The Space Congress® Proceedings

1993 (30th) Yesterday's Vision is Tomorrow's Reality

Apr 29th, 1:00 PM - 4:00 PM

Paper Session III-A - Overview of Space Station Freedom Avionics Design for Critical Functions

John Rush
NASA Space Station Freedom Program Office Rest on, Virginia

Scholarly Commons Citation

Rush, John, "Paper Session III-A - Overview of Space Station Freedom Avionics Design for Critical Functions" (1993). *The Space Congress® Proceedings*. 15.
https://commons.erau.edu/space-congress-proceedings/proceedings-1993-30th/april-29-1993/15

Overview of Space Station Freedom Avionics Design for Critical Functions

John Rush
NASA Space Station Freedom Program Office
Reston, Virginia

Space Station Freedom will be an orbiting laboratory facility resulting from a major investment by the United States and its International Partners. It is imperative that Space Station Freedom's avionics system be designed to be robust and capable of performing the critical functions necessary to protect our investment in this unique resource. This paper provides an overview of the design of the avionics system with regard to its resilient failure tolerant architecture.

I. Introduction

Space Station Freedom (SSF) will be an orbiting laboratory facility that will host a wide range of payloads during its thirty year lifetime. Each payload will require some set of facility resources and/or services such as electric power, heat dissipation, data services, manned attendance, etc. To provide these resources and services, and to maintain SSF as an orbiting manned vehicle, SSF will have a set of distributed systems, each providing a specific resource or service function.

In this paper the systems of interest will be those that have their functionality controlled by the SSF's avionics computers. Those systems and their principle functions are:

1) Electric Power System (EPS): Provides electrical power and power distribution to SSF electronic system and payload equipment.
2) Guidance, Navigation, and Control/Propulsion (GNCP): Provides SSF's attitude determination, attitude control, and maintains orbital altitude.
3) Data Management System (DMS): Provides the software execution, man-machine interface, data storage, and data transport resources and services used in the avionics system.

4) Thermal Control System (TCS): Provides heat dissipation services for SSF equipment.
5) Communication and Tracking System (CTS): Provides spacecraft to ground communication services via the Tracking and Data Relay Satellite System (TDRSS) and crew video and audio services.
6) Environmental Control and Life Support System (ECLSS): Maintains atmosphere in pressurized elements, controls water and waste processing, and provides fire detection and suppression.
7) Mobile Servicing System (MSS): Provides robotic services for maintenance and equipment transport outside of the pressurized elements.
8) Payload Executive System (PES): Provides management of payload execution.

Each of the above systems perform functions that are needed to make SSF an operating laboratory facility. For SSF to perform its mission all system provided functions should be available all the time. However, although each system's components will be designed to a high degree of reliability, there will be times during the thirty year mission of SSF when system components will fail. A way to enhance the availability of system functionality is to implement redundant system components in the design together with a mechanism to detect failures and switch in the redundant units when necessary. Of course, the addition of multiple redundant components adds weight, cost, and complexity to the overall spacecraft design. Therefore, the redundant component approach to assuring system function availability should be used selectively, concentrating on those system functions that are most vital.

II. A Functional Partition Model

The top level system function partitioning model depicted in figure 1 partitions the SSF system functions into three groups. The partitions are based upon the relative consequences to SSF resulting from loss of a system's function. The determination of the consequences of the loss of system functionality must consider a number of factors:

1) SSF systems are being designed to be maintainable on-orbit. Thus, system functionality can be restored by maintenance action by the crew.
2) Although SSF is being designed to be a permanently manned spacecraft, it will spend long periods of time in an unmanned state before Permanently Manned Capability (PMC) is achieved.

3) Some of the systems listed above perform functions that are vital for the SSF to survive as an orbiting spacecraft. Others, though necessary for SSF mission success, do not pose immediate catastrophic consequences to the spacecraft if the system's functional capability were lost.

For example, a loss of the GNCP system would result in the inability of the spacecraft to maintain attitude determination and control, thus leading to the inability to point solar arrays for power generation, point communication antennas for acquisition of TDRSS satellites, and place SSF in a stable attitude for shuttle docking. During unmanned operations such a function loss would be especially critical and could jeopardize station survival, since the next maintenance opportunity could be months away. On the other hand, loss of the PES system would hamper payload operations and endanger mission performance, however, as long as the other SSF system functions are being performed the PES could be restored to operational status through crew maintenance action at the next available opportunity.

A major functional partition in figure 1 is that between payload operations and core system functions. The payload operation functions are those that are necessary to keep the SSF payload compliment running and fully provided with facility services. The core system functions are those functions that are needed to keep SSF operating as an orbiting manned laboratory.

The core systems can be further partitioned into a set of essential functions needed for spacecraft survival and a set of spacecraft facility functions that support manned operations. As shown in figure 1, the essential system functions needed for spacecraft survival include the Electric Power System (EPS). Without electrical power, of course, no avionics function can be performed. GNCP system functions are also in the essential functions set. Without maintenance of spacecraft attitude it would be impossible to point the EPS solar panels correctly, dock the orbiter to the station, or to reboost the station to maintain orbital altitude. In order to keep the avionics system operating, the various avionics components must be kept within their operating temperature range. Therefore, the Thermal Control System (TCS) function must also be included in the set of spacecraft essential functions.

Together, the EPS, GNCP, and TCS systems alone can maintain the spacecraft in a stable orbital state for a few days. If the SSF were unmanned, in order to maintain a stable state over a longer period of time it would be necessary for ground controllers to communicate with the operating systems onboard. For example, synchronizing reboost activity with orbiter rendezvous plans and moving the Station to docking attitude would require ground commanding. Therefore, the Communication and Tracking System (CTS) must also be added to the set of spacecraft essential functions. However, it should be noted that only the S-band functional capability of CTS is really needed in this minimum set of survival functions. The Data Management System (DMS) is fundamental for any avionics function to be performed and therefore must be included in the set of spacecraft essential functions also. Those core system functions not included in the spacecraft essential function set in figure 1 are placed in the set of system functions needed to provide important laboratory facility capabilities. Included in the spacecraft facility functions are those system functions needed to conduct robotic servicing of truss mounted system components and the movement of equipment and payloads exterior to the pressurized modules. The man critical systems depicted in figure 1 are those that maintain the pressure, temperature, humidity, and breathable atmosphere aboard SSF and provide the general support services needed for manned operations, both inside and outside of the pressurized modules.

III. A Channelized Architecture

Each of the core systems is being designed with redundant components such that failure of a single component will not terminate performance of the system's function. For the systems performing spacecraft essential functions there will be triple component redundancy so that the system will continue to perform its functions even with two component failures.

An additional consideration in the design of SSF systems is that all system components depend upon power, data, and thermal resources and services. Therefore failures in EPS, DMS, or TCS components could propagate throughout other spacecraft systems. In order to prevent this from happening the core systems will implement a channelized design approach for connectivity of power, data, and thermal resources to core system components. In this channelized approach each core system has its components connected to form fault containment domains that resist propagation of a fault from one domain into the others.

A system performing a spacecraft essential function will have a minimum of three fault containment domains such that no two failures can disable the system from performing its functions, i.e. the system is two failure tolerant. The remainder of the core system functions, i.e. the spacecraft facility functions in figure 1, will be channelized into a minimum of two fault containment domains each, thus making them one failure tolerant systems.

Figure 2 illustrates how system components will be channelized into fault containment domains. In this case the fault containment domains for GN&C are depicted for the attitude determination function. The attitude determination function requires that the GN&C process control computer be connected to at least one Star Tracker (ST) or an Inertial Sensor Assembly (ISA). GN&C actually has four fault containment domains with respect to its own components, data bus connections, and power supplies. With respect to thermal services there are three fault containment domains since the Moderate Temperature Loop (MTL) of the TCS cools EPS equipment for power buses 3 and 4. Thus from the figure 2 diagram it can be shown that there is no combination of two failures, either in GN&C components or power, data, or thermal connections, that would result in loss of the essential attitude determination function.

IV. Failure Protection at the System Control Level

Each of the core systems is controlled by computer programs executing in one of four SDPs. Figure 3 depicts the four computers and their power, data, and thermal connectivity. In order to maintain core system failure tolerance the controlling computers must have power, data, and thermal connectivity that is two failure tolerant.

There will be eighteen buses used for data connection of core system components to the controlling SDPs. Each of the four SDPs will be connected to all eighteen data buses therefore allowing any of the four SDPs to run any core system's control program.

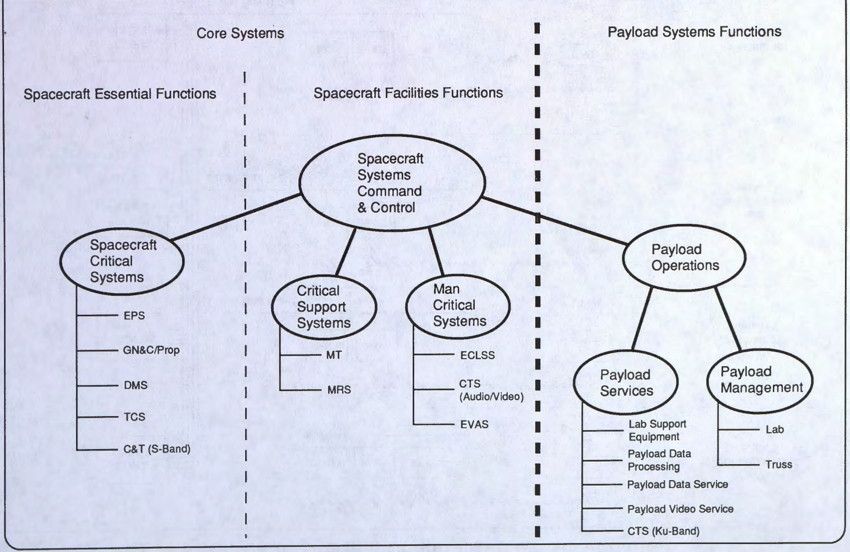
In order to protect against power failures each SDP will have at least two separate sources of power. In addition, three separate cooling loops will provide heat dissipation to the four computers.

The net result of the design for the core system control computers will be that no two failures of SDPs or their power, data, or thermal connections will result in loss of core system control processing. Therefore, the design will compliment the robust fault containment architecture for the each of the core systems.

V. Conclusion

The SSF avionics system design provides a resilient survival capability for the spacecraft where essential functions are at least two failure tolerant. A channelized architecture includes provisions for protection against failures in power, data, and thermal resource distribution to system components. The core system control computers are designed to assume control of any core system and are also protected from failures in power and thermal distribution channels.

Top Level SSF System Function Partitioning Model



Core Systems

Payload Systems Functions

Spacecraft Essential Functions

Spacecraft Facilities Functions

- Spacecraft Systems Command & Control
  - Spacecraft Critical Systems
    - EPS
    - GN&C/Prop
    - DMS
    - TCS
    - C&T (S-Band)
  - Critical Support Systems
    - MT
    - MRS
  - Man Critical Systems
    - ECLSS
    - CTS (Audio/Video)
    - EVAS
  - Payload Operations
    - Payload Services
      - Lab Support Equipment
      - Payload Data Processing
      - Payload Data Service
      - Payload Video Service
      - CTS (Ku-Band)
    - Payload Management
      - Lab
      - Truss

Figure 1

Power, Data, Thermal Channelized GN&C Function

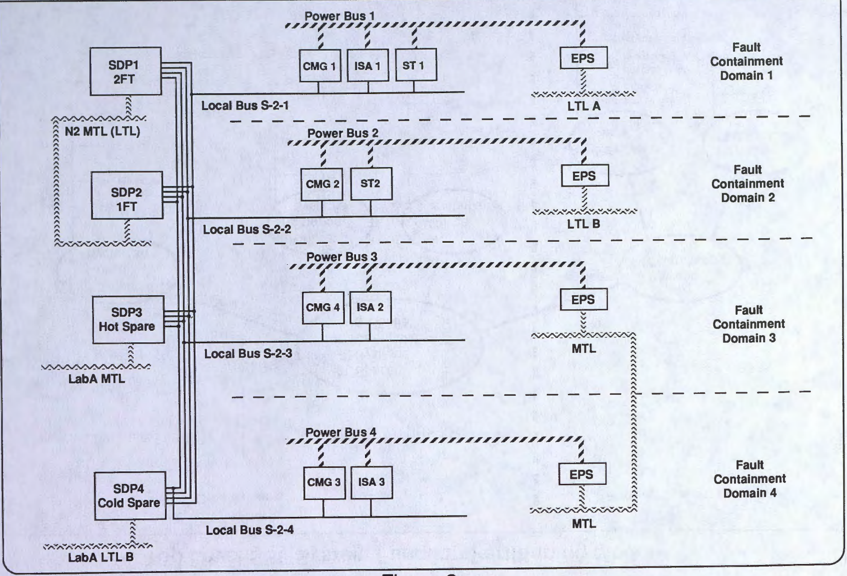
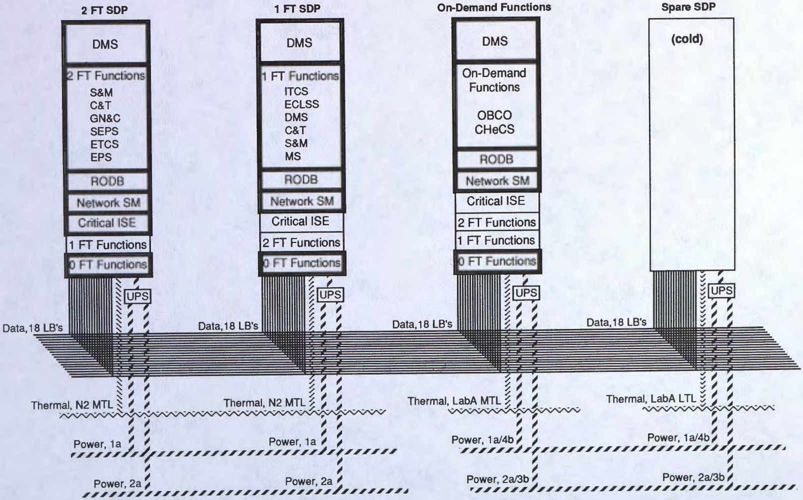


Figure 2

Two Failure Tolerant and One Failure Tolerant SDP Functions and Connectivity



- **Bold boxes indicate active functions in SDPs**

Figure 3