APP Failure Modes and Effects

ALMA-05.11.10.00-0001-A-GEN

2013-08-21

Prepared by:	Organization Role:	Date and Signature:
Michael Hecht	APP Project Manager	
Approved by:	**Organization Role:**	**Date and Signature:**
Nick Whyborn	System Lead Engineer	Digitally signed by Nick Whyborn DN: cn=Nick Whyborn, o, ou, email=nwhyborn@alma.cl, c=CL Date: 2014.01.22 08:04:13 Z
Released by:	**Organization Role:**	**Date and Signature:**
Shep Doeleman	APP Principal Investigator	29 Jan 2014

Lock

Change Record

Version	Date	Affected Section(s)	Author	Reason/Initiation/Remarks
A	2013-08-21	All	Michael Hecht	Initial draft

Table of Contents

1 Introduction

In addition to software modifications, the ALMA Phasing Project will be installing four new hardware subsystems, each of which can be readily removed to restore the current operating configuration. These subsystems are:

- 1 Hydrogen Maser and GPS to replace the current Rb clock time standard.
- 8 Phasing Interface Card (PIC) assemblies to generate a copy of the data stream for phasing and correlation. Short of complete failure, the PIC should not affect normal ALMA data acquisition.
- 1 Optical Fiber Link (OFL) to multiplex and demultiplex signals from the PIC at OAS to be recorded on the Recorders at OSF. The OFL is not connected to any components involved in normal data operations.
- 4 Mark 6 Data Recorders. These reside at OSF and do not interact in any way with normal ALMA data acquisition.

The following is a description of plausible failure modes, how they are detected, the impact on both normal and VLBI data acquisition, and the remedies required.

1.1 Applicable documents

The following documents are part of this document to the extent specified herein. If not explicitly stated otherwise, the latest issue of the document is valid.

Appl.	Document Title	ALMA Doc. Number
[AD01]		
[AD02]		

1.2 Reference documents

The following documents contain additional information and are referenced in this document.

Ref	Document Title	ALMA Doc. Number
[RD01]		
[RD02]		

1.3 Acronyms

The more complete list of acronyms and abbreviations used within this document are given below. For a complete set of acronyms and abbreviations, please go to the ALMA AIV web page.

Acronym	Definition
ALMA	Atacama Large Millimeter/submillimeter Array

1.4 Verb Convention

"Shall" and “must” are used when a specification or provision is mandatory. The verbs "should" and "may" indicate a specification or provision that is not mandatory.

2 Optical Fiber Link

2.1 Failure type: component failure of 10GbE optical module

Effects: One or some 10GbE SR/ZR modules cease to operate. Data going though the relevant OFL channel will be lost. The module failure can be detected by monitoring the OFL status. Manual fiber reconnection is required to switch the data stream from the failed port to the spare port.

Remedy: Failed module should be replaced with new one.

2.2 Failure type: component failure of fan

Effects: One or some fans stop running. Fan failure can be detected by monitoring the OFL status. If one fan stops, the OFL continues operation because it is designed to properly work even with only two fans (out of three) in operation. No data loss will occur.

If two fans are out of operation, all the 10GbE optical modules will be automatically stopped in order to protect the system from high temperature damage. In this case, all the VLBI data will be lost.

Remedy: Exchange of the failed fans with spares is required.

2.3 Failure types: component failure of power supply unit

Effects: One or two AC/DC converters stop operation. If one power supply stops, the other AC/DC converter immediately works as a hot spare, and the system will continue normal operation. No data loss occurs.

If both of the two power supply units fail, the OFL system is out of power and all the data will be lost.

Remedy: Exchange of the power supply units with spares.

3 PIC

3.1 Failure type: random component failure

Effects: The PIC partly or completely ceases to function. This might result from a short power supply glitch. The result of this failure for VLBI mode is the loss of one of eight data channels. The power supply glitch could have a transient impact on the ALMA correlator, though this is a very low probability given the multi-level power regulation system. For example, a correlator microprocessor might become uncommunicative. Monitors will alert the operator to the failure.

Remedy: The condition will be readily detected with routine monitoring and can be remedied with a system reset by the CCC. A small fraction of the data might be corrupted. It is recommended that the damaged PIC be replaced by a spare, and later repaired off-line.

3.2 Failure type: SEU-triggered bit flip

Effects: The PIC partly or completely ceases to function. In practically all cases, will require an FPGA personality reload, which can be commanded via the CCC, to recover. There is a very low probability that an SEU event could cause a permanent failure in which case the board would have to be replaced with a spare. It is also possible that an SEU event would cause the either the C167 or Power PC processor to operate erratically or become uncommunicative. The likelihood of these failures is quite small, and in fact much smaller than SEU-caused failures in the rest of the correlator, which ALMA simply now ignores. There should be no impact to normal correlator operation. For VLBI mode, one of eight channels may be corrupted. Monitors will alert the operator to the failure.

Remedy: Recovery for this failure simply requires a system reset.

3.3 Failure type: Connector contact resistance becomes too high

Effects: The PIC will fail to operate reliably. The failure may be intermittent. Diagnostics are provided to isolate such failures. Recovery may be possible by simply re-seating the connector or by replacement of the offending cable/connector. This type of failure will affect one of eight VLBI channels. It would have no impact on normal ALMA operations. Monitors will alert the operator to the failure.

Remedy: Replace the offending cable/connector.

4 MASER

4.1 Failure type: Unscheduled shutdown (soft)

Effects: When all power is quickly removed from the maser (ie. AC removed and UPS unplugged) the resulting state is stable. However, if the UPS is allowed to completely discharge (as may happen if the power fails and no one is available to either turn the maser off or place it into a low power standby mode) then some electronic systems may still operate while others will be shut down. In that state, there may be build-up of impurities on the walls of the bulb within the maser cavity, but in general the dissociator should cut off before the hydrogen levels get low (that is the situation that can cause impurities on the bulb walls).

Remedy: After such a 'soft' shutdown the physics package will not usually be damaged, though some electronics modules may fail and have to be replaced. This is a fairly easy operation. After a 'soft' fail the usual re-start procedure has to be followed: re-apply AC power, restart receiver and thermal systems, allow for thermal to equilibrate, start hydrogen then beam-stabilizer, wait 15min, then when Hydrogen is stable restart dissociator and the maser should start oscillating.

4.2 Failure type: Prolonded shutdown

Effects: If all power to the maser stops, the chemical getters will continue to provide vacuum integrity for at least a week, potentially longer. After 1 week, outgassing can raise the pressure above 0.1 millibar and the ion pump will be unable to restart. Checking the maser operation should be a standard procedure following restart after prolonged power interruption.

Remedy: If pressure rises above 0.1 mb, a turbopump is needed to bring the vacuum down to 10^{-6} bar. In the unlikely event that the maser vacuum system is exposed to air, the chemical getters need to be re-activated by heating to 400C. This has never been seen in the field except for clear accidents.

In normal operation, the maser requires ~100W, and during startup it may draw as much as 200W. In standby mode (no dissociator, no hydrogen, no
beam-stabilizer, etc...; only pump and thermal) the maser takes ~30W. If a power outage is scheduled (or imminent) then an operator can place the maser in this standby mode for longer UPS life.

It is important to monitor UPS batteries on a regular basis. They usually provide 55 amp-hr, and the maser typically draws 3 amps. Additional batteries in the UPS may be cascaded to lengthen the time the maser can operate without AC power.

4.3 Failure type: General timing failure

Effects: While these masers are extremely reliability, a number of failures might cause the timing signal to lose lock or become noisy. This would normally be readily apparent to an operator. Since communication with other units is with optical fiber, any voltage spikes, etc. will not propagate to other ALMA electronics.

Remedy: Temporarily replace maser with existing Rb clock (involves making 2 connections; 5 MHz clock to CRG and 10 MHz signal from CRG to LO). Call T4
Science for repair under service contract. While normal operations would be unaffected, VLBI mode will be ineffective until the maser is restored.

5 Recorders

5.1 Failure type: Media

Effects: Media failure is common and expected. The Mark 6 units are resilient with respect to failure of individual disks in the 8-disk modules and the only adverse effect is possible loss of data already written to the disk. The failure has no impact on normal ALMA operations

Remedy: The offending drives would typically be replaced before returning the modules to use subsequent to correlation. Reliability of various types and manufacturers of drives is constantly being evaluated.

5.2 Failure type: System disk

Effects: Failure of a system disk is less common than recorder media failure, but not unheard of. It would temporarily render the Mark 6 unit unusable, but data collection would continue on the remaining 3 units, resulting in partial loss of VLBI data. Such a failure would result in warning indicators for operators. The failure has no effect on normal ALMA operations.

Remedy: The unit is line replaceable, and a spare will be provided to ALMA.
Replacing or rewriting the system disk is straightforward (the software module can be downloaded from the Haystack web site).

5.3 Failure type: Other recorder failure

Effects: Data collection would continue on the remaining 3 units, resulting in partial loss of VLBI data. Such a failure would result in warning indicators for operators. The failure has no effect on normal ALMA operations.

Remedy: The unit is line replaceable, and a spare will be provided to ALMA. All electronic boards and modules are commercial-off-the-shelf and can be readily replaced.

6 Software

6.1 Potential for software to harm hardware

With two exceptions, all of the existing ALMA hardware that APP uses (antennas, frontends, backends, correlator) will be operated with existing ALMA software methods. The two exceptions are the LTA and TFBs where we are implementing commands to adjust the calculations performed in these components. Improper coding or commanding may produce erroneous results, but no physical harm is possible.

For the new hardware: the maser and optical fiber link systems are only monitored, not commanded. The PICs are commanded, but the only non-logical command is to apply or remove power, and the units may be left on or off indefinitely without harm. Finally, the recorders are commanded to make recordings; but these are server-class computers designed to operate for years. The only commands which change state are the record on/off commands. If improperly used, these may fill up the disks with useless data, or fail to record the useful data, but again, no physical harm can result from the software.