EM2 RFA Responses

- **RFA #1: Secondary Boot Code**
  - **Specific Request: Document and track to resolution the SBC TFFS bad block detection problem as a flight software discrepancy.**
  - **Reason/Comment: The SBC represents a critical component of the flight software system. This issue directly impacts the functional capability of this component and needs to be reviewed at a higher profile.**
  - **Submitted by: Ron Zellar/GSFC**

EM2 RFA Responses (2)

- **Response to RFA #1 (Secondary Boot Code):**
  - **Contrary to marketing materials, TFFS does not support bad block detection and marking. LAT FSW will use checksum algorithms to detect bad blocks. LAT FSW will mark bad blocks with a dummy file (e.g., by renaming a corrupted file) and reload the corrupted file elsewhere.**

EM2 RFA Responses (3)

- **RFA #2: Primary Boot**
  - **Specific Request: Please provide tradeoff between risks of using decompression and memory allocations in Primary Boot Code versus use of additional PROM to store uncompressed boot routines.**
  - **Reason/Comment: Possible Primary Boot Code corruption. Possible LCB ring buffer overwrite.**
  - **Submitted by: Mike Beims NASA IV&V**

EM2 RFA Responses (4)

- **Response to RFA #2 (Primary Boot):**
  - **The Primary Boot Code (PBC) is stored in RAD750 SUROM in an uncompressed format, so a failure of the decompression procedure will not corrupt the PBC nor prevent it from booting or operating.**
  - **The images for the Secondary Boot Code (SBC) and RTOS can be stored in either compressed or expanded formats. Should the PBC fail to inflate a compressed image, an uncompressed image can be uploaded and used as an alternative. If desired, images can be tested before uploading to verify that they can be inflated (to avoid wasting time and bandwidth on an 'uninflatable' image).**
  - **During inflation, the PBC handles memory allocation requests in the form of calloc calls from the ZLIB library functions. The PBC allocates this memory from a 280 KByte region of RAM that is dedicated to allocation requests from the ZLIB inflation library. The process of inflating a typical RTOS image requires approximately 50 KBytes of allocated memory, which is less than 1/5 of the amount available. In the unlikely event that the ZLIB functions consume the entire region, however, the PBC will refuse to allocate additional memory and the inflation procedure will fail. At this point, the PBC must be restarted to reclaim/free the previously allocated memory.**

EM2 RFA Responses (5)

- **Response to RFA #2 (Primary Boot, cont'd):**
  - **Additionally, an alternative RTOS image must be uploaded if the allocation overflow was caused by the particular attributes of the failing image.**
  - **Since the PBC refuses to allocate memory when it has exhausted its allocation pool, there is no risk that other memory, such as the LCB ring buffer or PBC data, will be corrupted by a 'run-away' inflation procedure.**

EM2 RFA Responses (6)

- **RFA #3: Instrument Configuration**
  - **Specific Request: Please provide analysis and test plan verifying that all possible configurations will not hurt hardware.**
  - **Reason/Comment: Complexity of possible configurations needs written analysis and test planning for verification of hardware safety.**
  - **Submitted by: Mike Beims**
- **Response:**
  - **See response to LAT CDR RFA #29 (next slide)**

EM2 RFA Responses (7)

- **CDR RFA #29: Instrument Configuration**
  - **Subsystem:C&DH**
  - **Requestors Steve Scott, Joe Bolek**
  - **Describe fault management for GLAST LAT. Describe fault management for GLAST LAT by the GLAST spacecraft. The description of fault management should include hardware and software (and operational techniques). Describe where requirements are defined and how they are verified.**
  - **Fault management for the GLAST LAT has not been adequately (i.e.., thoroughly) addressed.**

EM2 RFA Responses (8)

- **Response to CDR RFA #29 (Instrument Configuration):**
  - **The LAT is, from the fault management perspective, a simple system with few fault management requirements. In general, the faults that require in-orbit response result in LAT temperature exceeding low or high limits. In that case, the spacecraft turns off the LAT and activates an independent thermal control system.**
  - **Six key areas for fault management have been identified. They are high/low temperature excursions, high current, high voltage, ACD PMT protection due to SAA, processor fault, and software malfunction.**
  - **Of these, only high/low temperature excursions require spacecraft action. All critical LAT temperatures that require the SC to put the LAT in safe mode have been identified and documented in the LAT-SC ICD. LAT safe mode consists of disconnecting the SIU and DAQ feeds, activating both primary and redundant VCHP feeds to isolate the radiators and activating both survival feeds. Survival heater control is via thermostats.**
  - **High current protection is implemented with fuses. Each LAT heater is individually fused. The SIU's, EPU's, TEM's and GASU feeds are individually fused as well as the CAL electronics, Tracker MCM's, and ACD. In addition, all LAT power supplies contain thermal switches.**

EM2 RFA Responses (9)

- **Response to CDR RFA #29 (Instrument Configuration, cont'd):**
  - **High input voltages (>45V) at the SIU and DAQ feeds can damage the LAT electronics. Currently, the LAT does not require SC action since the maximum SC voltage is 35V. If Spectrum Astro identifies a failure on the SC bus that could cause the LAT input voltage to stray above 35 V, a requirement to safe the LAT will implemented. Currently, no failure mode for this scenario has been identified.**
  - **The ACD PMT's are protected from damage due to SAA in two ways. During normal operations, the SC issues a MIL-1553 message prior to entering the SAA region. Once the SIU receives this message, the gain to the ACD PMT power supplies is lowered. Once the instrument is out of the SAA region, the SC sends a 1553 message and the LAT resumes the science mission. In the event of a processor fault or software malfunction, the PMT's are protected by current-limiting resistors in the ACD high-voltage power supplies.**

EM2 RFA Responses (10)

- **Response to CDR RFA #29 (Instrument Configuration, cont'd):**
  - **LAT processor faults do not require additional direct fault protection. The processors do not have a survival thermal control function. There are operational scenarios where a processor fault could lock the VCHP heaters on or off. If the VCHP are locked on (radiators isolated from the LAT) with the LAT electronics powered on, the LAT temperature would rise. Once a critical LAT temperature exceeds a red limit, the SC will safe the LAT. In addition the VCHP reservoirs are over-temperature protected by a thermostat. In the event that the VCHP heaters are locked off (full heat rejection by the radiators) the LAT would cool down. Again, once a critical LAT temperature exceeds a red limit, the SC will safe the LAT. become thermally unstable. The ACD PMT protection in the event of a processor fault was discussed earlier.**
  - **The LAT software has no survival thermal control function. The operational scenario identified that requires fault management due to a software malfunction is with the VCHP heaters being locked on or off. The discussions that applied to the LAT processors apply here as well.**

New RFAs

- On with the Flight Unit RFA discussion…
- Blank RFA forms are available