V dc power on bus A (bus B) (with power applied) Refer to figure 5-5	Open	RPC	Zero	Zero	If overload condition causes RPC to remove power, crew may restore power after fault is cleared.
		Switch S29			
		Resistor			
		Motor switch		One	
	No output	Fuel cell			
		Main bus			
		ESS bus	One		
Cannot remove 28 V dc power on bus A (bus B)	Short	Switch S29	Zero	Zero	
		RPC			

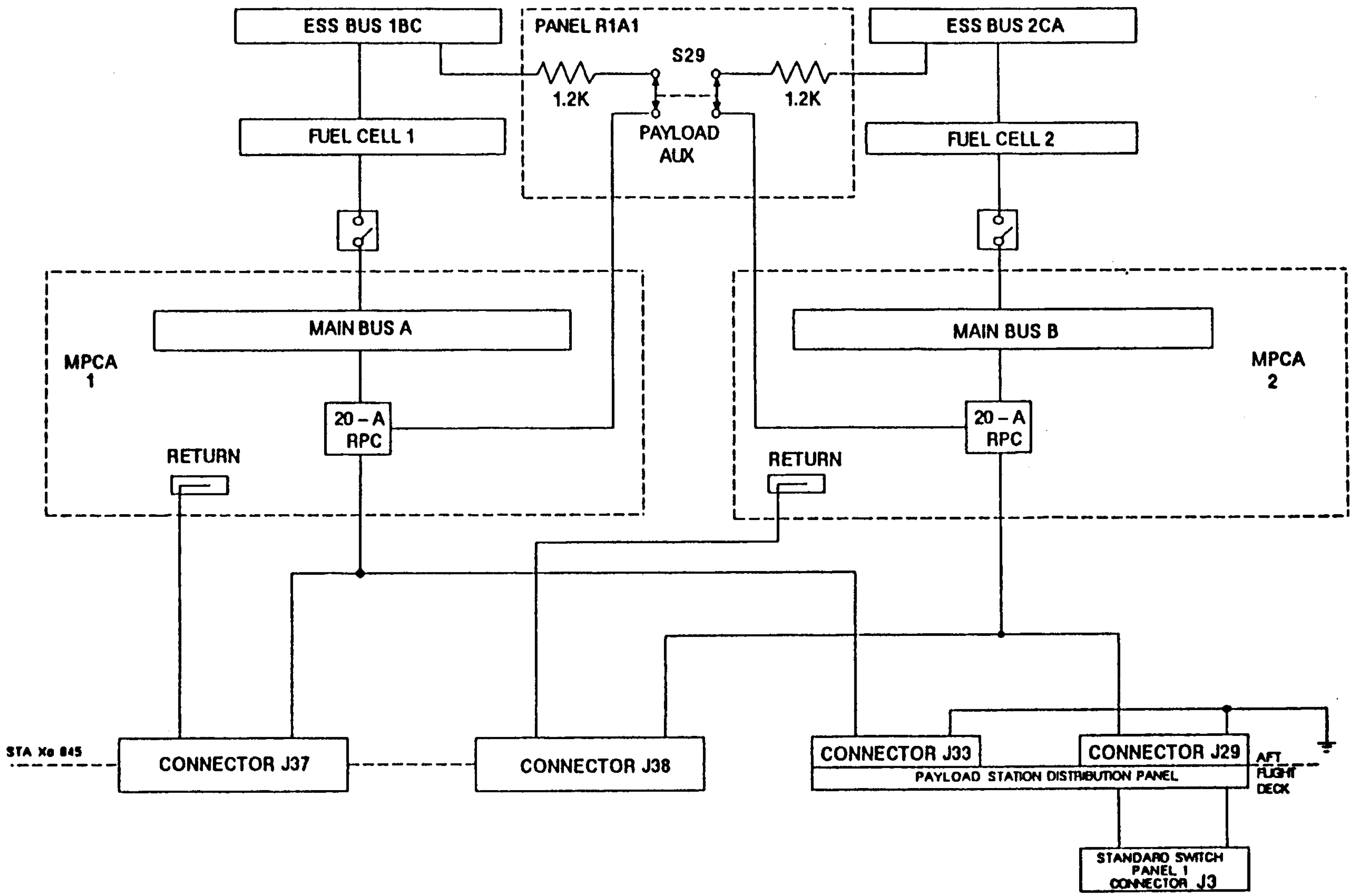


Figure 5-5.- Auxiliary 28 V dc power.

Table 5-6.- POWER SERVICES: 115 V AC 3-PHASE POWER
(Figure 5-6)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Total loss of 115 V ac 3-phase (with power applied)	Open	3-phase circuit breaker	Zero	Zero	Temporary overload may trip circuit breaker which may be crew resettable. Loss of a single component will result in loss of that phase only.
		Motor switch			
		Latching relay			
	No output	Single phase inverter			
		Single phase ac bus			
		Fuel cell		One	
		Main bus			
Inability to remove 115 V ac 3-phase power	Short	3-phase circuit breaker		Zero	

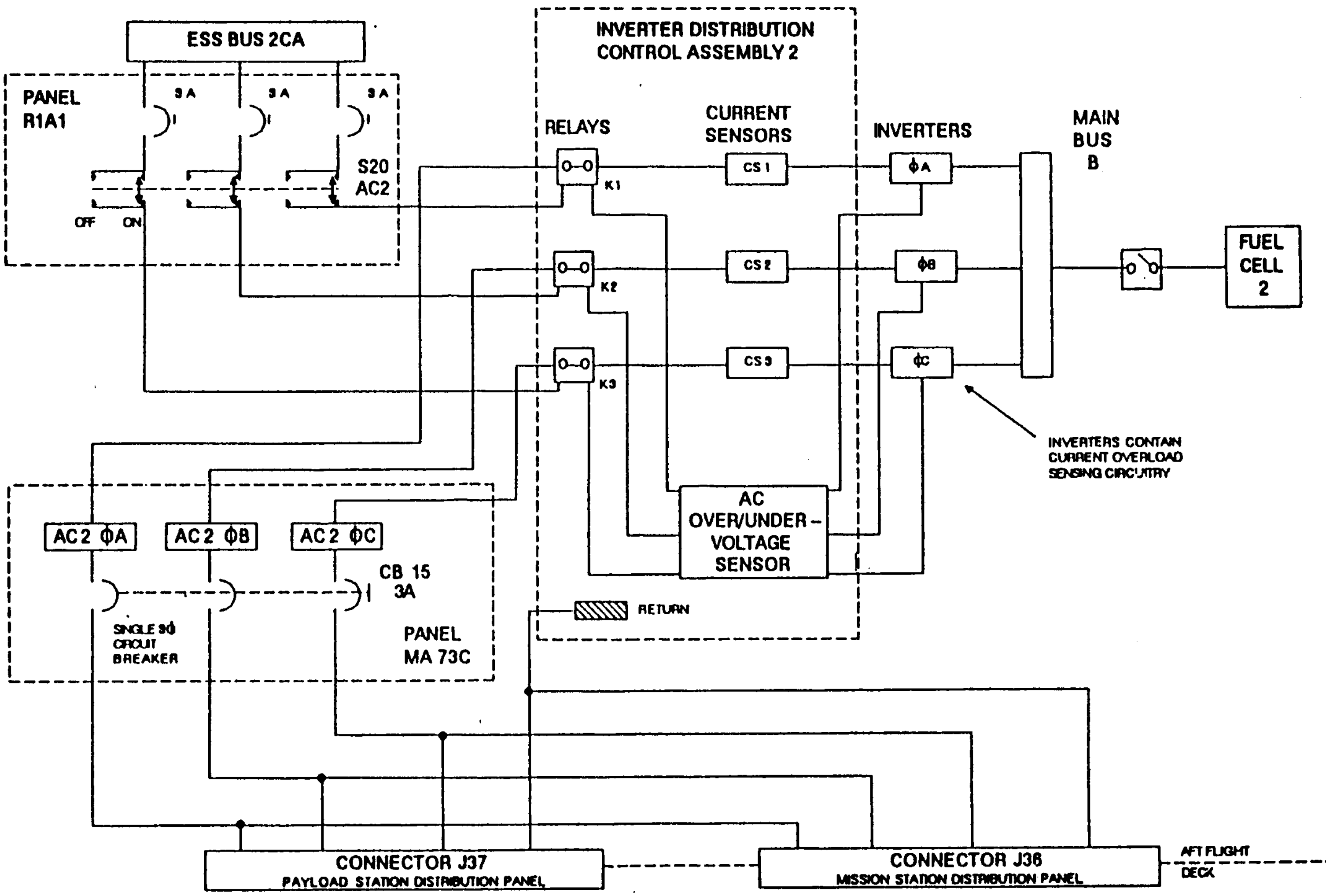


Figure 5-6a. - 115 V ac power (J36 and J37).

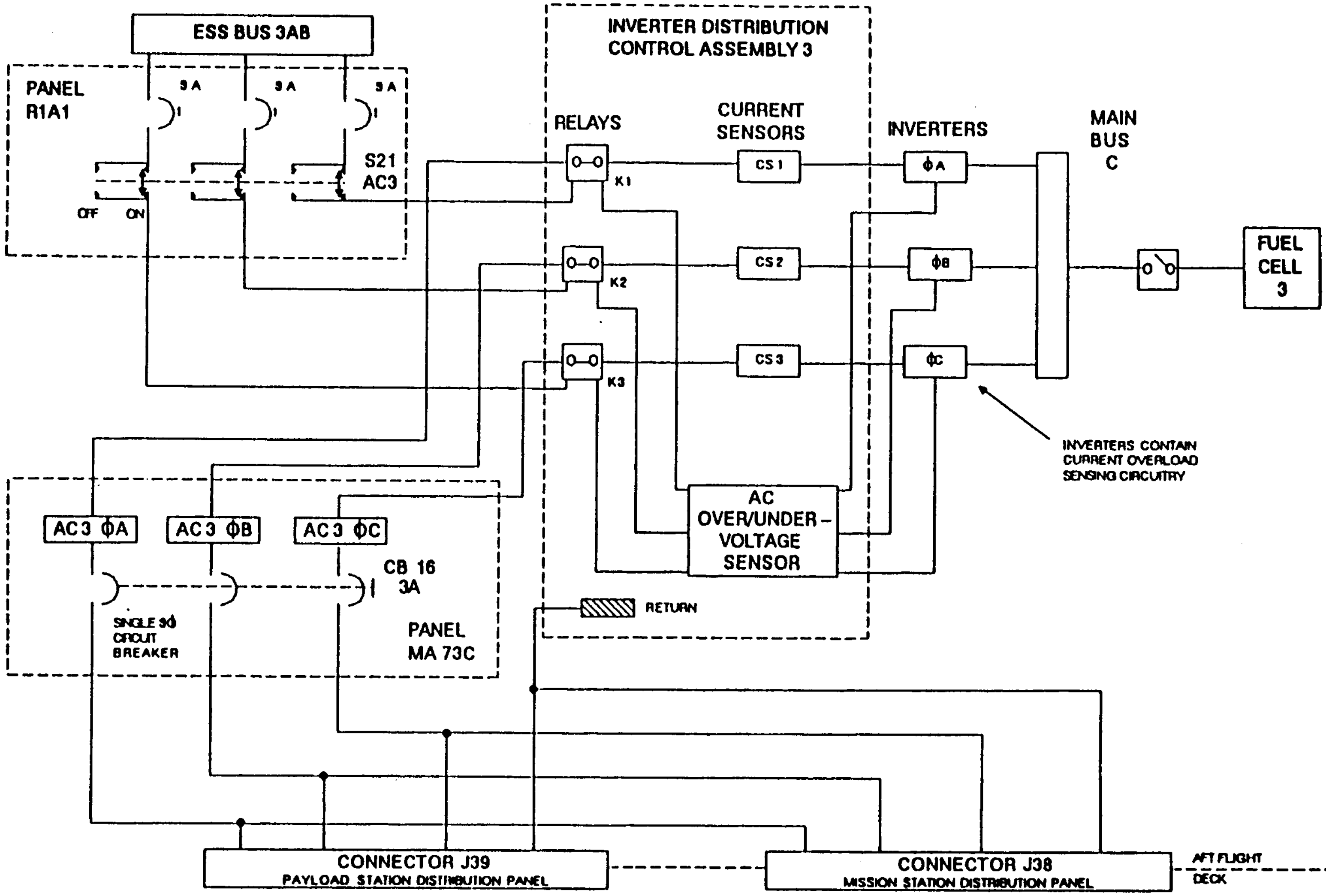


Figure 5-6b. - 115 V ac power (J38 and J39).

SECTION II: AVIONICS SERVICES

ICD 2-19001 PARAGRAPH	STS 80-0012A TABLE	PAYLOAD AVIONICS SERVICES
8.2.1	6-3	PAYLOAD DATA INTERLEAVER
8.2.2.1	5-16	MDM PF-1 & -2 DOL
8.2.2.2	5-15	MDM PF-1 & -2 DOH
8.2.2.3	6-5	MDM PF-1 & -2 DIL
8.2.2.4	6-6	MDM PF-1 & -2 AID
8.2.2.5	5-20	MDM PF-1 & -2 SIO
8.2.2.7	6-7	MDM PF-1 & -2 DIH
8.2.3	6-2	PAYLOAD RECORDER
8.24	5-21	KU-BAND SP
8.2.5	5-18	PSP
8.2.6	6-4	S-BAND SP
8.2.7	5-22	ACCU VOICE
8.2.8	5-12	CCTV
8.2.9	6-8	CWEA
8.2.10	5-13	MTU & PTB
8.2.11	5-23	PAYLOAD SAFING
8.2.12	5-17	PL-1 & -2 DBS
13.4.3.1	5-9	DEPLOYMENT/POINTING PANEL
8.3.1	5-19	PAYLOAD INTERROGATOR
7.3.3	5-7, -8	SSP-1 & -2 POWER
7.3.3	5-7	SSP-1 & -2 COMMANDS
7.3.3	6-9	SSP-1 & -2 INDICATORS
13.4.3.2	5-10	P/L ARMING & JETTISON
7.6	5-11	P/L RETENTION SUBSYSTEM

PAYLOADS

Figure II.- Payload avionics accommodations (overview).

Table 5-7.- AVIONIC SERVICES: PAYLOAD 28 V SWITCH COMMANDS - STANDARD SWITCH PANEL (NO. 1 AND NO. 2) (Figures 5-7a and 5-7b)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of 28 V dc powered switch commands to one (1/4) section.	Open	Switch CB2 (or CB4) Cabin bus (see page 43)	Zero*	Zero*	*One fault tolerant under specific conditions (see note 2 on page 18).
Unable to remove 28 V dc powered switch commands to one (1/4) section.	Closed	Switch CB2 (or CB4)	Zero	One	

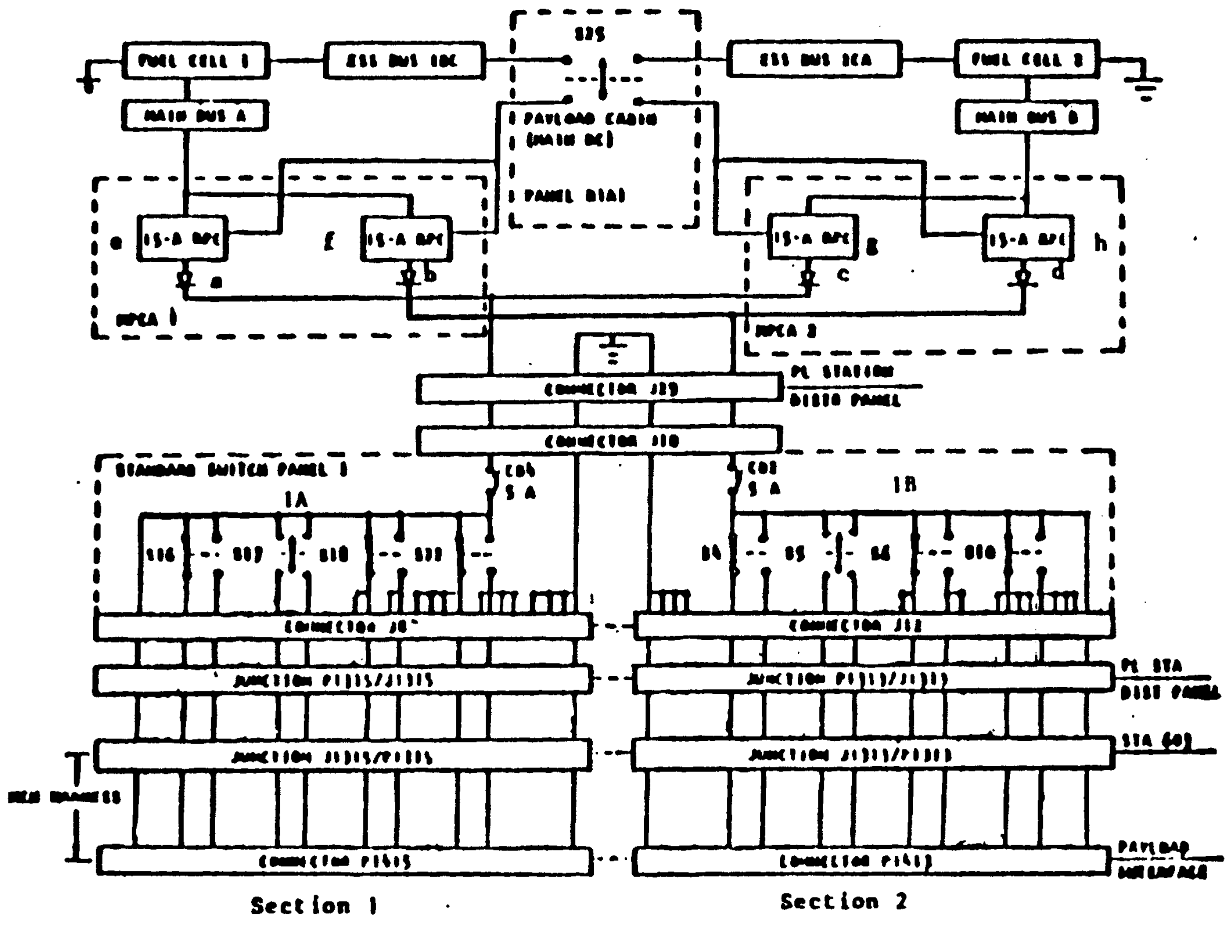


Figure 5-7a.- Standard Switch Panel 1 28 V commands.

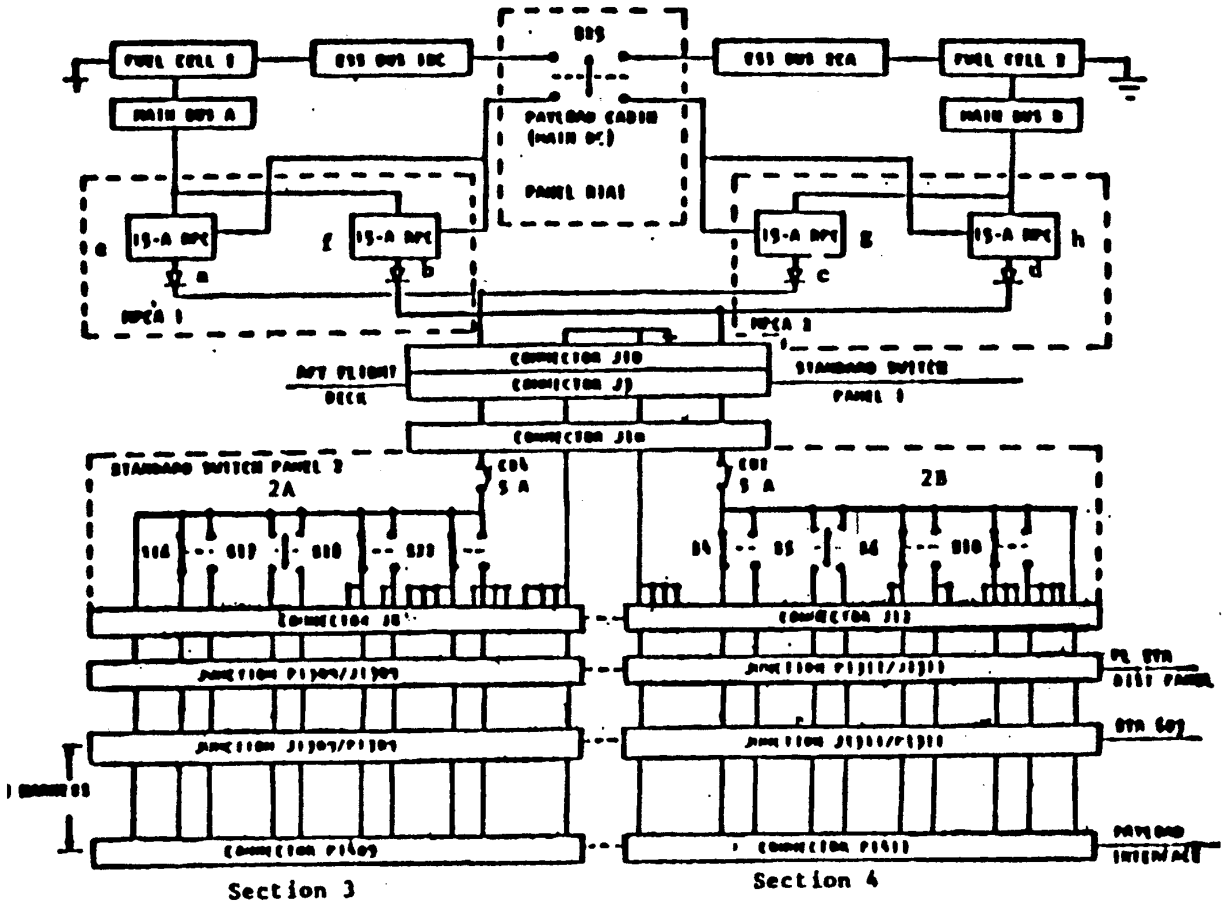


Figure 5-7b.- Standard Switch Panel 2 28 V commands.

Table 5-8.- AVIONICS SERVICES: STANDARD SWITCH PANELS
(Figures 5-8a and 5-8b)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of switch commands	Open or Close	Standard Switch Panel switches	Zero*	Zero*	*Use of any one switch can be considered one fault tolerant under certain specific conditions (see note 2 on page 18). Use of any two switches under certain specific conditions can be considered two fault tolerant (see note 3 on page 19).

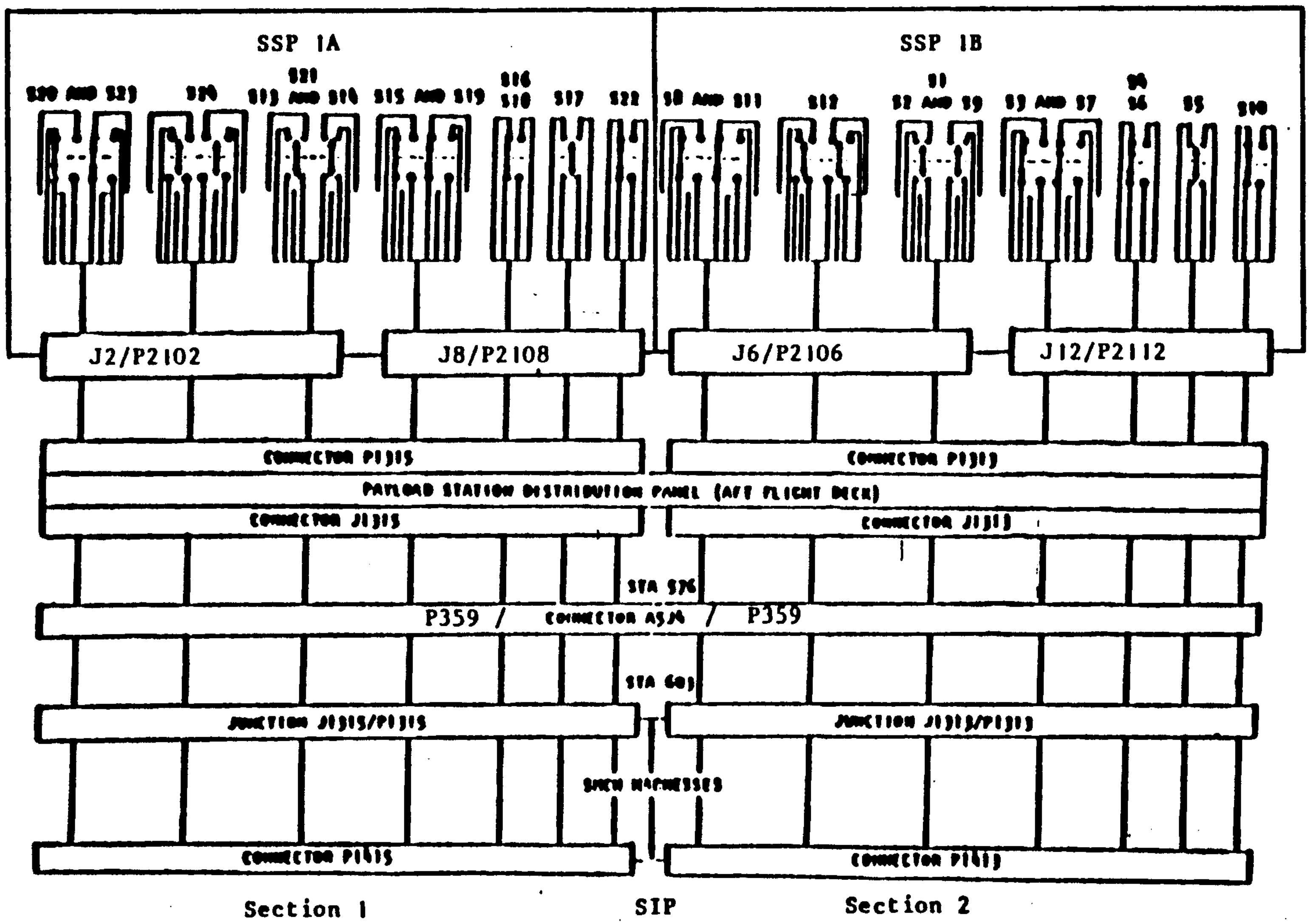


Figure 5-8a.- Standard Switch Panel 1.

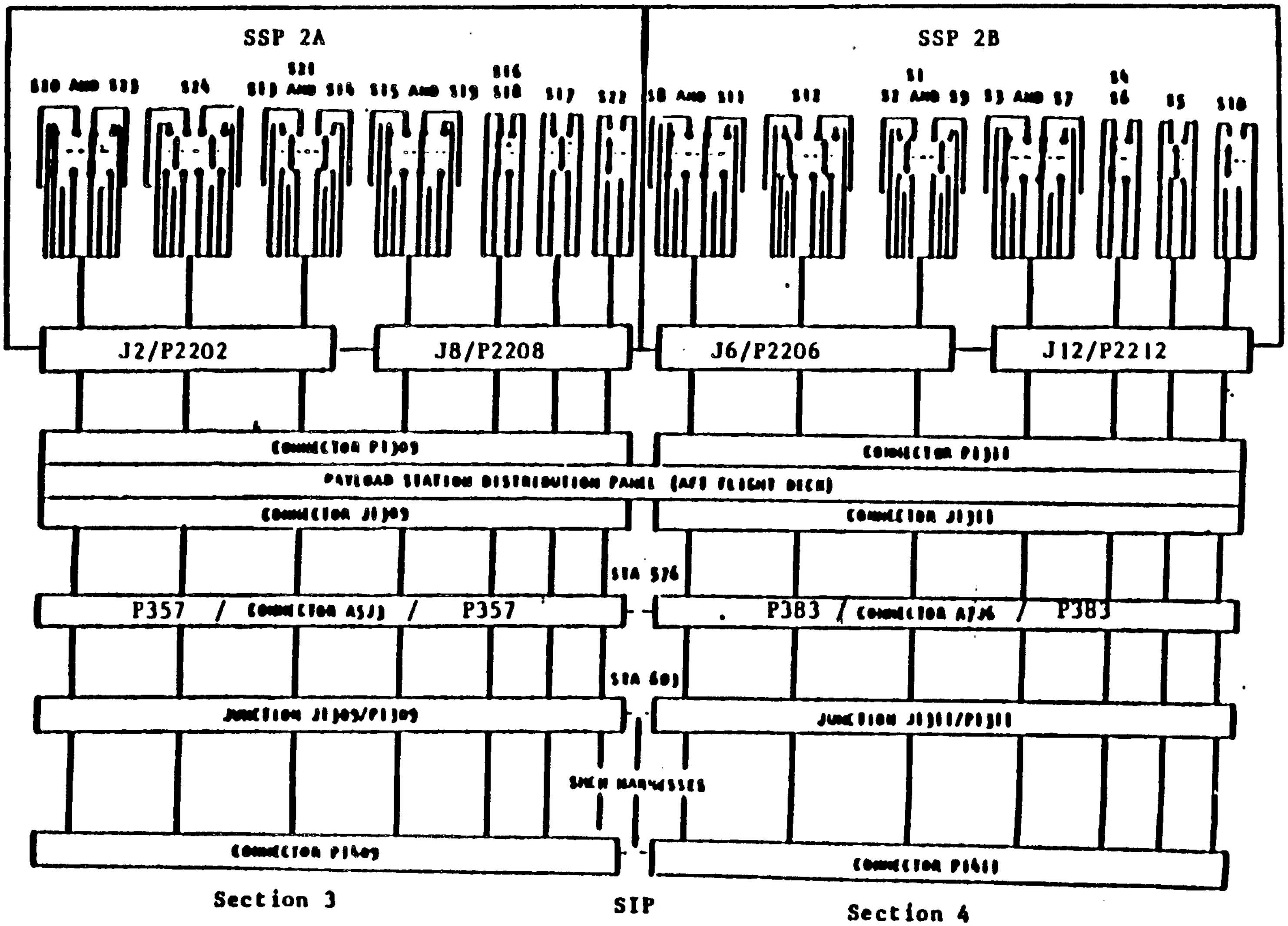


Figure 5-8b.- Standard Switch Panel 2.

Table 5-9.- AVIONICS SERVICES: PAYLOAD MANUAL POINTING CONTROL
(Figure 5-9)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Total loss of payload manual pointing control	Open	1 fuse (F2) (5A)	Zero	Zero	*Crew control switches are maintained on. Switches contain wicket guards to prevent inadvertent actuation. **Manual pointing controller contains 2 momentarily on pushbutton switches for roll control and 2 maintained-on switches for mode and gain control. Only the mode and gain switch- are wicket-guarded to prevent inadvertent actuation.
		1 power (crew) control switch of manual/ pointing panel*			
	No output	DC-to-dc converter of resistor and logic control circuits-converter			
Loss of power to manual pointing controller via Standard Switch Panel J10	See power services table 5-4	Loss of components of cabin payload payload bus system	See power services table 5-4		

Table 5-9.- AVIONICS SERVICES: PAYLOAD MANUAL POINTING CONTROL (Continued) (Figure 5-9)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
					The failure of payload cabin switch S25 can disable redundant power sources for all functions.
Total loss of payload pitch and yaw control (analog signals)	No output	DC-to-dc converter resistor and logic control circuits	Zero	Zero	Crew can switch to a redundant source of power. ***DC-to-dc converter is used to supply 10 V for discrete signals and 12 V for analog signals. These discrete and analog outputs are routed to the payload, mission unique, via a payload MDM or Remote Acquisition Unit (RAU).
		2 axis joy stick			
Total loss of payload roll control (discrete signals)		DC-to-dc converter 10-V output***			
	Open	2 MPC pushbutton switches**			

Table 5-9.- AVIONICS SERVICES: PAYLOAD MANUAL POINTING CONTROL
(Continued) (Figure 5-9)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Total loss of payload gain or mode control (discrete signals)	No output	DC-to-dc converter no 10 V dc***			Payload power control circuits must be able to inhibit premature power applications to prevent damage to the Orbiter and/ payload.
	Open	Control switch in both positions**			
Premature payload roll, mode, or gain control	Closed	1 of 2 crew-actuated push-button switches	Zero	Zero	
		1 of 2 crew-actuated toggle switches			Crew can deactivate manual pointing control.
Continuous payload roll, mode, or gain control		1 of 2 crew-actuated push-button switches			
		1 of 2 crew-actuated toggle switches			

Table 5-9.- AVIONICS SERVICES: PAYLOAD MANUAL POINTING CONTROL
(Concluded) (Figure 5-9)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Discrete signal over voltages (payload roll, mode, and gain control) (28 V max)	No output	2 dc-to-dc converter***			Multiple subcomponent failures internal to dc-to-dc converter are required to produce the noted failure condition.
Analog signal over voltages (payload pitch and yaw control) (28 V max)		Voltage regulation control***			

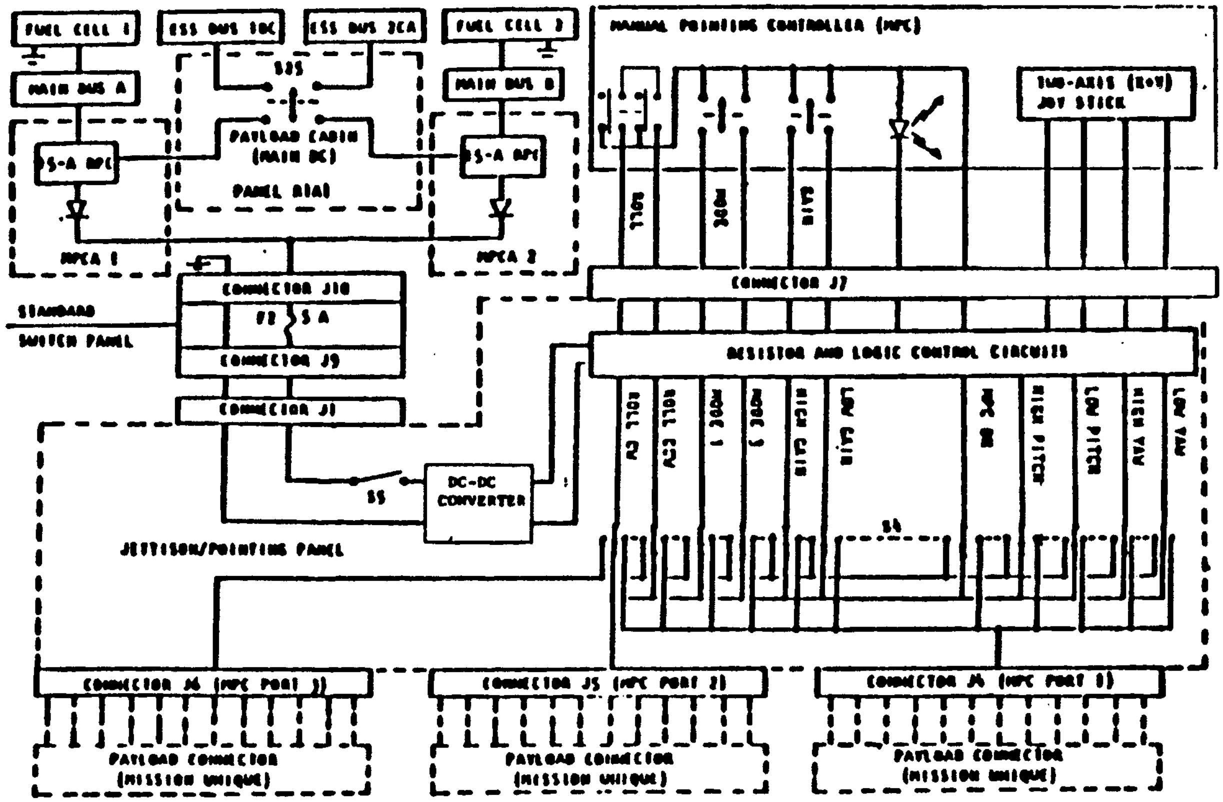


Figure 5-9.- Manual pointing control.

Table 5-10.- AVIONICS SERVICES: DEPLOYMENT POINTING PANEL
(Figure 5-10)

Failure effects	Failure mode	Failed component	Failure tolerance		Remarks
			w/o crew action	with crew action	
Loss of payload primary and secondary arming control functions	Open	DPP-S2	One	One	See general note 2.
		DPP-S1			See note 10-1.
		Standard Switch Panel fuse F3 or F4			See note 10-2.
Loss of payload primary and secondary deploy control functions	Open	DPP-S3	One	One	See general note 2.
		DPP-S1			See note 10-1.
		Standard Switch Panel fuse F3 or F4			See note 10-2.
Inadvertent payload arm or deploy function (not both)	Short	DPP-S2 and DPP-S3	Zero	Zero	See note 10-3.
Premature payload deploy (inhibit)	Closed	DPP-S1	One	One	See note 10-4.

Notes: 10-1. Because of mechanical redesign and proven high reliability of the rotary switch (S1), the failure mode which precludes switch rotation is considered noncredible. But internal breakage can cause shorting between any two adjacent contacts, or between any contact and the wiper, in addition to making the selected connection as well. The S-1 rotary switch will not short pole-to-pole (including any contacts and wiper) (see general note 4).

10-2. Power inputs to the DPP are independent and therefore one failure tolerant.

10-3. A rotary switch failure possibility (see note 10-1) can cause any other inadvertent arm or deploy function (not both) during this operation of another selected function on the DPP.

10-4. To prevent inadvertent operation crew control arming and deploy switches are lever-locked in the off position and contain wicket guards.

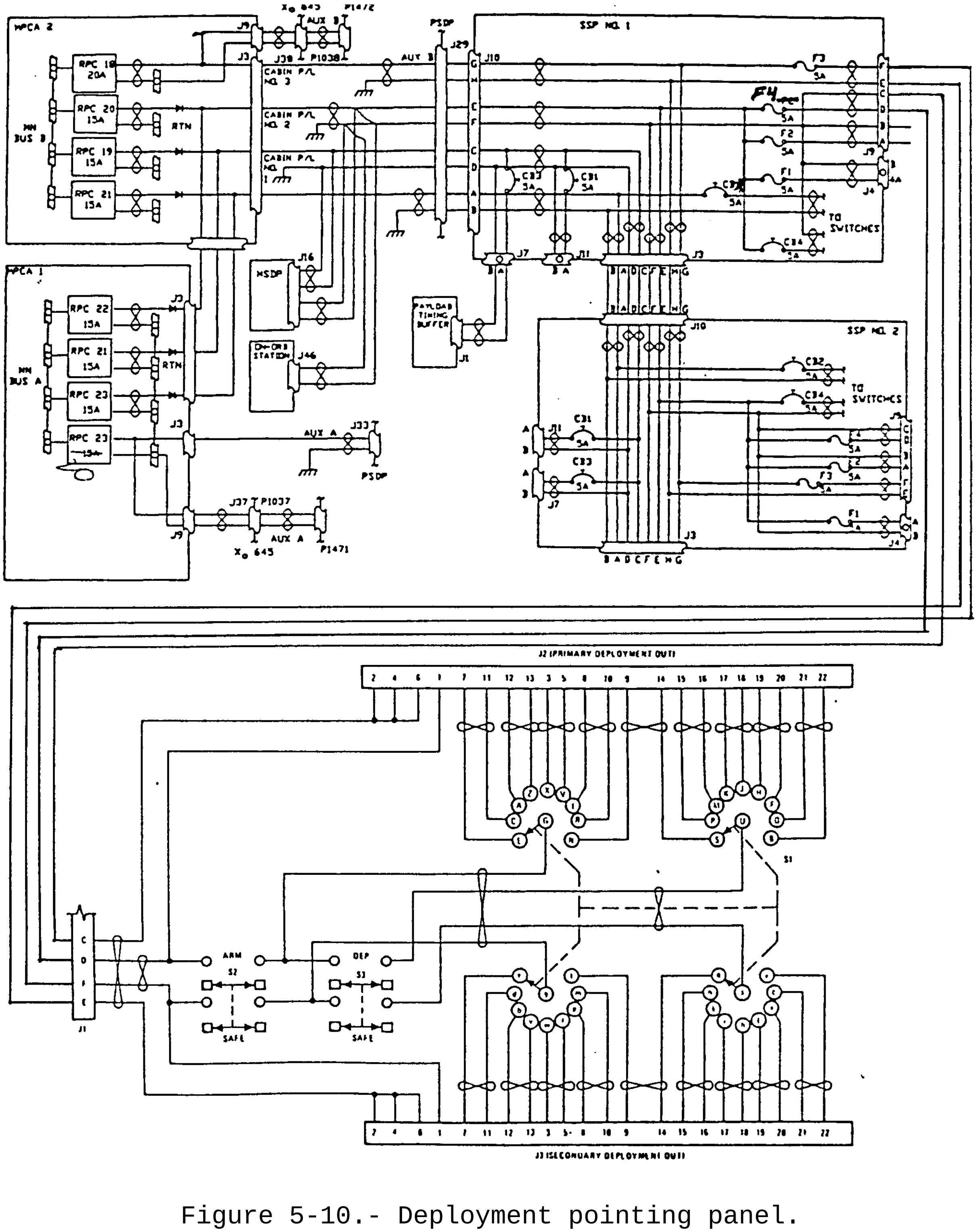


Figure 5-10.- Deployment pointing panel.

Table 5-11.- AVIONICS SERVICES: PAYLOAD RETENTION SYSTEM
(Figures 5-11 and 5-11a)

Failure effects	Failure mode	Failed component	Failure tolerance		Remarks
			w/o crew action	with crew action	
Loss of capability to release or latch payload	Open	Hybrid relay	One (two)	One (two)	See note 11-1.
		Limit switch			See note 11-0.
		3 amp fuse (F8 and F9)			
		1.2 K resistors			
		Logic power switches (S46,S47)			
		Actuator motor			
		Payload Select switch (S37)			See general note 4.
		Latch/release switches (S36, S42, S43, S44, and S45)			See note 11-2.
Premature release or latch operations of a nonselected payload retention mechanism	Shorts/closes	Hybrid relay	One (two)	One (two)	See notes 11-0 and 11-3.
		Payload Select switch			See note 11-4.
		Latch/release switch			See note 11-5.

Note 11-0. For the Launch, Ascent, Descent and the majority of the on-orbit mission phases, the PRLA system is two fault tolerant for inadvertent operation under the following conditions:

a. AC power is not applied to the hybrid relays (Payload Bay Mechanical Power "off");

b. PRLA System Logic Power is removed;

c. No latches are selected with the Release/Latch switches.

During certain on-orbit Orbiter operations which require powering of the ac power bus such as radiator deploy/stow, Ku antenna deploy/stow, RMS latch operations, RMS rollout operations, and PRLA operations, the PRLA system is one fault tolerant for inadvertent operation.

Note 11-1. The payload retention system provides two motor control systems to activate one latch. A latch will operate with the loss of one control system with an increased operating time.

Note 11-2. The Payload Select switch and the latch/release switches are wired electrically redundant and are considered the equivalent of one fault tolerant (see general notes 2 and 4).

Note 11-3. No single failure (contact breakage) can cause the inadvertent closure of all three ac power phase contacts within a hybrid relay. Internal debris jamming contacts in the closed position within a hybrid relay can result in all normally open contacts remaining closed, but prelaunch checkout should catch this anomaly, and Orbiter telemetry can verify that this condition does not exist before application of ac power to the contacts.

The only single point failure within the relay which can cause all contacts to prematurely fail closed is the hybrid circuit of the relay. However, this failure requires dc logic power to be present at the hybrid. The PRLA system procedures do not apply logic power to the relay until it is ready to be used.

Note 11-4. Due to the fact that both dc power hot and return wires are switched by the Payload Select switch, the PRLA system can be considered two-fault tolerant against inadvertent release of a latch in another Payload Select position.

Note 11-5. Inadvertent release of a latch not intended to be activated could occur if that associated latch/release toggle switch failed on and the ac power was applied. The system is zero fault tolerant to this condition if the A6A1 panel is powered, ac power is applied, and the latch is on the same position as the setting of the payload select switch (S37). The system is two fault tolerant to this condition if the A6A1 panel is powered, ac power is applied, and the latch is on a different position than the setting of the payload select switch (S37). Orbiter telemetry shall be used to verify the latch/release toggle switch has not failed-on prior to the application of ac power.

Note 11-6. For all on-orbit operations, the PRLA system is considered equivalent to one fault tolerant under the following conditions:

a. At least one fault tolerance as defined in NSTS 1700.7B is maintained on the payload side of the interface.

b. The third control, if required to complete the provisioning of two fault tolerant hazard control, must be provided via hardware, unless a contingency EVA is planned for this function.

c. All circuits used in this application, including redundancy, must be verified preflight.

d. Payload circuit design must provide for two electrical inputs, either of which will complete the must-work function.

For certain on-orbit operations, the avionics portion (not latches) of the PRLA system may be used as a system wherein two fault tolerant is required under the following specific conditions:

a. At least two fault tolerance as defined in NSTS 1700.7B is maintained on the payload side of the interface (refer to figure 5-11a for Orbiter side implementation);

b. Payload must verify the end-to-end performance of all paths of electrical and mechanical functions in flight immediately prior to exposure to a potentially hazardous condition;

c. Complete failure of Orbiter redundant services does not result in a hazard if failures occur prior to payload attempted use;

d. The time exposure to a potentially hazardous condition can be limited to 10 minutes nominally;

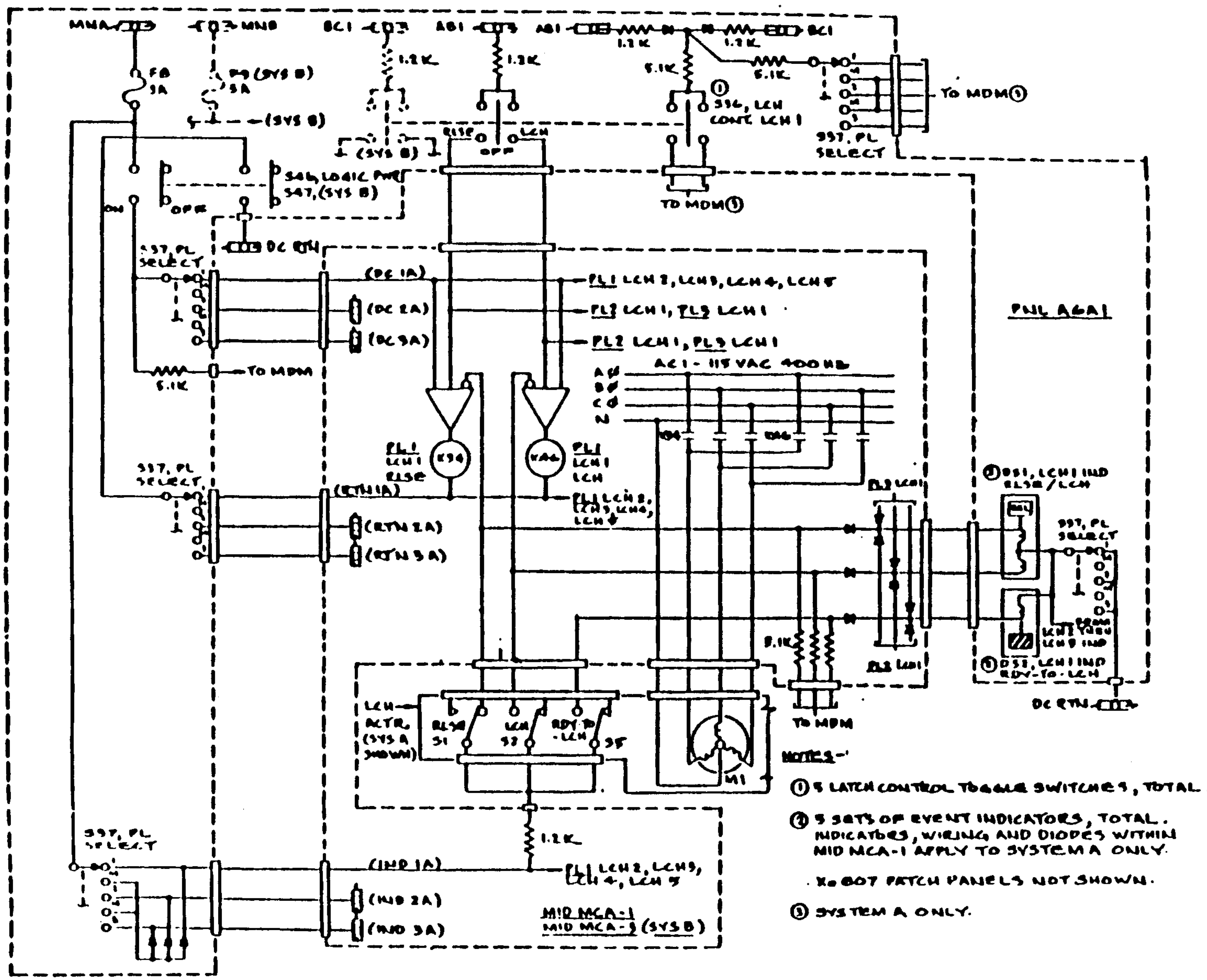


Figure 5-11. - Payload retention (System A).

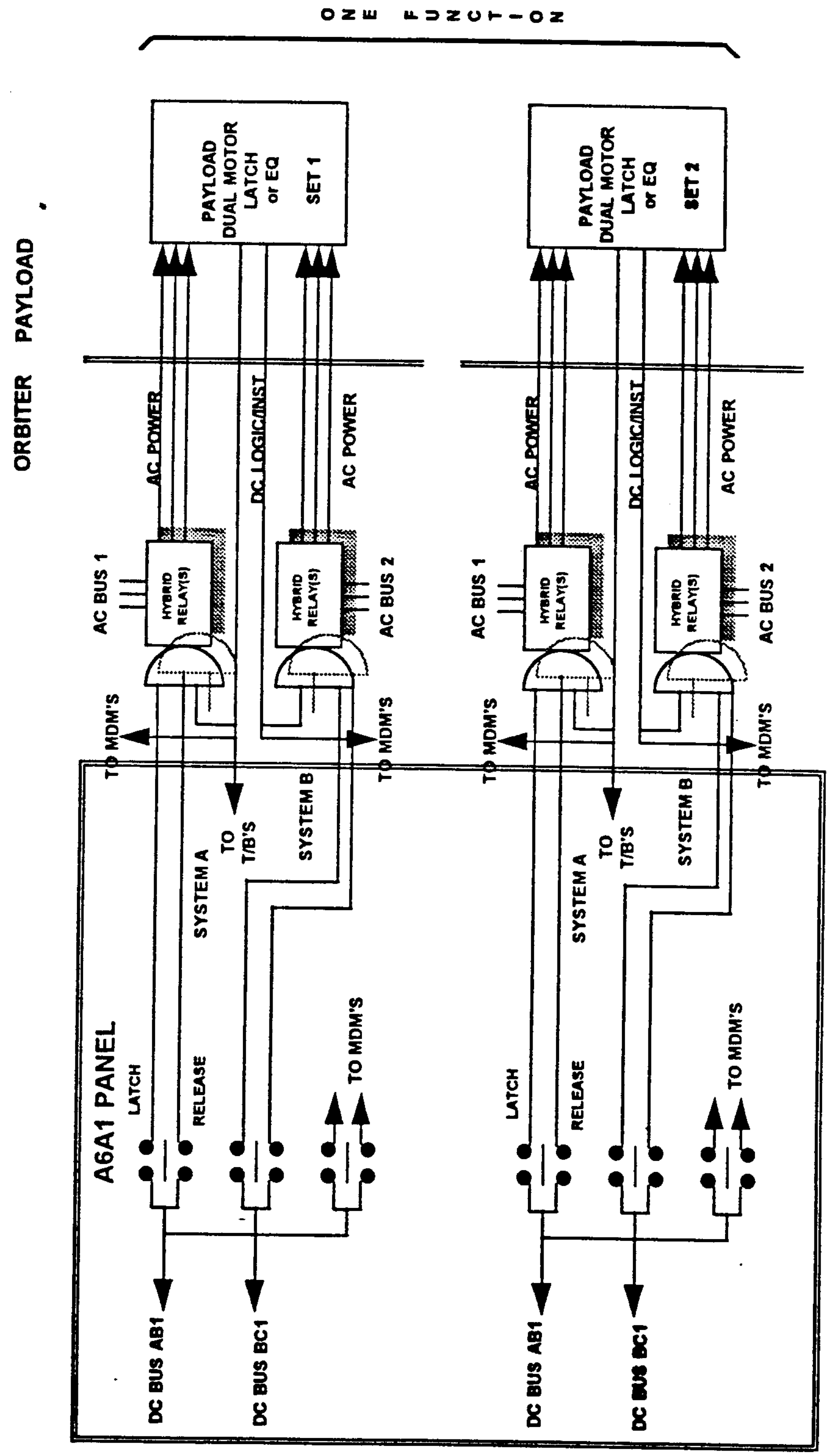


Figure 5-11a.- Payload retention system avionics interfaces for two fault tolerant equivalence.

Table 5-12.- AVIONICS SERVICES: CLOSED CIRCUIT TELEVISION (CCTV)
(Figure 5-12)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
No video transmission at monitors 1 & 2 down-link data and on-board re-corded data for payloads via payload interfaces connector P1402	No output	Video switch-ing unit	Zero	Zero	Loss of all P/L TV (TV1, TV2, & TV3 signals).
Orbiter TV signal not available at payload via payload in-terfaces con-nector P1402		Video switch unit			Loss of Or-biter TV.
Inability to address or operate ca-bin, keel, port RMS or middeck cam-eras (DLR, Camma, PAN, TILT IRIS, FOCUS, and Zoom func-tions inoper-able) via PSDP J55 and payload in-terface con-nector P1402		Remote control unit			Correct Sync Line command address and function codes are required for remote cam-era opera-tion. Loss of sync con-trol.

Table 5-12.- AVIONICS SERVICES: CLOSED CIRCUIT TELEVISION (CCTV)
(Continued) (Figure 5-12)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss or re-corded/play-back data		VCR			

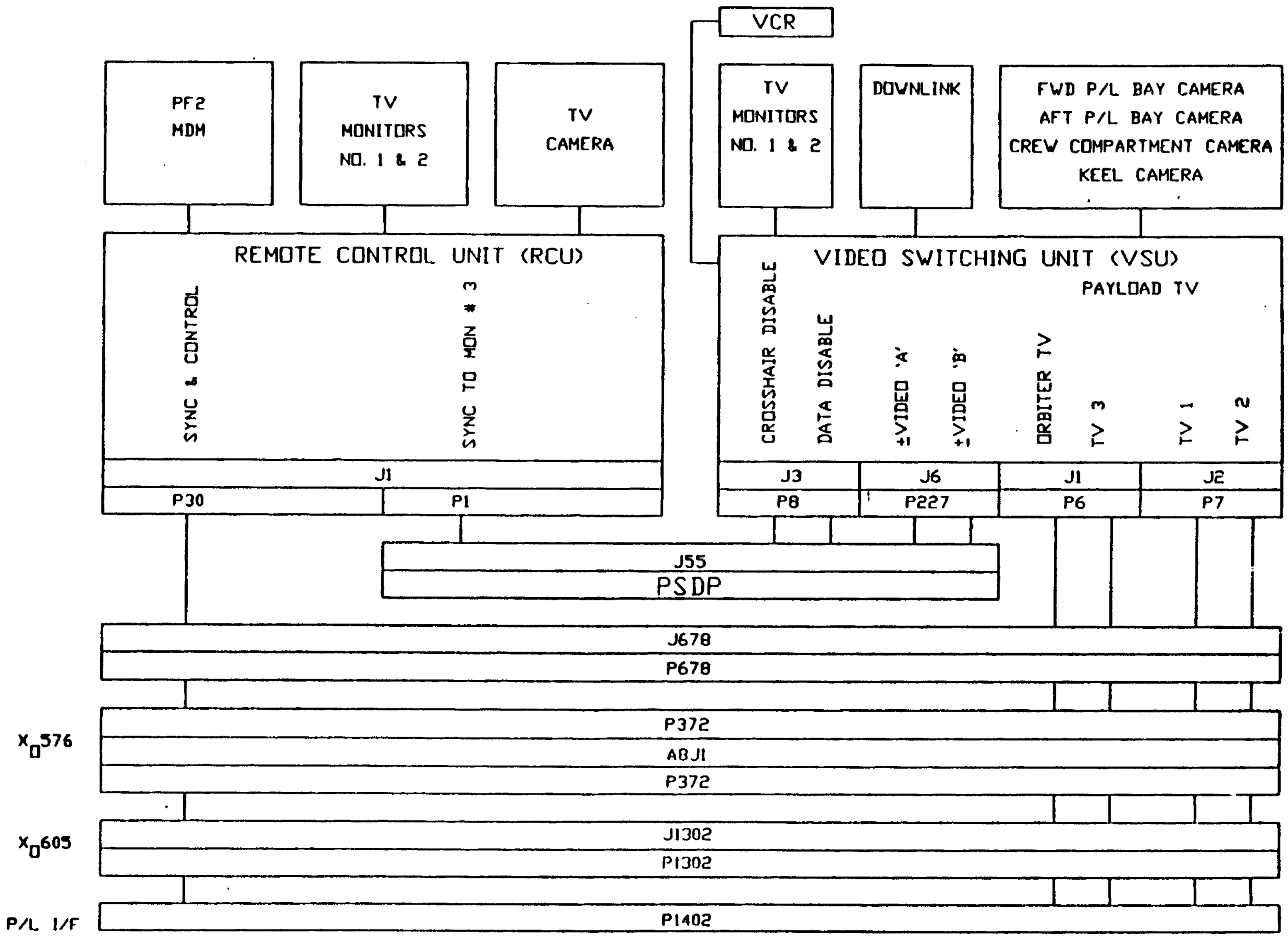


Figure 5-12.- Closed Circuit Television (CCTV).

Table 5-13.- AVIONICS SERVICES: GMT AND MET TIMING
(Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of GMT/ at all 1/4-SMCH services in sections 1-4 at pay-load inter-face connect-ors (J1401, J1403, J1405, and J1407)	No output	MTU	Zero	Zero	Failure mode due to fail-ures inter-nal to MTU. MTU internal redundancy consists of dual oscil-lators and a single power supply unit. Fail-ure of chip or common power supply would remove both strings and pose a single point failure mode.
		PTB			Failure mode due to sin-gle MTU sig-nal input into PTB and a single PTB power sup-ply.

Table 5-13.- AVIONICS SERVICES: GMT AND MET TIMING (Continued)
(Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Inaccurate timing references at payload interface connectors	Erroneous output	MTU	Zero	Zero	Failure mode due to 2 failures internal to MTU. MTU internal redundancy consists of dual oscillators and a single power supply unit. Each payload interface connector provides 2 GMT and 1 MET. Timing is provided at all 4 payload connectors by SMCH.
Loss of GMT/ MET to payload interface connectors	No output	MTU signal voltage regulation	Zero	Zero	Failure mode due to 2 failures internal to MTU. MTU internal redundancy consists of dual oscillators and a single power supply unit.

Table 5-13.- AVIONICS SERVICES: GMT AND MET TIMING (Continued)
(Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of GMT outputs to one section of 1/4-SMCH services (payload interface connectors P1401, P1403, P1405 and P1407)		Single PTB GMT or MET output line driver			PTB I/O isolation permits failure of one I/O function without adverse effect on another. Each section of SMCH provides 2 GMT.
Loss of the MET output to one section of the 1/4-SMCH services (payload interface connectors P1401, P1403, P1405 and P1407)					PTB I/O isolation permits failure of one I/O function without adverse effect on another. Only 1 MET provided each SMCH section. MET 2

Table 5-13.- AVIONICS SERVICES: GMT AND MET TIMING (Concluded)
(Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
					SMCH selec-tions: 1 (P1401): GMT 1 & 2 MET 1 2 (P1403): GMT 3 & 4 MET 2 3 (P1405): GMT 5 & 6 MET 3 4 (P1407): GMT 7 & 8 MET 4

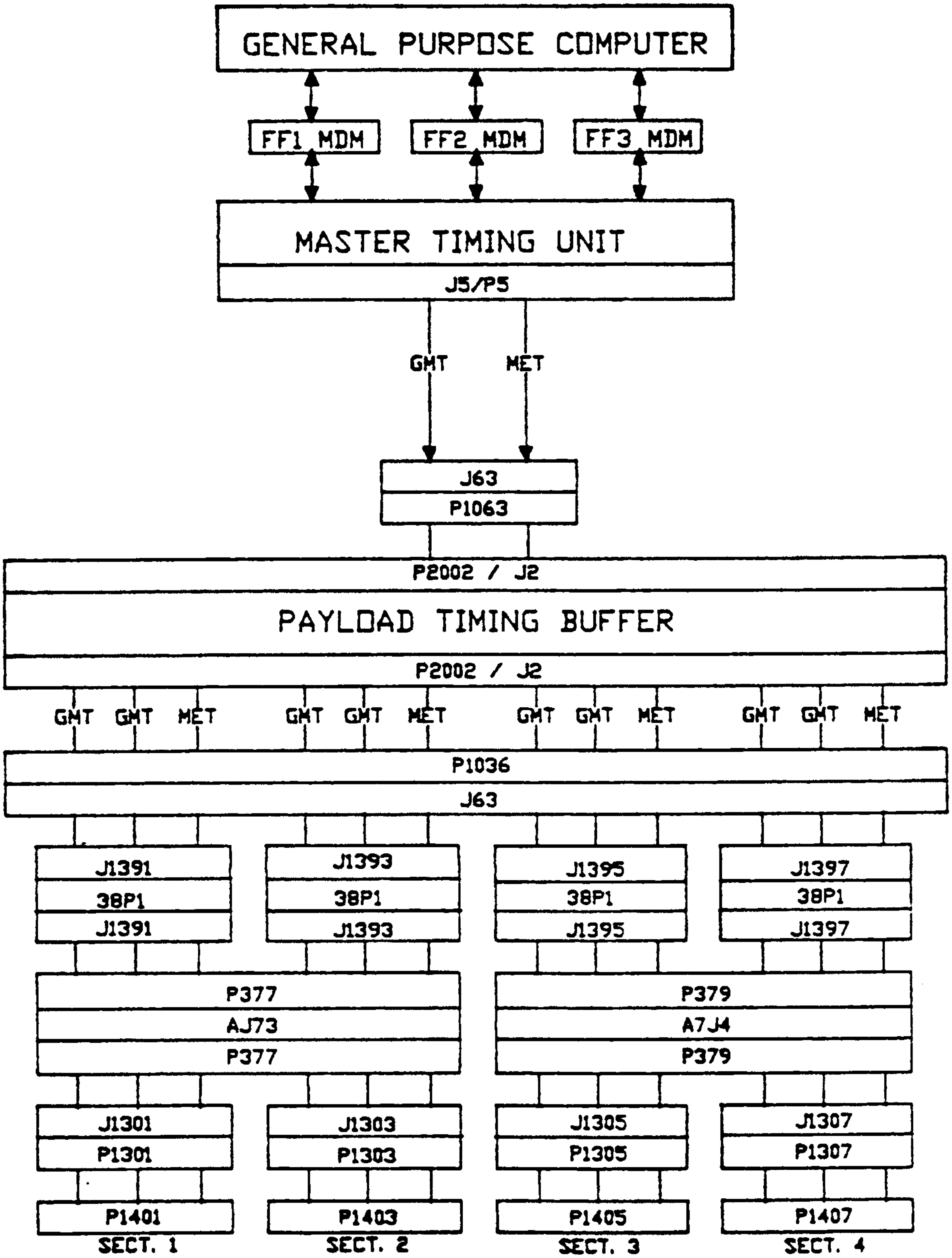


Figure 5-13.- Timing signals GMT and MET.

Table 5-14.- AVIONICS SERVICES: MTU REFERENCE FREQUENCIES
(Figure 5-14)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of all MTU reference frequencies at MSDP connectors J708 and J19	No output	MTU	Zero	Zero	Failure mode due to internal failure of MTU. MTU internal redundancy consists of dual oscillators and a single power supply. Failure of chip or common power supply would remove both strings and pose a single point failure mode.

Table 5-14.- AVIONICS SERVICES: MTU REFERENCE FREQUENCIES (Concluded)
(Figure 5-14)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
					MTU reference frequencies consist of 4.608 MHz, 100 Hz, 1 KHz, 1.024 KHz, and 10 Hz square waves. These non-standard services are available at MSDP. Coax cable required for 4.608 MHz square wave.

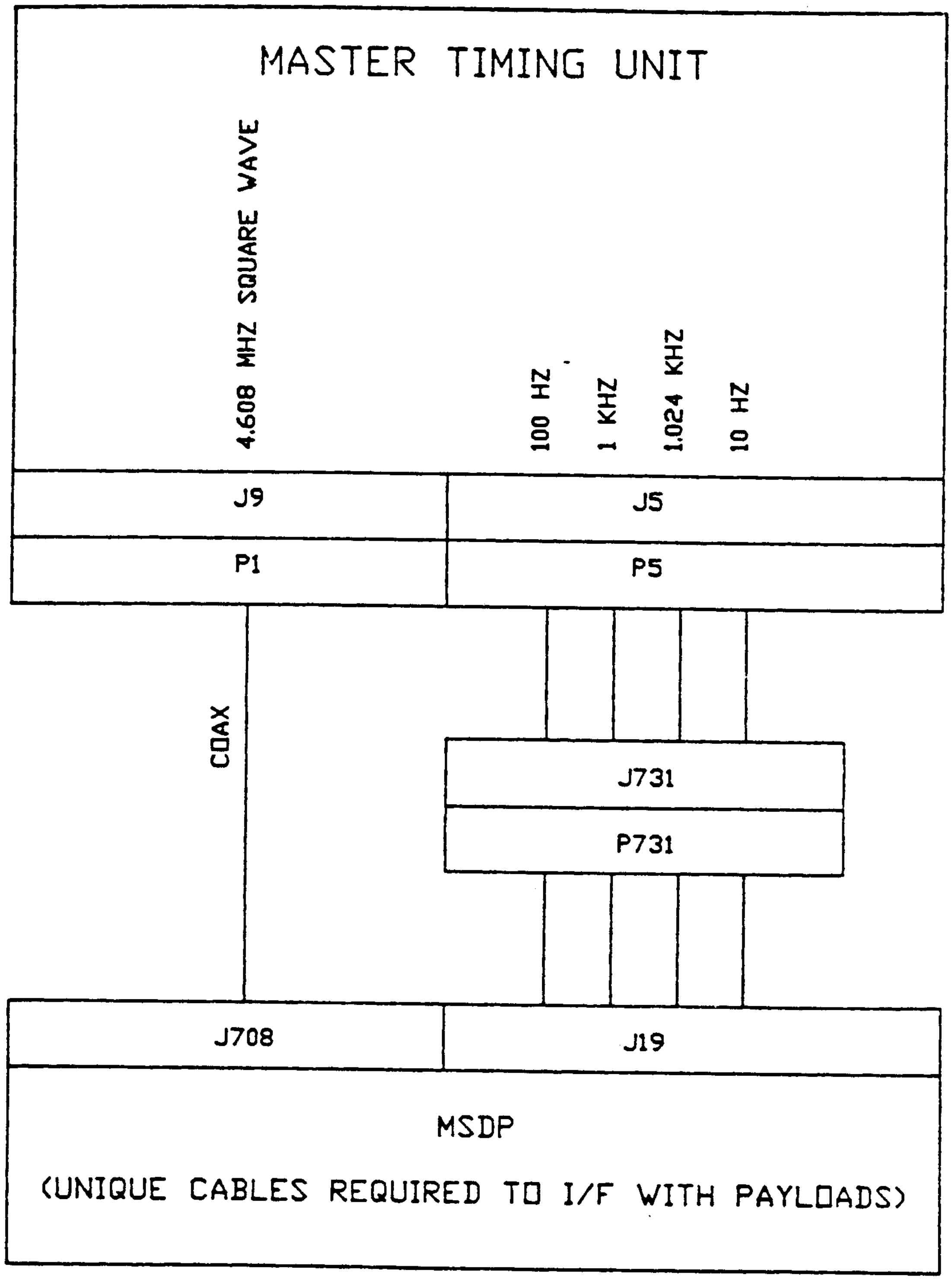


Figure 5-14.- MTU reference frequencies.

Table 5-15.- AVIONICS SERVICES: DISCRETE OUTPUT HIGH (DOH) COMMANDS
(Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of DOH commands to all 1/4-SMCH services in section 1-4 (payload interface connectors P1415, P1413, P1411, P1409 and P1437)	No output	PF1 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power supply must occur. Failure of GPC loaded with SM/PL software will require crew reassignment of another GPC to SM/PL software.
Total loss of DOH commands to payload interface connector P1408		PF2 MDM (other than IOM card)			
Loss of DOH commands at section 1 (P1415) and P1437		PF1 MDM IOM no. 14 channel 02	Zero	Zero	Redundancy is provided by internal redundancy of MDM operation but not on the IOM level; single point failure.
Loss of DOH commands at section 2-4 (P1413, P1411 P1409) and P1437		PF1 MDM IOM no. 2 channel 02			

Table 5-15.- AVIONICS SERVICES: DISCRETE OUTPUT HIGH (DOH) COMMANDS (Continued) (Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
					The standard DOH services are provided by SMCH from PF1 to the SMCH-SIP payload interface connectors P1415, P1413, P1411, and P1490. Non-standard DOH services are provided from PF1 to P1437 and from PF2 to P1408.
Loss of DOH commands at P1408	No output	PF2 MDM IOM no. 14 channel 02 PF2 MDM IOM no. 2 channel 02	Zero	Zero	Redundancy is provided by internal redundancy of MDM operation but not on the IOM level; single point failure.

Table 5-15.- AVIONICS SERVICES: DISCRETE OUTPUT HIGH (DOH) COMMANDS (Concluded) (Figure 5-13)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Inadvertent DOH commands initiated at payload interface connectors	Erroneous output	PF MDM (other than IOM card)	One	One	Multiple subcomponent failures internal to the MDM would be required to produce the failure condition.
Signal voltage to 28 V and current levels to 400 mA to payload interface connectors	Erratic output	PF MDM (other than IOM card)			Multiple subcomponent failures internal to MDM would be required to produce the failure condition. PF1 and PF2 are dedicated to the same GPC. Crew can reassign a GPC to provide SM functions to payloads and to control PF1 and PF2 MDM's.

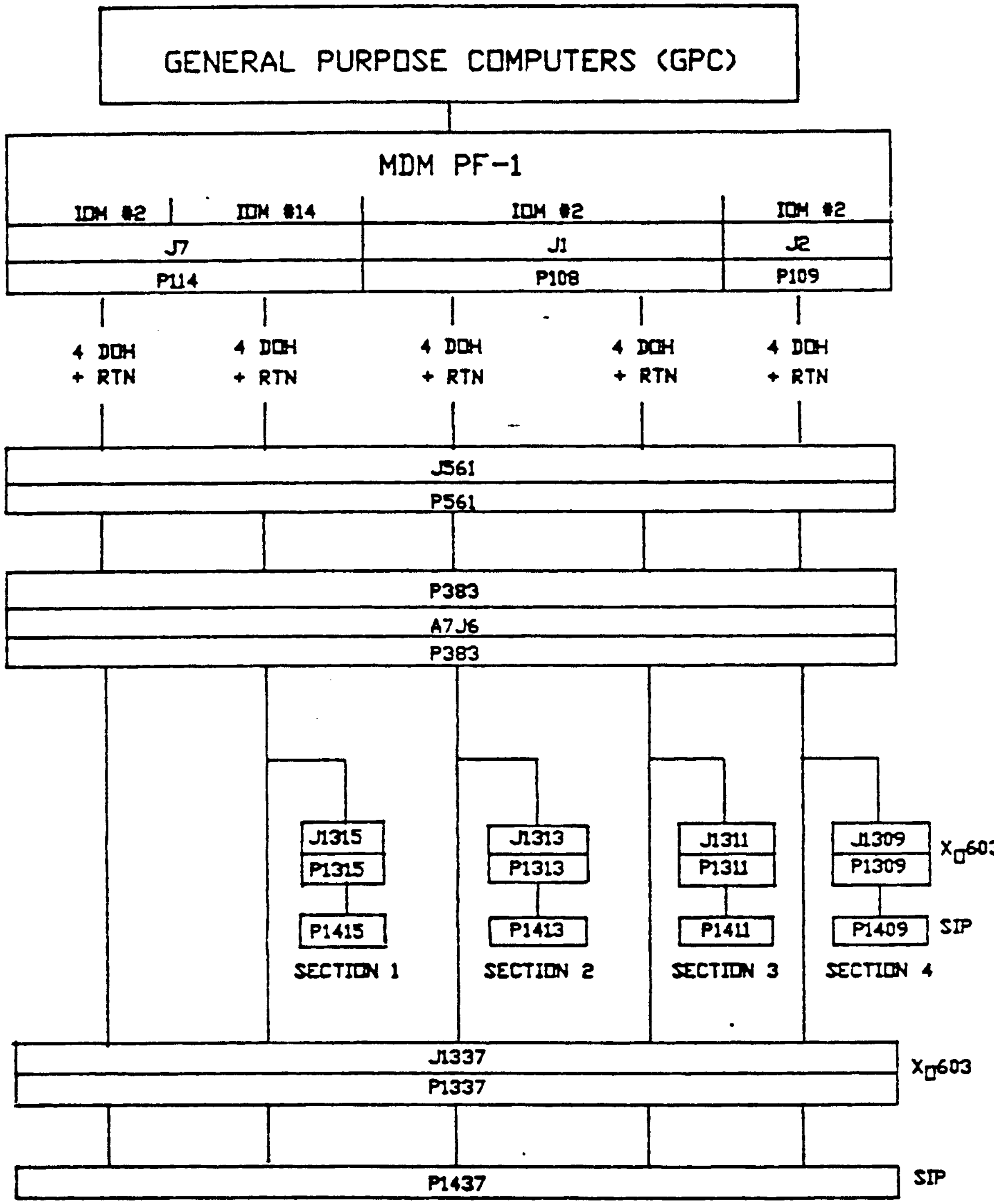


Figure 5-15a.- MDM PF1 DOH.

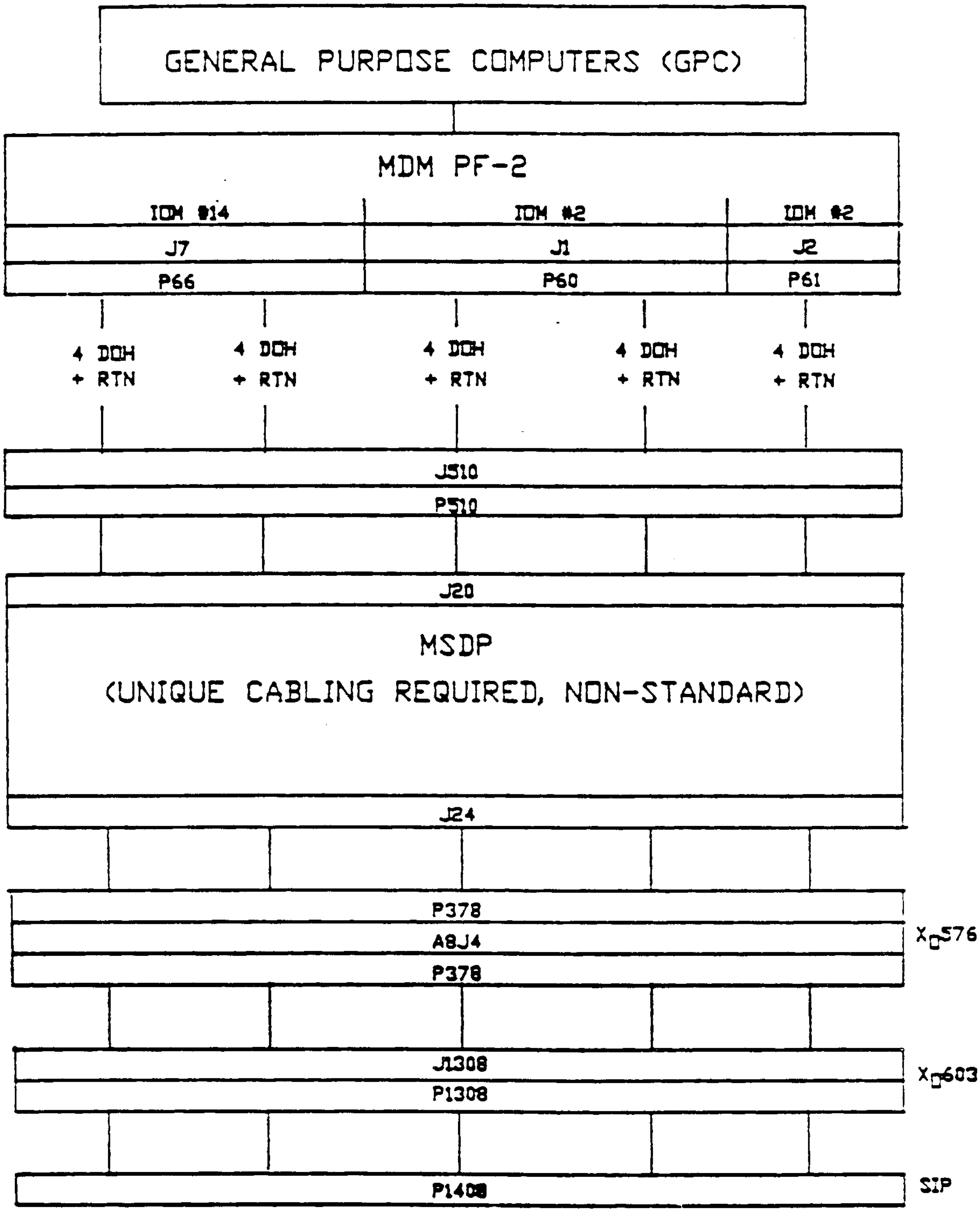


Figure 5-15b.- MDM PF2 DOH.

Table 5-16.- AVIONICS SERVICES: DISCRETE OUTPUT LOW (DOL) COMMANDS
(Figure 5-16)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of DOL commands to all 1/4-SMCH services in section 1-4 (payload interface connectors P1431, P1429, P1427, P1425)	No output	PF1 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power must occur. Failure of GPC loaded with SM/PL software will require crew reassignment of another GPC to SM/PL software PF2 to P1420.
Total loss of DOL commands to MSDP connectors J10 and J30		PF2 MDM (other than IOM card)			
Loss of DOL commands at section 1 (P1431)		PF1 MDM IOM no. 10 channel 02	Zero	Zero	Redundancy is provided by internal redundancy of MDM operation but not the IOM level; single point failure.
Loss of DOL commands at section 2-4 (P1429, P1427, and P1425)		PF1 MDM IOM no. 00			

Table 5-16.- AVIONICS SERVICES: DISCRETE OUTPUT LOW (DOL) COMMANDS (Continued) (Figure 5-16)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of DOL commands at sections 2 & 3 (P1429 and P1427)		PF1 MDM IOM no. 00 channel 02			The standard DOH services are provided by SMCH from PF1 to the SMCH-SIP payload interface connectors P1431, P1429, P1427, and P1426. Non-standard DOL services are provided PF2 to P1420. PF1 and PF2 are dedicated to the GPC. Crew can reassign a GPC to provide SM functions to payloads and to control PF1 and PF2 MDM's.
Loss of DOL commands at section 4 (P1425)		PF1 MDM IOM no. 00 channel 01			

Table 5-16.- AVIONICS SERVICES: DISCRETE OUTPUT LOW (DOL) COMMANDS (Concluded) (Figure 5-16)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of DOL commands MSDP connectors J10 and J30	No output	PF2 MDM IOM no. 00 channel 01-02	Zero	Zero	Redundancy is provided by internal redundancy of MDM operation but not on the IOM level; single point failure.
		PF2 MDM IOM no. 10 channel 02			
Inadvertent DOL commands initiated at payload interface connectors	Erroneous output	PF MDM (other than IOM card)	One	One	Multiple subcomponent failures internal to the MDM would be required to produce the failure condition.
Signal voltage to 28 V and current levels to 400 mA to payload interface connectors	Erratic output	PF MDM output signal voltage regulation			

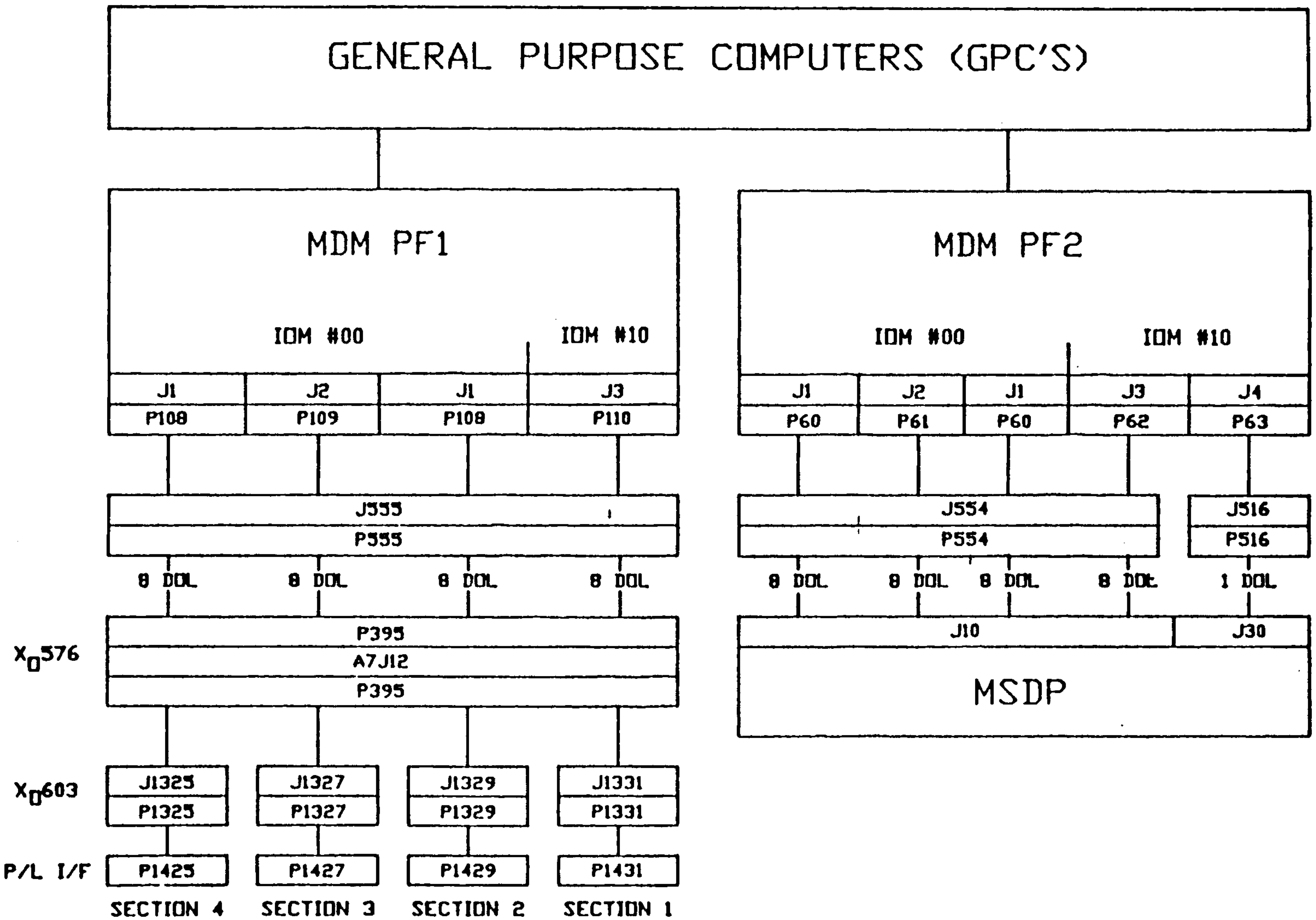


Figure 5-16.- PF1/PF2 DOL.

Table 5-17.- AVIONICS SERVICES: DATA BUS (PL1/PL2)
(Figure 5-17)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Bus data degraded or or lost to either payload interface connector (P1486 and P1487)	Open	DBC	Zero	Zero	Due to a single configuration
	Short				
	Open			One	Due to a dual port configuration
	Short				

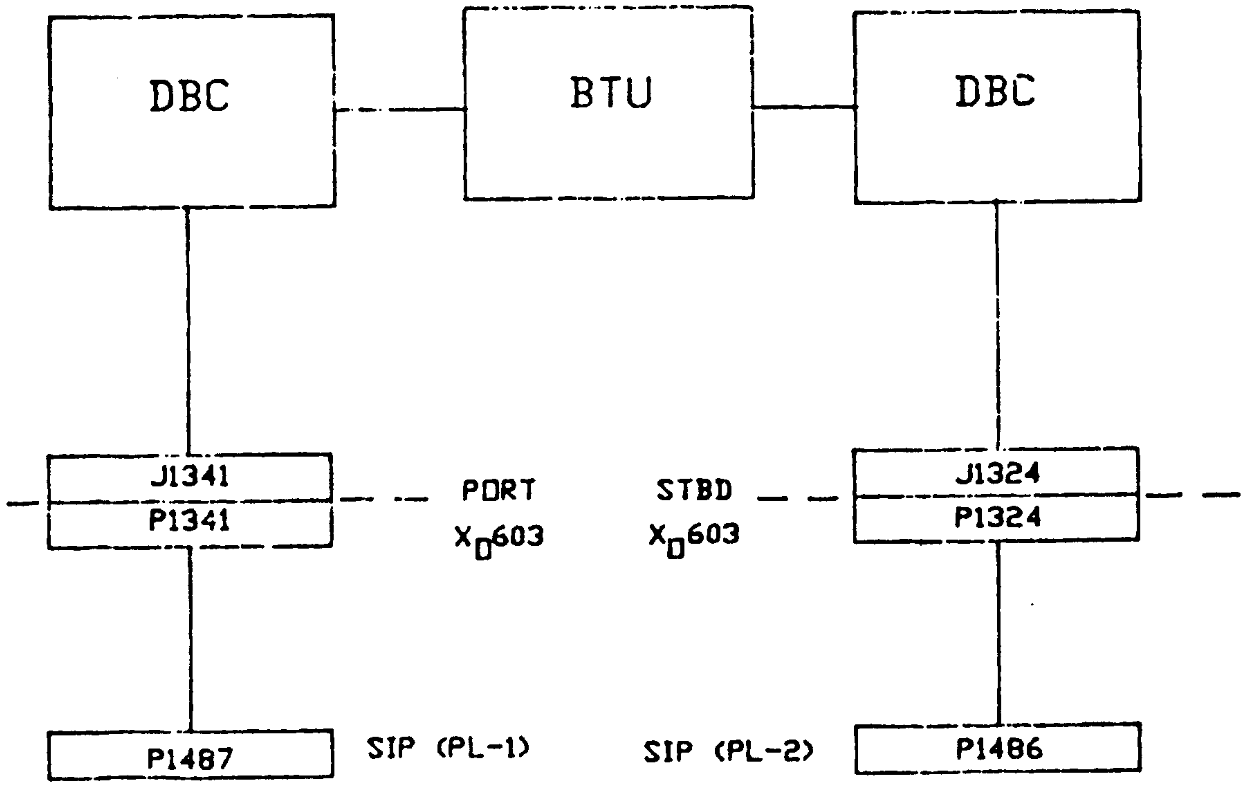


Figure 5-17.- Data bus interface (PL1/PL2).

Table 5-18.- AVIONICS SERVICES: PAYLOAD SIGNAL PROCESSOR (PSP)
(Figure 5-18)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of telemetry and command data to a detached payload via PSP/PI interface	No output	Payload Interrogator	One	One	Both payload Interrogators 1 & 2 must fail for total loss of cmd/ tlm.
		Payload signal processor			Both payload signal processors 1 & 2 must fail for total loss of cmd/ tlm.
Loss of command data to attached payloads in all 1/4-SMCH sections (payload interface connectors P1401, P1403, P1405, P1407)					Both PSP no. 1 & 2 must fail to lose all command paths to attached payloads. The standard PSP command services are provided by SMCH from PSP no. 1 and no. 2 to the SMCH-SIP payload interface connectors P1401,
Loss of 16 KHz subcarrier to attached and detached payloads					

Table 5-18.- AVIONICS SERVICES: PAYLOAD SIGNAL PROCESSOR (PSP) (Continued) (Figure 5-18)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
					P1403, P1405, and P1407. The optional service extra command channel is available at PSDP connectors J35 J19.
Loss of GPC commands to attached payloads in all 1/4-SMCH sections via PF1 MDM and PSP no. 1 (payload interface connectors P1401, P1403, P1405, P1407)	No output	PF1 MDM IOM no. 8 channel 01	One	One	Both command paths PF1/ PSP no. 1 and PF2/PSP no. 2 must fail to lose all commands to all 1/4-SMCH sections.
Loss of GPC commands to attached payloads in all 1/4-SMCH sections via PF2 MDM and PSP no. 2 (payload interface connectors P1401, P1403, P1405, P1407)		PF2 MDM IOM no. 8 channel 01			

Table 5-18.- AVIONICS SERVICES: PAYLOAD SIGNAL PROCESSOR (PSP) (Concluded) (Figure 5-18)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of telemetry from all 1/4-SMCH sections detached payloads via PSP no. 1 & no. 2 ground downlink		PDI	Zero	Zero	PDI loss is a single point failure in the telemetry processing.

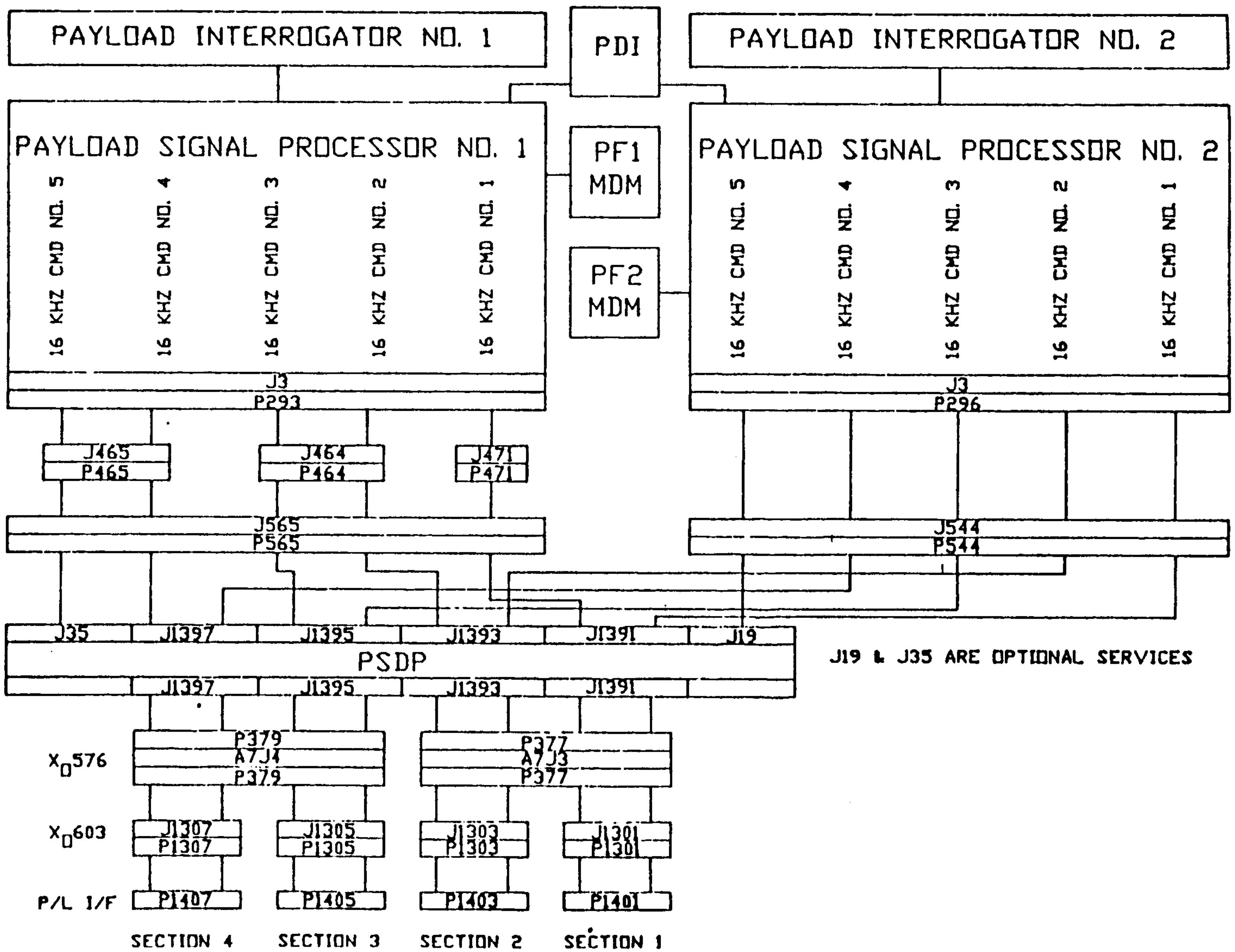


Figure 5-18.- Payload Signal Processor (PSP).

Table 5-19.- AVIONICS SERVICES: S-BAND PAYLOAD INTERROGATORS
(Figure 5-19)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of S-band RF command and data links from Orbiter to payload	Inoperative	S-band antenna	One	One	Antenna is polarized on both sides. Loss of either LHCP will force use of the opposite polariza- tion, how- ever, with degradation dependent on the unique payload.
	No output	S-band RF switch Payload Interrogator (LHCP or RHCP mode)			
		Payload Inter- rogator			Each inter- rogator is unique to 1 side of an- tenna and RF switch string. Antenna is contained in one assembly and polar- ized on left and right sides.

Table 5-19.- AVIONICS SERVICES: S-BAND PAYLOAD INTERROGATORS (Continued) (Figure 5-19)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
					RF switch Payload Interrogator Pos 1: PI no. 1 LHCP PI no. 2 RHCP Pos 2: PI no. 1 RHCP PI no. 2 LHCP
Loss of command and data to J35 and associated P/L unique ASE in the AFD	No output/ input	Payload Interrogator no. 1	One	One	Each Payload Interrogator is unique to 1 side of antenna and RF switch string.
Loss of command and data to J19 and associated P/L unique ASE in the AFD		Payload Interrogator no. 2			
Loss of detached payload telemetry via PI 1/ PSP 1 (PI 2/ PSP 2)		PI 1 to PSP 1			Alternate PI/PSP available.

Table 5-19.- AVIONICS SERVICES: S-BAND PAYLOAD INTERROGATORS (Concluded) (Figure 5-19)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of detached payload command via PSP 1/ PI 1 (PSP 2/ PI 2)		PI 1 from PSP 1 (2)			
Loss of detached payload teleme- via PI/Ku-band bent pipe		PI 1 to KUSP	Zero	Zero	Alternate PI available.

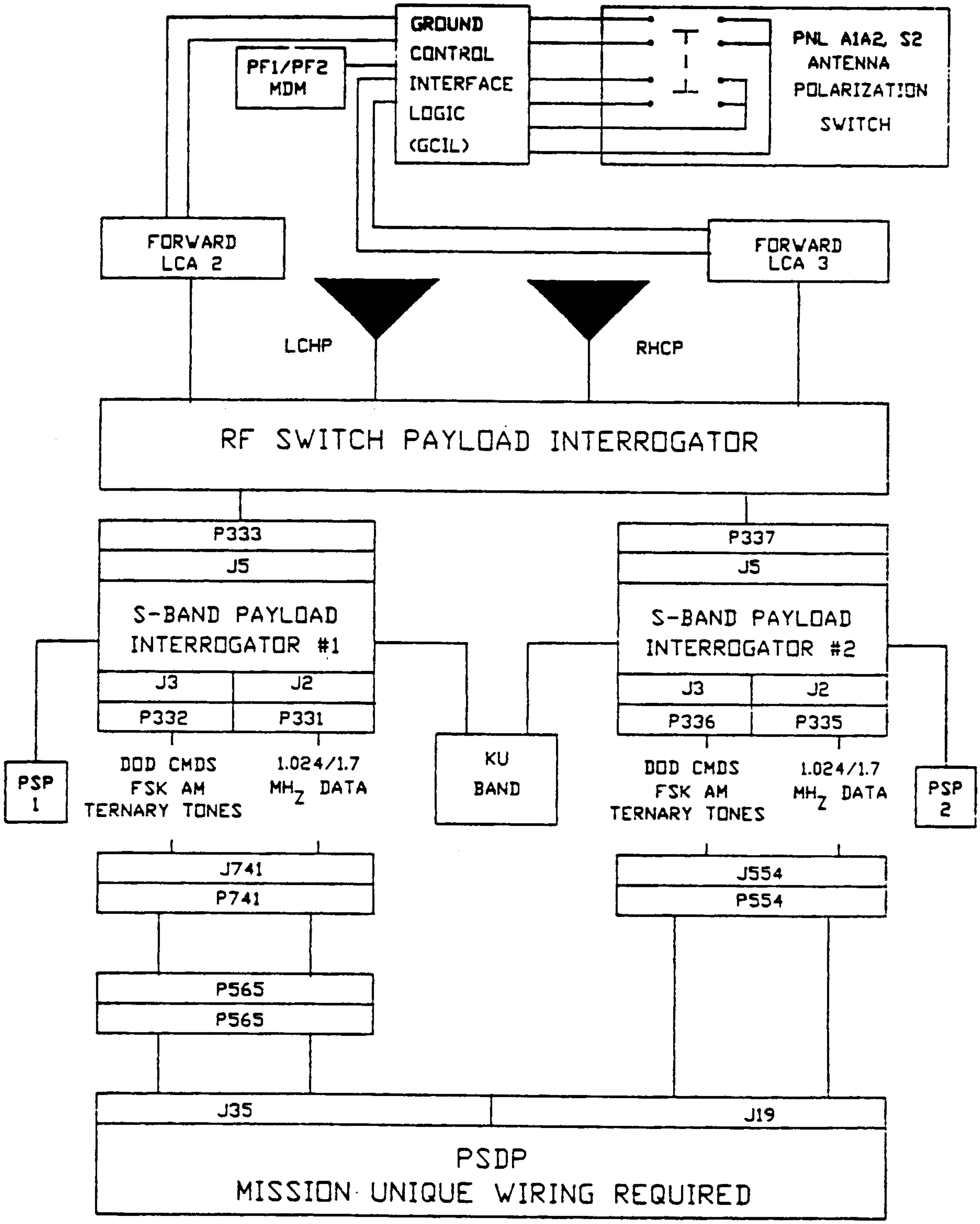


Figure 5-19.- Payload Interrogator (PI).

Table 5-20.- AVIONICS SERVICES: SERIAL I/O (S10) COMMANDS
(Figure 5-20)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of MDM SIO services to payloads via J35 of PSDP	No output	PF1 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power supply must occur.
		PF1 MDM IOM no. 15 channels 00-01	Zero	Zero	Redundancy is provided by 2 MDM's and internal redundancy of MDM operation but not on the IOM level; single point failure.
Total loss of MDM SIO to payloads via J40 to MSDP		PF2 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power supplies must occur. PF1 and PF2 are dedicated to the same GPC. Failure of GPC loaded with SM software will require

Table 5-20.- AVIONICS SERVICES: SERIAL I/O (S10) COMMANDS (Continued)
(Figure 5-20)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
					crew reassignment of another GPC with SM/PL software. MDM SIO services are nonstandard.
		PF2 MDM IOM no. 15 channels 00-01	Zero	Zero	Redundancy is provided by 2 MDM's and internal MDM operation but not on IOM level; single point failure.
Inadvertent SIO commands initiated at payload interface connectors	Erroneous output	PF MDM (other than IOM card)	One	One	Multiple subcomponents must experience simultaneous power transients.

Table 5-20.- AVIONICS SERVICES: SERIAL I/O (S10) COMMANDS (Concluded)
(Figure 5-20)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Signal voltages to 28 V and current levels to 500 mA at payload interface connectors	Erratic output	PF MDM output signal voltage regulation			Multiple subcomponent failures internal to the MDM would be required to produce the failure condition.

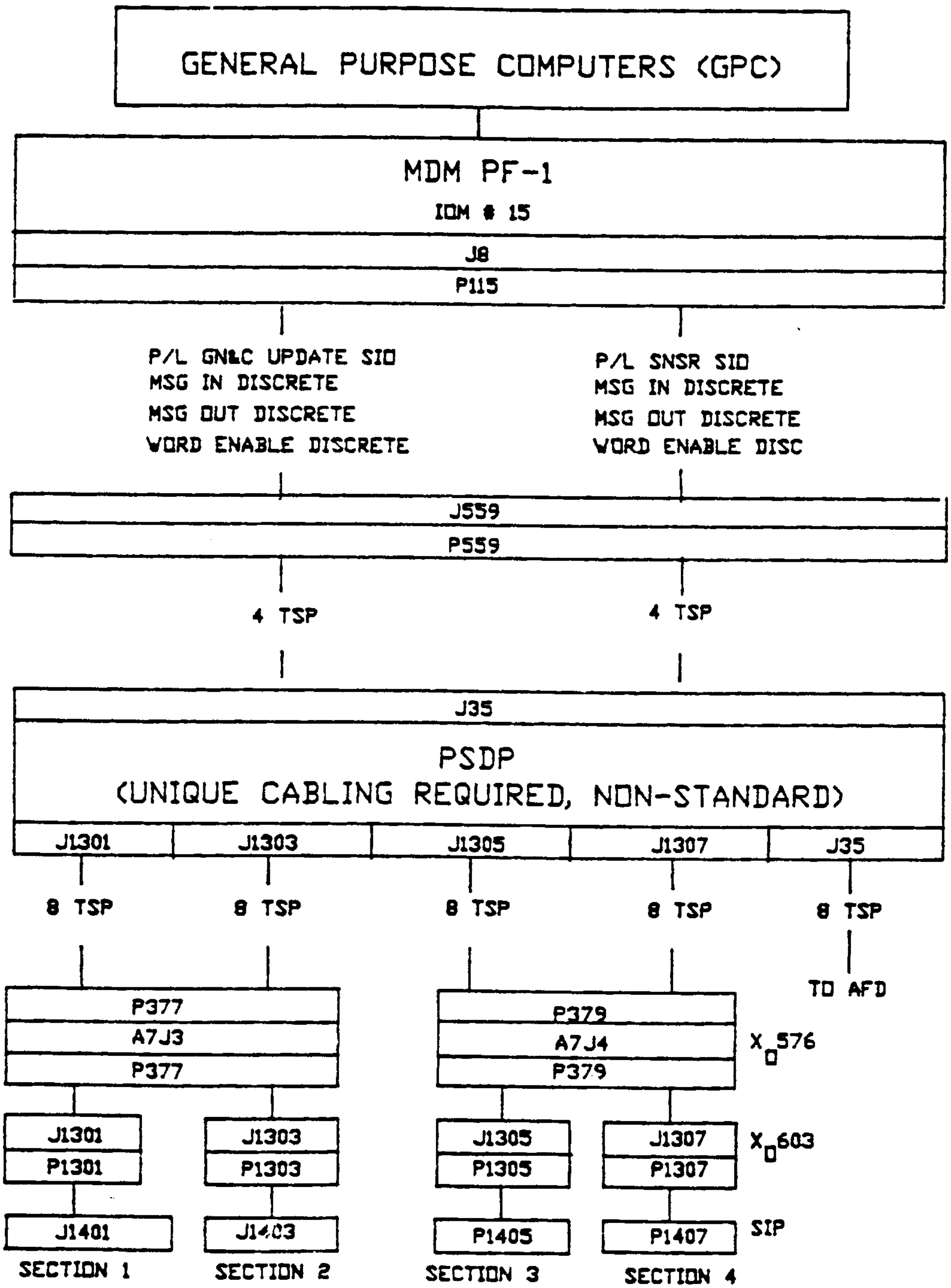


Figure 5-20a.- MDM PF1 SIO.

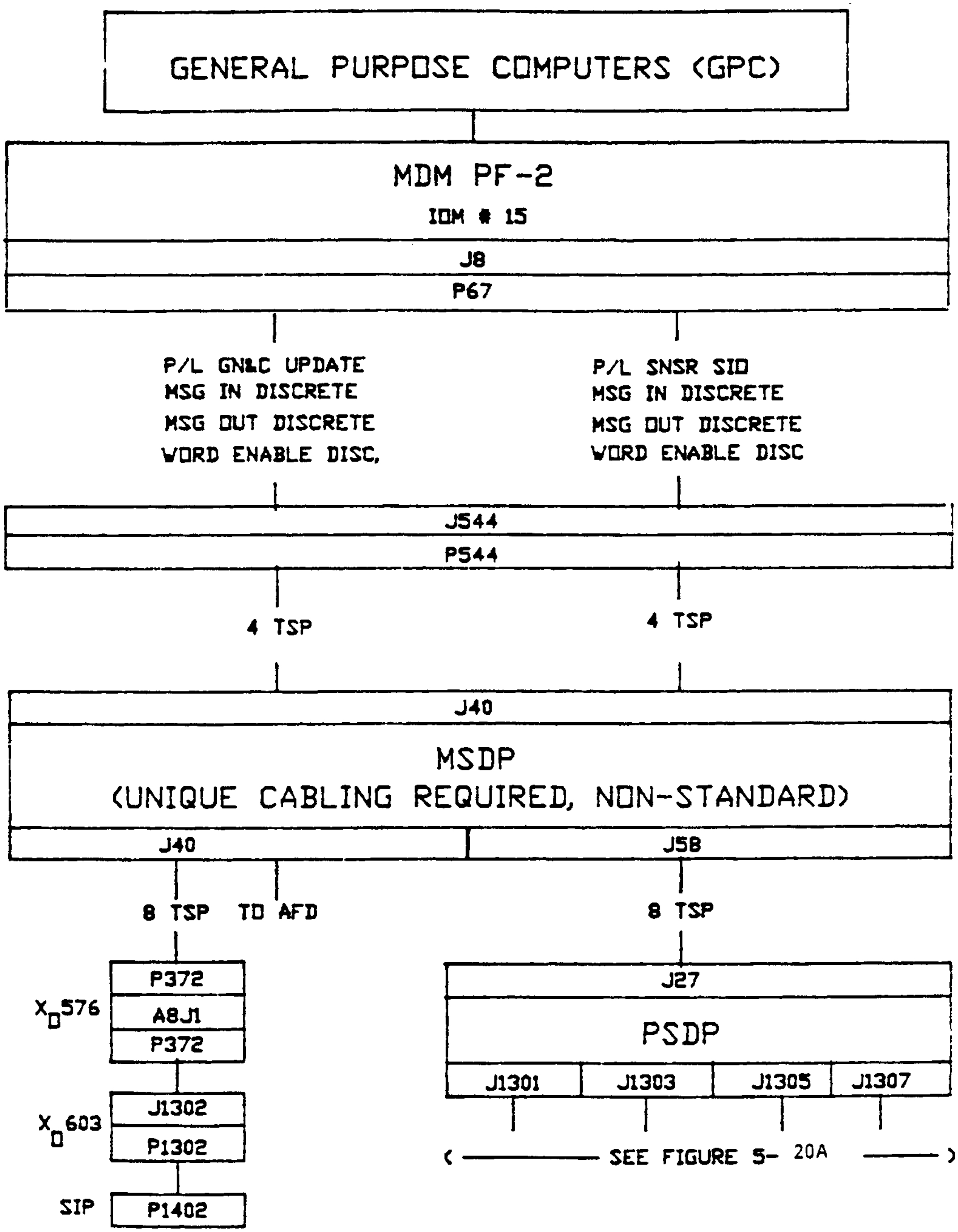


Figure 5-20b.- MDM PF2 SIO.

Table 5-21.- AVIONICS SERVICES: KU-BAND SYSTEM
(Figure 5-21)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of command and data communications with payload(s) via the Ku-band system payload interface connectors at the PSDP J724, J723, and J23	No output/ input	Deployed Assembly A (DA-A)	One	One	Multiple component failures required to produce the failure mode.
		Electronics Assembly 1A (EA-1A)			
		Signal Processor Assembly (SPA)			
Loss of mode 1, channel 2 forward link 128 kbps data and clock to PSDP J23		Forward link processing equipment in SPA	Zero	Zero	
Loss of mode 1, channel 2 return link high data rate payload digital data (16 to 1.02 kbps for BIO-L, M, S) at PSDP J23		Return link processing equipment in SPA			

Table 5-21.- AVIONICS SERVICES: KU-BAND SYSTEM (Continued)
(Figure 5-21)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of mode 1, channel 3 return link high data rate payload maximum digital data and clock (2-48 mbps NRZ-L, K, S for data and square wave for clock) at PSDP J724 (data) and J723 (clock)					Ku-band services are nonstandard services that require unique cable harness wiring to the appropriate connectors at the PSDP and to the particular cargo section (1-4).
Loss of mode 2, channel 3 return link high data rate analog or video (dc to 4.5 MHz) and digital (16 kbps to 4 mbps) data at PSDP J23	No output/ input	Return link processing equipment in SPA	Zero	Zero	

Table 5-21.- AVIONICS SERVICES: KU-BAND SYSTEM (Concluded)
(Figure 5-21)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of payload video input (CCTV) via Ku-band signal processor		Video switching network			
		Return link processing equipment in SPA			
Loss of payload data processing via the bent pipe mode					

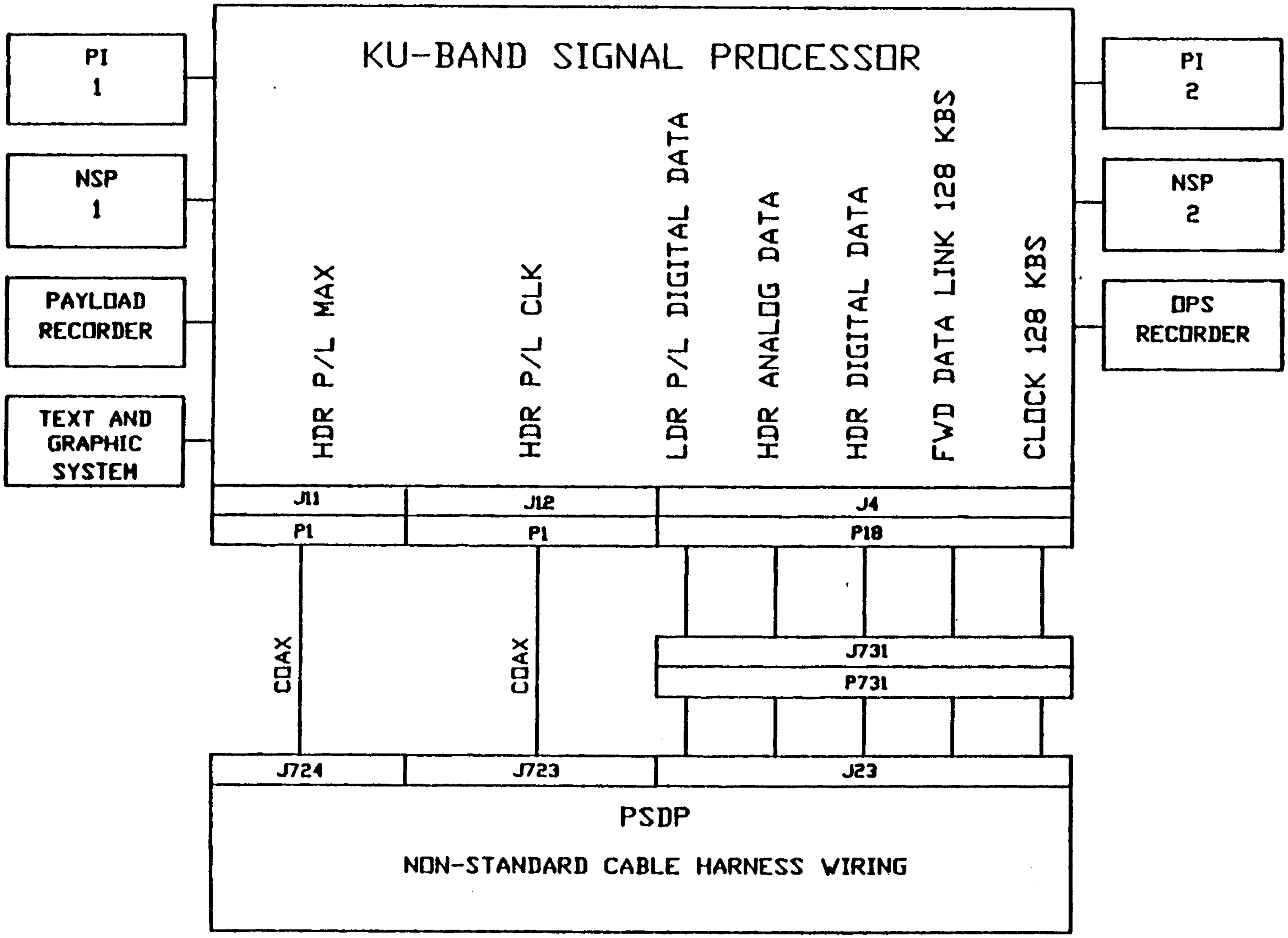


Figure 5-21.- Ku-band signal processor.

Table 5-22.- AVIONICS SERVICES: AUDIO CENTRAL CONTROL NETWORK (ACCN)
(Figure 5-22)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of duplex voice communications, paging, and warning to attached manned payloads via payload interface connector P1421	No output/ input	Audio Central Control Unit (ACCU)	Zero	Zero	Six 2-way (talk/listen) duplex analog audio channels are provided to attached manned payloads Air-to-Ground 1 (AG1) Air-to-Ground 2 (AG2) Intercom A (IC/A) Intercom B (IC/B) Air-to-Air (AA) Page.
Loss of intercom A and/or B to attached manned payloads via payload interface connector P1421		ICOM A and/or ICOM B audio circuits in ACCU	One	One	
Loss of Air-to-Ground 1 and/or 2 communications to attached manned payload via payload interface connector P1421		AG1 and/or AG2 audio circuits in ACCU			

Table 5-22.- AVIONICS SERVICES: AUDIO CENTRAL CONTROL NETWORK (ACCN) (Concluded) (Figure 5-22)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of Air-to-Air communications to attached manned payloads via payload interface connector P1421		A audio circuits in ACCU	Zero	Zero	
Loss of page channel communicator to attached manned payloads via payload interface connector P1421		Page audio circuits in ACCU			
Loss of aural caution and warning signals to manned attached payloads via payload interface connector P1421		Caution and warning tone select circuits in ACCU			

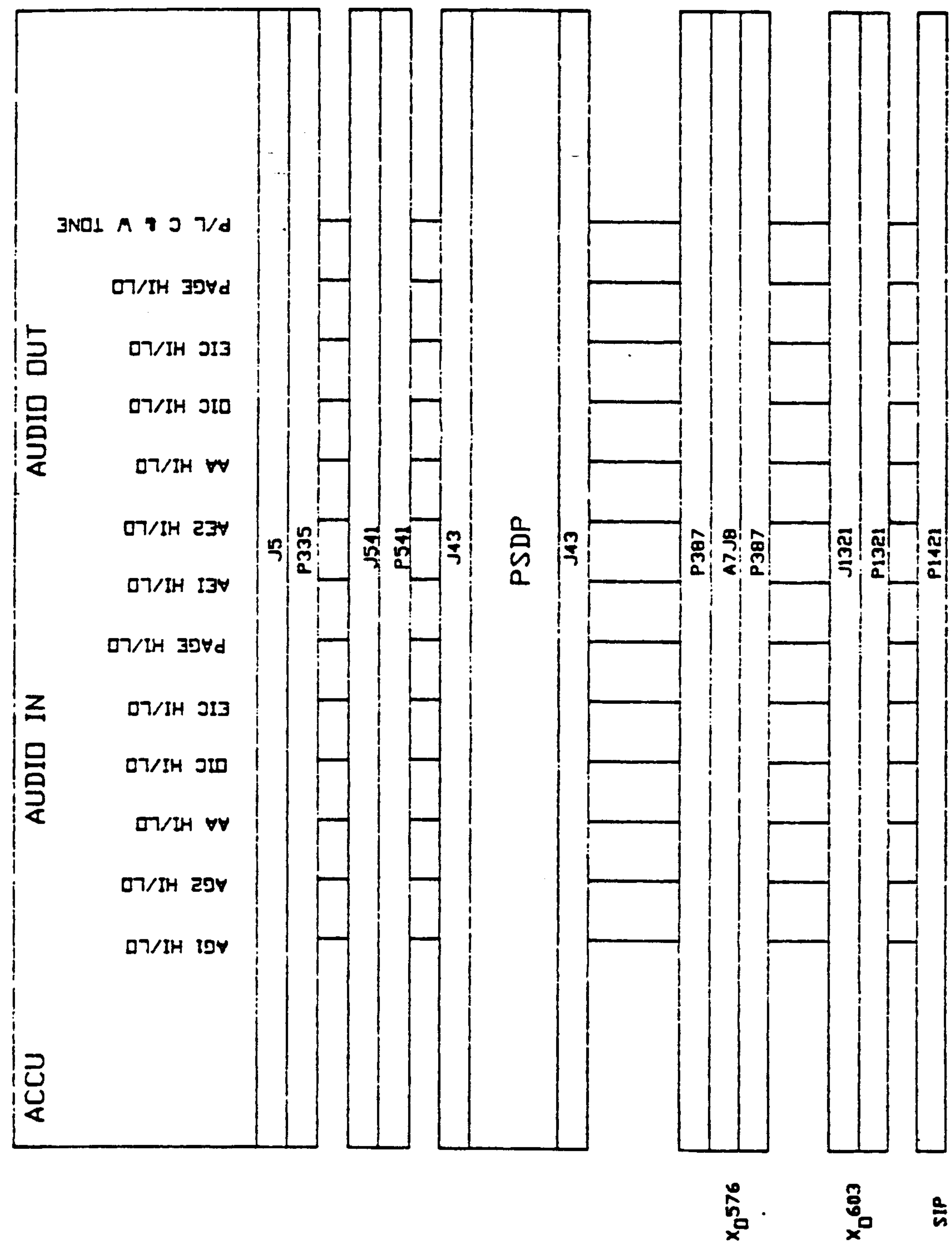


Figure 5-22.- Audio central control unit.

Table 5-23.- AVIONICS SERVICES: PAYLOAD SAFING CONTROLS
(SWITCH PANEL C3A5) (Figure 5-23)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of ACTIVE/SAFE command to payload	Open or close	Payload safing control switch	Zero*	Zero*	Five hard-wired switches on the center console of the flight deck provide ACTIVE/SAFE functions. All five switches are maintained on and do not contain guards. *Use of any one switch can be considered one fault tolerant under certain specific conditions (see note 2 on page 18). Use of any two switches under certain specific conditions can be considered two fault tolerant (see note 3 on page 19).

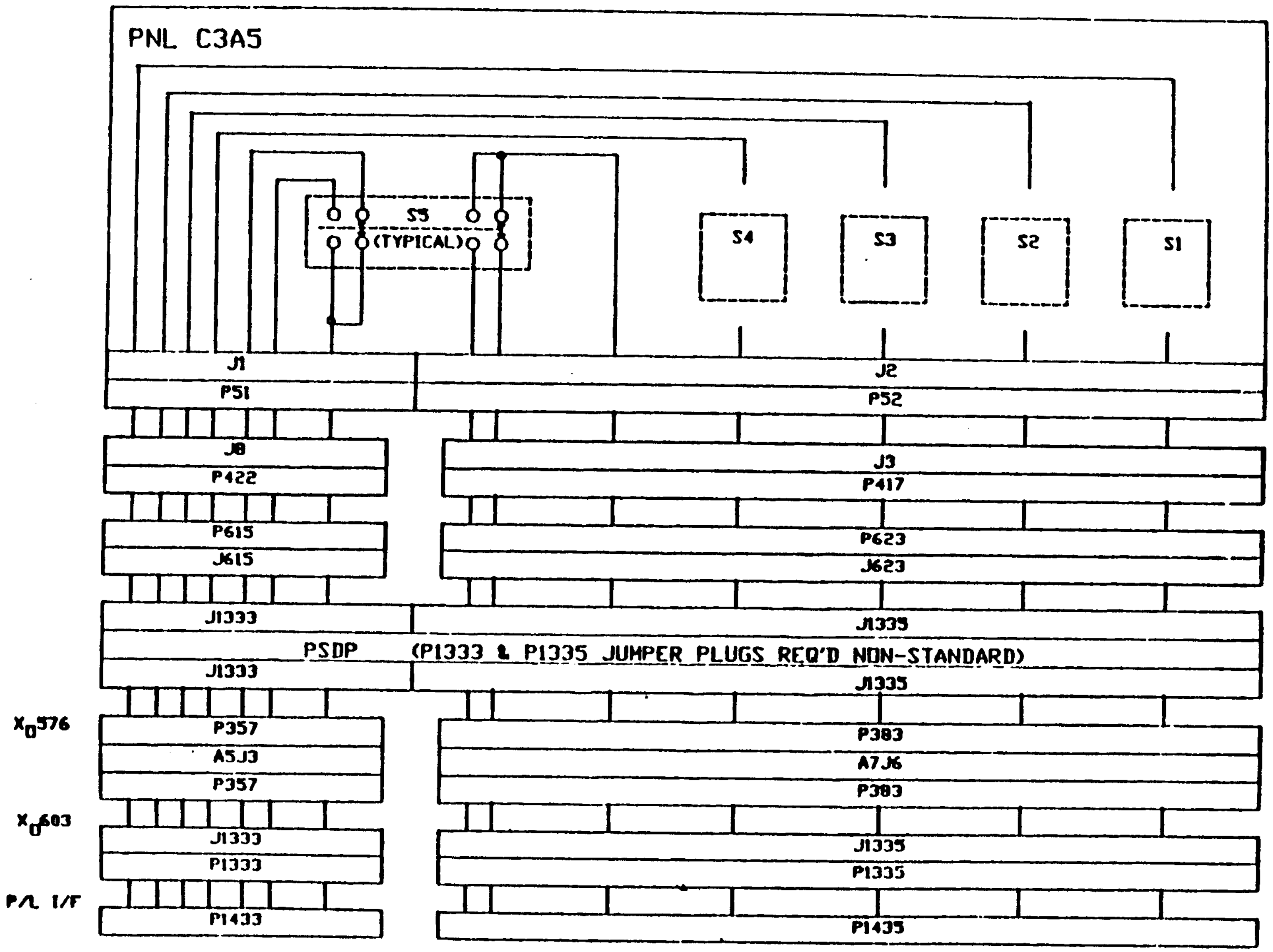


Figure 5-23. - Payload safing switches-C3A5.

Table 5-24.- ACTIVE COOLING PROVISIONS AT THE PAYLOAD HEAT EXCHANGER
(Figure 5-24)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Degraded cooling efficiency in payload primary or secondary coolant loop	Inoperative	1 flow propertioning valve module	One	One	Each Orbiter freon pump package contains redundant pumping elements.
Failure of 1 Orbiter coolant loop would result in crew termination of payload support.	Restricted flow	1 heat exchanger Orbiter loop	Zero	Zero	
	Leak				
	No output	1 Orbiter freon pump package (internal redundancy) in either primary or secondary coolant			

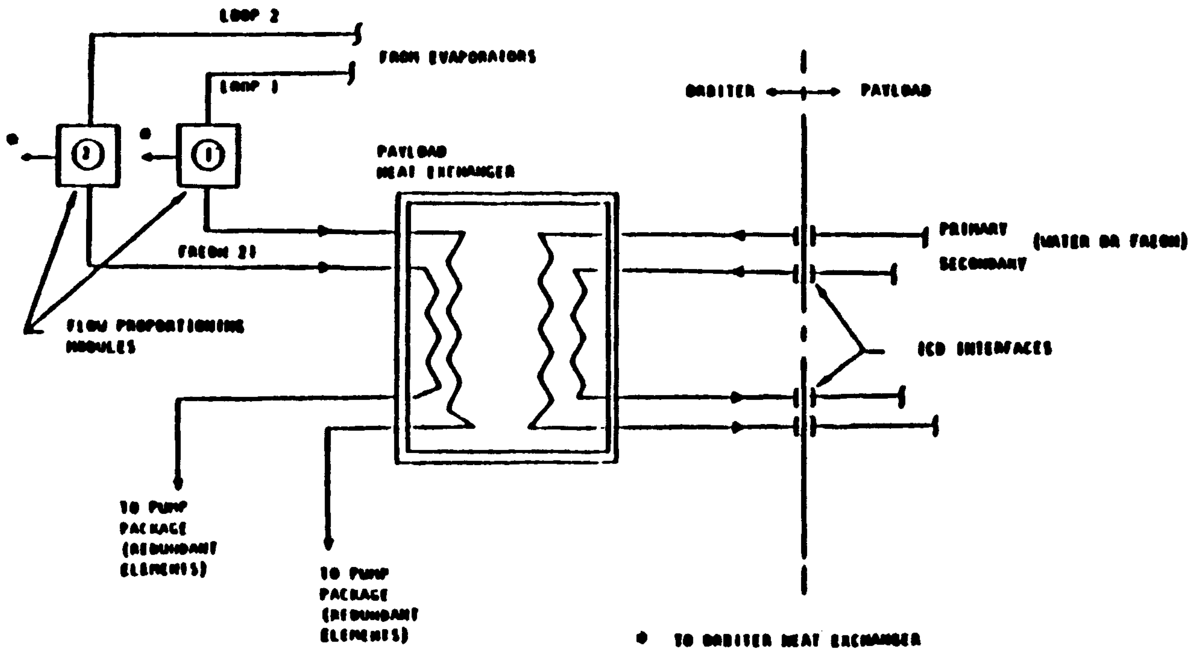


Figure 5-24.- Active cooling provisions at the payload heat exchanger.

6.0 PAYLOAD-TO-ORBITER SIGNAL PATHS

The payload-to-Orbiter signal functions were assessed to determine: (1) whether or not signal path failures could induce failure modes in the Orbiter hardware, and (2) the effects on the payload/Orbiter interface when the payload signal functions are not received or processed by the Orbiter.

The following payload-to-Orbiter signal paths were considered:

a. Payload data interleave (data and clock)

b. Multiplexer/demultiplexer (discrete input high, discrete input low, and differential analog inputs)

c. Payload recorder (analog and digital)

d. S-band signal processor (analog and digital data)

e. Caution and warning (analog and discrete)

f. Payload status indicator

To determine if generic failures initiated by the payload could induce failure modes in Orbiter hardware, a failure effects evaluation was performed on Orbiter hardware that interfaces directly with the payload-to-Orbiter signal paths.

The payload-to-Orbiter signal paths are shown in figure 6-1, and the failure effects associated with the inability of the Orbiter to receive and process this information are noted in table 6-1.

Table 6-1.- PAYLOAD-TO-ORBITER SIGNAL PATHS OVERVIEW

Payload-to-Orbiter interface	Interface failure characteristics	Effects on payload/ Orbiter interface
Caution and Warning (C&W) (analog and discrete)	C&W electronics fail to receive associated digital and analog data.	Payload hazards could not be readily detected, resulting in potentially unsafe operation.
Payload data recording (analog and digital)	Orbiter payload recorder fails to record digital or analog data on 1 or all 3 recording channels for subsequent downlink transmission.	Data cannot be stored for subsequent downlink transmission.
Payload data interleave (data and clock)	Payload data interleave does not receive payload data or process information for PCM downlink or GPC retrieval.	Payload functions via the GPC's would not be monitored or controlled, and payload data via the PCM would not be transmitted to the ground.
S-band FM signal processor (analog and digital data)	Loss of function/data electronics.	Cannot transmit payload data to ground stations.
MDM-discrete input high (DIH), discrete input low (DIL), differential analog inputs (AID)	MDM failure to receive payload monitoring data.	Payload functions via the Orbiter GPC's would not be monitored. Redundant MDM's are provided to monitor critical payload functions, if so utilized.
Payload status indicators	Loss of payload status indicators (talkbacks).	Payload status as a result of Standard Switch Panel commands cannot be monitored.

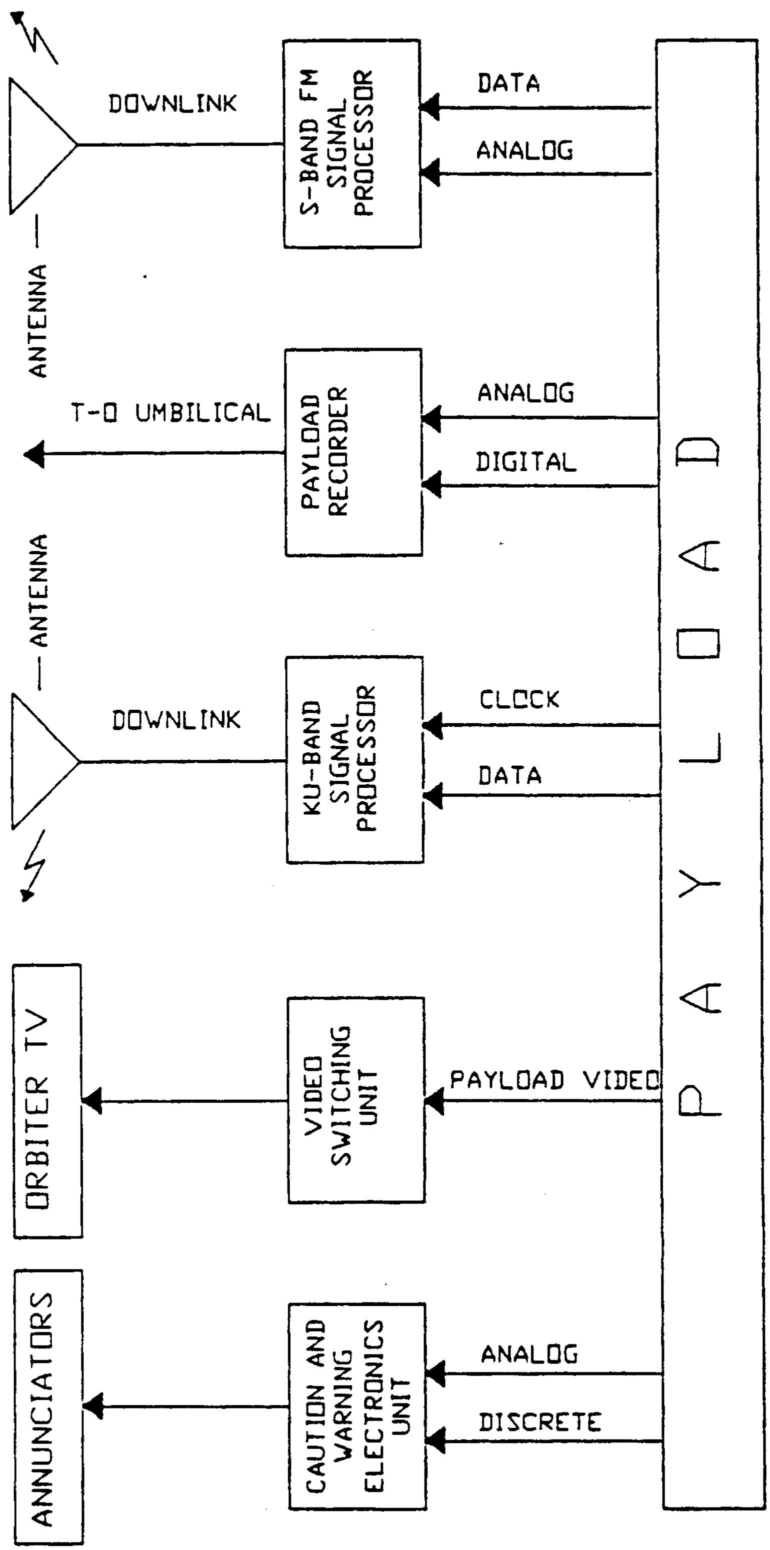


Figure 6-1.- Payload-to-Orbiter signals (sheet 1 of 2).

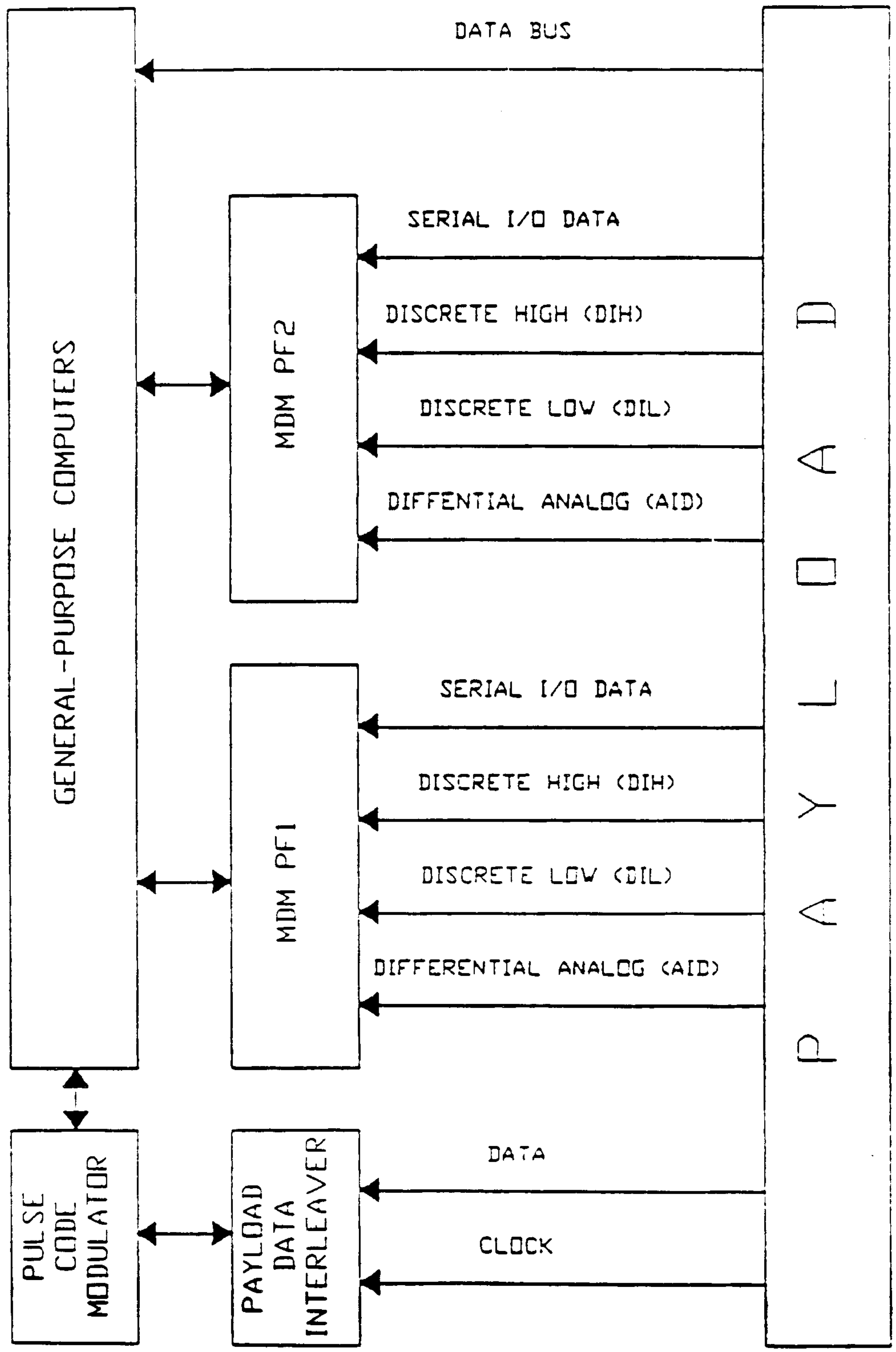


Figure 6-1.- Payload-to-Orbiter signals (sheet 2 of 2).

Table 6-2.- AVIONICS SERVICES: PAYLOAD RECORDER
(Figure 6-2)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of serial digital, parallel, and/or parallel analog data recording input from all 1/4-SMCH sections (payload interface connectors P1401, P1403, P1405, P1407).	No input	Payload recorder electronics unit	Zero	Zero	
Loss of analog/digital parallel playback to T-0 umbilical of data from all 1/4-SMCH sections (payload interface connectors P1401, P1403, P1405 and P1407).	No output		One	One	Tape may be saved and data recovered through an operable recorder on the ground. Loss of payload recorder services results in the inability to store payload data for playback transmission. Payload recorder standard services of

Table 6-2.- AVIONICS SERVICES: PAYLOAD RECORDER (Continued)
(Figure 6-2)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
					2 parallel digital channels and 1 analog channel are provided by SMCH to the SMCH-SIP payload interface connectors P1401, P1403, P1405, and P1407. Track allocations Section 1: Digital 1 & 2 Analog 9 Section 2: Digital 3 & 4 Analog 10 Section 3: Digital 5 & 6 Analog 11 Section 4: Digital 7 & 8 Analog 12

Table 6-2.- AVIONICS SERVICES: PAYLOAD RECORDER (Continued)
(Figure 6-2)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of serial digital playback from all 1/4-SMCH sections (P1401, P1403, P1405, P1407) to PSDP for T-0 umbilical or payload routing, S-band FM signal processor, and Ku-band signal processor.	No output	Payload recorder electronics unit	One	One	Tape may be saved and data recovered through an operable recorder on the ground. Payload recorder nonstandard services may be secured from the PSDP at interface connectors J13, J35, and J53.
Failure to record payload data from all 1/4-SMCH sections. (Payload interface connectors P1401, P1403, P1405, P1407.)	No input	Payload recorder transport unit	Zero	Zero	

Table 6-2.- AVIONICS SERVICES: PAYLOAD RECORDER (Continued)
(Figure 6-2)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Track 1-7 head - Loss of parallel digital data recording from sections 1-3 and 1/2 of section 4. Track 8-14 head - Loss of recording 1/2 section 4 parallel digital data and all parallel analog data from all 1/4-SMCH sections.		Single transport unit record head			
Track 1-7 head - Cannot omit recorded parallel digital data from sections 1-3 and 1/2 of section 4.	No output	Single transport unit repro head			Tape may be removed and replayed on an operable recorder on the ground.

Table 6-2.- AVIONICS SERVICES: PAYLOAD RECORDER (Concluded)
(Figure 6-2)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Track 8-14 head - Cannot omit recorded parallel analog data from sections 1-4 and 1/2 parallel digital data from section 4.					

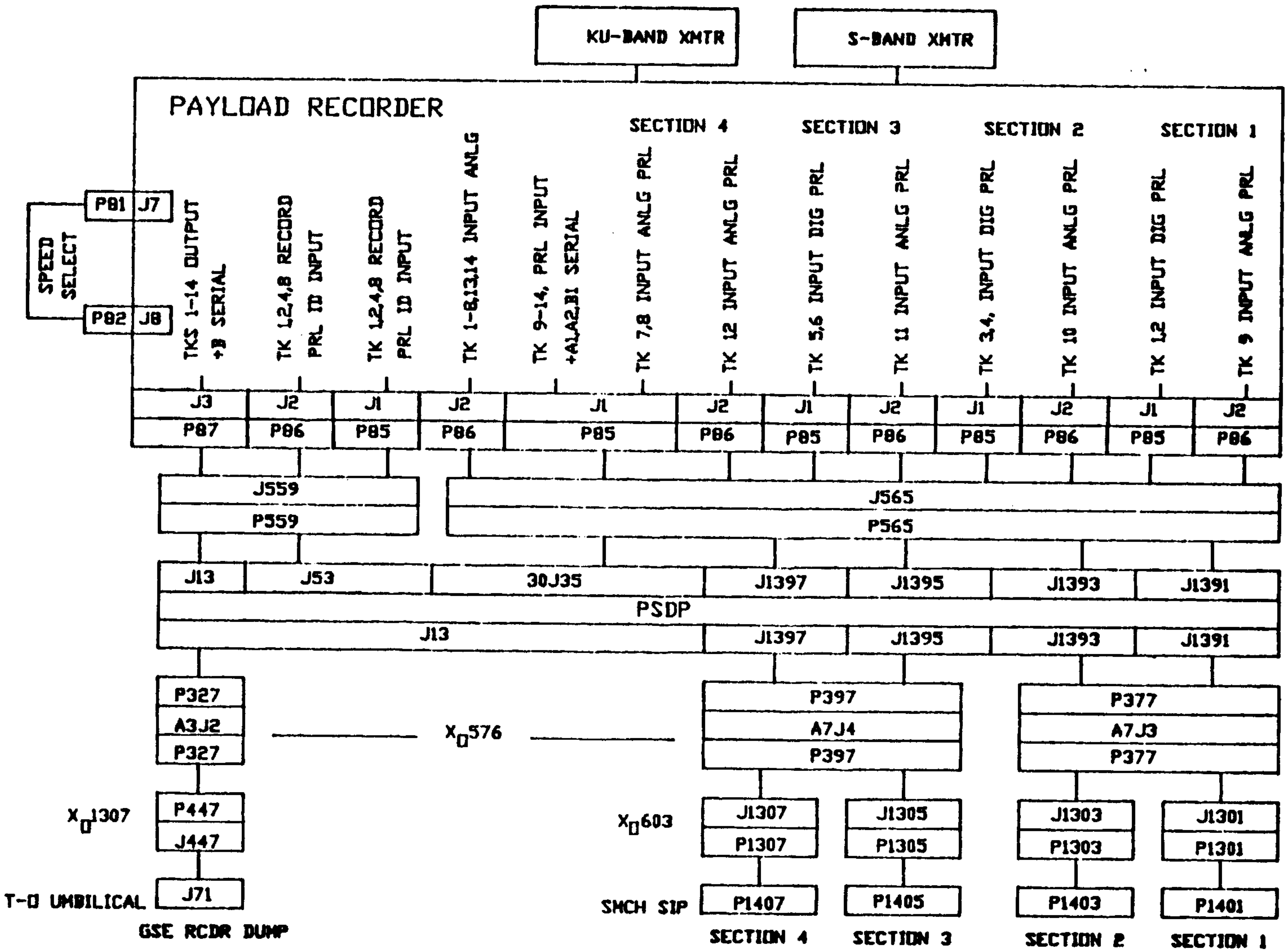


Figure 6-2.- Payload recorder.

Table 6-3.- AVIONICS SERVICES: PAYLOAD DATA INTERLEAVER
(Figure 6-3)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of payload data input from 1/4-SMCH services in corresponding section (payload interface connectors P1401, P1403, P1405, P1407) and J19 at PSDP.	No input	PDI input functional elements for attached payload 1-5 PDI ports	Zero PDI failure results in loss of payload input data. PDI is single-string, single-point failure.	Zero	The standard PDI services of 1 data channel per 1/4-SMCH section are provided from PDI to the SMCH-SIP payload interface connectors P1401, P1403, P1405, and P1407. Nonstandard services are provided from the PDI to J19 at the PSDP for a unique interface.
Loss of payload data input from S-band system (PSP 1 and 2) for detached payloads.		PDI input functional elements for detached payloads PSP 1 and 2 interface failure (PDI port 6)	Zero Both PSP's input to a common PDI part.	Zero	
Loss of payload data to PCMMU's 1 & 2 for downlink to ground and input to SM/ PL GPC for payload data monitoring.	No output	PDI output functional elements to PCMMU 1 or 2 via PIP 1/2	One Loss of data for downlink requires loss of interface to both PCMMU's.	One	

Table 6-3.- AVIONICS SERVICES: PAYLOAD DATA INTERLEAVER (Concluded)
(Figure 6-3)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of ability to reconfigure PDI. No immediate loss of payload telemetry data.		PDI interface to SM/PL GPC via PL 1 data bus	Zero	Zero PDI is attached to PL 1 data bus only. Crew may reconfigure if failure is at GPC.	
Loss of payload data from all sources (sections 1-4 and detached payloads).		PDI power supply	Zero	Zero	
Loss of PDI processing for assigned input port (sections 1-4 and PSP input).	No input	PDI decom failure	Zero	Three Crew may reassign input to an alternate decom.	

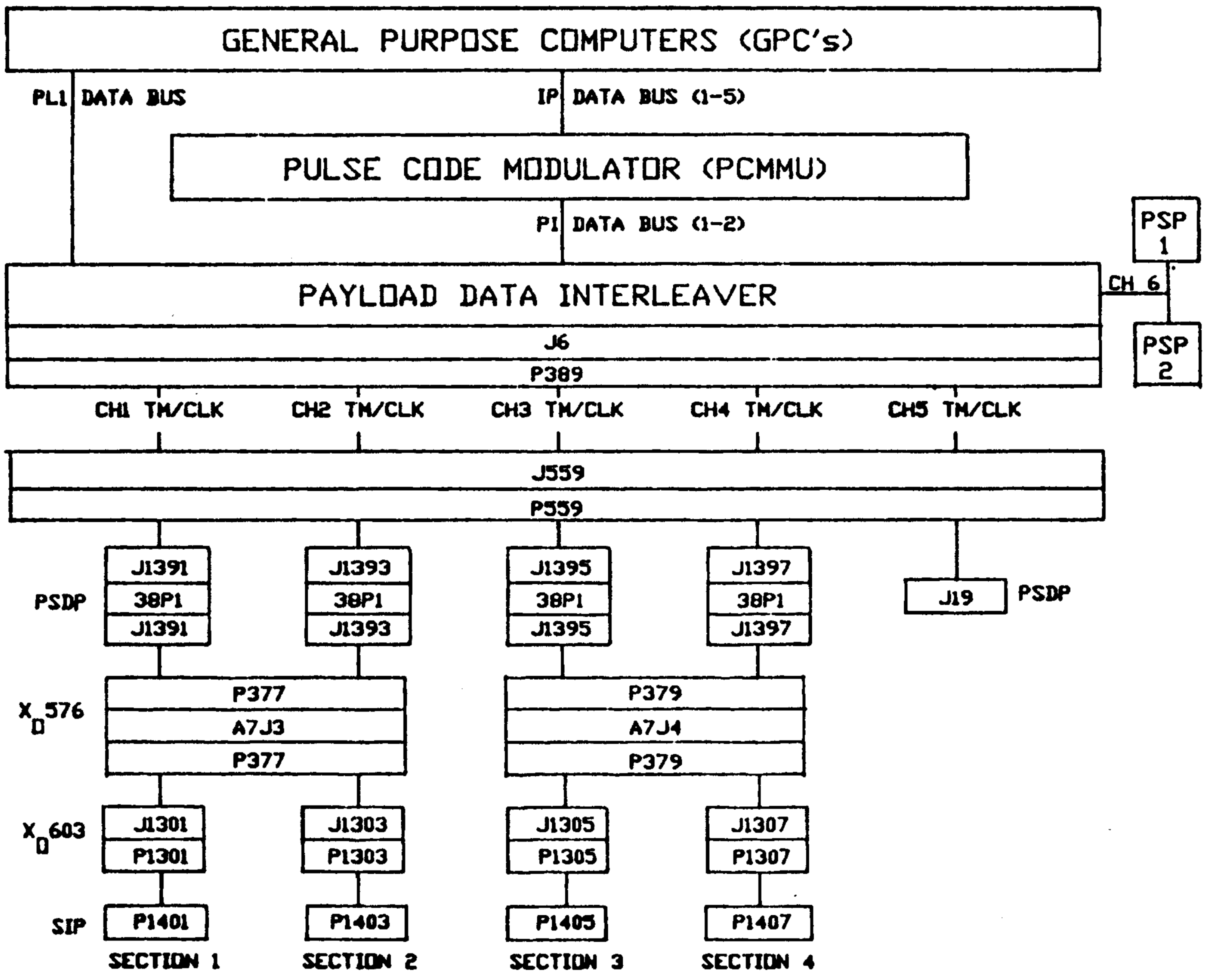


Figure 6-3.- Payload Data Interleaver (PDI).

Table 6-4.- AVIONICS SERVICES: S-BAND FM SIGNAL PROCESSOR
(Figure 6-4)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of attached payload data (wide band analog and digital signals encrypted data) from all 4 cargo sections for transmission to ground	No input	S-band FM signal processor	One	One	The FM signal processor is a fully redundant unit with inputs from all data sources routed to both S-band FM signal processor - unit no. 1 and unit no. 2.
Loss of payload recorder recorded data (256 kbps to 1.024 MPB's) input (3 serial, 14 parallel, or 14 analog tracks) to S-band FM signal processor					
Loss of payload video input (4 MHz TV) via video switching network/S-band signal processor					

Table 6-4.- AVIONICS SERVICES: S-BAND FM SIGNAL PROCESSOR (Concluded)
(Figure 6-4)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of attached pay-load wideband digital data inputs (200 bps to 5 Mbps)	Open	S-band FM data source switch (panel A1A3, S4)			The S-band FM signal processor will select one of seven inputs (5 payload and 2 Orbiter data) via the S-band FM data source switch (panel A1A3 S4) for transmission to ground.
Loss of attached pay-load wideband analog input (300 Hz to 4 MHz)					
Loss of en-crypted data input (256 kbps)					

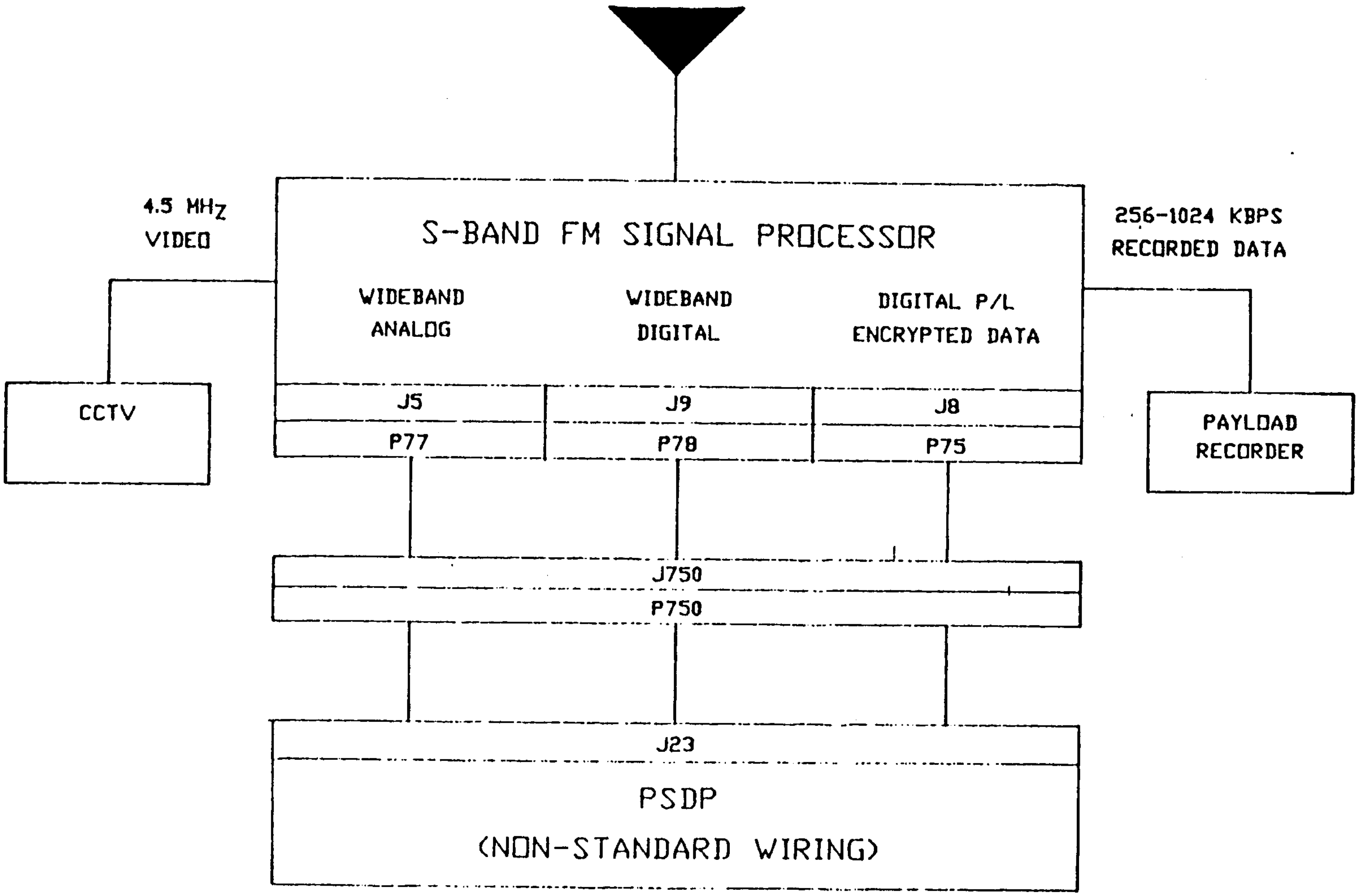


Figure 6-4.- S-band FM signal processor.

Table 6-5.- AVIONICS SERVICES: DISCRETE INPUT LOW (DIL) INPUTS
(Figure 6-5)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of DIL payload monitoring inputs from all 1/4-SMCH serves in sections 1-4 (payload interface connectors P1427, P1429, P1431, and P1419)	No input	PF1 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power supplies must occur. Failure of GPC loaded with SM/PL software will require crew reassignment of another GPC with SM/PL software.
Total loss of DIL payload monitoring inputs from payload interface connectors P1412 and P1420.		PF2 MDM (other than IOM card)			
Loss of DIL payload monitoring inputs from section 1 (P1431) and section 4 (P1425) payload interface connector P1419		PF1 MDM IOM no. 5	Zero	Zero	Redundancy is provided by 2 MDM's and internal redundancy of MDM operation but not the IOM level; single point failure.

Table 6-5.- AVIONICS SERVICES: DISCRETE INPUT LOW (DIL) INPUTS (Continued)
(Figure 6-5)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of DIL payload monitoring inputs from section 2 (P1429) and section 3 (P1427)		PF1 MDM IOM no. 13 channel 02			The standard DIL services are provided by SMCH from PF1 to the SMCH-SIP payload interface connectors P1431, P1429, P1427, and P1425. Nonstandard DIL services are provided from PF1 to P1419 and PF2 to P1420 P1412. Dedicated to the same GFPC, crew can reassign a GPC to provide SM functions to payload.

Table 6-5.- AVIONICS SERVICES: DISCRETE INPUT LOW (DIL) INPUTS (Continued)
(Figure 6-5)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
Loss of DIL payload monitoring inputs from payload interface connectors P1412 and P1420.	No input	PF2 MDM IOM no. 5 channels 01-02	Zero	Zero	Redundancy is provided by 2 MDM's and internal MDM operations but not on the IOM level; single point failure. Loss of DIL services results in the failure of the Orbiter GPC's to monitor payload functions.
Loss of DIL payload monitoring inputs from payload interface connector P1420.		PF2 MDM IOM no. 13 channel 02			
Loss of DIL payload monitoring inputs from section 1 (P1431)		PF1 MDM IOM no. 5 channel 01			
Loss of DIL payload monitoring inputs from section 4 (P1425) and P1419		PF1 MDM IOM no. 5 channel 02			

Table 6-5.- AVIONICS SERVICES: DISCRETE INPUT LOW (DIL) INPUTS (Concluded)
(Figure 6-5)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of DIL payload monitoring inputs from P1412 and P1420		PF2 MDM IOM no. 5 channels 01 & 02			
Loss of DIL payload monitoring inputs from P1420		PF2 MDM IOM no. 13 channel 02			

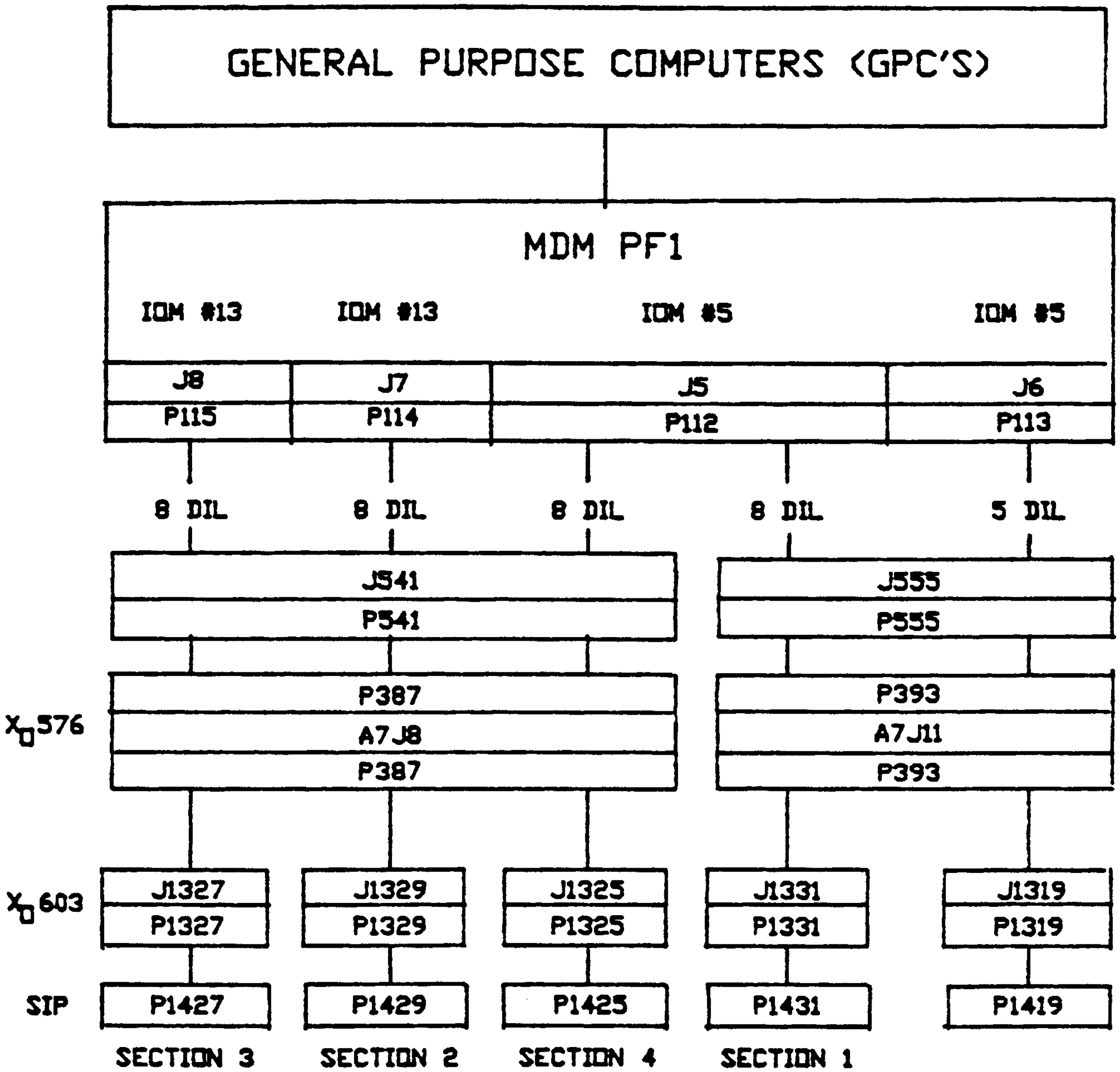


Figure 6-5a.- MDM PF1 DIL.

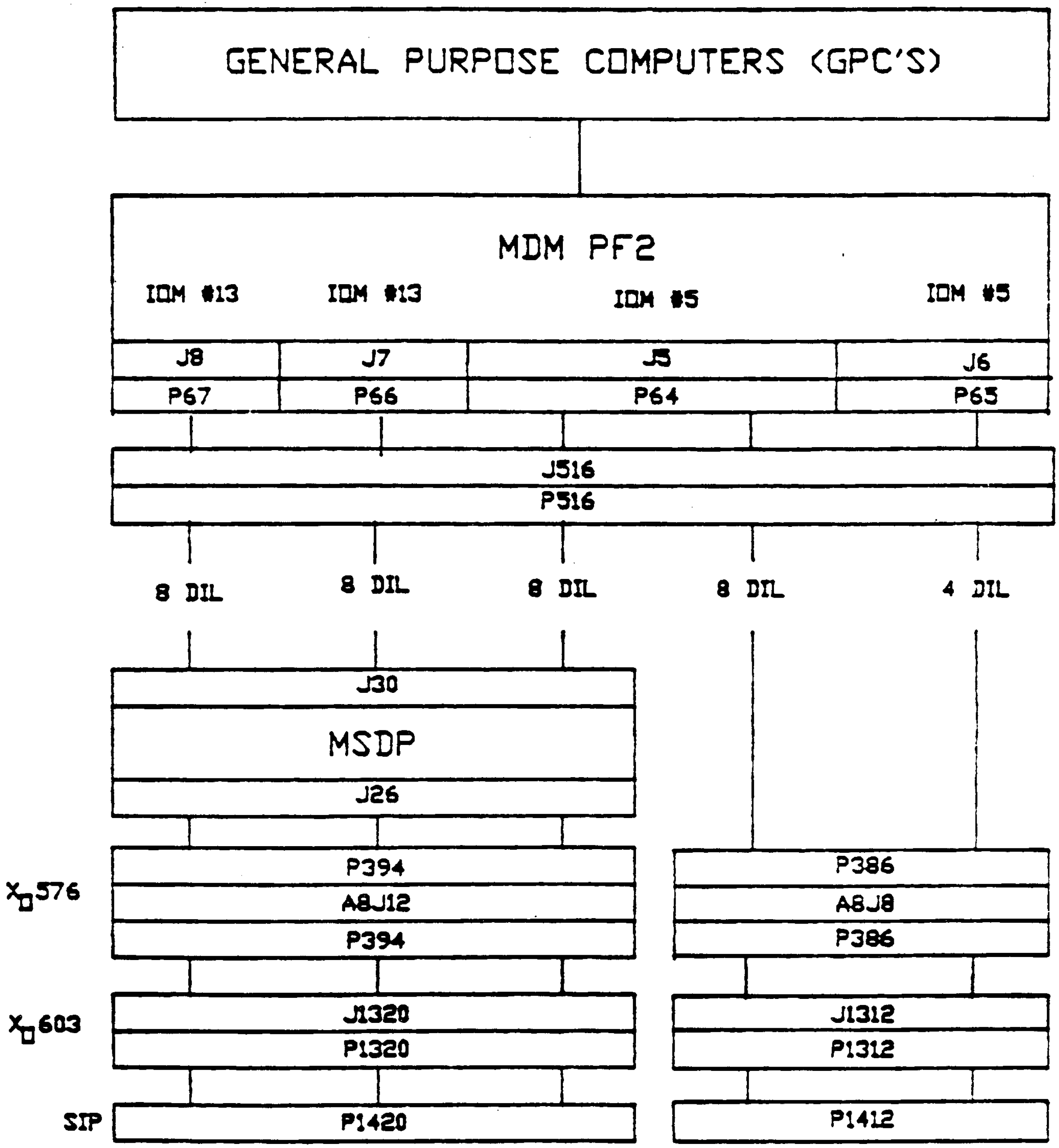


Figure 6-5b.- MDM PF2 DIL.

Table 6-6.- AVIONICS SERVICES: ANALOG INPUT DIFFERENTIAL (AID) INPUTS (Figure 6-6)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of AID payload monitoring inputs from all 1/4-SMCH services in sections 1-4 (payload interface connectors P1425, P1427, P1429, P1431, P1419, and P1414)	No input	PF1 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power supplies must occur. Failure of GPC loaded with SM/PL software will require crew reassignment of another GPC with SM/PL software. The standard AID services are provided by SMCH from PF1 to the SMCH-SIP payload interface connectors P1425, P1427, P1429, and P1431. Nonstandard services provided from PF1 to P1419, P1414 and from PF2 to P1416.
Total loss of AID payload monitoring inputs from payload interface connector P1416		PF2 MDM (other than IOM card)			

Table 6-6.- AVIONICS SERVICES: ANALOG INPUT DIFFERENTIAL (AID) INPUTS (Continued) (Figure 6-6)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
					PF1 and PF2 are dedicated to the same GPC. Crew can reassign a GPC to provide SM/PL functions to payloads.
Loss of AID payload monitoring inputs from all 1/4-SMCH service sections 1-4 (payload interface connectors P1425, P1427, P1429, P1431, and P1419)	No input	PF1 MDM IOM no. 11	Zero	Zero	Failure of primary and backup MIA, SCU, or power supplies of the occur. Failure of GPC loaded with SM/PL software will require crew reassignment of another GPC with SM/PL software. Loss of AID services re-
Loss of AID payload monitoring inputs from payload interface connector P1414		PF1 MDM IOM no. 1 channels 0-12			

Table 6-6.- AVIONICS SERVICES: ANALOG INPUT DIFFERENTIAL (AID) INPUTS (Continued) (Figure 6-6)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of AID payload monitoring inputs from payload interface connector P1416		PF2 MDM IOM no. 11 channels 0-6			sults in the failure of the ability of the Orbiter GPC's to monitor payloads.
		PF2 MDM IOM no. 1 channels 0-11			
Loss of AID payload monitoring inputs from section 4 (P1425)	No inputs	PF1 MDM IOM no. 11 channels 00-01	Zero	Zero	Redundancy is provided by 2 MDM's and internal MDM operation but not on the IOM channel level; single point failure.
Loss of AID payload monitoring inputs from section 3 (P1427)		PF1 MDM IOM no. 11 channels 02-03			
Loss of AID payload monitoring inputs from section 2 (P1429)		PF1 MDM IOM no. 11 channels 04-05			
Loss of AID payload monitoring inputs from section 1 (P1431)		PF1 MDM IOM no. 11 channels 06-07			

Table 6-6.- AVIONICS SERVICES: ANALOG INPUT DIFFERENTIAL (AID) INPUTS (Concluded) (Figure 6-6)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of AID payload mon-itoring in-puts from P1419		Loss of PF1 MDM IOM no. 11 channel 08			

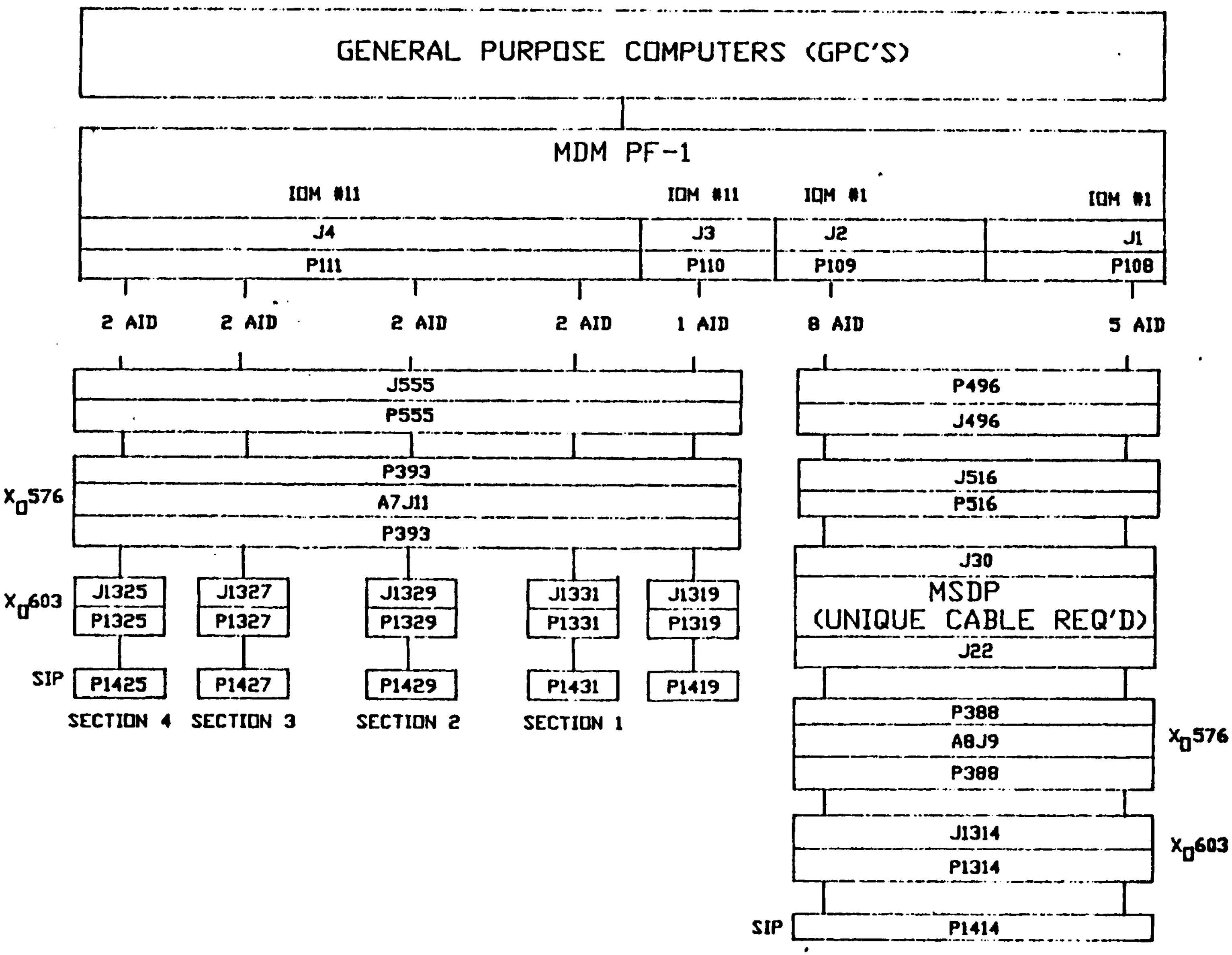


Figure 6-6a. - MDM PF1 AID.

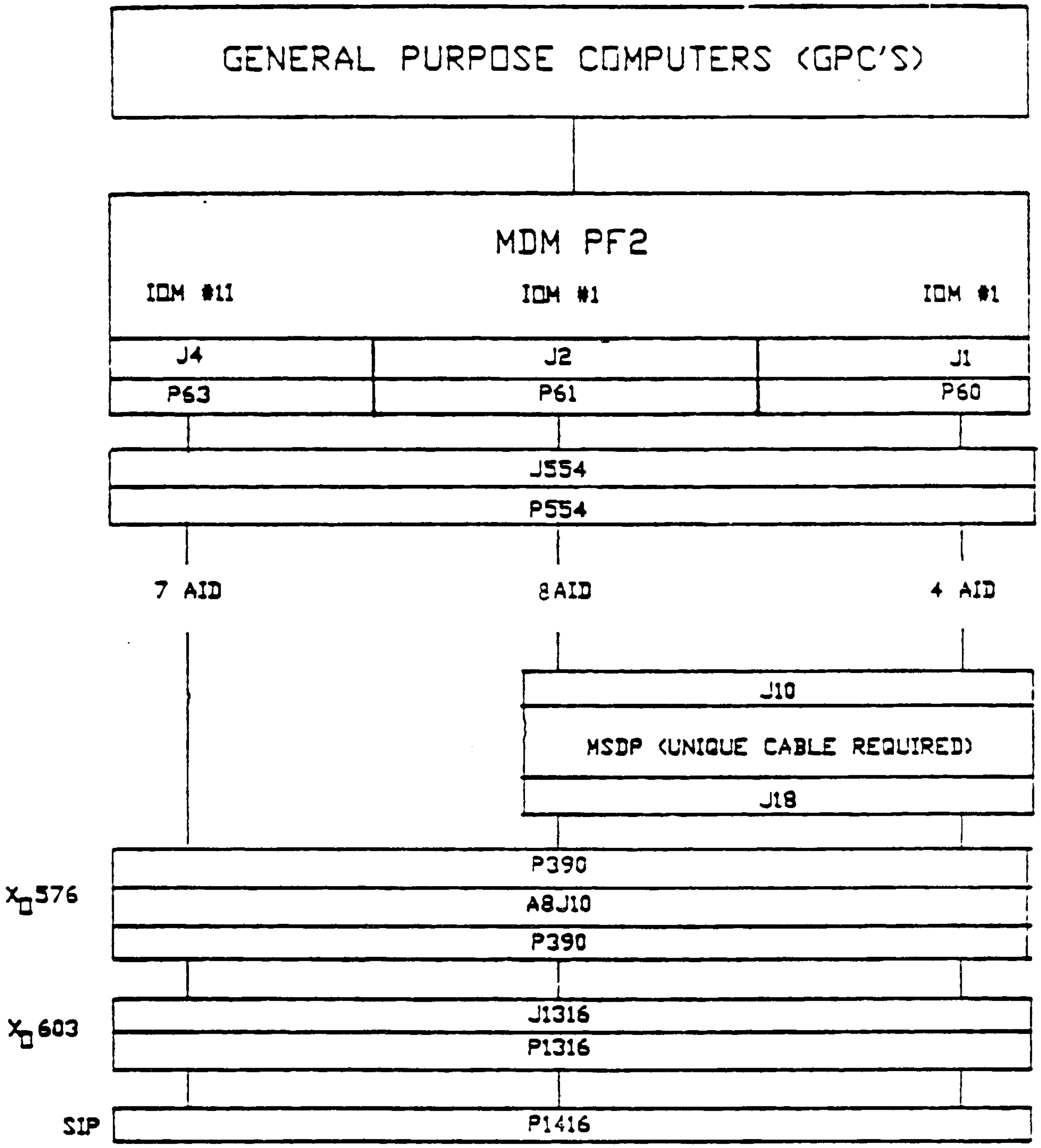


Figure 6-6b.- MDM PF2 AID.

Table 6-7.- AVIONICS SERVICES: DISCRETE INPUTS HIGH (DIH) INPUTS
(Figure 6-7)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Total loss of DIH payload monitoring inputs from MSDP J30 and J32	No input	PF1 MDM (other than IOM card)	One	One	Failure of primary and backup MIA, SCU, or power supplies must occur.
Total loss of DIH payload monitoring inputs from MSDP connectors J18 and J10		PF2 MDM (other than IOM card)			Failure of GPC loaded with SM/PL software will require crew reassignment of another GPC with SM/PL software.
Loss of DIH payload monitoring inputs from MSDP connectors J30 and J32		PF1 MDM IOM no. 6	Zero	Zero	Redundancy is provided by 2 MDM's and internal redundancy of MDM operation but not on the IOM level; single point failure.
		PF1 MDM IOM no. 6 channel 02			
Loss of DIH payload monitoring inputs from MSDP connectors J18 and J10		PF2 MDM IOM no. 6			

Table 6-7.- AVIONICS SERVICES: DISCRETE INPUTS HIGH (DIH) INPUTS (Concluded) (Figure 6-7)

Failure effects	Failure mode	Failed component	Failure tolerance w/o crew action	Failure tolerance with crew action	Rationale/ remarks
		PF2 MDM IOM no. 6 channel 02			Redundancy is provided by 2 MDM's and internal MDM operation but not on the IOM level; single point failure. MDM DIH services are nonstandard. PF1 and PF2 are dedicated to the GPC. Crew can reassign a GPC to provide SM functions to payload.

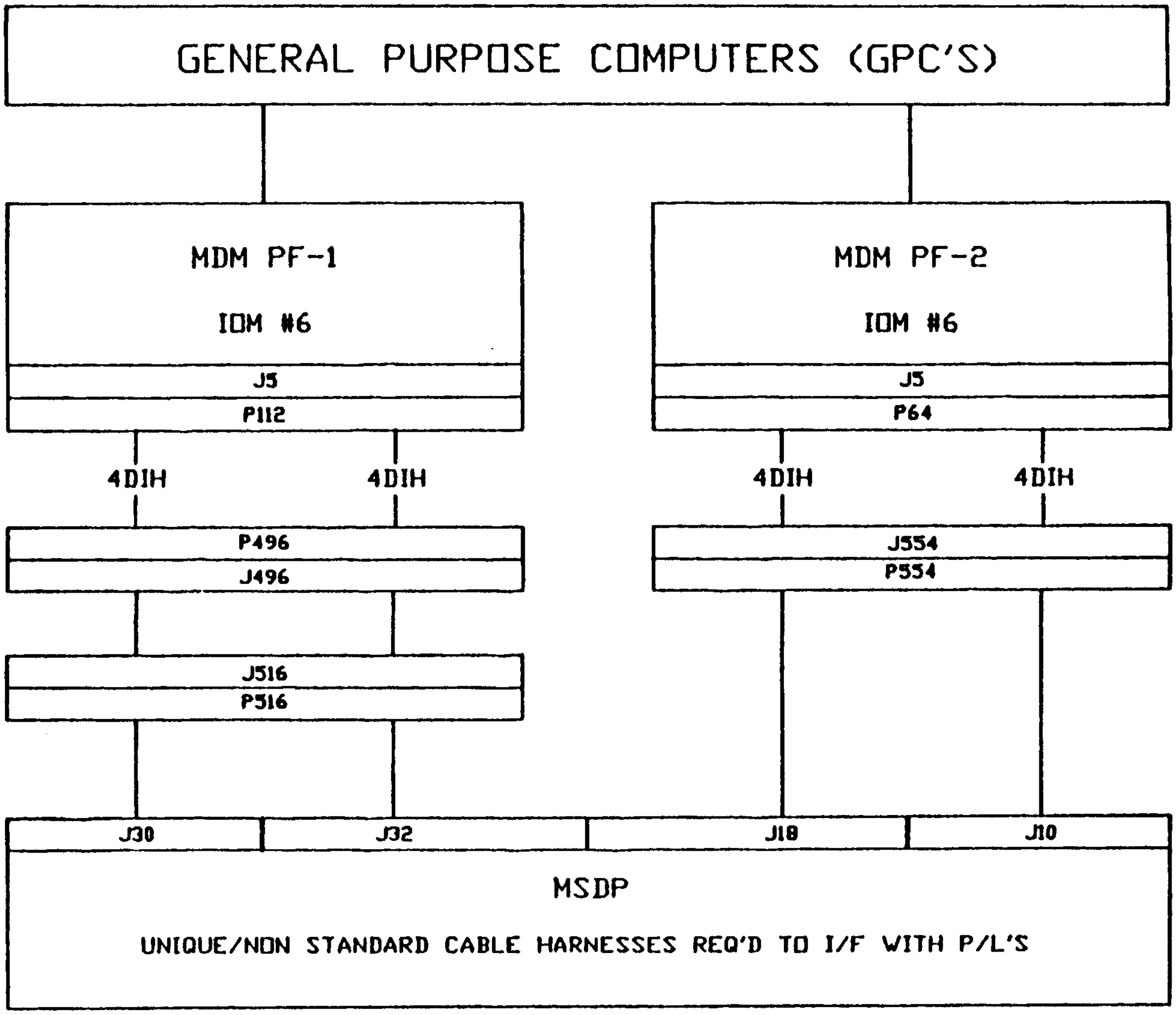


Figure 6-7.- PF1/PF2 DIH.

Table 6-8.- AVIONICS SERVICES: CAUTION AND WARNING ELECTRONICS ASSEMBLY (CWEA) (Figure 6-8)

Failure effects	Failure mode	Failed components	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of 2 fire/smoke inputs from attached manned payloads via MSDP connectors J20 and J12	No input/output	Caution and Warning Electronics Assembly (CWEA)	Zero	Zero	CWEA electronics failure to receive associated digital and analog data results in the loss of ability to readily detect payload hazards. This condition may result in a potentially unsafe operation.
Loss of 5 analog/discrete warning signals from attached payloads via payload interface connector P1423					

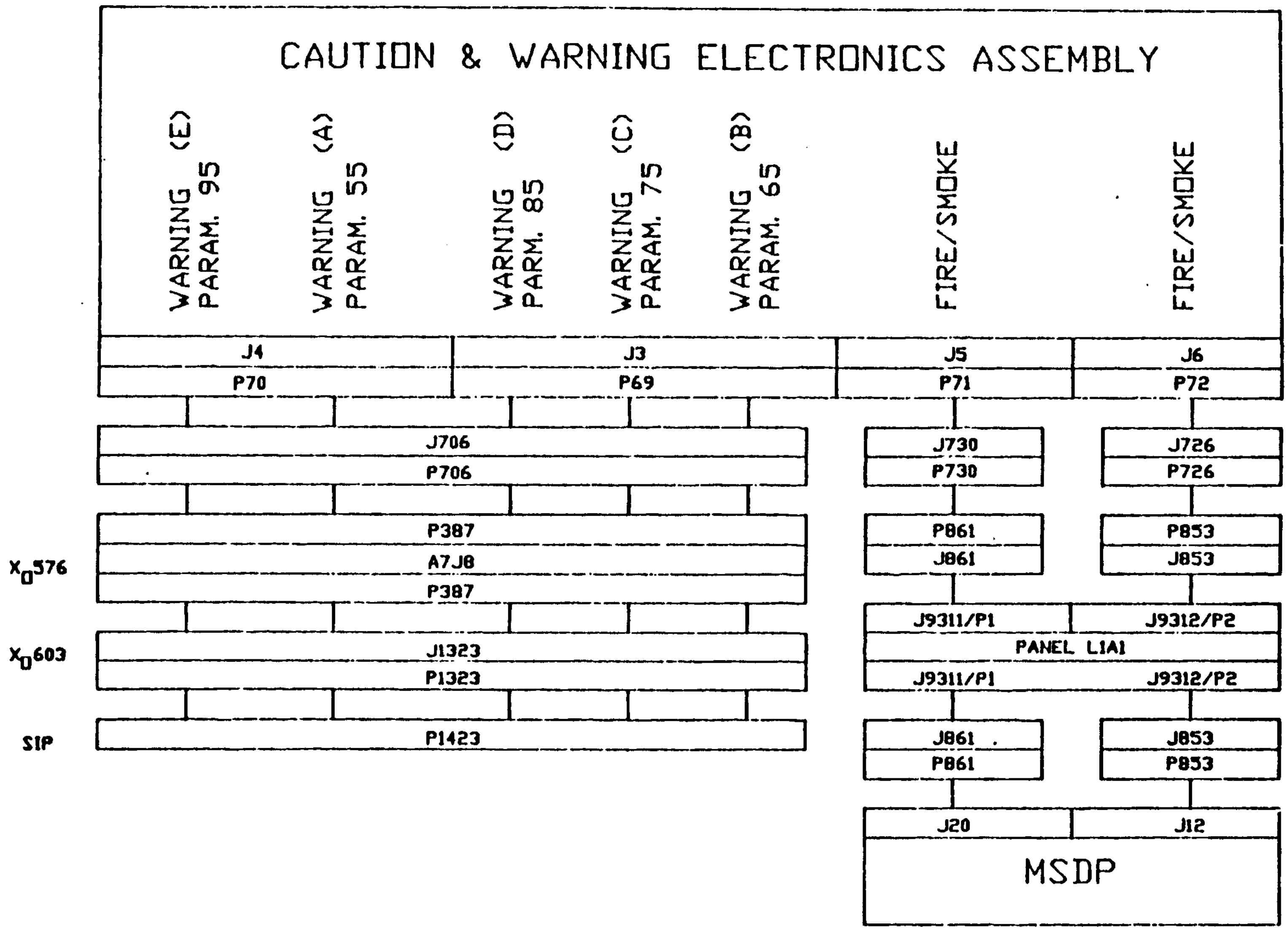


Figure 6-8. - Caution and Warning Electronics Assembly (CWEA).

Table 6-9.- AVIONICS SERVICES: STANDARD SWITCH PANEL PAYLOAD STATUS INDICATORS (Figure 6-7)

Failure effects	Failure mode	Failed component	Failure tolerance		Rationale/ remarks
			w/o crew action	with crew action	
Loss of payload status indication(s) for the associated 1/4-SMCH sections 1 - SSP 1A P1431 2 - SSP 1B P1429 3 - SSP 2A P1427 4 - SSP 2B P1425	Inoperative	SSP talkback(s)	Zero	Zero	Talkbacks consist of 1. Three position event indicator - ON = UP OFF = Stripe On = Down 2. Two position event indicator - ON = Gray OFF = Stripes Each SSP has two three-position indicators (DS1 & DS2 or DS13 & DS14) and ten two-position indicators (DS3 to DS12 or DS15 to DS24).

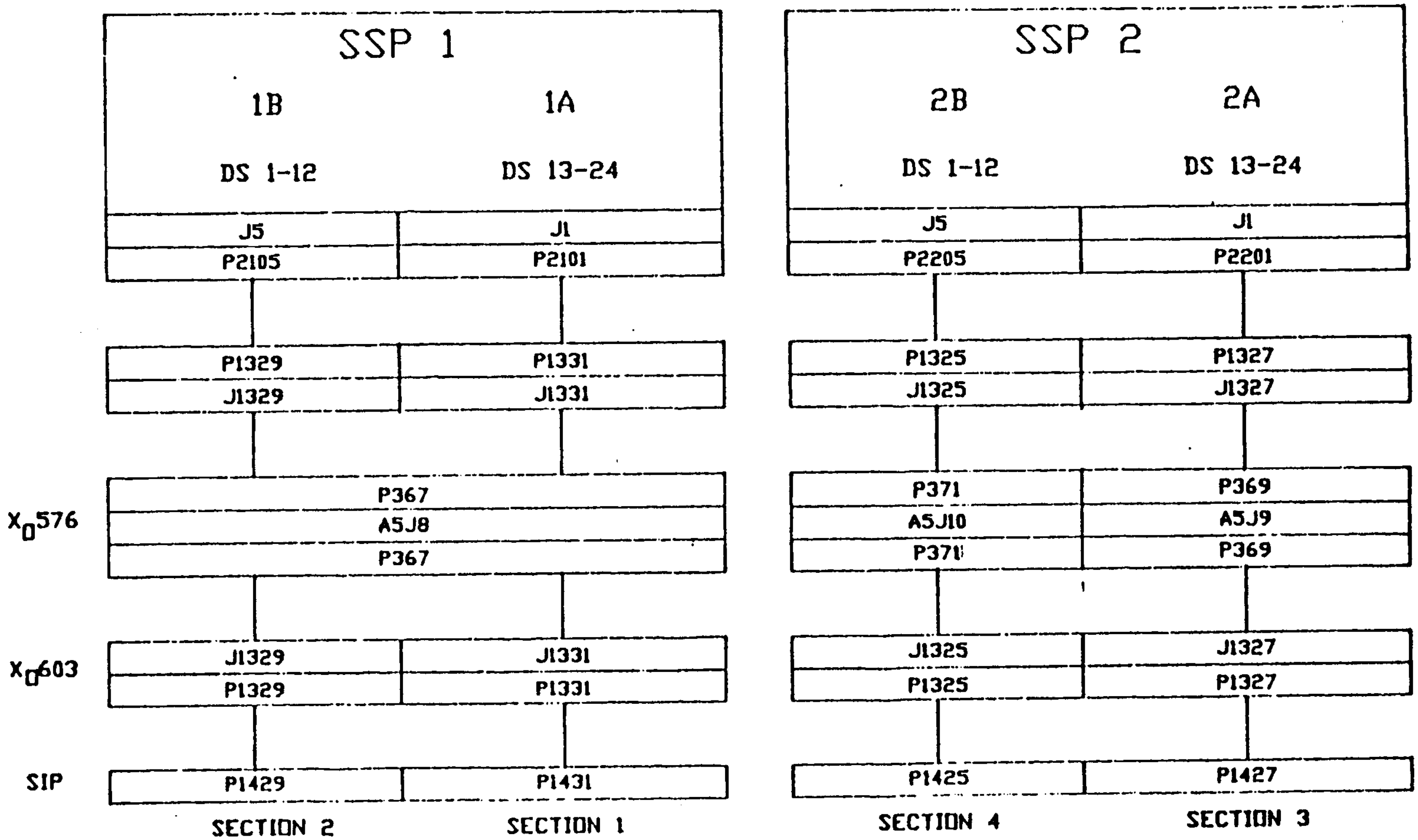


Figure 6-9.- Standard Switch Panel-1A and B and Standard Switch Panel 2A and B payload status indicators (talkbacks).