EVLA Monitor and Control Hardware
Critical Design Review
October 20, 2004, Socorro, New Mexico

Report of the Review Panel

1. The Review Panel

John Ford, Green Bank
Jeff Hagen, Arecibo/NAIC
Gary Hovey, DRAO/HIA
Jeff Kern, ALMA

2. Introduction

A Critical Design Review (CDR) of the EVLA Monitor and Control Hardware was held on Wednesday, 10/20/2004. The review was sponsored by NRAO, and was held in the auditorium of the Array Operations Center (AOC) in Socorro, NM. The CDR was one (1) day in length, and consisted of presentations and demonstrations from approximately 8:30AM until approximately 3:45 PM followed by a closed door discussion among the members of the Review Panel and Bill Sahr (EVLA Monitor and Control Group Leader) from approximately 3:45PM until approximately 5:45PM.

The topics covered by the CDR were:

- Module Interface Board (MIB) Hardware, including
  - MIB Capabilities
  - MIB PC Board Design
  - MIB RFI Test Results
  - MIB Interfaces to Devices
  - MIB Slot-IDs
- MIB Software
- The EVLA Monitor and Control Network
- EVLA Transition Hardware

There were two demonstrations - one of the telnet (TCP/IP) interface to the MIB Service Port, and one of a Java Device Browser interfacing to the MIB Service Port via a UDP connection.

3. Charge to the Panel

The primary purpose of the CDR was to determine if the MIB is ready for quantity production. Specific questions asked of the Review Panel were as follows:

1. Are the detailed requirements for the subsystem complete and adequate? The subsystem in question was primarily the MIB, and secondarily, the EVLA Monitor and Control Network.

With respect to the MIB, the specific issues raised were:

- Is it capable of executing commands in a timely fashion ? "Timely" was further defined to be the requirement that a MIB be capable of beginning execution of a command within 100 microseconds of the time stamp associated with that command.
- Will it produce monitor data in a manner sufficient to the task of monitoring the state of the system ?
- Is the MIB sufficiently RFI quiet?

2. Will the design selected for implementation meet the requirements ?

3. Are interfaces to other subsystems defined adequately and completely ?

4. Has adequate attention been given to issues related to quantity production and maintenance of the subsystem ?

4. Reviewers Comments

4.1. Timely Execution of Commands by the MIB

Given that the MIB can queue up to 50 time-tagged commands, there is some ambiguity in the specification. Is it necessary that all 50 commands begin execution within 100 microseconds of the time tag ? It seems unlikely that the MIB could handle such a requirement. It should be specified how many of the time-tagged commands, or which time-tagged commands are required to be started within 100 microseconds of the time tag. It is recommended that once this specification has been clarified, that software tests be designed and conducted to insure that the MIB meets the specification.

4.2. Production of Monitor Data

All specifications seem to support this function. It is not clear that the MIB could simultaneously produce all monitor points at maximum rates. Should the specification specify the minimum number of monitor transactions per second that the MIB must support ?

Further, it is recommended that some well thought-out tests be conducted, using multicast, to determine that the MIBs really support the requirements in this area. In particular, attention should be paid to the issue of dropped UDP packets.

If dropped packets are found, one possible topic to investigate is Reliable UDP (RUDP).

4.3. RFI Quiet

No specification on allowable emission levels was made available, but the board seems to be remarkably quiet. The tests presented demonstrated that a MIB by itself produces an acceptable level of RFI, however the SPI bus and the clock lines for the timer were in a quiescent state during those tests. It is strongly recommended that worst-case tests be conducted, with SPI and clock lines active, and ethernet traffic proceeding at its maximum rate.

Further, no compatibility requirements have been established for allowable radiated and conducted RFI within a module. Because the unit will be housed with RF and other analog circuits, RFI from the MIB may affect their operation. Conversely, it is possible that the MIB may be affected by strong signals from circuitry such as LO's, though this is less likely. It is worth investigating conducted RFI by measuring the

spectrum on MIB signal and power lines. If not already done, consider filtering the supply lines on the MIB board.

In general, intra-module RFI should be carefully reviewed, and module designers must account for MIB-generated RFI in all RFI-sensitive designs. It is suggested that connections be provided and any other necessary provisions be made to allow the entire MIB to be enclosed in a separate shielded enclosure, should doing so prove necessary.

Is there a contingency plan for the case of a module affected by RFI from a MIB ?

4.4. Will the design selected for implementation meet the requirements?

The design will meet the requirements, however:

- Temperature, shock, and vibration requirements should be specified, with a statement of how it was decided that these specifications are met - either through analysis or direct testing.
- Tests should be run to determine if the network stack in the MIB is sufficient to the demands that will be placed upon it. Performance, in packets per second or bytes per second, between a MIB and a PC should be measured for udp, tcp, and multicast mode. What overhead, if any, is there in enabling multicast mode? Will all MIBs in an antenna see and be required to handle multicast packets from the others ?
- Will the other tasks in the MIB - production of monitor data, receiving commands, module control - compromise the ability of the MIBs to meet the requirement that commands begin execution within 100 microseconds of the time tag ?
- Does the software depend upon 100% delivery of packets (no dropped packets) to avoid system problems ?
- The dependence of MIB software development upon a commercial Windows product limits the longevity of the device. Every effort should be made to adapt the GNU toolset to software development on the MIBs. A gcc cross-compiler for the TriCore architecture does exist.
- There are three identical connectors on the MIB board to which ribbon cables can be connected. Keying of the connectors is recommended (by all 4 reviewers).

4.5. Are interfaces to the other subsystems defined adequately and completely ?

The interfaces are adequately defined. Ethernet is a capable standard, and the large number of I/O options for interfacing to module hardware can easily satisfy future needs.

4.6. Slot-ID

The slot-ID mechanism is a good idea. Since slot-ID does allow for board swapping and easy testing, all module hardware should have a software available serial number for reliability tracking. This feature would also allow a snapshot of all modules in the array to be taken. Additionally, the use of revision numbers throughout the system, for both hardware and software changes is encouraged. These revisions numbers should be available via software, perhaps as monitor points.

That the D30x modules seem to be an exception to the otherwise universal application of the slot-ID scheme is an issue. A solution not too different from the application of slot-ID to the other modules needs to be found. Would a penetration of the D30x module be possible if the SPI lines were heavily filtered and the clock regenerated outside of the module ? Alternatively, would it be possible to have a serial prom (or similar circuitry) in the D30x module that provides some or all of the needed information?

4.7. MIB status

How do the connected devices know the MIB is functioning ? Rather than having each device/module designer handle this matter on an ad hoc basis, it is suggested that a bit be defined for this purpose.

4.8. Security

Security is an issue. The demonstrations during the CDR highlighted the necessity of making it difficult to accidentally connect to running systems. The use of ethernet in combination with UDP and TCP/IP make the MIBs very accessible. Implementation of the "in use" flag or some other method of protecting the MIB from unwanted (or unintended) commands should be put in place. On-line control of the MIBs should be more difficult to access, requiring a further response or verification. These steps should be given a high priority. Since they are not in the critical path, they will not naturally receive emphasis. The GBT failed to address this issue and is still suffering from that decision.

4.9. Has adequate attention been given to issues related to quantity production and maintenance of the subsystem?

Overall, yes. For the most part, this issue seems to be adequately handled by the fact that commercial vendors are willing to commit to fixed price contracts. The staff at the AOC is capable of building and repairing the MIBs. The recommended level of spares is 10% more MIBs than required and a spares inventory of 20% of key parts. The idea of buying spare boards and parts without going to the expense of building all of the spare MIBs is a good one. NRAO's 12-meter telescope (with it's 70's vintage filterbanks) still survives because of its vast collection of spare parts.

Temperature and power cycling of a number of units to determine reliability over the supply voltage is recommended. Further, temperature cycling of the units over the worst-case storage temperature should be a part of the manufacturing plan. A written manufacturing and production test plan document, detailing how the units are to be built and tested should be developed.

The following issues have been raised with respect to the MIB printed circuit board (PCB):

- In general the MIB layout is quite dense. As a result, there is little room for adding circuit modifications or substituting an out of production part should it be required in the future.
- The clearance of the mounting holes is very tight and may preclude the use of screws. If the plan is to use press fit nylon standoffs to secure the board, it should be noted that they can come loose and are less secure than screws.
- Most of these problems are driven by the size of the board. If practical, increasing the size of the board would ameliorate these issues.
- The production cost of the board is on the high side. Is it possible to further optimize the board for production ? Would consultation with board and assembly vendors make it possible to further decrease both cost and the likelihood of manufacturing defects ?

5. Other Issues

5.1. MIB Software and MIB Performance

The MIB software is quite complete and straightforward from a system perspective. It appears that the MIB hardware should be quite capable of supporting the planned software, though it is not self evident that this statement is true.

For safety critical systems such as motor and heater controls, it is essential that commands expire if communications are lost or the host goes down. It may be useful to have a timeout specified for or

associated with such commands. This issue could be handled in a general way by the watchdog timer, or it may be desirable to have a programmable timeout that is passed as a parameter with the command.

The performance of the MIB has not been fully understood. It has been demonstrated that the MIB is capable of meeting all current demands on it. But, by how much is not known. The reviewers strongly encourage testing of the MIB to the failure point. How many messages can be handled within the 52 ms window set by the heartbeat? What is the peak and average message load that can be accommodated? From the design it appears that these numbers should be sufficient for the foreseeable uses of the MIB, but it is important to have these numbers well defined. From the discussions, it sounds as if delay tracking will be one of the most difficult tasks for the MIB. It might be useful to use delay tracking to help define the requirements on the MIB.

Memory resources appear to be adequate. Performance tests showing peak and average CPU loading, and MIB response times for these CPU loads were not presented. Without such tests, it cannot be known that the MIB meets the system requirements.

Since a large number of MIBs are planned, it would be appropriate to have a written statement from each module/device designer that specifies what they expect the MIB to do. This suggestion is not viewed as critical since the MIB is a relatively general device.

5.2. The EVLA M&C Network

One concern is that the plan for the network depends on advertised specifications of the manufacturers equipment, which are not always clear. The requirements for the network could be improved by establishing response times, expected burst and average traffic, and reliability. These metrics should include a margin of about 50%.

Testing to failure should be extended to the network. Although multicasting is a mature and standard technology, there can always be unforeseen difficulties in this type of network. The specification of switches usually assumes a Poisson distribution of packet traffic. At the array, the traffic will be highly coherent, with the implication that while a switch may be able to handle the average load, the peak load may exceed its capabilities. Demonstrating that the chosen switches are capable of handling the network traffic should be done before many of the switches are purchased.

The network requirements and design seems to need additional support. Either by analysis or simulation, the scalability of the system should be assured. The EVLA M&C network will contain more nodes than all of the AOC. Effects of switch management software, broadcasts, multicasting, etc. should be analyzed. One software package that would be useful for this task is "opnet modeler". It may be desirable to cooperate with a university to have this analysis done as a research project, rather than buying the software for a one-time use.

It is suggested that an end-to-end analysis of the data rates, maximum allowable latency, and any round-trip algorithms, such as RF path balancing, be done, and that final estimates of the time to run these algorithms be determined and approved.

The suggested analysis of the EVLA M&C Network is not a prerequisite to proceeding with quantity production of the MIBs. It is probable that the MIB and the software can cope with the results of the analysis.

It is not clear that the MIBs can inter-communicate. If the MIBs rely solely on the host to insure that a set of antenna MIBs are working properly, an extra burden is placed on network and host reliability. It is not

clear that other network and system configurations were considered, and why the planned configuration has the most merit.

Availability and cost of fiber-optic switches may not conform to the projections being made for the EVLA. Contrary to expectations, copper is proving usable for 1Gbit and even 10Gbit networks. This development may lead to decreased availability and higher costs for fiber-optic switches.

5.3. Fractional Day Number Precision

Does the fractional day number have sufficient precision? In the slalib package this quantity is handled by two doubles, a day number and a fraction. If the timing is always on the 19.2 Hz heartbeat, this item is not an issue.

5.4 Watchdog Timer

Concerning the discussion of the watchdog timer and what to do for the case of a shutdown. If the system does the right thing on bootup, what to do on shutdown need not be an issue. Once failed, it is almost impossible to expect software to work. Given this logic, the watchdog timer should always issue a message and reboot. This behavior should be changed only when a particular problem is being investigated.

The functionality of the watchdog timer routine appears minimal. This routine should also check that all tasks are operating properly and that the MIB is communicating with a host. As mentioned in the subsection on MIB Status, it is suggested that a bit be dedicated to the purpose of informing a device that the MIB is functioning normally. This bit would be useful for safety critical devices, such as antenna motion controls, to allow a device to go to a safe state if the MIB is not functioning normally.

6. Overall

Overall the MIB is in a very good state, a well thought out and careful design. No flaws in design or implementation serious enough to preclude quantity production of the MIB have been found. However, additional work and testing needs to be done in the areas of RFI, MIB performance, and network characteristics and scalability. One difficulty with the CDR was that the requirements for the MIB are poorly defined.