SAFING AND FAULT PROTECTION FOR THE MESSENGER MISSION TO MERCURY

*Robert C. Moore, The Johns Hopkins University Applied Physics Laboratory,
Laurel, Maryland 20723-6099*

Abstract

The **ME**rcury Surface, Space **EN**vironment, **GE**ochemistry, and **R**anging (**MESSENGER**) mission is a NASA Discovery-class, deep-space mission to orbit the planet Mercury. Its purpose is to map the planet surface using various scientific instruments and explore the interior of the planet using measurements from instruments such as a magnetometer and observation of planetary libration. This paper discusses the architecture and implementation of the methods by which faults in the MESSENGER spacecraft are detected and the effects of those faults mitigated. The responsibility of the redundant Fault Protection Processors (FPPs) is to detect faults and take autonomous corrective actions that will keep the spacecraft healthy and safe.

MESSENGER Safing Architecture

Mercury is the second-smallest planet in our solar system and the one closest to the Sun. Temperature changes at the planet are among the most extreme in the solar system: surface temperatures range from 90 K through 700 K (–183°C through +427°C) [1]. Temperature is therefore a prime design consideration for any spacecraft that approaches or orbits Mercury. Figure 1 shows that the MESSENGER spacecraft has two large solar arrays that convert solar energy into electrical power for the spacecraft. The rest of the spacecraft is shadowed from direct sunlight by a sunshade. Almost the entire MESSENGER mission must be flown with the sunshade between the spacecraft and the Sun. Any attitude anomaly that exposes all or part of the spacecraft to direct sunlight must be corrected within fifteen minutes or permanent damage to the spacecraft may result. This is a prime driver of requirements for the safing and fault protection functions onboard.

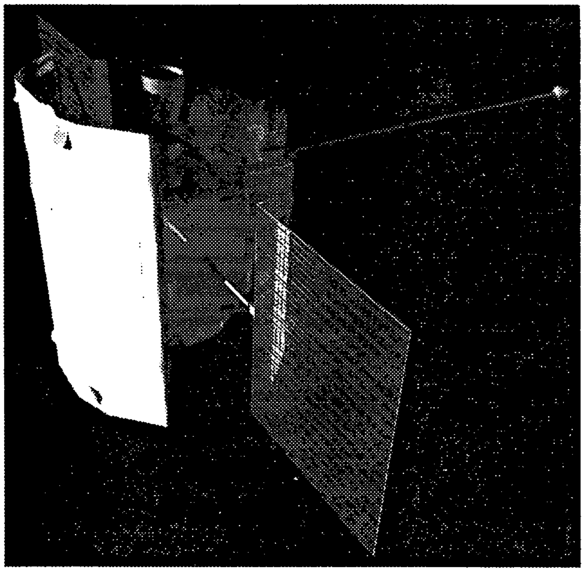

Figure 1. MESSENGER Spacecraft

The MESSENGER spacecraft is controlled by an onboard main processor. The main processor (MP) is a RAD6000 design that supplies up to 25 Mips of throughput. All command and data handling (C&DH), guidance and control (G&C), and some power system control is performed by software resident on the MP. The MP has a 8-Gb solid-state data recorder (SSR) associated with it, to record telemetry data for later transmission to Earth. The MP and its SSR are packaged in an integrated electronics module (IEM) that houses much of the MESSENGER avionics. For reliability the IEM is fully redundant; that is, there are two identical IEMs in the MESSENGER spacecraft (Figure 2).

Each IEM also contains a separate fault protection processor (FPP) that is always powered on. The two FPPs are responsible for implementing the safing and fault protection for MESSENGER.

0-7803-7367-7/02/$17.00 © 2002 IEEE

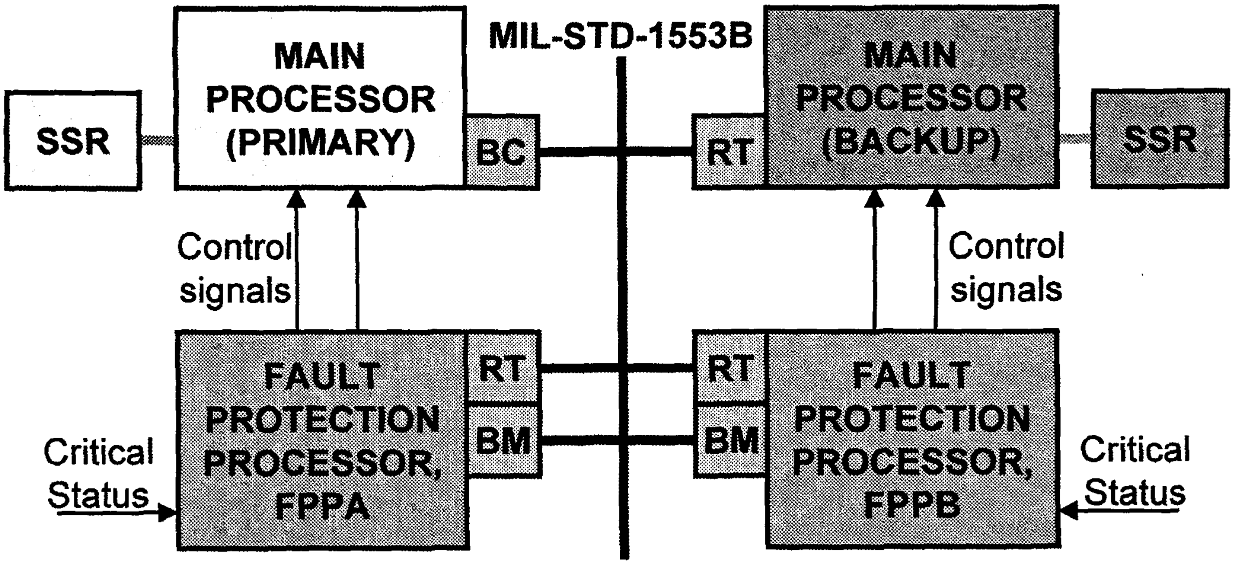

Figure 2. MESSENGER's Four-Processor Safing and Fault Protection Architecture

Normal inter-processor communications are accomplished using a standard MIL-STD-1553B bus. One of the two MPs serves as bus controller (BC), and the other processors (and many other subsystems on the spacecraft) function as remote terminals (RTs). The two FPPs also function as bus monitors (BMs) for the bus. A relay in the power switching and distribution unit (PDU) determines which of the two MPs serves as BC. Each FPP "knows" if the MP in its IEM is BC or not. The FPP in the same IEM as the BC MP is designated as the "primary" FPP, and the other FPP is designated as the "backup" FPP.

Using its RT and BM functions, each of the FPPs gathers status and engineering data (such as subsystem heartbeat) from the MP and the other subsystems. These data are then analyzed to determine if a spacecraft fault has occurred.

Spacecraft Mode Demotions

Spacecraft faults are designated as "recoverable," "serious," or "critical." Recoverable faults are those for which no spacecraft mode demotion is required. Serious faults take the spacecraft down from its operational mode to its safe-hold mode. Critical faults, or serious faults that persist after a mode demotion, will cause the spacecraft to demote to its lowest safe mode: Earth-acquisition mode. Refer to Figure 3.

Operational Mode

The operational mode of the spacecraft is the normal system mode. In operational mode:

- Normal C&DH and G&C functions are performed by the MP
- Flight software supports normal payload (instrument) operations and science data collection and processing
- Software uploads and diagnostics are supported
- Continued operations are supported following any recoverable fault

Safe-Hold Mode

The safe-hold mode of the spacecraft is the first level of safing. In safe-hold mode:

- The G&C tasks still know time and orbit ephemeris, so attitude inertial reference is maintained (if one star tracker remains active)

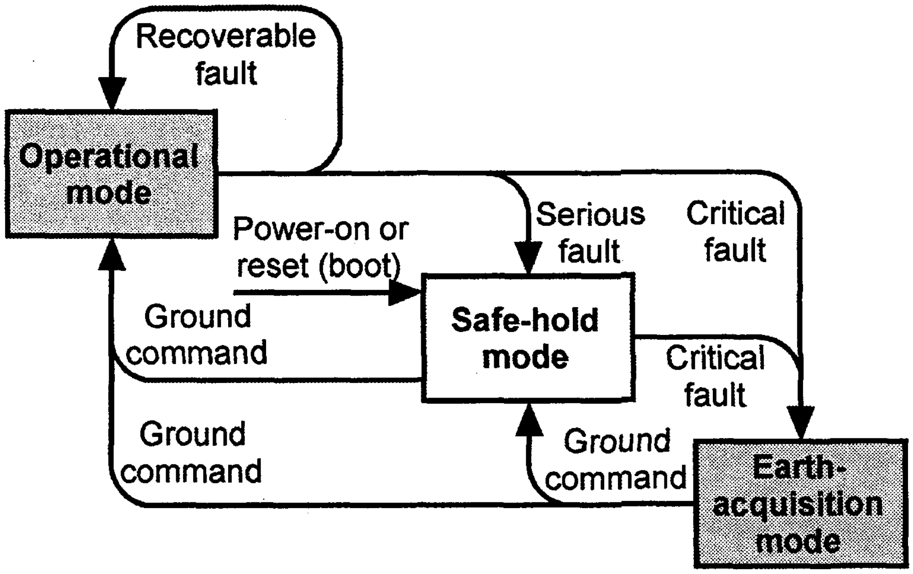

Figure 3. MESSENGER Mode Demotion Diagram

- Critical MP software parameters are reloaded from E^{2}PROM (electrically erasable, programmable read-only memory)
- Time-tagged command execution is suspended in the MP
- Playback of SSR data is suspended
- The sunshade is pointed at the Sun
- Radio-frequency (RF) components are reset, then configured for “emergency” communications with Earth
- Solar array and power system control continue in a known mode
- Survival heaters and fuel tank heaters are enabled (under control of software or local thermostats)
- All instruments in the science payload are commanded to stand-by mode

Only a ground command from Earth can promote the spacecraft back up to operational mode from safe-hold mode.

Some of the causes for entering safe-hold mode are:

- Persistent battery discharge
- Battery charger health not okay
- Battery temperature out of bounds
- Persistent Sun-keep-in (SKI) violation
- Excessive thruster use (since most recent ground contact)
- MP fails its built-in self test
- G&C tasks indicate a serious fault
- MP unexpectedly resets
- MP unexpectedly demotes to safe-hold mode
- MIL-STD-1553B bus activity stops

Earth-Acquisition Mode

The Earth-acquisition mode of the spacecraft is the lowest level of safing. In Earth-acquisition mode:

- The G&C tasks assume that time and orbit are both unknown, and that inertial attitude reference is also unknown
- Time-tagged command execution is suspended in the MP
- Playback of SSR data is suspended
- If a low state-of-charge (LSoC) condition exists for the battery, a suite of LSoC autonomy rules is enabled and the power system electronics are reset
- RF components are reset, then configured for “emergency” communications with Earth

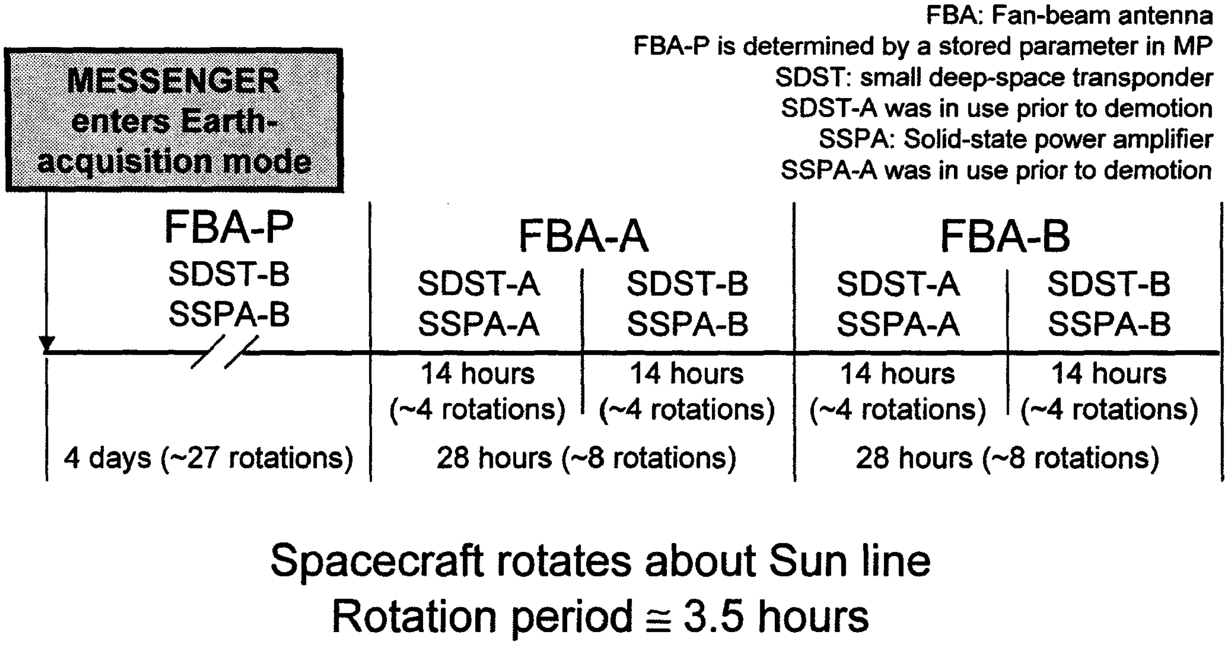
FBA: Fan-beam antenna
FBA-P is determined by a stored parameter in MP
SDST: small deep-space transponder
SDST-A was in use prior to demotion
SSPA: Solid-state power amplifier
SSPA-A was in use prior to demotion
MESSENGER enters Earth-acquisition mode
FBA-P
SDST-B
SSPA-B
FBA-A
SDST-A
SSPA-A
SDST-B
SSPA-B
FBA-B
SDST-A
SSPA-A
SDST-B
SSPA-B
14 hours (~4 rotations)
14 hours (~4 rotations)
14 hours (~4 rotations)
14 hours (~4 rotations)
4 days (~27 rotations)
28 hours (~8 rotations)
28 hours (~8 rotations)
Spacecraft rotates about Sun line
Rotation period ≅ 3.5 hours

Figure 4. Earth-Acquisition Mode RF Rotation Sequence

- The sunshade is pointed at the Sun (using data from the Sun sensors)
- The spacecraft rotates about the Sun line at one rotation every 3.5 hours
- RF components are enabled according to a fixed schedule (Figure 4)
- Survival heaters and fuel tank heaters are enabled (under control of software or local thermostats)
- All instruments in the science payload and the payload processor are commanded OFF

Only a ground command from Earth can promote the spacecraft back up to safe-hold or operational mode from Earth-acquisition mode.

Some causes for entering Earth-acquisition mode are:

- Battery LSoC
- No ground commands received for at least several weeks
- G&C tasks report a critical fault
- MP unexpectedly demotes to Earth-acquisition mode

Processor Boot Sequence

When powered on or reset, each of the four processors follows an identical boot sequence. The processor first detects if it is an MP or a FPP. If it is a FPP it looks to see if it should remain in boot mode or if its self-test indicates a critical internal failure. If neither of these is true the processor boots to its application code.

If the processor is an MP it looks at discrete signals to see if it is the primary or the backup MP. If it is the backup MP, then it will remain in boot mode. If it is the primary MP, it configures its MIL-STD-1553B bus protocol controller as BC and executes its internal self-test. If the self-test passes, then the processor loads and executes application code. If there is a failure in the self-test, the processor delays for several extra seconds and then attempts to load and execute its application code. This boot sequence is summarized in Figure 5.

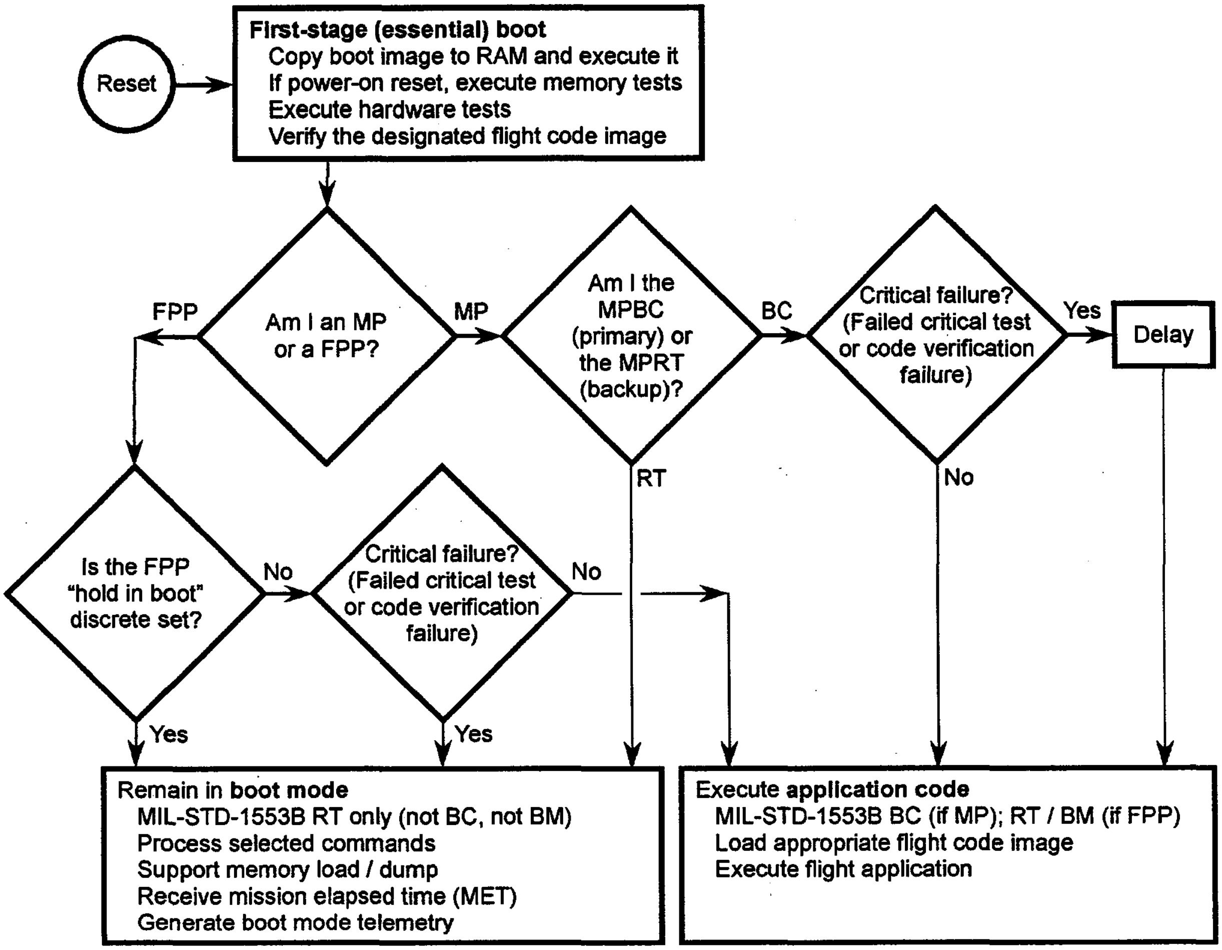
Reset
First-stage (essential) boot
Copy boot image to RAM and execute it
If power-on reset, execute memory tests
Execute hardware tests
Verify the designated flight code image
Am I an MP or a FPP?
FPP
MP
Am I the MPBC (primary) or the MPRT (backup)?
BC
RT
Critical failure? (Failed critical test or code verification failure)
Yes
No
Delay
Is the FPP "hold in boot" discrete set?
No
Yes
Critical failure? (Failed critical test or code verification failure)
No
Yes
Remain in boot mode
MIL-STD-1553B RT only (not BC, not BM)
Process selected commands
Support memory load / dump
Receive mission elapsed time (MET)
Generate boot mode telemetry
Execute application code
MIL-STD-1553B BC (if MP); RT / BM (if FPP)
Load appropriate flight code image
Execute flight application

Figure 5. MESSENGER Processor Boot Sequence

"Bad MP" Sequence

One of the primary tasks of the FPP is to evaluate the health and proper operation of the MP. There are numerous anomalies for which the FPP must assume that the MP is no longer functioning properly. In these situations the FPP follows a carefully designed "bad MP" sequence.

IEM-A is the primary IEM, which is normally the IEM that is used to control the MESSENGER spacecraft. This IEM initially contains the MP that is bus controller for the MIL-STD-1553B bus.

Each MP (one in each of the two IEMs) can be booted using either of two pre-stored application code images. The FPP has the choice of using a fresh load of the current software or loading the backup software instead. The backup software is usually the next most recent version of the flight code, which presumably does not have the same "bugs" as the most recent version.

The "bad MP" sequence is divided into five transitions. Refer to Figure 6. The first transition attempts to use fresh hardware and a fresh load of the current application code. This transition forces a demotion from operational mode to safe-hold mode.

If the fault is not corrected by transition one, a second transition is attempted. In transition two the fresh hardware is used with a fresh load of the backup software. Again the spacecraft is kept in safe-hold mode (unless it was already in Earth-acquisition mode).

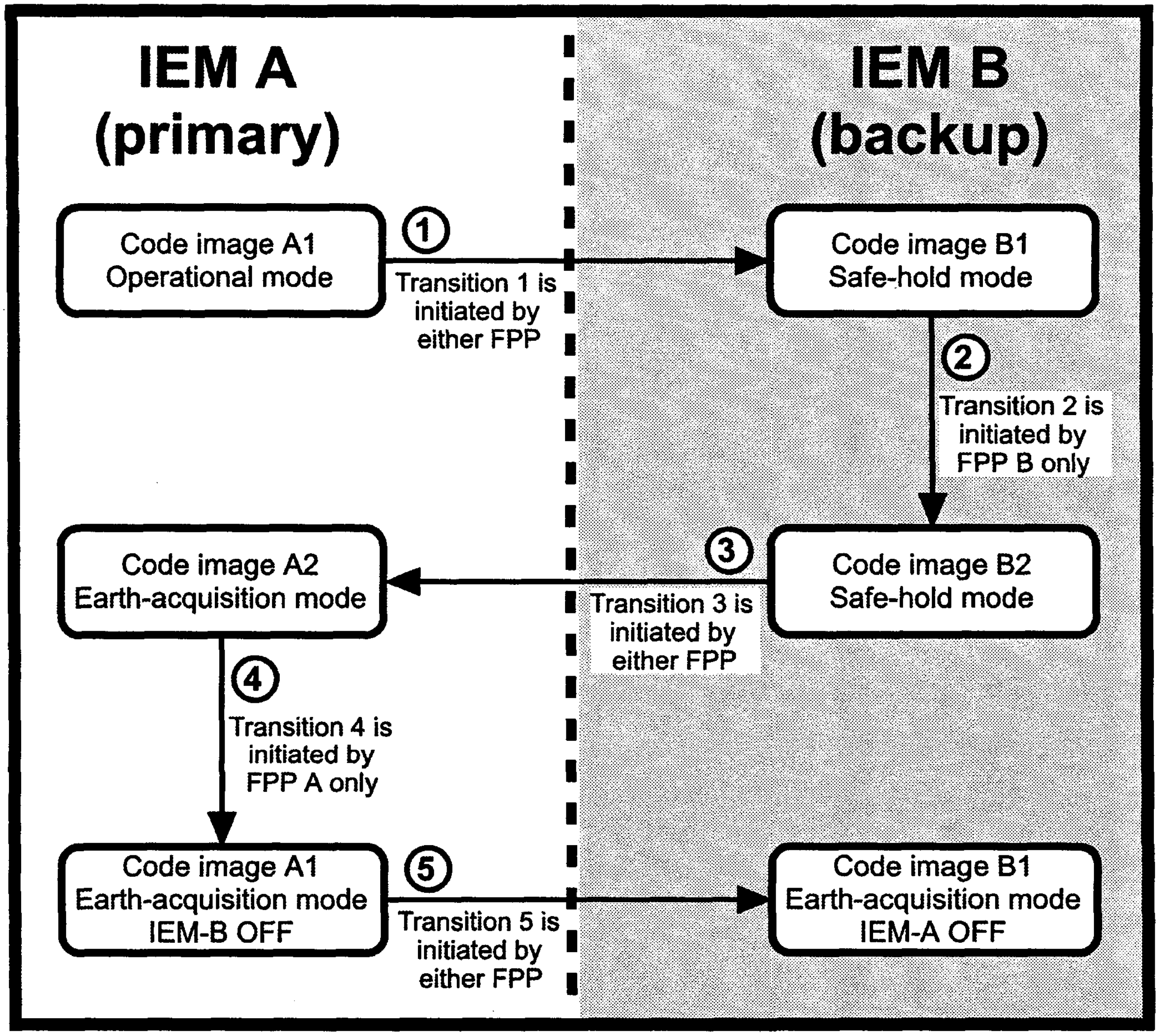

Figure 6. MESSENGER "Bad MP" Sequence

Notice that for any single hardware or software fault in the MP system, a working MP will have been found by the completion of transition two. There are, however, several unlikely hardware faults that could prevent the working MP from functioning properly. One is a "babbling" MIL-STD-1553B protocol controller or transceiver, which could prevent the "good" MP from properly controlling the MIL-STD-1553B bus.

Transition three uses the original hardware with backup software, in Earth-acquisition mode. Transition four uses the original hardware with a fresh load of the original software, but powers OFF the backup IEM. Note that this condition results in the loss of any data stored on the SSR in the backup IEM. Transition five uses the backup hardware and a fresh load of the flight software, but powers OFF the primary IEM.

Fault Recovery Duration

If bad processor hardware or software has resulted in an attitude error, so that all or part of the spacecraft is no longer being shielded from direct sunlight, in the worst case there are only fifteen minutes in which to correct the problem before serious thermal problems arise. From the "bad MP" sequence diagram (Figure 6) one can see that at most two transitions are required to find a working MP/flight software combination.

Figure 7 shows the timing budget for recovery from a serious or critical attitude fault. From the time the attitude violation (for example, a Sun keep-in violation) first is detected until the spacecraft is fully shielded again from direct sunlight, no more than fifteen minutes (900 seconds) may elapse.

P — Persistence of autonomy rule = 15 seconds

I — Main Processor Initialization duration = 135 seconds

R — Recovery duration (worst case) = 300 seconds

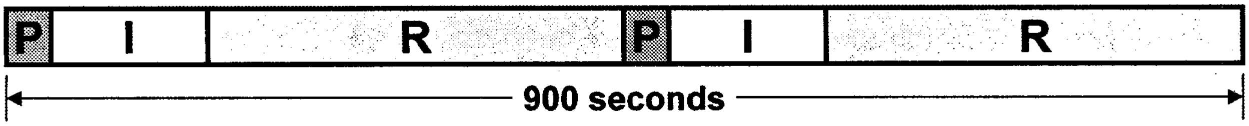

Figure 7. Attitude Fault Recovery Timeline

The two transitions of the "bad MP" sequence may each be divided into three segments: (1) the persistence of the autonomy rule that detects the fault, (2) initialization duration for the MP, and (3) worst-case attitude recovery duration.

Autonomy rules are of the form "if premise then action," where "premise" is an expression that evaluates to logic zero (false) or logic one (true). If the premise evaluates to "true" for *M* out of *N* rule evaluations, then the action is taken. The latter feature means that each autonomy rule has a degree of persistence; that is, it will not "fire" on a single out-of-bounds condition but must wait until the fault has been detected multiple times.

Persistence duration for each rule is specified by that rule. Typically rule persistence duration is in the range from one through sixty seconds. In the budget of Figure 7 the persistence duration for an attitude violation rule has been assumed to be fifteen seconds.

Initialization for the MP involves several sequential operations:

• Execute boot code	75 s
• Initialize memory	30 s
• Initialize power distribution unit	6 s
• Initialize inertia measurement unit	8 s
• Initialize star tracker	6 s
• Initialize G&C data pipeline	4 s
• Permit attitude estimator to stabilize	6 s
Total MP initialization duration:	135 s

Based on the results from simulations, the worst-case attitude recovery duration (a full 180° slew under worst-case conditions) requires 4–5 minutes. Taking 5 minutes as the worst case, we use 300 seconds in the recovery duration budget (Figure 7).

Figure 7 shows that the worst-case recovery duration, assuming two transitions of the "bad MP" sequence are required, is 900 seconds.

Acknowledgment

I am indebted to David A. Artis of The Johns Hopkins University Applied Physics Laboratory, MESSENGER Software Lead Engineer, from whose original work Figure 5 has been adapted. Used by permission.

I am also indebted to Andrew G. Santo of The Johns Hopkins University Applied Physics Laboratory, Mission System Engineer for the MESSENGER program, for his invaluable assistance in generating the “bad MP” sequence.

References

[1] Sietzen, Jr., Frank, “Messengers to the Inner and Outer Limits [Mercury and Pluto],” *Aerospace America*, vol. 40, no. 2 (February 2002), pp. 36–40.