VIKING LANDER DESIGN AND SYSTEMS INTEGRATION

John Goodlette
Martin Marietta Corporation

MR. GOODLETTE: Good Afternoon. I want to address something generally on the subject of integration today, but one which I believe that you, in your deliberations, will eventually face. That is the subject of malfunction protection. There is a dilemma that is there for us all: to return the maximum amount of scientific data that we can, while choosing allocations of our resources to guarantee to the best of our ability to be able to return what we set out for.

Viking is pretty complicated. Many of you are participants on Viking or have been at some point in its development. I will try to address today the question of redundancy. I will describe the principles that we have used for Viking; give you a few examples of some of the implementation; what is not protected and why; and draw the conclusions relative to the effects of this on your mission planning and even on your system test programs.

In your deliberations, as I have noticed today, you very properly were paying attention to those things relative to the science objectives and then the mission design. But when you decide the system that will, in fact, get you there (and you have a very difficult problem I believe, in choosing a common threat to the system that is a multiple planet investigation), you will face the question of how much redundancy should be planned, and how it should be mechanized in order to maximize the chance of getting the data back.

In other words, you want to give yourself a way out in the presence of failure, particularly when you are flying a mission. The things you work with are the same things that we have had to

work with: our resources limit, the weight, the power, the money and the data capacity. We chose to follow a principle which goes back to the basic objective of Viking: to land on the planet and acquire data from the surface. Therefore, the first principle in our redundancy was to guarantee the ability to land so that we could provide the data return from the post-landed scientific experiments and, while entering, to acquire atmospheric entry data. We also chose to require most of the decisions, if possible, to be made by the man on the ground, and to have the spacecraft be as simple as possible. This same principle led to the protection of the downlink, which is, of course, the real method by which we get the data back.

Today, I am going to show you a few examples of some subsystems and how we chose to mechanize them. We also used other constraints which you have discussed. They are very real and very important. We tried to limit ourselves to what was available in current technology or, if it wasn't there, to apply our resources to developing it before we mechanize it into a major space system.

Could I have the first slide, please? This is a pretty standard looking fully-redundant RCS reaction control. (Figure 4-12).

On Viking, we do the deorbit impulsive maneuver for the lander system and the attitude control down to the point of deploying the parachute with a single hot gas system. It uses hydrazine, is mechanized with 16 eight-pound thrust engines (which you see at the bottom of the chart there), and it is fully redundant with series valves at each engine. It can tolerate single failures at any point. I will note in passing that we did not try to protect against such things as leakage or rupture of the propulsion plumbing.

The valves are mainly associated with the loading of the gases and the propellants and the necessary unloading in the event we have to recycle after terminal sterilization at the Cape.

RCS DEORBIT PROPULSION SUBSYSTEM

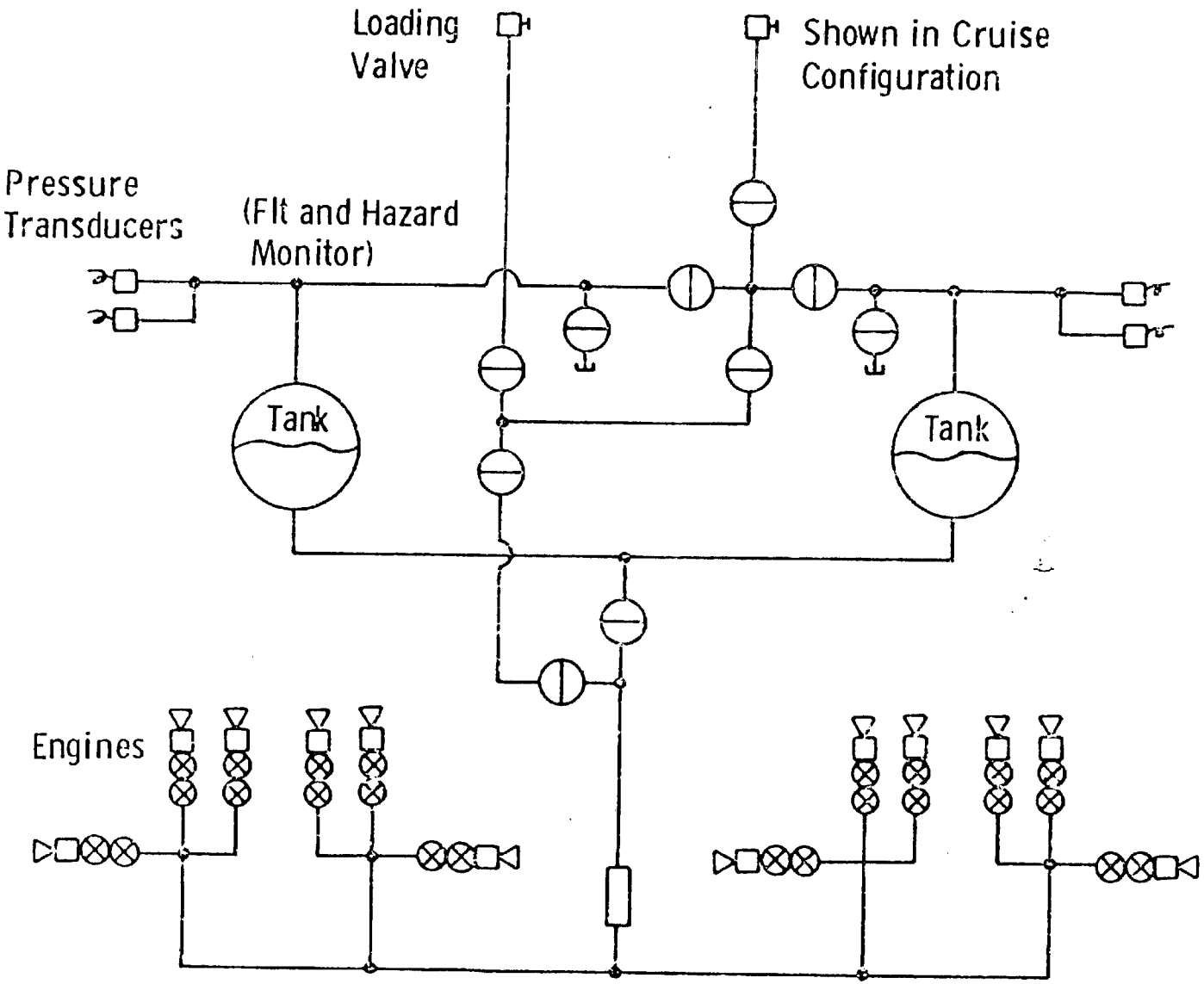


FIGURE 4-12

Figure 4-13 schematically presents the Thermal Control System. We made an attempt to keep the thermal system as passive as possible, but it does have some active elements. There are two active thermal switches mounted immediately under the two RTG's which serve as the only power source the lander has after it separates from its orbiter bus. We do use the orbiter power, of course, with its 680 watt solar array, in the cruise mode and the pre-separation checkout. But after transfer to lander internal power, RTG's are all we have. We use the waste heat from the RTG through the thermal contractors.

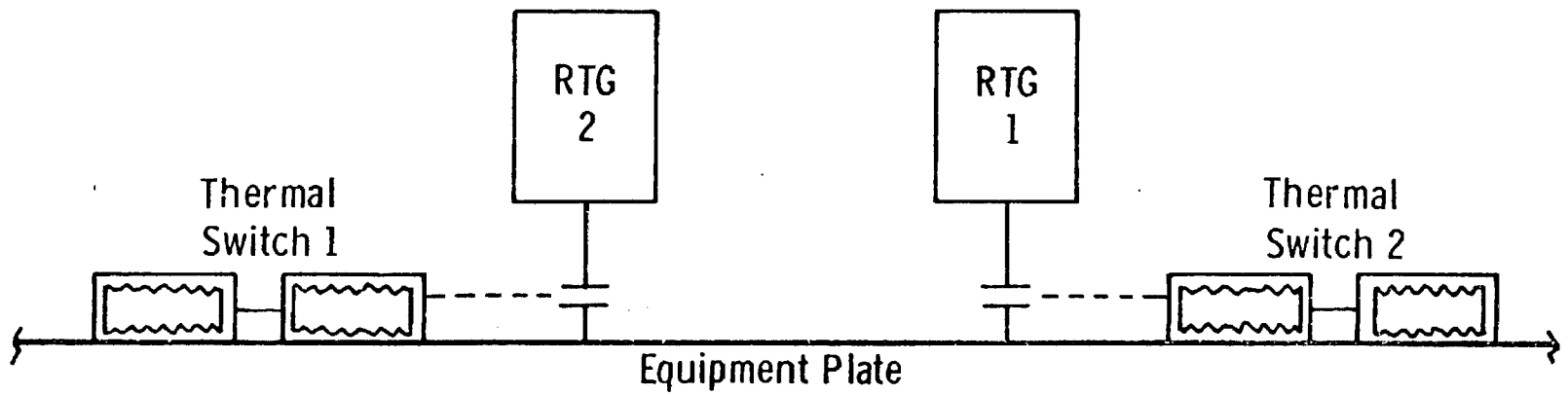
You will notice that it is mechanized with redundant bellows to protect and guarantee no single failure will lose us the contact.

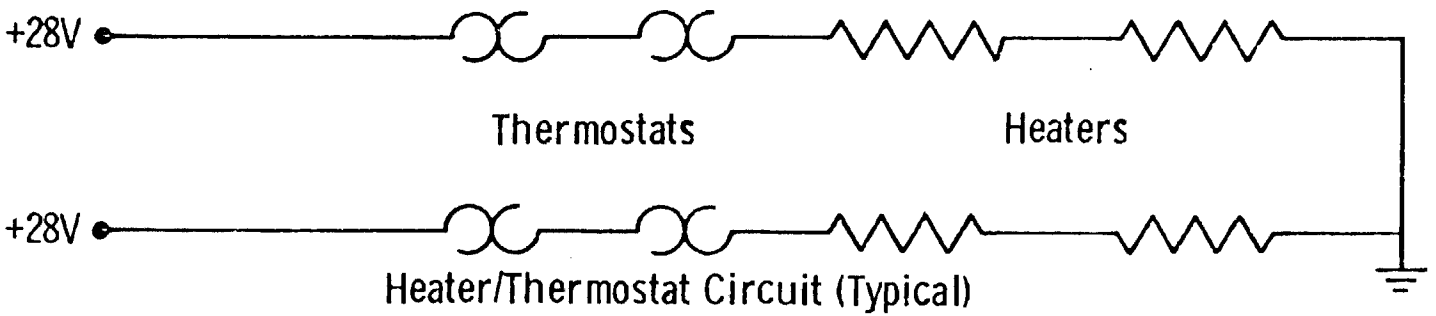
I might say that the chart seems to imply that we can tolerate the loss of one thermal switch. That isn't really true, unless we were very lucky with respect to some of the atmospheric environments in the summer on Mars. We need both of those switches.

The bottom of the chart describes a pretty standard way of mechanizing thermostats and heaters through series parallel thermostatis switches. We do not try to protect against shorts, generally, in the system, but we do protect against failure open and failure closed in the thermostats. Raw bus power is used for line and tank heaters in the propulsion system, which is on the cold side of the spacecraft on its transit outward from earth to Mars. The lander is opposite side from the sun with respect to the orbiter and, therefore, gets relatively cold.

The deorbit system is mounted on the aeroshell and the terminal engine system is mounted on the lander. Both of them are dry beyond the isolation valve and, therefore, it is necessary to use heat to protect some of the feed lines into the deorbit system, some of the pyro valving, and to keep the propellant itself above the freezing point of hydrazine, which is about 35 degrees Fahrenheit.

THERMAL CONTROL SYSTEM - ACTIVE ELEMENTS





Heater/Thermostat Circuit (Typical)

Usage: All Propulsion Tanks (4 Circuits)
Deorbit Feed Lines (1 Circuit)
Terminal Engine Pyro Valve
Deorbit Feed Line Back-Up Circuit (New)
(BPA Bypass)

No Exceptions to Policy In Heater/Thermostat Circuits

FIGURE 4-13

As shown on Figure 4-14, pyrotechnics is straightforward. We use two independent energy sources off the bus through two pyrotechnic control assemblies, the LPCA's as noted in the chart. The mechanization is fairly standard in that they are enabled, then they are commanded, and then disabled, all by the computer functions through the guidance computer.

We use a single bridge wire squib arrangement with two initiators per end item, but we do not protect against mechanical single point failures down stream of the initiator. That is to say, there is usually only one set of nuts, one set of pin pullers, and so forth.

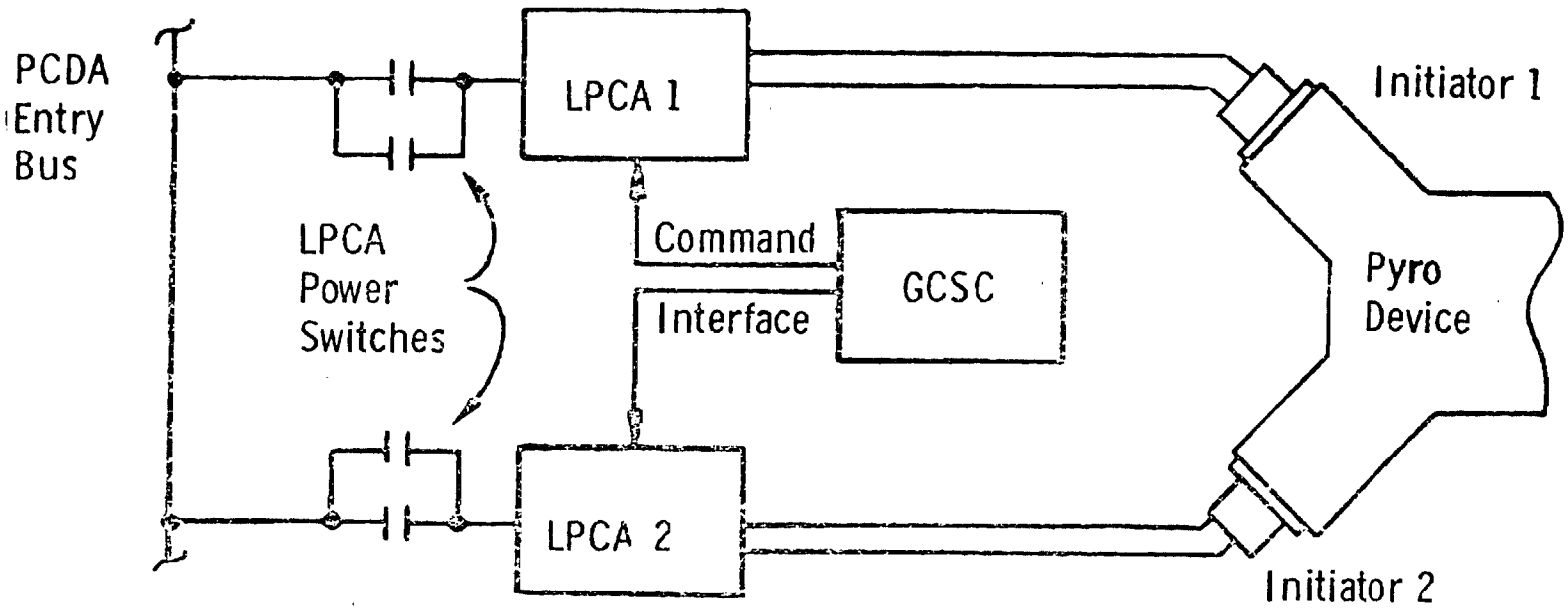
The power subsystem on Figure 4-15 is, of course, extremely important to the overall mission success. It is used both during entry and after landing.

To the left of this line is the Viking orbiter, which is based upon the Mariner technology, built by JPL and its suppliers, and we very carefully tried not to require more of the orbiter than is implicit in that Mariner technology. On the other hand, you will find, if you examine the orbiter, that their mechanization principles for redundancy are, to the best degree we are both able, identical. The orbiter supplies the power during cruise. There is a system aboard the lander called the bioshield power assembly which provides dual regulation and dual battery charging that is commandable by uplink from the ground. And that machine stays with the bioshield base, which is attached to the orbiter, and does not enter and land. And, therefore, it is the only thing in the lander system that does not have to be terminally sterilized.

The next assembly, the power subsystem outlined within this line is our power control and distribution assembly.

As you see, we use two SNAP 19 derivative RTG's in series. There is a single point failure in the cabling in between, you might

PYROTECHNIC SUBSYSTEM



15 Pyro Device Functions are Single Point Failures

FIGURE 4-14

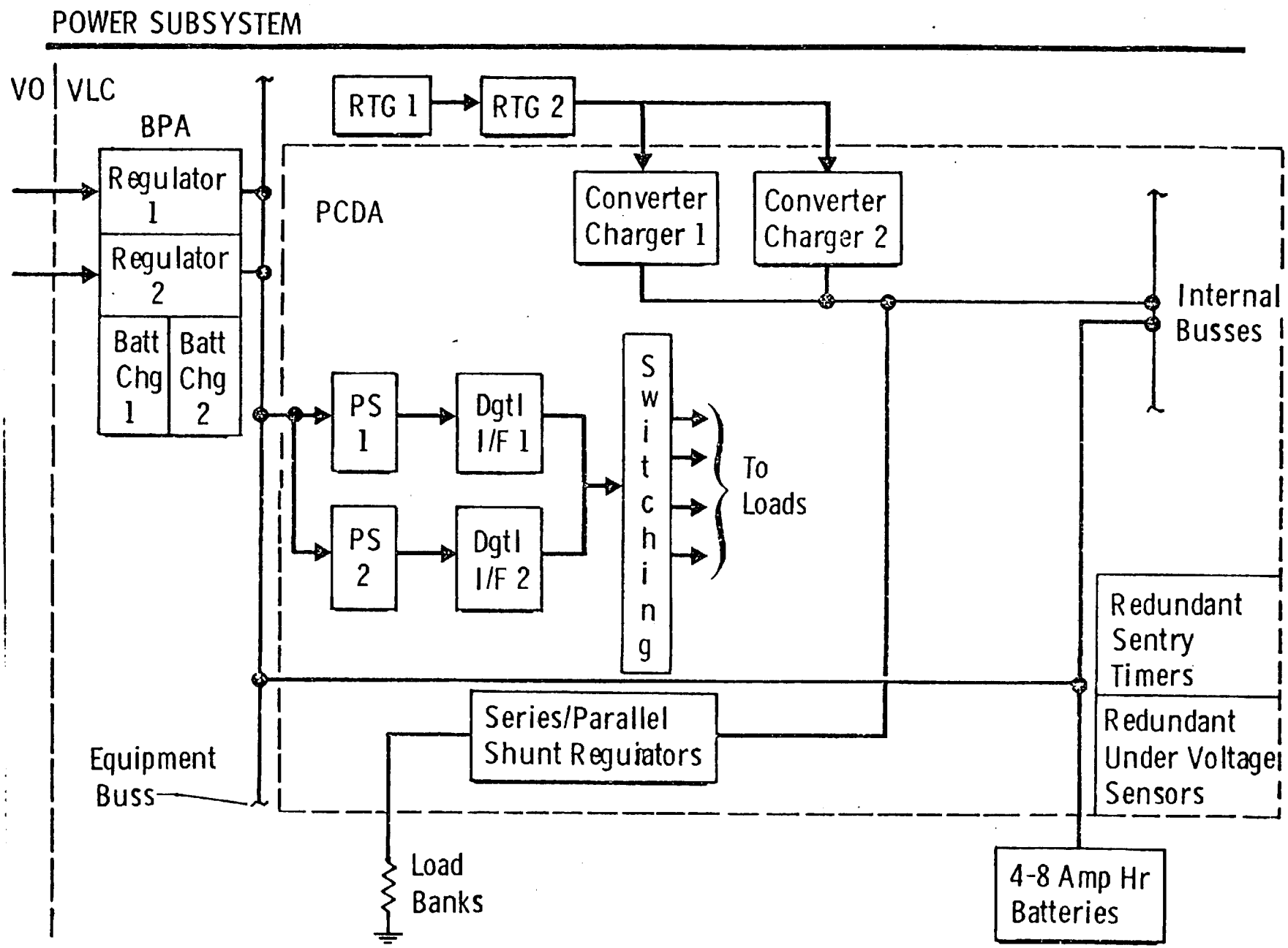

POWER SUBSYSTEM
VO
VLC
BPA
Regulator 1
Regulator 2
Batt Chg 1
Batt Chg 2
RTG 1
RTG 2
PCDA
Converter Charger 1
Converter Charger 2
Internal Busses
PS 1
PS 2
Dgtl I/F 1
Dgtl I/F 2
Switching
To Loads
Redundant Sentry Timers
Redundant Under Voltage Sensors
Series/Parallel Shunt Regulators
Equipment Buss
Load Banks
4-8 Amp Hr Batteries

FIGURE 4-15

notice. But, generally, we then go to dual converter chargers and we have series parallel shunt regulators and we are able to dissipate additional load over and above that immediately needed through lander body-mounted load banks.

We have four eight ampere hour nickel cadmium betteries. Three are required to land and two are required to survive post-land. Sterilizable batteries were a technology problem that was quite important in the beginning.

Our measured capacity after stand times of 25 months, which is somewhat more than the expected lifetime of the mission, has been just above ten ampere hours. Nickel cadmium batteries are sterilizable and one almost gets the impression that one way to make good batteries is to make them tolerate heat sterilization.

You will also notice that there is a dual path for all switching functions. There are two sets of power supplies and two sets of digital interfaces with the guidance computer, which also serves as the sequencer in the mission, both during entry and after landing.

There are two on-board decision points shown over here on the right side. There is a redundant sentry timer, and an under voltage sensor. Their function is required since the lander is out of sight of Earth after landing approximately half of the time, and one really doesn't have real time control. Their function is to place the lander in a safe condition, open the command receivers, and wait for Earth to intervene by command.

Figure 4-16 presents the guidance and control. We have to soft land, of course, on a windy planet, and that leads us to a 3-axis stabilization system. We have to transfer the reference from a celestial reference picked up from the orbiter, navigate inertially

GUIDANCE AND CONTROL SUBSYSTEM

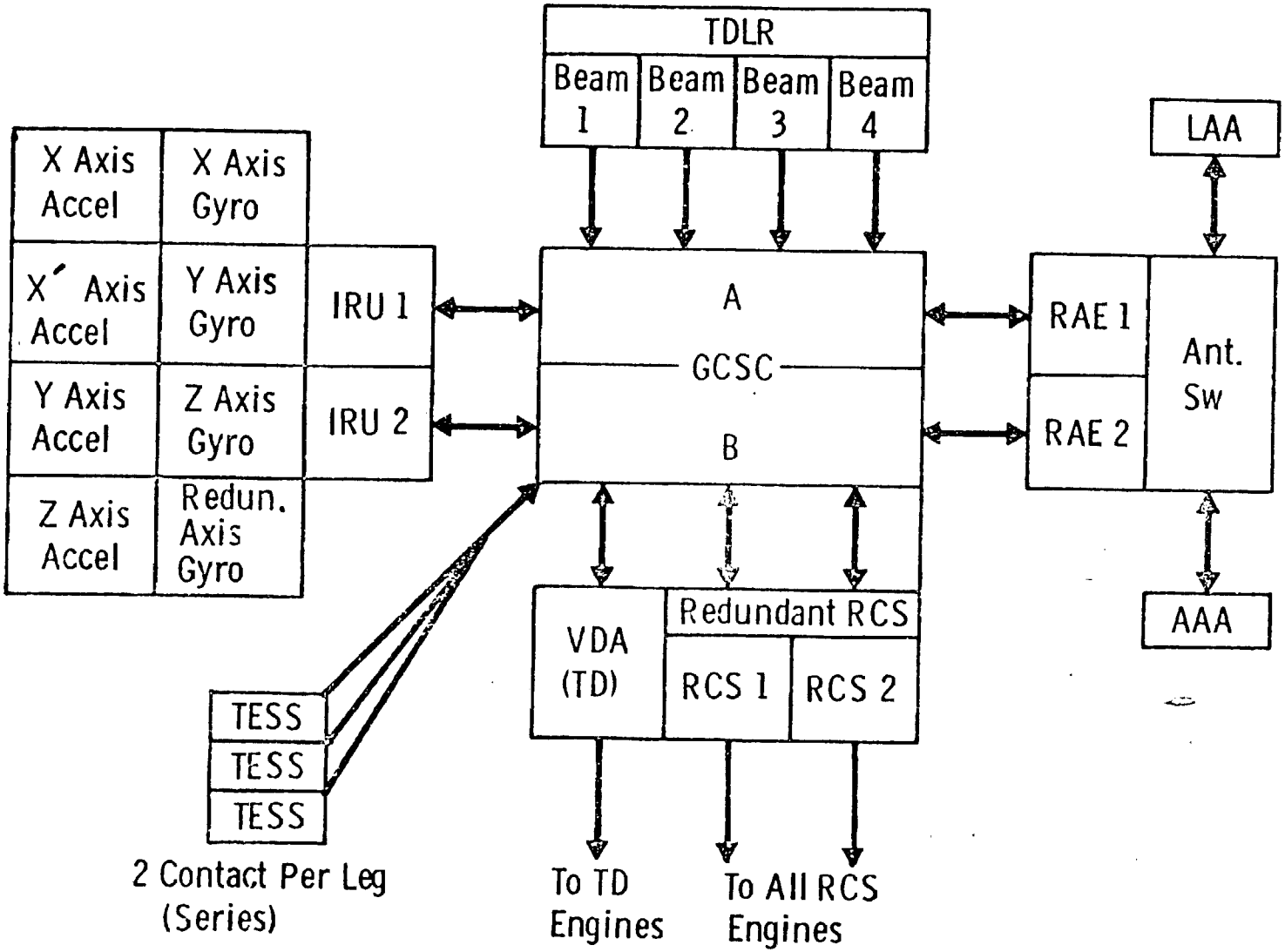


FIGURE 4-16

downward in the inverse of the ballistic missile problem, and then we have to transfer the reference locally to the ground, removing the lateral and the longitudinal velocities in order to land. The equipment required to do this is gryoscopes, at least one accelerometer, a computer, a Doppler velocity measuring radar, and a ranging radar, and the necessary functions to control the engines, which we call valve drive amplifier functions. Finally, there must be a way to shut things down, and we have terminal engine shut down switches. These guidance elements are all redundant.

An on-board decision is made to select between two sets of electronics for the radar altimeter during entry. There are two antennas, one looking through the aeroshell, and another used after aeroshell is separated. There is a switching function between these antennas.

The Doppler radar, called the TDLR, is a four-beam system such that any three beams will solve the equations of motion. There are four independent power supplies, and they are on all the time.

There are four sets of gyros shown in this column, an orthogonal set, X, Y and Z, and one skewed such that one can choose in pre-separation checkout which three to mechanize, and the equations of motion and the software are designed to tolerate the use of any of the three of four on the entry. To land, you really only need one accelerometer longitudinally. However, for entry science reasons, we have also lateral accelerometers; and, to provide the redundancy, we have doubled up on that longitudinal accelerometer. The one to use is chosen in pre-separation checkout. So there really are two IRU's. It is beautiful little package, incidentally. It weighs about 30 pounds with its eight inertial instruments and its shock isolator.

Finally, the terminal engine shut down switches have two series contacts per leg: as we fly into the ground, any closure

of both switches on one leg will shut the engine down. And if you bounce and hit another leg, you get another chance - as a matter of fact, you get three chances at it.

The deorbit system valve drive amplifiers are redundant through the electronics, but the terminal engine system and its valve drive amplifiers are single string. We reached the weight limit and were unable to provide redundancy here. There is a mechanization for six engines that is well known, but we could not pay the penalty of that weight.

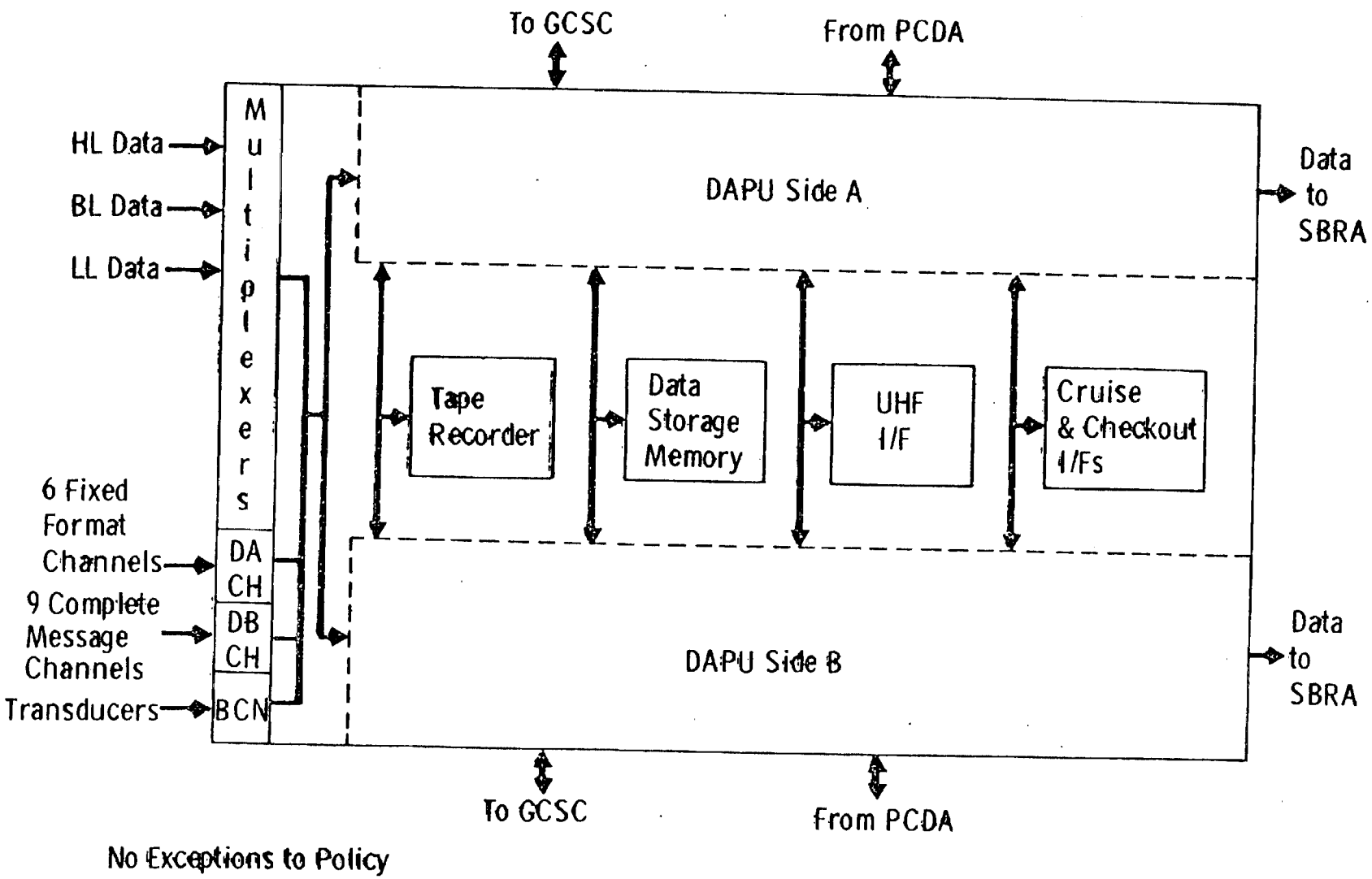
Finally, the guidance computer is block redundant. It has two 18,000K memories, two processors, two power supplies. One of the systems is selectable before separation to enter with: but if both are good, you then have the chance to use them after landing, and the sentry timer in the power subsystem is a device by which, in the event of failure, the lander is shut down to wait for a transfer to the other side by ground command.

Figure 4-17 presents the Telemetry Subsystem which is pretty straight forward. The basic collection device is the data acquisition and processor. The data is analog, digital, high level, low level, and bi-level data; all are converted by DAPU to six fixed format digital channels. The scientific instruments and engineering transducers are the basic source of the data.

The storage systems are functionally redundant. There is a fast access data storage memory of about 200 K capacity, and a slower access 40 million bit tape recorder: it has four tracks and is able to read and write in either direction. The data processer accepts the data, formats the data, and modulates the carriers for the output to the radio systems. These include the UHF system, which is the relay with the orbiter, and the S-band system which is a direct link to the Earth.

On Figure 4-18 is the communications subsystem, the radio subsystem. There is a functional redundancy as I described earlier.

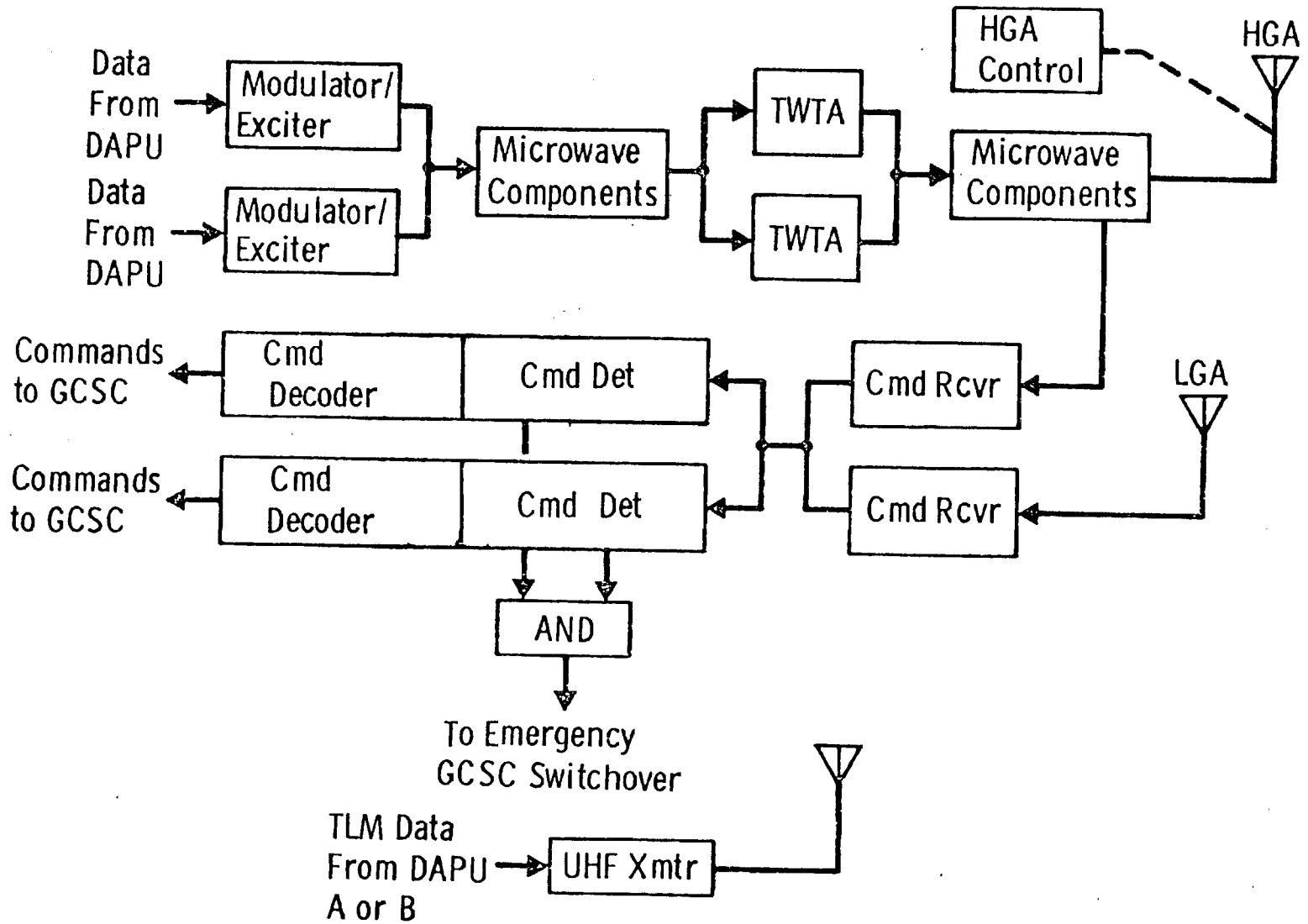
VIKING TELEMETRY SUBSYSTEM



No Exceptions to Policy

FIGURE 4-17

VIKING COMMUNICATIONS SUBSYSTEM



No Exceptions to Policy

FIGURE 4-18

The system has several commandable data rates. The lander can relay through the orbiter with a single string UHF system at a maximum rate of 16,000 kilobits per second after landing; and normally that is the one we will choose. The orbiter, of course, buffers that by a factor of four to get back down to, say, four thousand or by a factor of eight to get to 2K. Lower rates, however, are used during entry. We normally transmit at 2,000 bits per second, but we double that toward the end as we interleave one set of new data with old data delayed about a minute in order to avoid the blackout problem on entry.

The communications system does have the ability to do some on-board switching between the exciters, the command control unit, the microwave components, the two 20-watt TWTA's and the antennas.

There are two ways to get to the dual command receivers: through the low gain antenna or the high gain antenna.

I would like to summarize by saying that the choice of malfunction protection is pretty far-reaching. When you define the spacecraft hardware and its interfaces very carefully and relate it to the science mission, I think you will find that all of your operational alternatives of support software and your system test program will be very heavily influenced by how much redundancy you choose to use. To give you one final number, what I have shown you totals about 170 pounds of hardware in the Viking system for redundancy reasons only. Approximately ten percent is devoted to redundancy.

Thank you.

MR. CANNING: Are there any questions? I had one myself. Would you put up the slide on the guidance and control? The issue is, here, you say, that you have four of these radars, I guess they are, and any three of them can work. Suppose one of them starts working badly, then how do they decide amongst themselves which one is working right?

MR. GOODLETTE: In the pre-separation checkout, you can inhibit the beam you observe to be bad. If one fails during use, a "data good" software flag drops and the software ignores that beam. What you get is a mixed solution.

MR. CANNING: This would be a place where redundancy might in fact introduce, that is, if any one of them goes wrong, a failure mode.

MR. GOODLETTE: Exactly

MR. CANNING: Rather than eliminating failure modes.

MR. GOODLETTE: I think the time you spend on the front end choosing redundancy is very, very important because you can certainly drive yourself into a corner if you have more redundancy that you can use or you can test; it can cause you failures, unless you carefully choose and test the mechanization.

MR. CANNING: My own experience with failures, and I have had a couple, has been that mostly the systems that failed were highly redundant and, in some cases, the very existence of redundancy caused the trouble.

MR. GOODLETTE: That can happen.

UNIDENTIFIED SPEAKER: I didn't quite understand that. Did you way there is a majority voting system in here that would check it after you separate the lander, or does this have to be done by command?

MR. GOODLETTE: No. you can disable one of the beams, but if they are working at pre-separation checkout, there will be four beams operating. The reason for that is that as you swing on the parachute, for example, you can wipe one or more of the beams off the limb of the planet and, therefore, the solution of the equations of motion can lose input. To solve all of the

quations all the time, you only need three.

UNIDENTIFIED SPEAKER: While it is doing that determination, does the computer have the capability to switch off a beam and switch another one in?

MR. GOODLETTE: Not that. What we really do is we inertially navigate down all the time. If you do not get a data signal good from at least three beams, then you continue the inertial navigation. What you really have is about two second update time so that you are updating the inertial velocity reference with a two-second time constant. And if you miss it for upwards of twenty or thirty seconds, that will really do nothing more than delay the time that you update that system. You eventually have to get only a few good seconds to land.

MR. SEIFF: Is the TDLR system involved in the pre-separation checkout?

MR. GOODLETTE: Yes, there will be measurements.

MR. SEIFF: In other words, you check it out just a few hours prior to committing?

MR. GOODLETTE: Yes. Pre-separation checkout starts about 30 hours ahead of entry, and we are able to disable a failure by command.