SYSTEM REQUIREMENTS SPECIFICATION

EVLA Correlator Monitor & Control

Project Document:

Revision 1.0

Preliminary Draft

Bruce Rowen, December 5, 2002

National Radio Astronomy Observatory

Array Operations Center

P.O. Box O

Socorro, NM 87801-0387

Revision History

Date	Version	Description	Author
12-5-2002	1.0	Initial draft	Bruce Rowen

Table of Contents

1 Introduction

1.1 Purpose

The primary goal of this document is to provide a complete and accurate list of requirements for the EVLA Correlator Monitor & Control System.

The primary audience of this document includes, but is not limited to, project leaders, the designers and developers of the system and the end user. The document may also be of interest to EVLA project scientists and engineers or as a reference for individuals involved in similar projects with similar requirements.

Much of this document is based on preliminary ideas and concepts from NRC-EVLA Memo #015 [8] and previous System Requirement Documents [5] and [9].

The requirements contained in this document are numbered based on the section/subsection in which they appear.

1.2 Scope

The Correlator Monitor & Control System provides the physical link between the WIDAR Correlator hardware and the EVLA monitor & control system. It is the primary interface by which the correlator is configured, operated, and serviced.

The primary functions of the Correlator Monitor & Control System are as follows:

- Receive configuration information from the EVLA M&C system and translate this info into a physical correlator hardware configuration.
- Process and transfer dynamic control data (models, filter parameters, etc), and monitor data (auto correlation products, state counts, etc.)
- Monitor Correlator and correlator subsystem health and take corrective action autonomously (where possible) to recover from hardware and computing system faults.
- Perform limited amounts of real-time data processing and probing such as providing tools to collect and display auto correlation products.
- Allow for easy system access to aid testing and debugging.

1.3 Definitions, Acronyms, and Abbreviations

1.3.1 Definitions

Administrator – An individual with unrestricted access to all aspects of the system.
Real-time – Monitor and control operations which have hard deadlines that when missed result in data corruption/loss.
Backend – A computer system that performs final real time post-correlation processing on data received from the correlator baseline boards.

CMCS – Correlator Monitor and Control System
MCCC – Master Correlator Control Computer
CPCC – Correlator Power Control Computer
CPU – Central Processing Unit. In this document CPU refers to a single board computer or computer system
e2e – End-to-End System (archive)
M&C – Monitor and Control System
EVLA – The VLA Expansion Project
RFI – Radio Frequency Interference
SyRS – Refers to the *System Requirements* document.
SRS – Refers to the *Software Requirements Specification* document.
VCI – Virtual Correlator Interface.

1.4 References

1) ANSI/IEEE Std 830-1998, IEEE Recommended Practice for Software Requirements Specifications
2) ANSI/IEEE Std 1233-1996, IEEE Guide for Developing System Requirements Specifications
3) EVLA Memo No. 15, Scientific Requirements for the EVLA Real-Time System
4) EVLA Project Book
5) EVLA System Requirements (SyRS)
6) EVLA Architecture and Design
7) Refined EVLA WIDAR Correlator Architecture, NRC-EVLA Memo# 014, Brent Carlson, Oct. 2, 2001.
8) EVLA Correlator Monitor and Control System, Test Software, and Backend Software Requirements and Design Concepts, NRC-EVLA Memo # 015, Brent Carlson, Jan. 23, 2002.
9) EVLA Correlator Backend, Software Requirements Specification.

1.5 Overview

The remainder of this document contains a more detailed description of the Correlator Monitor and Control System as well as the primary requirements necessary to design and build the system. Section 2 provides a general description of the Correlator M&C System. Section 3 details the requirements of the product and is the core of this document.

The format of the document follows that outlined in the IEEE STD 830 document, IEEE Recommended Practice for Software Requirements Specifications.

2 Overall Description

2.1 Product Perspective

The EVLA Correlator Monitor and Control System is responsible for correlator configuration, real time monitor/control, and hardware testing/servicing. The CMCS exists as an integrated part of the overall EVLA Monitor and Control Structure. The CMCS will provide a level of abstraction to modularize the correlator system within the EVLA environment. The "gateway" to the correlator will be through the Virtual Correlator Interface (VCI) which will exist as a software entity on the MCCC.

The CMCS will be designed and implemented as a Master/Slave network with one computer system coordinating the activities of a number of "intelligent" hardware control processors. The Master is expected to handle the bulk of the monitor/control interface with the outside world whereas the slaves will be only concerned with the correlator hardware systems under their direct control. This topology will place the real-time computing requirements in the slave layer and the quasi real-time, network-chaotic loads into the master layer. One of the primary benefits of this structure is isolation (ease of serviceability, programmability) of the correlator hardware from the EVLA M&C environment. The system is expected to be redundant in critical areas and highly modular.

2.2 Product Functionality

2.2.1 Monitoring

The Correlator monitor subsystem will provide EVLA system wide access to all correlator system states (including the M&C supervisor system state). Some of this information will be provided on a time synchronous basis as required by other systems (backend, monitor archive, data archive, etc.) and other information will only be presented on a request basis. The CMCS will be a fully observable system with the only limits placed on information access being those imposed by hardware, bandwidth, and/or security restrictions. Error and status messages will be provided in a concise time/location referenced format to upper system levels in a content controllable manner.

2.2.2 Control

Correlator configurations and control instructions will be received from the EVLA M&C system in a form suitable for translation by the MCCC. The translation will provide the correlator with specific goal oriented hardware configuration tables to satisfy the configuration requested by the EVLA M&C. A second interface with a human GUI will also allow for configuration of the correlator hardware, preferably through the same table structures used above. This translation interface will be called the Virtual Correlator Interface (VCI).

2.2.3 Data Output

Specific data sets required by the Backend Data Processing System (state counts, auto correlations, etc) will be provided in a timely and robust fashion over a secondary virtual network. Ancillary monitor data including system health, error messages and configuration echoes will be spooled such that temporary loss of network communication with the EVLA M&C network will not result in loss of monitor data. Data sample rates and contents will be fully controllable via either the EVLA M&C or the Backend processing controller.

2.2.4 Data Input

The MCCC will accept external data feeds for models, time standards, fiber-link phase corrections and other required data to be packaged with control data delivered to the correlator hardware.

2.2.5 Recovery

The ability to attempt recovery from failure or hot-swapped hardware devices will be built into this system. Should a CMIB subsystem fail and not respond to reboot requests or other self-heal attempts, an alert notice will be issued so appropriate personnel can affect a hardware repair. The CMIB subsystem will then be automatically restarted and configured back into the current operational environment.

MCCC health will be monitored by internal software processes (watchdogs) and external systems (the CPCC). Should a non-recoverable MCCC system failure occur, the backup MCCC system will be activated automatically via the CPCC or by external human intervention? It is intended that both primary and secondary MCCC systems maintain full CMCS state information such that any hard failure (unrecoverable) in the primary node can be corrected by simply rerouting M&C communications to the secondary.

Watchdog processes and the MCCC will likewise monitor CPCC health. Due to the more hardware specific connections and controls of the CPCC, actions taken by external system upon hard failures are TBD.

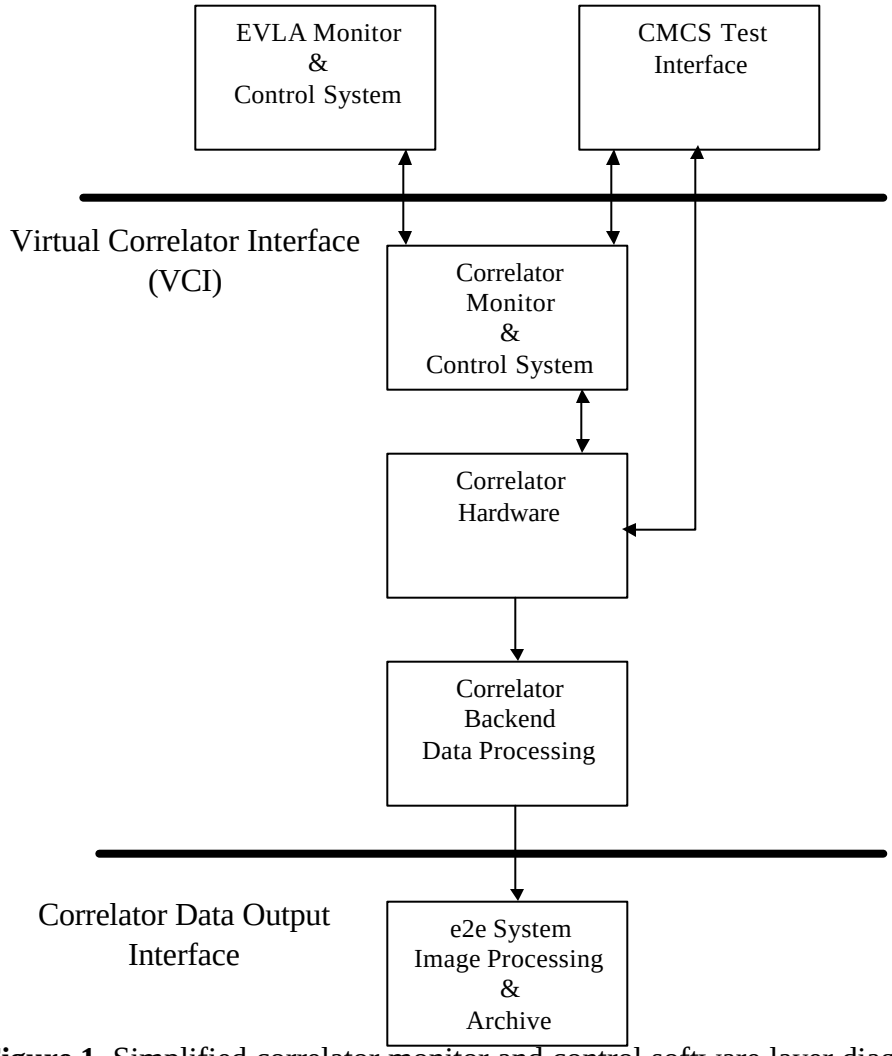

Figure 1. Simplified correlator monitor and control software layer diagram

2.3 User characteristics

All use of the Correlator Monitor and Control System will be through the VCI or MCCC. Software tools will be provided to assist the user at all access levels from system wide configuration and control to a low level CMIB command line instruction.

2.3.1 Array Operator

The primary contact with array operations will be via status and error messages channeled through the Monitor and Control System.

2.3.2 Engineers and Technicians

The ability of the Correlator System to achieve and maintain high reliability and uptime will be vitally dependent upon reliable operation and rapid diagnosis and repair of faults in the hardware and software systems. These individuals will be responsible for performing corrective and preventive maintenance along with periodic performance tests and upgrades. Engineers and technicians will need tools to inspect and monitor individual CMIB layer devices from remote locations and have the ability to fault trace to a specific hot-swappable subsystem.

2.3.3 Software Developer

These individuals are responsible for developing the software and will interact with the system to ensure that it is functioning properly. The software developer requires remote access to the system so that troubleshooting can be accomplished away from the EVLA and during non-working hours.

2.3.4 Web User

A few authorized individuals may be allowed access to parts of the system that are usually considered restricted.

2.4 Constraints

2.4.1 Criticality of the Application

The Correlator Monitor and Control is a critical component in the Astronomical data path. If it is unavailable, incoming astronomical data will be lost.

2.4.2 Computer Hardware Limitations

The ultimate determiner of a reliable and available correlator is dependent on the stability of the CMCS network and control computers. Functionality needs to be modularized to provide the easiest means of fault detection and repair.

2.4.3 Computer Software Limitations

The ultimate ease of use and flexibility of the correlator is rooted in the CMCS software. Full access is required with a high level of data integration to provide the user with a logical and coherent interface.

2.5 Assumptions

2.5.1 Configuration Data Stream

It is assumed that the Correlator will receive configuration data in a format that is unambiguous and results in a convergent hardware configuration (requested configuration is valid and achievable).

2.5.2 Auxiliary Data

It is assumed that all auxiliary data needed for real time update of correlator parameters (delay models, fiber round trip phase corrections, time codes, dynamic configuration data, etc.) will be provided directly by the EVLA M&C system or by dedicated servers.

2.5.3 Outgoing Data Stream

It is assumed that the backend data processing and EVLA M&C systems will be capable of accepting output data rates (both those required and those requested) generated by the CMCS.

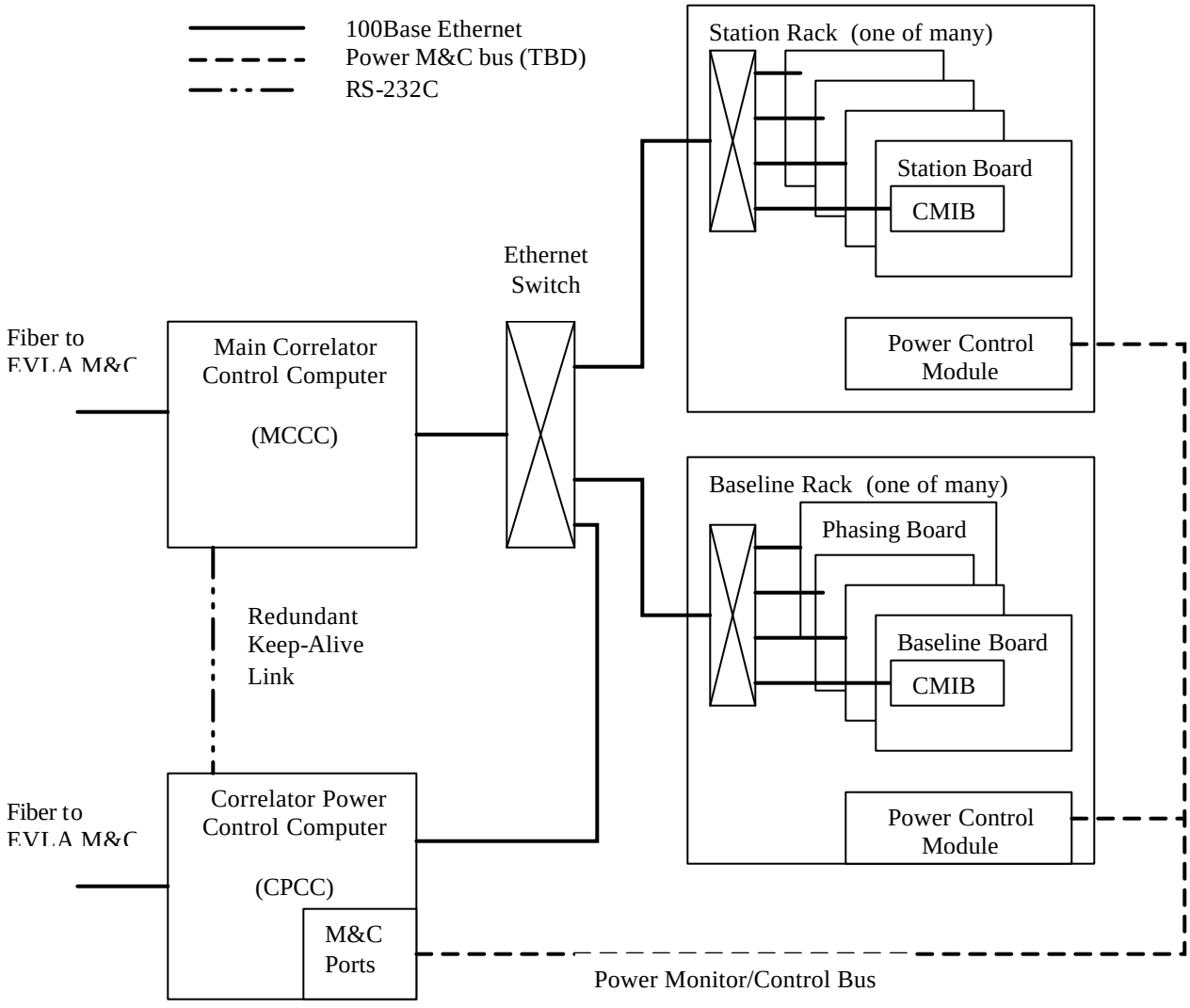

Figure 2. CMCS network connection topology (Only two racks/subsystems shown)

3 Specific Requirements

3.1 Communication Network Interface Requirements

3.1.1 Correlator CMIB, MCCC, CPCC Interface

.

	Description
3.1.1.1	Network Protocol – *The interface between the CMIB, MCCC, and CPCC shall be Ethernet (IEEE 802.3 compliant) of 100 Mbits/sec or better data rate.*
3.1.1.2	Network Topology – *The interface shall be transformer coupled copper twisted pair unless other materials are required for noise (RFI), ground isolation, or physical layout constraints (long distances).*
3.1.1.3	Network Distribution - *Network switches shall be employed to distribute traffic within a correlator rack and where their use will significantly reduce overall network wiring complexity*.
3.1.1.4	Network Isolation – *The MCCC-CMIB, MCCC-CPCC, and MCCC-EVLA M&C networks shall be on separate physical interfaces.*
3.1.1.5	Redundant Communication - *There shall be a redundant communication path (serial RS-232c or equivalent) between the MCCC and CPCC to provide for remote reboot in the event of a networking or computing failure.*

3.1.2 MCCC to EVLA M&C Interface

Req. ID	Description
3.1.2.1	Network Protocol – *The interface between the MCCC and external networks (EVLA M&C) shall be Ethernet (IEEE 802.3 compliant) of 100 Mbits/sec or better data rate*.
3.1.2.2	Network Topology – *Pathways penetrating the correlator shielded room shall be fiber optic or other low RFI material to meet RFI specifications.*
3.1.2.3	Security - *Network routers/switches shall be employed at the MCCC-EVLA M&C interface level (or higher) to protect the MCCC from unauthorized access and irrelevant network traffic.*

3.1.3 CMIB to Correlator Hardware Interface

Req. ID	Description
3.1.3.1	Hardware communications – *The CMIB daughter board shall communicate with the correlator carrier boards via either the PCI or ISA busses*. Alternative communication paths may be through a serial or parallel connection as required.
3.1.3.2	Hardware identification – *The CMIB shall be capable of reading a 16-bit identifier from the host correlator board*. This identifier will be used to form a unique IP address for CMIB network addressing and allow carry over IP addressing for hot swap modules.
3.1.3.3	Hardware addressing – *The CMIB shall be able to read back the contents of all writeable hardware control registers where meaningful*. It is desired that the state of the correlator hardware be available through interrogation across the CMIB bus for monitoring and fault tolerance.
3.1.3.4	Hardware Booting – *The CMIB shall have control of hardware "warm boots" such that an external command from the MCCC to reboot the CMIB shall have an option to force a hardware warm boot.*
3.1.3.5	Hardware Visual Health Monitoring – *The carrier board for the CMIB shall have an externally visible indicator (LED or other) that will provide a user with a physical indication of CMIB operational status (red = fault, green = ok).*

3.2 Computer Functional Requirements

3.2.1 General

Req. ID	Description
3.2.1.1	Power Supplies– *Where applicable, all computers and peripherals shall be powered though UPS type devices with sufficient capacity for the computers to safely coordinate a system wide shutdown of the correlator hardware in the event of a prolonged power outage.* The UPS devices need the ability to signal the CMCS when a power outage has occurred and keep the CMCS apprised of time remaining on backup power.
3.2.1.2	Accessibility – *All computers within the CMCS system shall have the ability for authorized users to directly access individual systems for maintenance and monitoring through remote logins.*
3.2.1.3	Self-Monitoring – *Each computer system in the CMCS shall have a hardware based watchdog timer configured to reboot the system in the case of a system hang.* Reboots should result in minimal system interruptions with the offending CPU reconfiguring and returning to service autonomously.

3.2.2 CMIB

Req. ID	Description

3.2.2.1	Form Factor– *The CMIB shall conform to both electrical and physical PC104+ standards.*
3.2.2.2	Module Features – *The CMIB shall contain 64 Mbytes or greater of SDRAM, IDE hard disk interface, minimum of one serial and one parallel interface, PCI/ISA buses, 100BaseT network interface, capacity to boot and run a generic COTS operating system in a near real-time environment from local non-volatile storage.*
3.2.2.3	Operating System – *The operating system/module combination shall be capable of supporting the real-time requirements of the correlator hardware, hardware monitor/control/diagnostics with support for standalone "test bench" operation with simulated control data generation, and the ability to access and upgrade correlator hardware PLD/FPGA personalities through its network connection.*

3.2.3 MCCC

Req. ID	Description
3.2.3.1	Form Factor – *The MCCC shall be a high availability type general-purpose computer capable of supporting multiple Ethernet interfaces, COTS operating systems, and support server/host services for the CMIB operating system.* This computer may exist as a hot swappable or redundant CPU device capable of self-healing where possible.
3.2.3.2	System Isolation – *The MCCC shall have all required disk and file system facilities installed locally such that the system can boot and run in a stand-alone configuration.* This should allow the correlator CMIBs to boot, configure, and run without any communication outside of the correlator M&C network.

3.2.4 CPCC

Req. ID	Description
3.2.4.1	Form Factor – *The CPCC shall be a high availability type general-purpose computer capable of supporting a COTS operating system and have the ability to accept a large number of external hardware status signals (power, temp, etc) either directly or through external interface hardware.* This computer may exist as a hot swappable or redundant CPU device capable of self-healing where possible.
3.2.4.2	System Isolation– *The CPCC shall have all required disk and file system facilities installed locally such that the system can boot and run in a stand-alone configuration.* This requirement is to allow correlator power monitoring and control to continue in the event of an M&C network failure.

3.3 Performance Requirements

3.3.1 Hardware

Req. ID	Description
3.3.1.1	Processing Software Performance – *The CMCS processors shall be*

	capable of meeting all data processing deadlines and anticipated future requirements
3.3.1.2	Processor Hardware Performance – *The CMCS processors shall be capable of responding to correlator hardware inputs (interrupts) in a deterministic fashion with sufficient performance to avoid data loss, corruption or overflows.*

3.3.2 Software

Req. ID	Description
3.3.2.1	Errors – *All lower system error and debug messages shall be present at the MCCC layer*. Aside from a networking or CPU failure, It should never be necessary to directly access a CPU to display error messages.
3.3.2.2	Error Message Access – *All system error and debug messages shall be categorized in a logical fashion such that message traffic can be filtered as to content, detail, and message rate*. Personnel interested in error messages should be able to easily filter the error message stream.
3.3.2.3	Time Stamps – *All messages passed between CMCS system layers shall have both UTC and wall clock time stamp information appropriate for the message type.* Error messages will be stamped with their discovery time, control messages will be stamped with their generation time. Other message internal time stamps can be used as monitor/control parameters as deemed necessary.
3.3.2.4	Test Software. - *Software shall be provided that allows an authorized user full access to all messaging, monitor, and control traffic throughout the CMCS*. This software will provide full system access for testing, debugging, and control while the correlator is off line or under the control of the EVLA M&C system.
3.3.2.5	Test Software GUI. *A Graphical User Interface shall be provided as an interface to the CMCS test software that allows for a convenient and configurable tool to access the CMCS remotely through the VCI.*

3.4 Reliability/Availability

Req. ID	Description
3.4.1	Auto-correction – *the CMCS shall be self-monitoring.* It will be capable of detecting, reporting on and automatically taking action to remedy or lessen the impact of, at a minimum, the following types of abnormal conditions: processor hardware failure, operating system hangs or crashes, temperature or voltage deviations, computational performance below minimum specifications, computational error rates above maximum specification, internal communications failures, and external (with the EVLA M&C) communications disruptions.
3.4.2	Software – *the software part of the system shall be able to perform without total system restart due to internal failure between system maintenance windows.*
3.4.3	Hardware – *the hardware part of the system shall be able to perform indefinitely without complete loss of service, except in the event of total failure of primary and backup power*.

3.4.4	Loss of Control Data– *the system shall be able to continue processing of all correlator configuration/control events until the queues of parameters are exhausted and external communications are restored*
3.4.5	Standby Mode – *the system shall be able to sit at idle and resume operations with minimal (amount TBD) delay*.

3.5 Serviceability

Req. ID	Description
3,5,1	Hardware Accessibility – *all system processing and interconnect hardware shall be readily accessible for maintenance, repair, replacement and/or reconfiguration*. This excludes items that due to their physical location, are not practical to configure for ready access (i.e. backplanes)
3.5.2	Software Accessibility – *all systems and application source code shall be available to or on the systems that execute it*.
3.5.3	Debugging – *all software application modules shall be debuggable.* They should be organized such that all inputs and outputs can be simulated if necessary.
3.5.4	Processes – *all software processes shall be killable, restartable, debuggable and testable with minimal impact on normal system operations.*

3.6 Maintainability

Req. ID	Description
3.6.1	Software tools – *software tools and pre-built applications that do not have source code available shall come with a complete diagnostic package and customer support*.
3.6.2	Operating Systems – *operating system software shall either have source code available or come with sufficient diagnostics and customer support.*

3.7 Scalability

Req. ID	Description
3.7.1	Hardware – *I/O, communications, and processing hardware shall be easily expandable, reconfigurable, augmentable and replaceable to meet increasing data traffic and processing demands imposed by EVLA science, Correlator changes, and availability of new hardware.*
3.7.2	Transparency – *3.7.1, above, shall be accomplished in manner that is transparent to processing, communications and I/O software functions with the possible exception of recompilation of executables*.
3.7.3	Seamlessness – *3.7.1, above, shall be accomplished in a manner that is seamless, in that it does not affect hardware modules or software functionality that it meets at interfaces*.

3.8 Security

The CMCS needs a robust security mechanism in place so that unauthorized users are not allowed access. Authorized users are expected to be restricted to software and hardware development, testing, maintenance and operations personnel.

All users of the CMCS must be uniquely identified. This could be done via a username and associated password scheme that would authenticate and authorize the user access to the system and, if applicable, grant the user access to restricted or controlled parts of the system. If a user cannot be identified, they will not be given access. In order to monitor all past access to the system, all attempts to access the system should be logged.

Users' needs and expectations from the system will be different. Systems operations should be given unrestricted access to all aspects of the system and should have the authority to grant and revoke privileges on a per-user basis. Development, testing and maintenance personnel, on the other hand, require access to some parts of the system, but not all, indicating that an access level is needed that allows privileges to be granted on a per-user and what-do-you-need-to-do basis.

Req. ID	Description
3.8.1	*All users of the system shall login using some form of unique identification.* (e.g., username and password)
3.8.2	*All login attempts shall be done in a secure manner.* (e.g., encrypted passwords)
3.8.3	*A system administrator shall have unrestricted access to all aspects of the system.*
3.8.4	*Each user shall have a set of system access properties that defines the user's privileges within the system.* (e.g., the subsystems a user may control or system tools the user may access).
3.8.5	*The administrator shall have the ability to create and add a new user to the system.*
3.8.6	*The administrator shall have the ability to remove a user from the system*.
3.8.7	*The administrator shall have the ability to edit a user's system access properties*.
3.8.8	*The administrator shall have the ability to block all access to the system for all users or selectively by user*. (All blocked users with active sessions shall automatically be logged off.)

3.9 Installation and Upgrades

Req. ID	Description
3.9.1	Operations Activities – *the system shall continue operations, although not*

	necessarily at full capacity, on all unaffected resources during partial shutdowns for maintenance, repair and/or upgrade.
3.9.2	Replaceability –*modular design principles shall be employed to the maximum extent possible. Maximal practical use of available "hot-swappable" devices and components shall be made*.

3.10 Documentation

Req. ID	Description
3.10.1	Hardware – *complete and comprehensible hardware systems specifications and configuration information shall be readily available*.
3.10.2	Software Coding Practices– *software system and application code shall be well documented and written in a generally familiar language or languages (preferably not more than two). Software shall be written in a style that is easily readable and using practices that allow for minimal confusion.*

.