FAULT PROTECTION DESIGN OF THE QUIKSCAT AND SEAWINDS INSTRUMENTS

Matthew B. Bennett, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA
Joseph F. Smith, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA
William B. Wilkinson, Federal Data Corporation, Pasadena, CA

Abstract

The QuikScat and SeaWinds instruments are radar scatterometer instruments that will be used to measure ocean surface winds. The QuikScat instrument will be launched on a dedicated spacecraft in November 1998, and the SeaWinds instrument will be launched on the Japanese ADEOS-II spacecraft in the summer of 2000.

The instrument is designed to continuously operate in wind observation mode for nearly the entire three year mission. However, a number of fault and external conditions can occur that will interrupt the instrument's continuous wind observations. These types of faults include failures in the radar unit's TWTA, communication errors between the instrument's three subsystems, software errors in the computer subsystem, and possible effects of cosmic ray or solar induced single event upsets on the instrument electronics.

In general, the philosophy of the instrument's autonomous fault protection is to perform different levels of resets in order to clear the fault for each particular type of problem. In general, the instrument attempts to recover from the fault in a manner that will allow the instrument to resume normal operations without ground intervention. However, if the autonomous algorithms in the instrument do not clear the fault with a reasonable level of effort, then the instrument places itself into a safe standby mode and waits for ground interaction. In no case does the instrument attempt to recover from faults by switching redundant units. The switching of redundant units will only be performed under command and control from the ground.

This paper describes the various fault protection mechanisms that have been designed into the spacecraft to react to selected faults and failures in the instrument. In addition, it explains how these mechanisms escalate their response when a fault is not cleared by their initial recovery attempt. Also, this write-up describes the actions that the spacecraft will take on behalf of the instrument in the case of a spacecraft bus failure that will require the shutdown of the instrument.

Background

The QuikScat and SeaWinds instruments are scatterometer microwave radar instruments. They are designed to provide a measurement of ocean surface wind velocity over 90% of the earth's ice free oceans every two days. The instruments will be operated continuously to provide global, long term wind vector data. The data will be used in the study of ocean circulation, climate, and air-sea interactions, and in weather prediction. Present plans are for two SeaWinds instruments to be flown in the next two years. The first instrument (SeaWinds on QuikScat) will fly on the dedicated QuikScat spacecraft launch in November of 1998. This instrument is a replacement for the successful NSCAT instrument which was lost due to a ADEOS-I spacecraft failure on June 30, 1997. A drawing of the QuikScat spacecraft appears in Figure 1,

below. The second SeaWinds instrument (SeaWinds on ADEOS) will be launched with four other instruments on the Japanese ADEOS-II spacecraft in the summer of 2000. A drawing of the ADEOS-II spacecraft appears in Figure 2, below.

Each instrument consists of three separate subsystems (see Figure 3 at the end of this paper). Each subsystem is backed up by a fully redundant unit. The Scatterometer Electronics Subsystem (SES) consists of

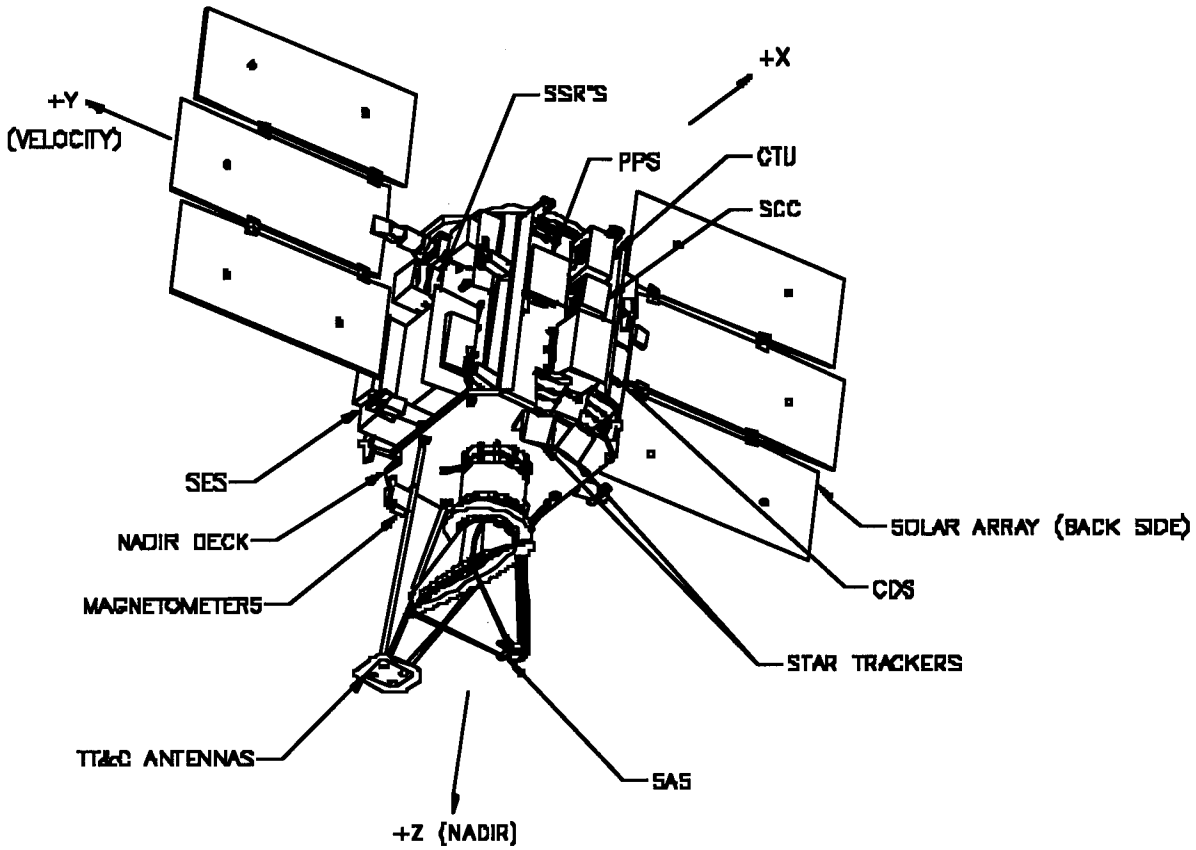
- the radar transmitter,
- the receiver,
- the traveling wave tube amplifier (TWTA), and
- the radar signal processing and control electronics.

The SeaWinds Antenna Subsystem (SAS) consists of

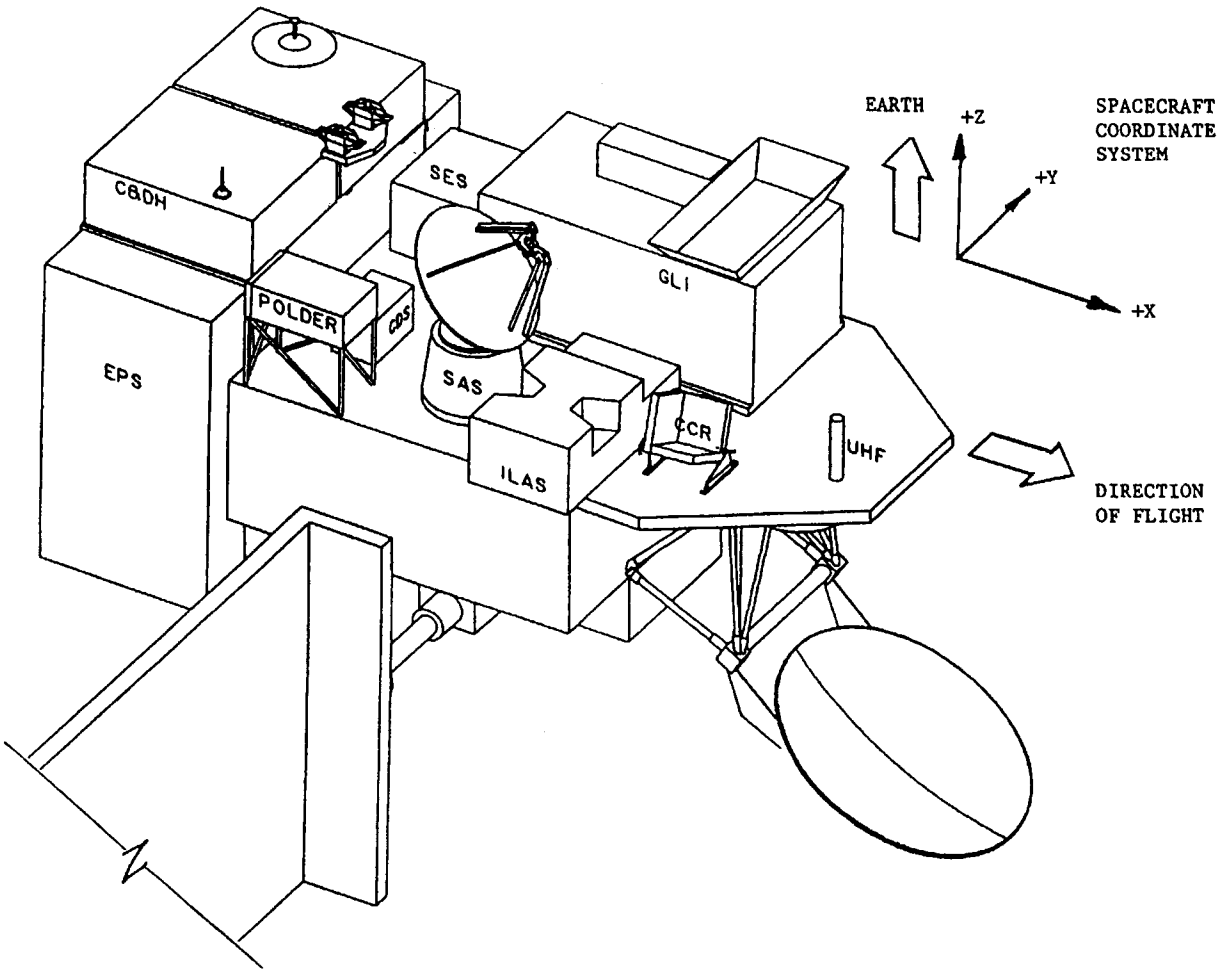
- the radar antenna,
- the spin motor, and
- the motor control and monitoring electronics.

The Command and Data Subsystem (CDS) is the command, control, and data handling center for the instrument, and the command, telemetry, and power interface with the spacecraft.

The differences between the QuikScat & SeaWinds versions of the instrument include the interfaces to the spacecraft for command, telemetry, power, and switching, and the addition of survival heaters for QuikScat.



QUIKSCAT SPACECRAFT
NADIR VIEW
FIGURE 1



ADEOS-II SPACECRAFT
FIGURE 2

General Fault Protection Approach

The instrument and the spacecraft incorporate a variety of fault protection features with the primary objectives of: (i) avoiding permanent damage or degradation to the instrument, and (ii) avoiding disruption of normal operations, to the instrument itself, or to the spacecraft. Efforts are made to minimize the loss of science data. In no case is autonomous action taken to swap to redundant units.

Hardware Provided Fault Protection

Hardware Under-Voltage Trips

Each subsystem element (SES electronics, TWTA, CDS, and SAS) has hardware under-voltage trip and reset features. Each subsystem power supply resets and inhibits its operation when its input voltage falls below specified trip levels. Also, the spacecraft shuts down the instrument electronics if the spacecraft bus voltage drops below the undervoltage trip point. The QuikScat spacecraft performs the shutdown by removing power from the payload electronics bus and automatically supplying it to the instrument survival heaters. The ADEOS-II spacecraft accomplishes it by switching the instrument power relays to the thermal safe mode configuration. Thermal safe mode consists of all subsystem electronics switched off, and all subsystem replacement heaters turned on. A 2 out of 3 voting relay configuration is used to

protect against a single failure in the thermal safe mode relays.

TWTA Hardware Safing

The TWTA hardware removes high-voltages and prevents RF transmission in response to anomalous TWTA under-voltage and over-current conditions. The TWTA responds to these anomalous conditions by entering a reset mode that removes the high voltages for a cathode warm-up period (approximately 210 seconds). For undervoltage conditions, the warm-up period is not started until the input voltage returns to normal levels.

SAS Hardware Spin Inhibit

The SAS antenna is mechanically caged during launch. The SAS electronics contain a stall enable feature that prevents continuous application of power to the drive motor when in the caged configuration.

Memory Integrity Protection

An error detection & correction code protects the CDS RAM memory against single bit errors like those caused by radiation induced single event upsets (SEUs). If a single bit error is detected during a read of a memory location, then the hardware automatically corrects the data, and rewrites it to the proper memory location.

To insure the integrity of parameters in SES RAM memory, the CDS automatically resends operating parameters to the SES at the beginning of each telemetry packet cycle. The SES processor executes software from radiation hard PROM to provide additional protection against SEUs.

Internal Computer Fault Monitoring

The CDS and SES computers provide internal fault protection for watchdog time-outs. In addition, the CDS has an algorithm for responding to missed CDS interrupts. Finally, the CDS employs a two level reset response mechanism. This mechanism attempts to restore the instrument's operating mode with a "soft" reset" before resorting to a full "hard" reset.

Watchdog Time-Out

Both the CDS and SES computers have watchdog timers. The watchdog timers countdown from a starting value of 0.5 seconds. Each timer is reset to its starting value periodically during nominal computer processing. A fault occurs if a watchdog timer counter reaches zero. A fault implies that the computer has experienced a failure that prevented it from resetting the timer. An example of such a fault is an infinite loop caused by an error in program memory.

In response to a watchdog time-out, the corresponding subsystem resets itself and attempts to continue normal operations. The CDS will perform a "soft" reset in response to a watchdog time-out. After it is complete, the CDS will continue operations in the current mode with the current set of variable parameters. The SES will perform an SES reset in response to a watchdog time-out. After it is complete, the CDS will (per normal operations) reload the SES with parameters and continue operations in the current mode.

Missed Interrupt Faults

Missed interrupt fault protection protects against CDS hardware and software failures that cause processor overruns or any other malfunction that prevents CDS from servicing interrupts in the expected order. The CDS services interrupts using a polling mechanism. The interrupts nominally occur in a deterministic order. If the CDS detects that an interrupt is asserted out of order, it is counted as a missed interrupt. If the missed interrupt count during a telemetry packet is nonzero and less than the fault threshold, then the CDS assumes that the cause is a power on transient. In this case, the CDS resets the SES to resync it to the CDS. If the number of missed interrupts is equal to the fault threshold or greater, then the CDS assumes there is CDS software problem, and performs a "soft" reset.

CDS Two-level Reset Processing

The CDS flight software implements two levels of resets: a "soft" reset and a "hard" reset.

The purpose of the "soft" reset is to provide a graceful recovery from faults. The

"soft" reset returns the instrument to the operating mode and state that was in effect when the reset occurred. Flight software code is reloaded from PROM, but critical variables needed for restoring the instrument operating state are retained. Also restored are ultra-critical variables that provide error diagnostic telemetry. Variables are restored using a 2 out of 3 voting scheme. If all three copies disagree, then default values are loaded. The events that can cause a "soft" reset are

- A "soft" reset command from the spacecraft,
- A missed interrupt fault,
- A multiple SES data error fault,
- A multiple SAS data error fault, or
- A CDS watchdog time-out.

The purpose of the "hard" reset is to attempt an autonomous last resort recovery from a fault. This is accomplished by the CDS forcing a "hard" reset after the third "soft" reset within 5 minutes. Hard reset processing makes no attempt to restore the instrument operating mode. The instrument is initialized to standby mode. If the TWTA was on when the "hard" reset occurred, the TWTA will still be powered when the instrument goes to standby mode. However, the TWTA is safe because the instrument is in standby mode, and the SES will not be transmitting. Software is reloaded from PROM and only the ultra-critical variables are restored. The events that can cause a "hard" reset are

- A CDS hardware power on reset,
- A CDS unrecoverable operating system fault, and
- 3 CDS "soft" resets within 5 minutes.

CDS Provided Fault Protection

The CDS software provides for the detection of errors, the recovery, and the safing of the instrument, in response to the anomalous conditions described below.

TWTA Initialization/Reset Faults

A TWTA fault protection trip is caused by either an undervoltage or overcurrent condition within the TWTA. The CDS periodically monitors the SES engineering telemetry status word for the presence of TWTA trips. For persistent TWTA trips, the CDS immediately turns off the TWTA and commands the instrument to standby mode. Intermittent trips are handled by the TWTA internally. The TWTA resets to its nominal power on state 210 seconds after a single trip. Intermittent trips may be seen at initial turn on. Outgassed contaminants released by launch vibrations could cause such trips.

CDS performs the following processing to filter out intermittent trips. Upon detection of a trip, the CDS increments a trip counter. The CDS increments the counter every cycle that a trip condition exists. If a trip condition is not present during a cycle, then the CDS decrements the trip counter. The CDS executes the recovery response if the trip counter reaches the persistence threshold.

Low TWTA Drive Power Faults

The CDS monitors the TWTA drive power during transmissions in order to protect the TWTA from the adverse effects of low drive power. If the TWTA drive power persists below the fault threshold, then the CDS disables the TWTA grid in all instrument modes to protect the TWTA from low drive power. Also, the CDS transitions to receive only mode to insure transmissions are stopped. The SES and TWTA are left in their faulted power configuration to allow the ground to diagnose the fault.

SES Supplemental Heater

The SES supplemental heater is used to warm the SES when the TWTA is unpowered. The CDS automatically turns the SES supplemental heater off during transitions to modes that require the TWTA to be powered on. This protects against the ground forgetting to unpower the heater. The SES supplemental heater may cause an SES over temperature fault if it is left on while the TWTA is powered.

Missing Equator Crossing Fault

The spacecraft sends an equator crossing signal to the instrument once per orbit when it crosses the ascending node. The CDS maintains an orbit step counter which is reset when it receives this signal. CDS uses the orbit step counter to index into tables of radar parameters that are orbit position dependent. These parameters are doppler and range coefficients

used to compute the transmit frequency and receive gate delay.

If the spacecraft does not send the equator crossing signal to the instrument, the orbit step counter overflows and rolls over. When the orbit step counter rolls over, it points to the first entry in the doppler and range coefficient tables. CDS continues to operate using these doppler and range table entries. CDS also continues to increment the orbit step counter. If an equator crossing signal is still not received upon the counter reaching the second orbit step, then the CDS reports a missing equator crossing error in telemetry, and continues operations as normal.

If the equator crossing signal fails permanently, then the CDS has an alternate mechanism for resetting the orbit step. The instrument can be commanded to estimate the orbit period and reset the orbit step automatically. This mechanism can also reset the equator crossing time in response to synchronization commands sent by the operations team. These commands can be transmitted as often as necessary to maintain the required orbit step accuracy.

Subsystem Communication Errors

The CDS monitors its communication with the SES and SAS subsystems for data errors. If possible, the CDS resets the subsystem having the problem. If the errors do not clear within a defined period of time, then the CDS assumes the CDS flight software is at fault, and performs a "soft" reset.

SES Data Errors

The CDS detects an SES data error when the SES sends an incorrect amount of data to the CDS within the prescribed time period. The SES should return a deterministic amount of data to the CDS for each command and engineering telemetry request. Data corrupted by transmission anomalies or parity errors are dropped by the CDS hardware. When too few data are received, the CDS cannot determine which data were not received. The CDS treats the data received as if it is in the expected order and puts that data in telemetry. However, it marks the remaining positions in telemetry (where data should have gone) with error codes.

Multiple SES Data Error Faults

A multiple SES data error fault is defined as at least 8 different SES data errors during a telemetry packet. At the first occurrence of this fault, the CDS resets the SES the end of the telemetry packet. In the case that the SES may have experienced a POR or a watchdog time-out, the CDS waits for the fifth telemetry packet, and checks again for the fault. If the fault persists in the fifth telemetry packet, the CDS assumes the fault lies within itself, and initiates a "soft" reset.

SAS Data Errors

The CDS detects a SAS data error when the SAS sends an incorrect amount of antenna position data to the CDS within the prescribed time period. SAS data errors are handled like SES data errors with the following additions. The CDS uses the antenna position to compute the SES doppler shift and receive gate delay. In the case of a SAS data error, the CDS estimates the antenna position based on the last valid SAS antenna position data. Upon returning from a POR, the CDS initializes the antenna position to zero until a valid input is received from the SAS.

Multiple SAS Data Error Faults

A multiple SAS data error fault is defined as at least 8 different SAS data errors during a telemetry packet. In the case that the SAS may have experienced a POR, the CDS waits for the fourth telemetry packet, and checks again for the fault. If the fault persists, the CDS assumes the fault lies within itself, and it initiates a "soft" reset.

SES Single Event Upset Faults

The SES may experience SEUs when the spacecraft flies over the South Atlantic Anomaly. The CDS uses a countdown timer to reset the SES periodically for automatic recovery from these potential SEUs. The countdown timer is restarted at each ascending node crossing. The default value for the countdown duration is the time it takes the spacecraft to cover 75% of an orbit. This duration results in an SES reset once per orbit over the South Pole.

Spacecraft Provided Fault Protection

The ADEOS-II and QuikScat spacecraft provide fault protection to the instrument for spacecraft faults and for monitoring selected instrument analog measurements.

Spacecraft Faults

QuikScat Undervoltage Response

The QuikScat spacecraft removes power from the payload bus when the spacecraft bus experiences an undervoltage fault. Powering off the payload bus turns off all instrument electronics and replacement heaters. When the payload bus is unpowered, the spacecraft automatically applies power to the instrument survival heaters through a separate power interface.

SeaWinds Light Load Mode Response

The ADEOS-II spacecraft will command the instrument to thermal safe mode in response to anomalous spacecraft conditions (e.g., spacecraft bus under-voltage, loss of attitude control). The instrument thermal safe mode powers all instrument subsystem electronics off and all replacement heaters on.

Spacecraft Response to Instrument Faults

Temperature Measurement Monitors

The spacecraft monitors selected instrument passive analog temperature measurements. The spacecraft responds to all out of bounds conditions (a temperature too high or too low) by first commanding the instrument into standby mode. The spacecraft then powers off the subsystem with the out of bounds condition, and turns on its replacement heater. If the subsystem with the out of bounds condition is the CDS, then the entire instrument is commanded to thermal safe mode.

SeaWinds Spin Rate Monitor

In addition to temperature measurements, the ADEOS-II spacecraft monitors the SAS antenna spin rate. The spacecraft responds to an out of bounds spin rate condition by

- Commanding the instrument to standby mode,
- Powering off the SAS electronics, and
- Turning on the SAS replacement heater.

Conclusion

A spacecraft instrument fault protection design has been implemented with the following key features:

1) A fault response escalates the scope of its response if its first attempt to recover from a fault is unsuccessful.

2) The actions taken for a fault response depends on whether the instrument health may be at risk.

3) If the instrument health may be at risk:

   - A fault response is chosen that maximizes the safety of the instrument. Protection of science data is a lower priority.

4) If the instrument health is not at risk:

   - The fault response attempts to restore the instrument's operating mode, parameters, and nominal science data collection.
   - The first response chosen is the one with the smallest impact to nominal instrument operations.
   - Instrument safing and discontinuation of nominal operations is taken as the response of last resort.

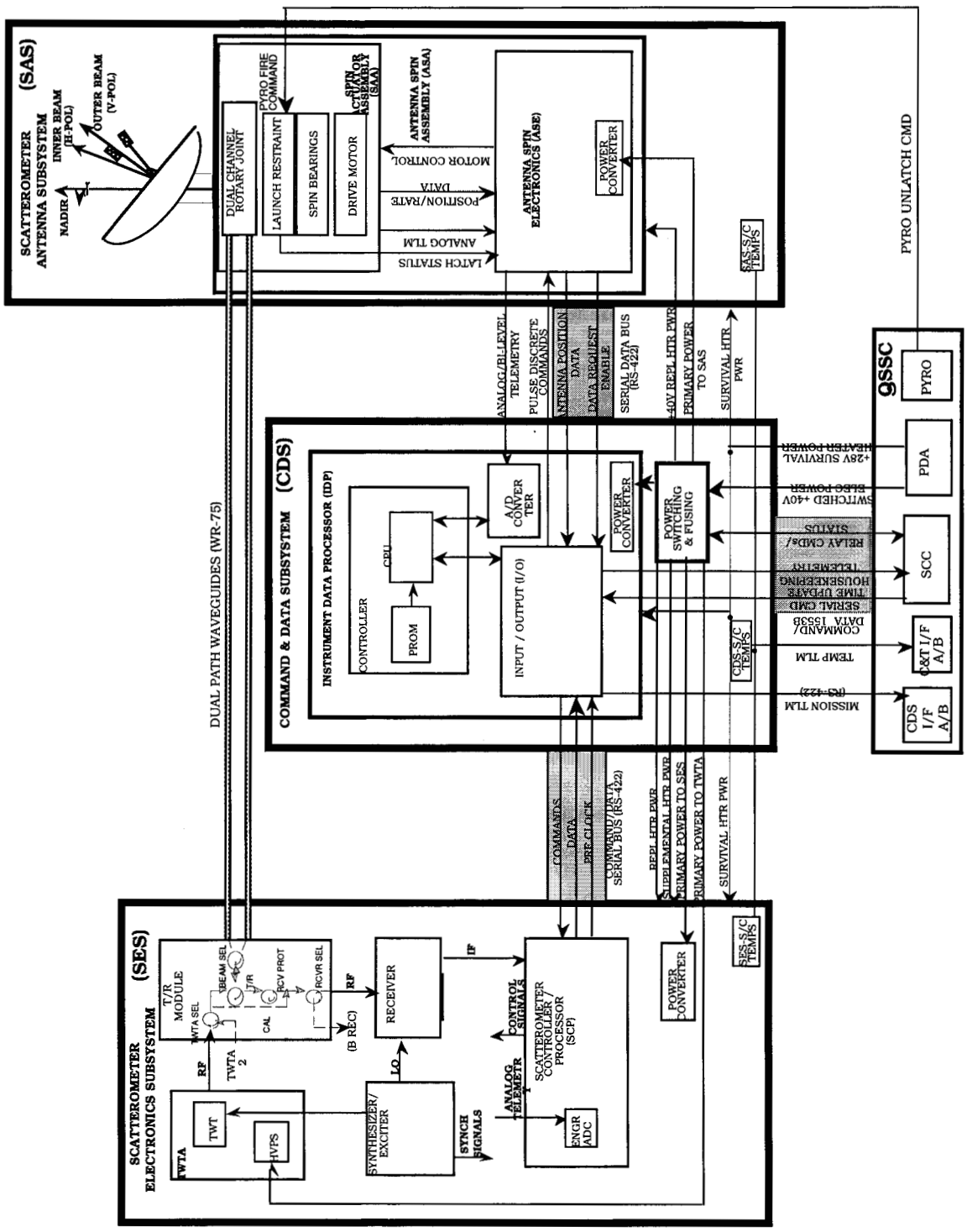


Figure 3. QuikScat Scatterometer Block Diagram