ALMA Memo 600

ALMA Development Study

Integrated Alarm System for the ALMA Observatory

Erich Schmid – ESO
Emilio Barrios – JAO
Bernhard Lopez – JAO
Tzu-Chiang Shen – JAO
Alessandro Caproni - ESO

Appendix 1:

Report for an Integrated Alarm System for the ALMA Observatory, ESA/ESOC

Appendix 2:

Technical Report Integrated Alarm System UI Front-End Workshop, INRIA Chile

European Organisation for Astronomical Research in the Southern Hemisphere

Atacama Large Millimeter/submillimeter Array

ESO ALMA Support Centre

ALMA Development Study

Integrated Alarm System for the ALMA Observatory

Document Number: ESO-287159

Document Version: 1

Document Type: Design Report (DER)

Released On: 2016-06-30

Document Classification: Public

Prepared by: Schmid, Erich

Validated by: Schmid, Erich

Approved by: Wild, Wolfgang

Name

Authors

Name	Affiliation
Erich Schmid	ESO
Emilio Barrios	JAO
Bernhard Lopez	JAO
Tzu-Chiang Shen	JAO
Alessandro Caproni	ESO

Change Record from previous Version

Affected Section(s)	Changes / Reason / Remarks

Contents

1 Introduction

1.1 Overview

ALMA is a complex operational environment consisting of many components ranging from a power plant, site monitoring systems and the 66 antennas, each equipped with numerous high-tech devices, to a computing, networking and database infrastructure. All these components are distributed over a large physical area in a harsh environment. Each component must function correctly to allow the observatory to conduct successful observations, and each failure cannot only bring on-going observations to a halt, but in some cases also lead to more wide-ranging failures that may be costly to recover from, if an initial alarm is not dealt with swiftly.

It is an essential task of the array operators at the OSF to monitor all the components and to react quickly on any abnormal situation. In such a complex environment it is impossible to carry out this task without a proper alarm system.

This report contains the results of a development study into an integrated alarm system for the ALMA observatory. The incentive for this study came as the result of discussions between key people of operations, engineering and computing at the OSF, which clearly identified the need for such an initiative. The head of the European Integrated Computing Team (ICT-EU) proposed the funding of this study to the management of the ESO ALMA Support Centre (EASC) in mid 2015, who quickly approved this as an internal study with limited funding for travel and expert consulting services, while the contributions of ALMA staff were done “in-kind” as part of the regular ALMA work assignment, which was also approved by management of each ALMA partner. The study was led by ICT-EU with major contributions from operations, engineering and computing staff at the Joint ALMA Observatory (JAO). The total duration of the study was, as originally planned, nine months, during which all the desired outcomes have been achieved.

1.2 Applicable Documents

The following documents, of the exact version shown, form part of this document to the extent specified herein. In the event of conflict between the documents referenced herein and the content of this document, the content of this document shall be considered as superseding.

AD references shall be specific about which part of the target document is the subject of the reference.

AD	Document Nr.	Version	Document Title	Part / Section
AD1	ESO-271448	1	Internal ALMA Development Study Proposal: Integrated Alarm System for the ALMA Observatory	all

1.3 Reference Documents

The following documents, of the exact version shown herein, are listed as background references only. They are not to be construed as a binding complement to the present document.

RD Nr.	Document Nr.	Version	Document Title
RD1	YA-711	Feb 2011	Principles for alarm system design; Norwegian Petroleum Directorate http://www.ptil.no/getfile.php/Regelverket/Alarm_system_design_e.PDF
RD2		Vol.2, No.1 – May 2011	Investigating Facility Managers' Decision Making Process through a Situation Awareness Approach; International Journal of Facility Management http://ejournals.library.gatech.edu/ijfm/index.php/ijfm/article/viewArticle/35/51
RD3	ALMA-SW-NNNN	1.8	ACS Alarm System – Software Architecture and How-to Manual http://www.eso.org/projects/alma/develop/acs/OnlineDocs/AlarmSystem.pdf
RD4		October 23, 2010	Alarm system guidelines; Alessandro Caproni http://www.eso.org/projects/alma/develop/acs/OnlineDocs/AlarmSystemGuidelines.pdf
RD5	Emerson Chloride 80-NET Brochure		Chloride 80-NET from 60 to 500 kW *Secure Power for Mission Critical Applications* http://www.emersonnetworkpower.com/en-EMEA/Products/ACPower/Documents/Chloride-80-NET/MKA4L0UK80NET.pdf
RD6	General Electrics SG Series UPS Brochure		SG Series UPS 10-600 kVA three phase 400 Vac with ultra-high efficiency eBoost™ technology http://apps.geindustrial.com/publibrary/checkout/GEA-D1100-GB?TNR=Brochures%7CGEA-D1100-GB%7Cgeneric
RD7	General Electrics Multilin F35	5.8x	F35 Multiple Feeder Protection System UR Series Instruction Manual http://www.gegridsolutions.com/products/manuals/f35/f35man-v1.pdf
RD8	1B025 - ESO ALMA	17a	Turbomach Human Machine Interface (Chapter 5)
RD9	LIT-1201531	7.0	BACnet® Controller Integration with NAE/NCE Technical Bulletin http://cgproducts.johnsoncontrols.com/met_pdf/1201531.pdf?ref=binfind.com/web

RD10	ESA/ESOC Document	28/04/2016	Report for an Integrated Alarm System for the ALMA Observatory
RD11	INRIA Chile Document	18/04/2016	Technical Report Integrated Alarm System UI Front-End Workshop

1.4 Definitions, Acronyms and Abbreviations

This document employs several abbreviations and acronyms to refer concisely to an item, after it has been introduced. The following list is aimed to help the reader in recalling the extended meaning of each short expression:

ACA	Atacama Compact Array
ACS	ALMA Common Software
ADE	ALMA Department of Engineering
ALMA	Atacama Large Millimeter/sub-millimeter Array
AOG	Array Operations Group
AOS	ALMA Array Operations Site
API	Application Programming Interface
BACI	Basic Access Control Interface (provided by ACS)
BACnet	Building Automation and Control Networks
CCTV	Closed Circuit Television
CERN	Conseil Européen pour la Recherche Nucléaire
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-The-Shelf
EASC	ESO ALMA Support Centre
ESA	European Space Agency
ESO	European Southern Observatory
FTE	Full Time Equivalent
GUI	Graphical User Interface
HCI	Human-Computer Interaction
HVAC	Heating, Ventilation, and Air Conditioning
ICT	ALMA Integrated Computing Team
INRIA	Institut national de recherche en informatique et en automatique
ISM	International Staff Member
JAO	Joint ALMA Observatory
JSON	JavaScript Object Notation
LAN	Local Area Network
LASER	Large Hadron Collider Alarm Service
LSM	Local Staff Member
NAOJ	National Astronomical Observatory of Japan
NN	No Name
NRAO	National Radio Astronomy Observatory (USA)
POC	Point-Of-Contact
OSF	ALMA Operations Support Facility
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCO	ALMA Santiago Central Office
SNMP	Standard Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TMCDB	Telescope Monitoring and Control Database
UPS	Uninterruptable Power Supply
WSDL	Web Services Definition Language
XML	Extensible Markup Language

2 Motivation and Approach

2.1 Motivation

The ALMA observatory currently uses a variety of tools to monitor the status of the hardware and software components that constitute ALMA, and to detect alarm conditions from these components upon which the operators, engineers and support staff at the observatory must react.

While the main science operations system, consisting of the 66 ALMA array elements, the baseline and ACA correlators, data processing infrastructure and the ALMA archive has been developed as an integrated system that is controlled by the ALMA software, much of the supporting infrastructure that is nevertheless critical for the system as a whole, has to date not been integrated into a consolidated monitoring and alarm system. The array operators are not directly responsible for operating and monitoring some of these related systems, such as the power plant, HVAC systems or weather stations, but it is still of utmost importance for them, as the central point of ALMA operations, to not only have full situational awareness of all the systems that comprise ALMA, but also to be able to centrally monitor the correct functioning of all systems and notify the responsible groups of any alarm conditions for quick action.

This study addresses the need for and the requirements to be met by a central integrated alarm system for the ALMA observatory.

2.2 Approach

This study took the following approach to identify the requirements and high-level design for an integrated alarm system:

1. Identify all the hardware and software systems that comprise the ALMA observatory operations on-site, which are relevant for an integrated alarm system.
2. For all the systems identified in the previous step, document the existing alarm systems and available interfaces to access relevant data.
3. Engage an external alarm system expert to analyse the existing systems and to provide a report outlining possible ways forward.
4. Engage a human-computer interface expert to draft possible user interfaces to present alarm information in an integrated and consistent fashion.
5. From all the information gathered in the previous steps, compile a report (this document) to stipulate the requirements for an integrated alarm system.
6. Provide a possible way forward to define an ALMA development project to design, implement and deploy an integrated alarm system.

The remainder of this document presents the requirements for an integrated alarm system, followed by some design considerations for the eventual implementation of such a system.

3 Requirements for the Integrated Alarm System

This section defines the high-level requirements for an integrated alarm system for the ALMA observatory. These requirements have been mainly derived from the day-to-day array operations work by including operators, engineers and support staff in this study, as well as from the reference documents “Principles for alarm system design” [RD1], the situation awareness concepts presented in [RD2] and the ESA report [RD10].

3.1 Definition of Terminology

The following table presents a list of terminology used throughout this document. It is not meant to be complete nor binding for the eventual implementation of an integrated alarm system, but will be useful for the understanding of this document.

ALMA staff	All the people currently working on ALMA. This is not limited to JAO staff in Chile, but includes all staff at the executives and partner institutes assigned to ALMA.
Component	Any part, hardware or software that comprises the ALMA observatory. Specifically any such part that will be monitored by the integrated alarm system and can produce alarms, directly or indirectly. Components are hierarchical and can contain any number of sub-components.
System	A top-level component that constitutes a major part of the ALMA observatory.
Subsystem	A first-level sub-component of a system. Subsystems do not contain other subsystems.
Primary alarm system	The alarm system panels the array operators at the OSF interact with. This is a pure user interface consideration and does not imply a separate underlying alarm system per se.
Secondary alarm system	Read-only alarm system panels for ALMA staff. This is a pure user interface consideration and does not imply a separate underlying alarm system per se.
Alarm	The notification that a component has entered an abnormal condition.
Alarm status	An alarm can have four states: 1. **New**: the operator has not yet responded to the alarm and the alarm condition is still active. 2. **Acknowledged**: the operator has acknowledged the alarm, but the alarm condition is still valid. 3. **Shelved**: The operator has removed the alarm from the display. 4. **Cleared**: the component has entered a normal status after a previous alarm condition. Any alarm must be acknowledged or shelved by an operator, even if it is cleared (by the system). As a consequence these states are neither sequential nor exclusive. The final state for an alarm will normally be *acknowledged* and *cleared*.

Alarm response	The operator can respond in two ways to a new alarm: 1. **Acknowledge**: the operator has taken the required action to deal with the alarm condition. This does not imply that the alarm condition has been cleared yet. 2. **Shelve**: the operator has decided to not take action on the alarm, but rather remove it from the display and stop it from reoccurring.

3.2 Introduction

This introduction summarises some key ideas and concepts for the new integrated alarm system. As such it is neither part of the requirements definition, nor should it be mistaken as a functional or design specification. Its sole purpose is to provide the reader with background information for the better understanding of the detailed requirements and the high-level design concepts that are outlined in the following sections.

As specified in [RD1] an alarm system is a basic operator support system for managing abnormal (also called non-nominal) situations and it has the following two functions:

1. To warn the operator about a situation that is not normal; alarms must be relevant to the operator's role at the time, indicate what response is required, be presented at a rate the operator can deal with, and be easy to understand.
2. To serve as an alarm and event log, which can be used for an analysis of incidents and to optimise operations.

The alarm system must provide *useful* information and functionality to support the array operators' tasks. Information must be presented and handled in a way that is compatible with human capabilities and limitations, so that the alarm system remains *usable* for the operators in all situations.

While the scope of this study is clearly limited to an actual *alarm* system and not a generic monitoring and control system, it became clear during the study, in particular when taking the ESA system and their experience as an example (see [RD10]), that a system that simply presents alarms without any visual context information will not be suitable to satisfy the needs. It has been identified that the best representation will be based on high-level status displays of the inherently hierarchical ALMA observatory, with drill-in capabilities to identify the root cause and appropriate action to be taken for any abnormal situation. Simple, self-explanatory and above all consistent colour coding and audio-visual effects will be used to draw the operators' attention to problems and assist them in taking the appropriate action.

Note: The term *monitoring* (or any variation thereof) will be used in the remainder of this document with the meaning of *monitoring the alarm system*. It must not be confused with the ALMA monitoring system that stores monitor point data for analysis, nor with the regular monitoring tasks carried out routinely by operators.

A conceptual example of such hierarchical displays and navigation between them is shown in Figure 1 below.

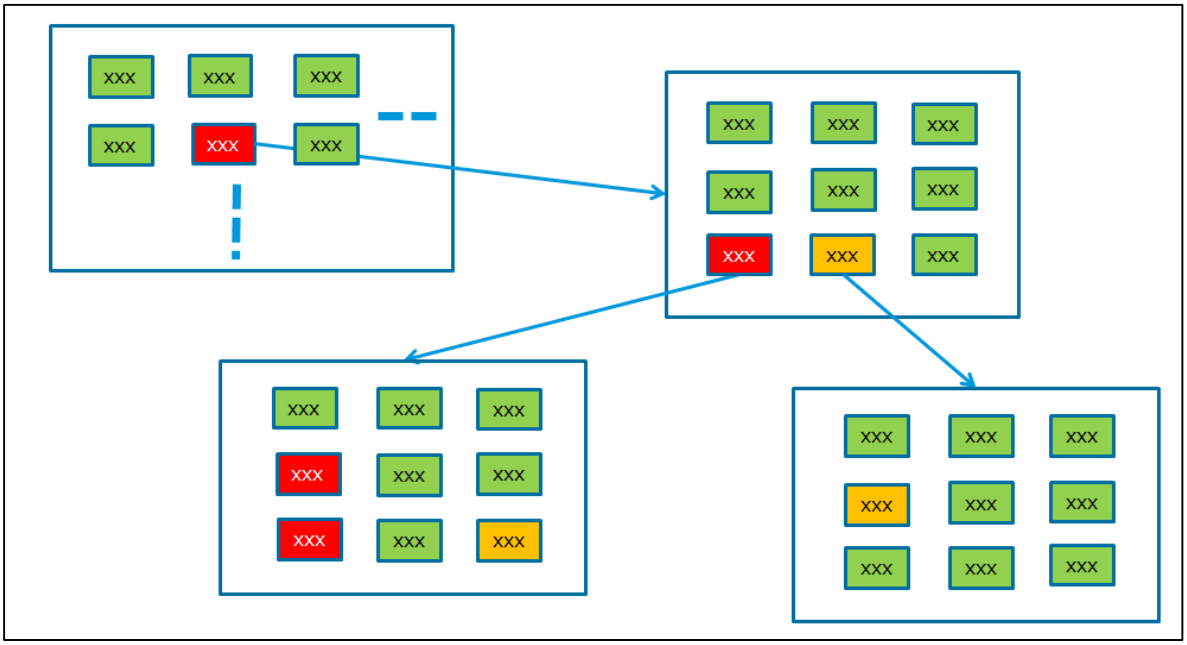


Figure 1 - Conceptual display visualisation and navigation

The top-left box represents a top-level view of several components, e.g. a particular subsystem of ALMA. The red box inside shows an alarm condition for one of these components. Yellow boxes represent components that report a less severe alarm, e.g. a warning. The blue arrows illustrate drilling in to more detailed views of the components reporting alarms. This can be continued until the most detailed component that is actually reporting the abnormal status is visualised.

This diagram helps to express the following needs:

- There is a need to define several displays that show information related to the monitored systems.
- There is a need to display components, which summarize an overall status of other components. For example, an array element should summarize the information from all the antenna subsystems (such as: front end, backend, calibration device, etc.) - conceptually, this relationship of components can be visualized as a tree where each parent summarizes the state of its children.
- The monitored components need to display information (related to their value or overall state)
- There needs to be navigation between components of a display and a new display (i.e. by clicking on a monitored component a new display will open).
- There needs to be different colour coding to express different states of the monitored components. The colour coding and the general usability must be consistent for all display panels.

Some of the monitoring displays (for example a top level status display, or a high level mimic display) will need to be always visible, in order for the operator to always see the overall status of the system. This is particularly important to ensure that no important alarm notification can be missed, while investigating another, perhaps less critical, alarm.

The displays shall be configurable (via a configuration tool) which will enable arranging their appearance, navigation and behaviour. Configuration changes will require the appropriate access rights and it must be possible to apply version control in order to save and load certain well-known configurations. Regardless of the architecture of the integrated alarm system, the configuration tool is targeted to the following:

- Definition of displays and navigation between components and displays
- Definition of the behaviour of the components in each display
    - Behaviour includes all the information that is needed to identify if a component is in an abnormal condition. This implies that the configuration tool must have access to the available monitoring and alarm information in order to be able define the behaviour of the components according to conditions based on this information.

Depending on the operational needs for the configurability of the displays, the complexity and features of the configuration tool shall be adapted. If, for example, the displays and behaviour of the displayed components is not expected to change often, then the effort for developing the configuration tool should be traded-off with the expected effort for the manual configuration of the displays and the behaviour of the displayed components.

A complementary display, showing more information for each component which is in an abnormal status (for example more information on the reason on why this component is in an abnormal status) will enable having more detailed information and also provide an overview of the components which are abnormal.

Moreover, the system shall enable two modes of interaction. A mode where an operator may perform control actions (i.e. acknowledge or shelve an alarm) and a read-only mode where an operator or other staff may only observe. The read-only mode is of particular importance for any number of secondary alarm panels that will e.g. allow engineers to monitor only a subset of the system. A particular use case could be an engineer who monitors only one particular type of antennas from their own office. They will see all the relevant alarms and status information and can investigate the details, but they will not be able to acknowledge or shelve any of the alarms. This task will remain with the operators on duty in the main control room.

The following sections summarize a set of requirements capturing the core functionality of the system. Each requirement is expressed by the information in the description as well as the information in the comment.

3.3 Requirements from Assumptions and Limitations

Requirement Id	**Description**	**Qualifier**
REQ-LIM-001	The integrated alarm system shall be designed as a stand-alone tool that has no code-level dependencies on the ALMA software.	Mandatory
Comment		
The integrated alarm system's main function is to report the status and alarms of all of the other subsystems in ALMA, irrespective of which of these systems are active at any one time. Under no circumstances must any of the monitored systems be able to adversely affect the ability to monitor the other systems, nor to have a negative impact on the alarm system itself.		

Justification
The alarm system must be a stable tool with very high availability that can in principle function without any of the monitored subsystems being active, i.e. reporting just that status.

Requirement Id	**Description**	**Qualifier**
REQ-LIM-002	The integrated alarm system shall be compliant with the general guidelines applicable for the ALMA software.	Mandatory
Comment		
Where possible and practical, the allowed operating system, third party software and hardware platforms adopted for the ALMA software must be used. Any deviations from these de-facto standards must be approved by ICT management.		
Justification		
Although the integrated alarm system will not strictly be a regular part of the ALMA software, it will need to be maintained by ICT and must also interface with the ALMA software, e.g. to retrieve configuration information from the ALMA TMCDB or Dashboard database.		

3.4 General Requirements

Requirement Id	**Description**	**Qualifier**
REQ-GEN-001	Operators shall receive instruction and systematic training in all realistic operational usage of the alarm system.	Mandatory
Comment		
Training should cover user interfaces, prioritisation rules, suppression mechanisms, alarm acknowledgement, and action reports.		
Justification		
The operators' familiarity with the system will ensure to get the maximum benefit out of the alarm system and ensure the integrity of the ALMA observatory.		

Requirement Id	**Description**	**Qualifier**
REQ-GEN-002	The integrated alarm system shall be properly documented and clear roles and responsibilities shall be established for maintaining and improving the system.	Mandatory
Comment		
Documentation must also be kept up to date, so web (Wiki) based documentation will be preferred.		

Justification
Should be self-evident.

Requirement Id	**Description**	**Qualifier**
REQ-GEN-003	It should be easy for process experts to build and maintain knowledge and expertise of the alarm system over time.	Desirable
Comment		
System should be built in such a way that it reflects the real-life set up in such a way that the representation is self-evident to operators and engineers, and hence there is no real learning curve.		
Justification		
The margin for user error must be kept to a minimum.		

Requirement Id	**Description**	**Qualifier**
REQ-GEN-004	It shall be possible to continuously tune/improve the integrated alarm system.	Mandatory
Comment		
Necessary e.g. to include new failure modes or to integrate new subsystems, etc.		
Justification		
ALMA will continue to evolve throughout its lifetime.		

3.5 Functional Requirements

Requirement Id	**Description**	**Qualifier**
REQ-FUNC-001	The integrated alarm system shall be explicitly designed to take into account human factors and limitations.	Mandatory
Comment		
Alarms shall always be presented at a rate and in a form that allows the array operators to have time to recognize and understand them, and adequate time should be allowed for the array operator to carry out his response, as described by the situation awareness concept model [RD2] illustrated in Figure 2 below.		
Justification		
The alarm system must be manageable by the available ALMA staff.		

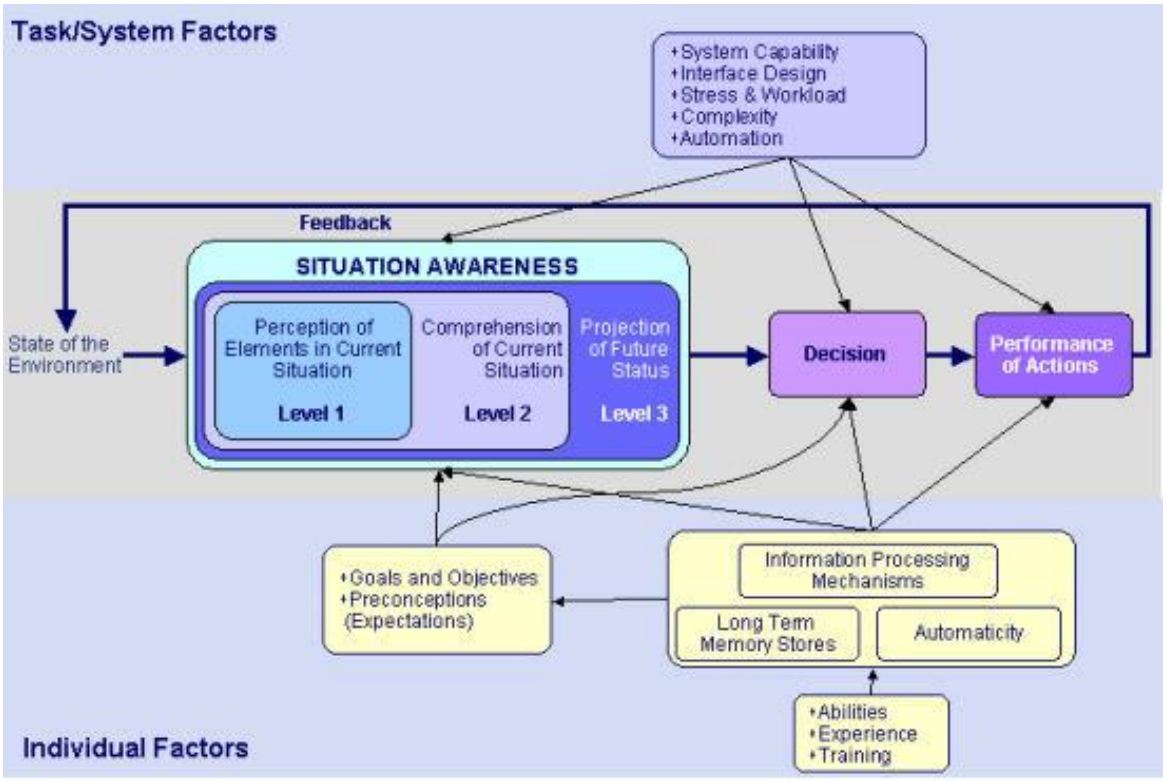


Figure 2 - Endsley's model of situation awareness

Requirement Id	Description	Qualifier
REQ-FUNC-002	The integrated alarm system shall show a top-level status of all monitored systems summarizing their health state.	Mandatory
Comment		
This includes all systems that will be monitored (power plant, weather stations, ALMA antenna array, etc.). The top-level status of each system shall summarize the status of all elements that belong in the monitored system.		
Justification		
Core functionality.		

Requirement Id	Description	Qualifier
REQ-FUNC-003	The main alarm display shall be usable under all process conditions, presenting alarm information in a form and at a rate that the operator can cope with.	Mandatory
Comment		

The alarm system must be decoupled from all other systems in such a way that no malfunctioning of any other system (hardware or software) can affect its ability to continue reporting alarms from other systems.
Justification
Core functionality.

Requirement Id	Description	Qualifier
REQ-FUNC-004	The integrated alarm system shall provide two different modes of operation: 1. One main operator system (primary system), which allows the operators to interact with. This system must show all the alarms from all the systems. 2. An arbitrary number of secondary systems that can be used in read-only mode only. These systems can either be configured identically to the main operator system, or only show a subset of available system and hence alarm and status information.	Mandatory
Comment		
There will only be one alarm system that the operators on duty interact with. Hence this system must always show the complete alarm information of all the monitored systems. The secondary systems may be used for specific purposes, e.g. engineering staff to monitor only a specific antenna type, or science staff to only monitor on-going observations. As such secondary systems should also be available from outside the OSF, i.e. the SCO and executive sites. Secondary systems should be configurable by the end users and not rely on some central authority.		
Justification		
Secondary systems will provide useful specific information to specific roles.		

Requirement Id	Description	Qualifier
REQ-FUNC-005	It shall be possible to navigate from a component of a display to a new display.	Mandatory
Comment		
The new display may be shown in a predefined position by replacing an existing display or be a new display completely. The arrangement of displays shall reflect the physical or logical structure of the monitored systems, i.e. by navigating to a new display from the “Antenna Array”, it should contain all array elements, and other relevant information.		
Justification		

Core functionality. Intuitive root cause identification by “drilling-down”.

Requirement Id	Description	Qualifier
REQ-FUNC-006	The system shall present a display with all components that are in abnormal status.	Mandatory
Comment		
This display shall contain all components, which are in abnormal status, e.g. in a tabular format. Each component shall provide all available information for the reason of the abnormal status (i.e. the reason that triggered an alarm). This display shall contain only the components, which triggered abnormal status and not the components that are in abnormal status as a result of summarizing the state of other components (i.e. if the HVAC system of antenna *DA43* is in alarm, then the summarizing components “Array Element DA43” or “Antenna Array” should not be included in this list). It should, however, be possible to expand any shown element in both directions, i.e. the summary components it is contained in, as well as all the (sub-) components it contains.		
Justification		
Additional information for root-cause identification. Summary of all active alarms at system level.		

Requirement Id	Description	Qualifier
REQ-FUNC-007	The behaviour of each component shown in displays shall be configurable based on the incoming monitoring and alarm information.	Mandatory
Comment		
This is expected to be done offline as part of the configuration of the system. Incoming monitoring information is considered all the input to the integrated alarm system, which includes all necessary information from all the other monitoring and alarm systems that will be integrated. For example, it shall be possible to define the alarm conditions of a component based on received alarms and monitoring information.		
Justification		
Core functionality. Needed in order to be able to define complex alarm conditions based on the state of the monitored systems.		

Requirement Id	Description	Qualifier
REQ-FUNC-008	It shall be possible to define components on displays based on properties of other components.	Mandatory
Comment		
These are often referred to as “synthetic parameters” or “custom parameters”. For example it shall be possible to define a parameter that has a value, which is a combination of values or other		

properties of other components. The components which are referenced might also have “synthetic parameters” themselves.

For example, we should be able to define a parameter which has a value defined as an expression of values of other parameters:

Parameter A = (Parameter B + Parameter C) / 2

As a real example taken out of the configuration of one of the ESA ground stations, Parameter /MCM1/LDC1/204, which is defined in the context of a Down Converter, calculates a *Derived L-Band* frequency by taking into account the validity and values of other parameters.

The actual definition using the algorithmic language of the system is presented below just for reference to a sample algorithm:

Value Algorithm

```
select
  UNDEFINED
          when VALID (/MCM1/LDC1/201.VALUE)= FALSE

  9040 - /MCM1/LDC1/201.VALUE
          when VALID (/MCM1/LDC1/206.VALUE)= TRUE AND
/MCM1/LDC1/205.VALUE = "X-BAND";

  /MCM1/LDC1/201.VALUE - 22400 - /MCM1/LDC1/206.VALUE
          when VALID (/MCM1/LDC1/206.VALUE)= TRUE AND
/MCM1/LDC1/205.VALUE = "KA-BAND";

  UNDEFINED otherwise

Endselect
```

.

Justification
This is needed in order to be able to define custom monitored components combining information from other components.

Requirement Id	**Description**	**Qualifier**
REQ-FUNC-009	It shall be possible to access configuration information.	Mandatory

Comment
This is not information that is being monitored. It is configuration information entered by the operator or retrieved via a configuration system. For example, the operating mode of an observation, configuration status of an array element or other information that is important to the system but is not being monitored. This information shall be usable in defining the behaviour (i.e. alarm conditions) of components.
Justification
Enables using configuration information for the determination of the state of monitored components.

Requirement Id	Description	Qualifier
REQ-FUNC-010	It shall be possible to determine if the systems are monitored reliably.	Mandatory
Comment		
Reliably means that the presented status of a component is up-to-date and correct. It may not be possible to have a single definition of reliable, which covers all cases, but it must be part of the definition of each monitored component. E.g. some components may require a status update every few seconds, while for others it could be a much longer time interval. This shall be visualized accordingly to the associated components in displays. For example if because of a network issue, or because of an error with a device being monitored, the integrated alarm system cannot obtain reliably a value or alarm information, this should be reflected in the related components that base their behaviour on the input information.		
Justification		
Ability to know if the system can reliably monitor the relevant systems.		

Requirement Id	Description	Qualifier
REQ-FUNC-011	It shall be possible to manage and visualize abnormal states according to a clearly defined workflow.	Mandatory
Comment		
This includes concepts such as alarm acknowledgement, alarm shelving and alarm severity states as defined in [RD4]. However, the detailed alarm states and workflow shall be defined in detail in the next phase of the project. The ability to acknowledge or shelve multiple alarms utilizing the hierarchical nature of the system shall also be explored (for example by acknowledging an alarm at a system level, all the underlying alarms will be acknowledged)		
Justification		
Core functionality. Alarm management and presentation.		

Requirement Id	Description	Qualifier
REQ-FUNC-012	It shall be possible to use equipment templates for the configuration of the system.	Mandatory
Comment		
This is needed in order to ease the configuration of the system. There shouldn't be the need for example to individually define all antennas, but it should be possible to use as template the configuration of the elements for one antenna to define another one.		
Justification		
Ease of configuration		

Requirement Id	Description	Qualifier
REQ-FUNC-013	All abnormal conditions and the subsequent operator responses shall be archived	Mandatory
Comment		
This refers to all abnormal status information such as alarm conditions, inability to monitor a system etc. Operator responses (e.g. alarm acknowledgement or shelving) must be directly linked to the reported abnormal condition. All archived information must carry sufficient detail to report on the efficiency of the system, e.g. average response times,		
Justification		
Incident investigation, system performance metrics		

Requirement Id	Description	Qualifier
REQ-FUNC-014	The integrated alarm system shall be context sensitive, showing only alarms that are relevant under the current conditions.	Mandatory
Comment		
Alarms should support different system states like start-up, power-cut, shutdown, preventive/corrective maintenance, science observations, and antenna elements availability as presented in the ALMA Dashboard. Relevant means that an alarm provides only information that is useful and meaningful at the current point in time. E.g. during a full system restart, there should be no alarms indicating that the connection to a particular array element is broken.		
Justification		
The alarm system must be optimised to support operations and always be relevant, irrespective of the current situation.		

Requirement Id	Description	Qualifier
REQ-FUNC-015	There shall be an administrative system for handling access control and full version control of changes made to the alarm system.	Mandatory
Comment		
There shall only be one read/write (operator) instance of the alarm system at any one time, which can be used to acknowledge or shelve alarms. There may be many read-only instances, possibly also remotely, e.g. from the SCO or Executive sites. All alarm system instances (read/write and read-only) will require user login, which may include permissions as to which systems can be monitored. The general rule that ALMA staff should have (read-only) access to all information about the system shall apply. Only such information that is restricted due to contractual obligations		

may be shielded from particular user groups. Read/write access must only be granted to array operators at the OSF. All changes to any of the interfaces must be logged and be reversible. Special permissions must be available to configure the systems.
Justification
The alarm system, in particular the operator instance, must be tightly controlled to avoid accidental or deliberate unapproved modifications.

3.6 Maintenance Requirements

Requirement Id	Description	Qualifier
REQ-MAINT-001	It shall be possible to add new monitored components by configuration, requiring the appropriate administrative access rights.	Mandatory
Comment		
This assumes that the monitoring interface is already implemented. If for example a new piece of equipment is added to an antenna, or if there is a need to monitor an additional piece of equipment, which is not already monitored (but with the system being interfaced already), then this shall be possible by configuration without a new release of the software.		
Justification		
Configurability and ease of maintenance.		

Requirement Id	Description	Qualifier
REQ-MAINT-002	All alarm limit settings shall be systematically determined and documented during design, commissioning and operations.	Mandatory
Comment		
The system must be properly configured before it is brought into production, and must be kept up to date at all times.		
Justification		
Configurability and ease of maintenance.		

Requirement Id	Description	Qualifier
REQ-MAINT-003	Operators should be permitted to change alarm limits.	Desirable
Comment		

While the main configuration needs to be carefully controlled, it may at times be useful for the operators to change some boundary conditions, to avoid invalid alarms or repetitive alarms. Any such change must be logged, it must be clearly visible on the main displays that such action has been taken and there must be an easy way to return to the standard settings.
Justification
Configurability.

Requirement Id	Description	Qualifier
REQ-MAINT-004	The integrated alarm system shall be designed in such a way that future extensions or changes in alarm sources can be accommodated without requiring major software rewrites or modifications.	Mandatory
Comment		
Some of the currently monitored systems will be replaced in the future by systems that have different interfaces or an increased scope of to be monitored components. There can also be completely new systems added, or already existing systems that cannot currently be monitored could be equipped with such functionality. It could e.g. be possible that antenna transporters will be providing live monitoring information in the future.		
Justification		
Expandability.		

3.7 Performance Requirements

Requirement Id	Description	Qualifier
REQ-PERF-001	The alarm system shall be fault tolerant. Critical information, e.g. fire alarms, must be always available.	Mandatory
Comment		
This requires a design that puts the integrity of the alarm system itself first and shields possible failures in particular connections to monitored systems from the system as a whole. Such failures must be reported in the alarm system, and it must be possible to recover from them without restarting the alarm system as a whole. The alarm system considered here is, by definition, not suitable for the handling of safety critical alarms. Such alarms must be covered in special alarm systems and handled by specifically trained operators. Nevertheless such alarms should also be shown to the array operators, both for situational awareness and to enable them to carry out precautionary measures for indirectly affected subsystems.		
Justification		
The array operators need full situational awareness.		

Requirement Id	Description	Qualifier
REQ-PERF-002	System delay to an alarm condition shall not exceed 2 seconds.	Mandatory
Comment		
This should be measured from the time an alarm condition occurs on any of the included subsystems and its appearance on the operator main alarm panel. Waivers to this rule may be granted for certain subsystems, but this must be well justified and documented.		
Justification		
Alarm notification must happen in near real time to ensure the integrity of the observatory and its operations.		

Requirement Id	Description	Qualifier
REQ-PERF-003	It shall be possible to monitor 50.000 information elements.	Mandatory
Comment		
Information elements are all individual monitoring and alarm information monitored from other systems. For example a value of a sensor is 1 information element and the information that a certain piece of equipment is in alarm condition is 1 information element.		
Justification		
Monitoring scalability.		

Requirement Id	Description	Qualifier
REQ-PERF-004	It shall be possible to define 10.000 “synthetic parameters”	Mandatory
Comment		
Synthetic parameters are custom parameters that base their value on properties of other parameters.		
Justification		
Monitoring scalability.		

Requirement Id	Description	Qualifier
REQ-PERF-005	Performance requirements for the alarm system should be defined.	Desirable

Comment
Tools and methods for measuring performance indicators like rate of incoming and suppressed alarms, number of alarms in main and shelve list, operator response times, reported/fixed alarms problems, etc., should be implemented. See Figure 3 below.
Justification
Required for fine tuning and optimising the alarm system.

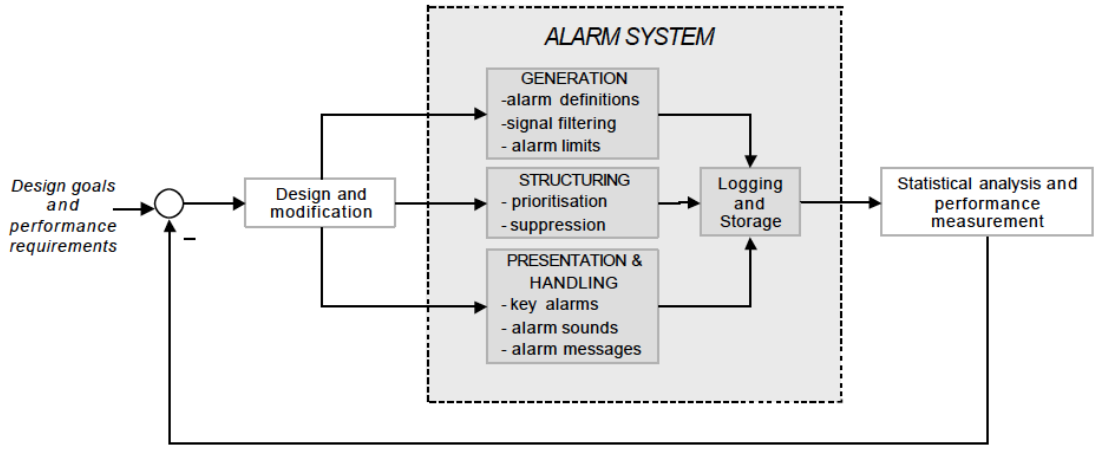


Figure 3 - Alarm system improvement illustrated as a feedback loop

3.8 Alarm Handling Requirements

Requirement Id	Description	Qualifier
REQ-HAND-001	Every alarm shall require an operator response.	Mandatory
Comment		
New alarms will be clearly visible, e.g. through a blinking mechanism, and must be acted upon by the operator. Acknowledgement implies that the operator has taken the required action(s). Another possible response is the shelving of an alarm.		
Justification		
Core functionality		

Requirement Id	Description	Qualifier
REQ-HAND-002	Every defined alarm shall include possible actions to be taken by operators and other actors.	Mandatory

Comment
The operator must be provided with easy access to the alarm definition, which must include clear and unambiguous instructions on how to react to the alarm condition.
Justification
Core functionality

Requirement Id	**Description**	**Qualifier**
REQ-HAND-003	For each alarm, operators shall be able to quickly see the priority and alarm state (new, acknowledged, shelved, cleared)	Mandatory
Comment		
Each visible alarm must provide this core information through clear and consistent design of the user interface. No drill-in shall be required to get this core information.		
Justification		
Quicker reaction time for critical alarms.		

Requirement Id	**Description**	**Qualifier**
REQ-HAND-004	It shall be possible that certain alarms automatically notify additional people.	Mandatory
Comment		
For certain critical alarms one or more people can be notified automatically either through email, SMS or other TBD methods. In principle this functionality will be available for any alarm. The responsibility for responding to an alarm in the integrated alarm system, however, remains with the operator.		
Justification		
Quicker reaction time for critical alarms.		

Requirement Id	**Description**	**Qualifier**
REQ-HAND-005	For every alarm that is triggered, the suggested or expected operator action shall also be displayed on the main operator panel.	Mandatory

Comment
It is important that such details do not hide other relevant information, e.g. other alarms in the main operator panel.
Justification
Ensure correct action is taken.

Requirement Id	**Description**	**Qualifier**
REQ-HAND-006	Alarm acknowledgement (and shelving) should be possible from lists, process displays and overview displays on all the workstations.	Mandatory
Comment		
This is only applicable for all displays that are part of the primary operator system. Secondary systems cannot be used to acknowledge or shelve alarms.		
Justification		
Usability		

Requirement Id	**Description**	**Qualifier**
REQ-HAND-007	All displays shall be updated within 2 seconds when an alarm is acknowledged.	Mandatory
Comment		
The system must also be resilient to the same action being taken from different panels.		
Justification		
Usability		

Requirement Id	**Description**	**Qualifier**
REQ-HAND-008	It shall be possible to acknowledge each new alarm separately.	Mandatory
Comment		
In particular it shall be possible to acknowledge summary alarms at the most detailed component level, which should normally be the default action.		
Justification		

Usability.

Requirement Id	Description	Qualifier
REQ-HAND-009	It shall be possible to acknowledge all alarms from a hierarchy at any level.	Mandatory
Comment		
Some caution may be required here, because this means that all alarms can also be acknowledged at the “Observatory” root level. May require some additional level of approval, e.g. by a manager on duty. TBD.		
Justification		
Usability. Quick recovery from emergency situations, e.g. power blackout.		

Requirement Id	Description	Qualifier
REQ-HAND-010	Alarm sounds shall disappear when all the relevant alarms are acknowledged.	Mandatory
Comment		
Justification		
Usability		

Requirement Id	Description	Qualifier
REQ-HAND-011	It shall be possible to shelve individual alarms only.	Mandatory
Comment		
Shelving of a hierarchy of alarms similar to REQ-HAND-009 described above for acknowledgement of alarms is not foreseen.		
Justification		
Usability		

Requirement Id	Description	Qualifier
REQ-HAND-013	Shelved alarms, which are not acknowledged within 12 hours, should be suppressed and a problem report generated.	Desirable

Comment
Such reports should be automatically generated by the system, following observatory standards and templates.
Justification
Keep the system in a usable and clean state at all times.

Requirement Id	**Description**	**Qualifier**
REQ-HAND-014	Key alarms should require an authorization mechanism to avoid being shelved by the operators without proper action being taken.	Mandatory
Comment		
Approval e.g. by the manager on duty.		
Justification		
System stability		

Requirement Id	**Description**	**Qualifier**
REQ-HAND-015	All operator responses, i.e. acknowledgment or shelving, including any comments shall be reported and logged by the alarm system.	Mandatory
Comment		
Justification		
Process improvements, post-mortem analysis.		

3.9 Presentation Requirements

Requirement Id	**Description**	**Qualifier**
REQ-PRES-001	A main alarm display shall be provided.	Mandatory
Comment		
The alarm system must always have a main alarm display visible when running. It must be able to display all the alarms that are present in the configured system. Most of these alarms will be shown in summary elements, but it is important that any alarm condition will be visible from the main overview panel, e.g. through a blinking and appropriately colour coded element.		

Justification
Core functionality.

Requirement Id	**Description**	**Qualifier**
REQ-PRES-002	The main alarm display shall support the task of monitoring and controlling the behaviour of observatory components by attracting the operator's attention towards process conditions that require attention or action.	Mandatory
Comment		
Justification		
Core functionality.		

Requirement Id	**Description**	**Qualifier**
REQ-PRES-003	The main alarm display shall show only alarms that are relevant in the current process conditions.	Mandatory
Comment		
This means that e.g. array elements that are not being used for operations must not produce any alarms in the main alarm display. Since such alarms may be useful for engineering and commissioning activities, secondary (read-only) displays may be configured to include such alarms.		
Justification		
Situational awareness.		

Requirement Id	**Description**	**Qualifier**
REQ-PRES-004	The main alarm display shall only present all active and real alarms that are not automatically suppressed or manually shelved.	Mandatory
Comment		
This follows the “dark screen” concept, meaning that in normal operations there will be no visible alarms, unless operator action is required for the current operational context.		
Justification		
Situational awareness.		

Requirement Id	Description	Qualifier
REQ-PRES-005	For each alarm, operators shall be able to quickly see the priority and alarm state (new, acknowledged, cleared).	Mandatory
Comment		
Justification		
Situational awareness.		

Requirement Id	Description	Qualifier
REQ-PRES-006	Alarm lists shall be: 1. Chronologically ordered by default 2. Designed such that repeating alarms do not cause them to become unusable (i.e. same alarm filling up several lines in the list)	Mandatory
Comment		
This is applicable for tabular presentation of alarms.		
Justification		
Usability.		

Requirement Id	Description	Qualifier
REQ-PRES-007	Alarm lists shall be sortable by any displayed column with a clear indication that the current display deviates from the default ordering (see REQ-PRES-006) and an easy return to this default ordering.	Mandatory
Comment		
This is applicable for tabular presentation of alarms.		
Justification		
Usability.		

Requirement Id	Description	Qualifier
REQ-PRES-008	There shall be displays with spatially dedicated alarms	Mandatory

	(tiles/annunciator displays)	
Comment		
Operators can effectively use pattern recognition that enables them to cope with a large number of alarms. Does not show the chronological ordering of the active alarms.		
Justification		
Usability.		

Requirement Id	Description	Qualifier
REQ-PRES-009	Alarms should be integrated in process displays. (See animation here: Alma signal path, and Figure 4)	Mandatory
Comment		
The hierarchical structure used by default to represent the observatory does not always make it obvious how an alarm from a particular component can affect the current workflow. This should become more obvious by such process displays.		
Justification		
Situational awareness.		

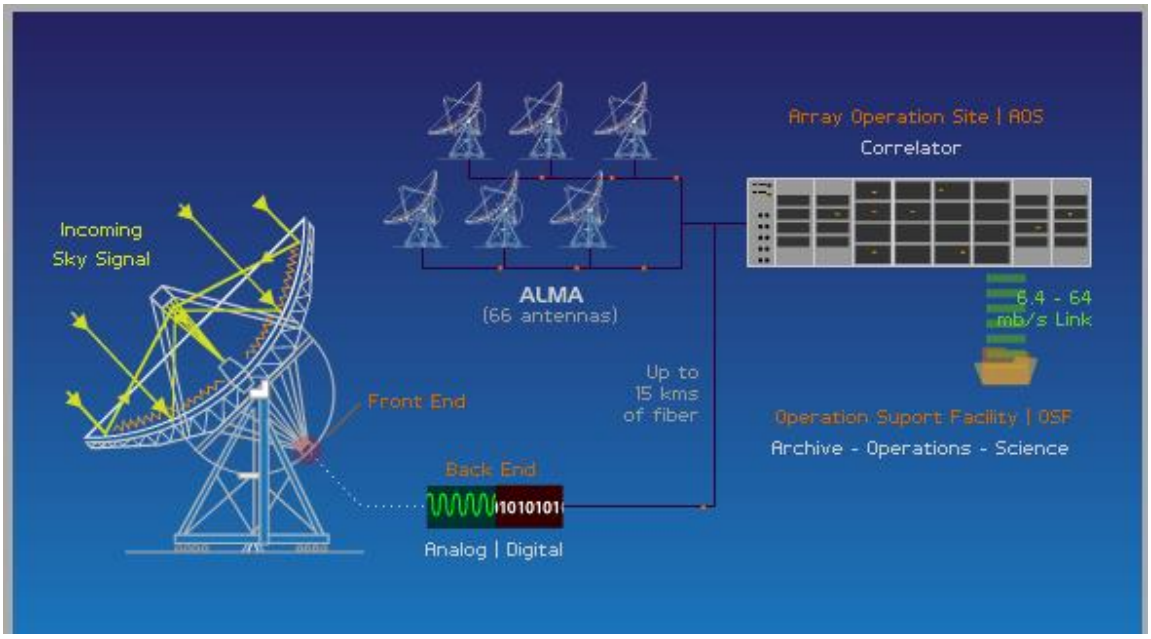


Figure 4 - ALMA signal path visualisation

Requirement Id	Description	Qualifier

REQ-PRES-010	The priority of alarms shall be coded using colours and possibly other means (see 5.2.2)	Mandatory
Comment		
Justification		
Usability.		

Requirement Id	**Description**	**Qualifier**
REQ-PRES-011	Audible alarm annunciation should be used when new alarms arrive. A maximum of four different alarms sounds is recommended to easily distinguish them.	Desirable
Comment		
The configuration of such alarm sounds will be easily configurable by the operators (using the appropriate access control, of course), as this requires a fair amount of refinement to make it useful in all circumstances.		
Justification		
Usability.		

Requirement Id	**Description**	**Qualifier**
REQ-PRES-012	There should be a central means to silence audible alarms with strict procedures to prevent it from being misused.	Desirable
Comment		
Justification		
Usability.		

Requirement Id	**Description**	**Qualifier**
REQ-PRES-013	Alarm information shall be informative and easy to understand. It shall be available at all relevant workplaces.	Mandatory
Comment		

Justification
Usability.

5 Design Considerations

This section provides some considerations on the eventual design of the integrated alarm system. It is not a complete design specification, nor is it meant to be making design decisions that have to be taken unchanged into the full functional and design specifications that will be elaborated as part of the development project.

The following sections are based on the operational experience of the authors of this document, and on the reports by ESA (see [RD10]) and INRIA (see [RD11]) and reiterate the core recommendations from these reports. The details available in these reports are fully applicable as an outcome of this study.

For easier readability we present the design considerations in a top-down fashion, starting at the presentation level and then drill down into the internal design and interfaces to alarm sources.

5.1 User Interfaces

5.1.1 Observatory Overview Panel

One of the core concepts of the integrated alarm system is to have a single entry point to monitor all the systems and their components that together make up the ALMA observatory. This requires a system overview panel that is always visible in the ALMA control room and provides a comprehensive and intuitive overview of the observatory that is at the same time providing enough detail to quickly identify the problematic areas and summarising inherently complex areas to avoid confusion. Figure 5 shows a mock-up of the overview panel.

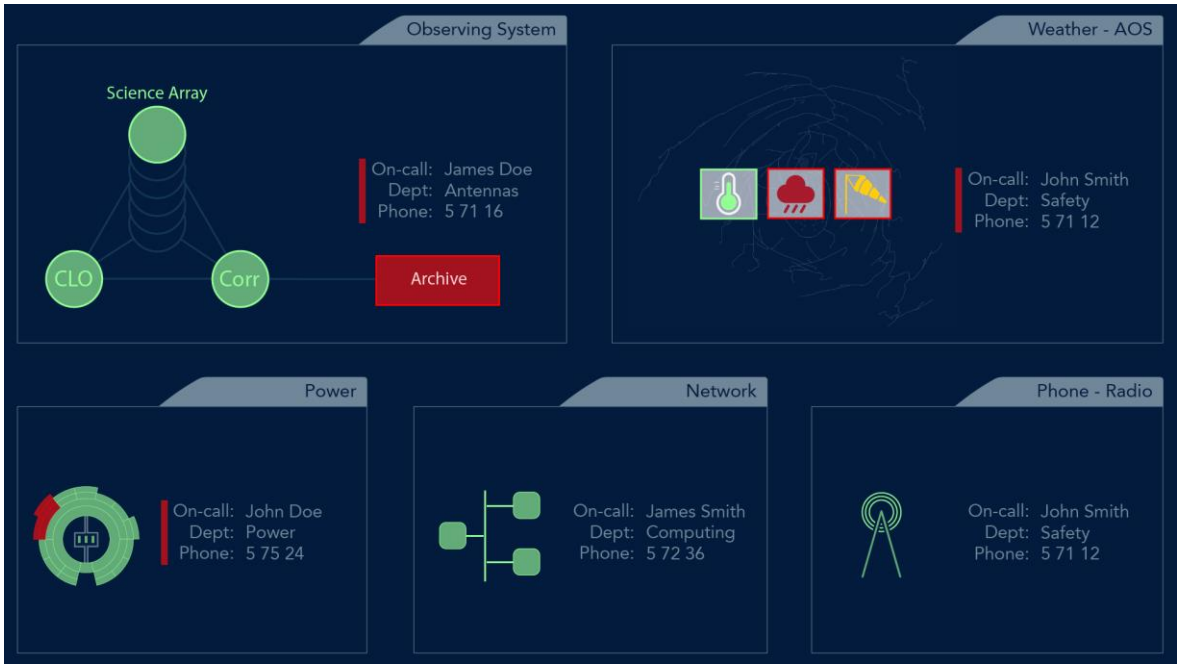


Figure 5 - Observatory overview panel

The overview panel shows the status and possible alarm conditions for all the components monitored by the integrated alarm system by summarising the overall status

of such components that are representing a potentially very deep hierarchy of individual components.

The above mock-up should perhaps show much more detail in the *Observing System* part and utilise more screen real estate for that, as this is the main focus area for the array operators. The detailed layout will evolve from initial prototype installations and is expected to be gradually perfected only when it is used in real operations. The same applies for all other mock-up panels.

From the overview panel it must be possible to drill in to more detailed panels, to open a tabular representation of all active alarms, or to directly address alarm conditions (see 5.2). For all these actions it is of utmost importance that the observatory overview panel remains visible and active at all times. This will be achieved by all secondary display panels and dialog boxes being shown on a separate monitor without blocking the overview panel for input or output.

5.1.2 Secondary Display Panels

From the observatory overview panel any number of panels displaying more details on a particular part of the system can be accessed. These panels can either be opened directly from the overview panel on demand or, for subsystems that need to be constantly monitored, they can be visible in separate monitors continuously. All visible panels will be updated by the integrated alarm system at the same time, reflecting any changed status or alarms in a synchronised fashion. The delay between updates shall be no more than 2 seconds to ensure a fully synchronised user experience.

All detail display panels must be fully configurable, requiring administrator access rights. Some of the panels will be designed using HCI templates as shown in the samples below. For such panels it is acceptable to require changes at the code level, also requiring new software versions of the integrated alarm system itself. But the integrated alarm system must also cater for the creation of generic panels using a standard panel template and generic widgets that represent the various components. It must be possible to create and modify such panels without requiring code changes, through the use of a generic configuration tool or panel editor, which the integrated alarm system will provide. Such panels will be particularly useful for the read-only secondary displays used e.g. by engineering outside the control room to monitor particular parts of the system during certain activities.

The following figures show some initial mock-up displays that were elaborated during the HCI workshop at the observatory. Full details can be found in [RD11].

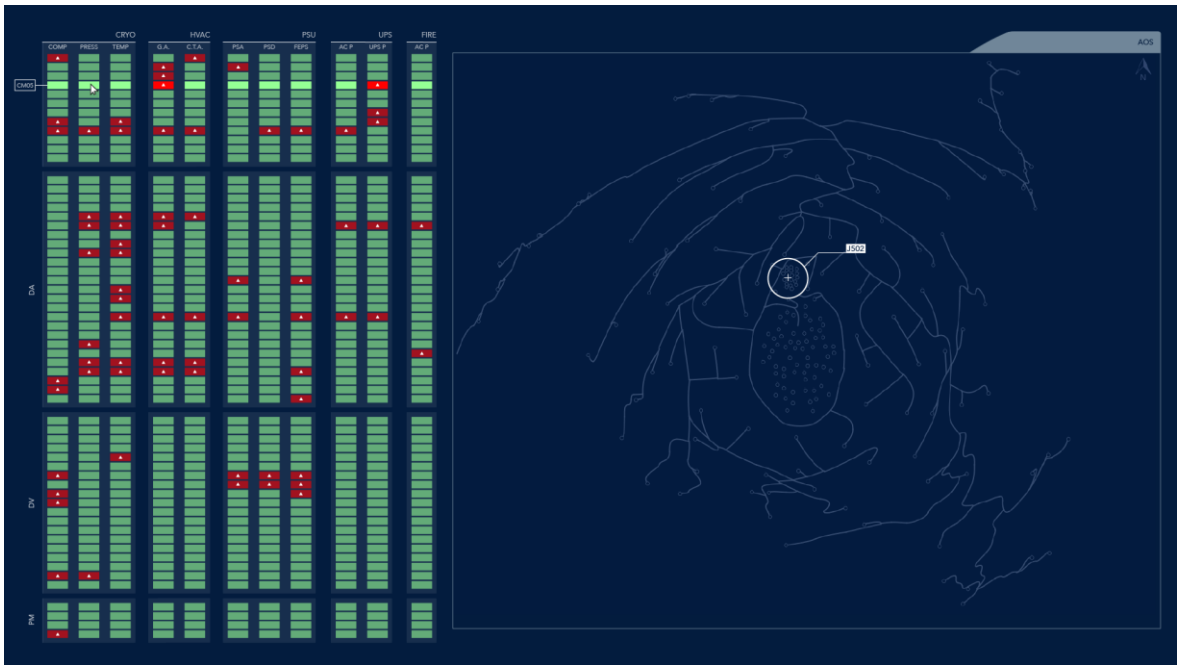


Figure 6 - Overview display of all ALMA array elements, including geo-location of selected antenna

Figure 7 - Display of OSF and AOS buildings showing real location of HVAC systems, fire alarms and other supplies

Figure 8 - Display of power generation and distribution elements

Figure 9 - Display of AOS weather stations using geo location of each station

A slightly different panel is shown in Figure 10. Rather than visualising equipment it shows the workflow of scheduling blocks that are being observed. Its primary use is intended for monitoring on-going science observations.

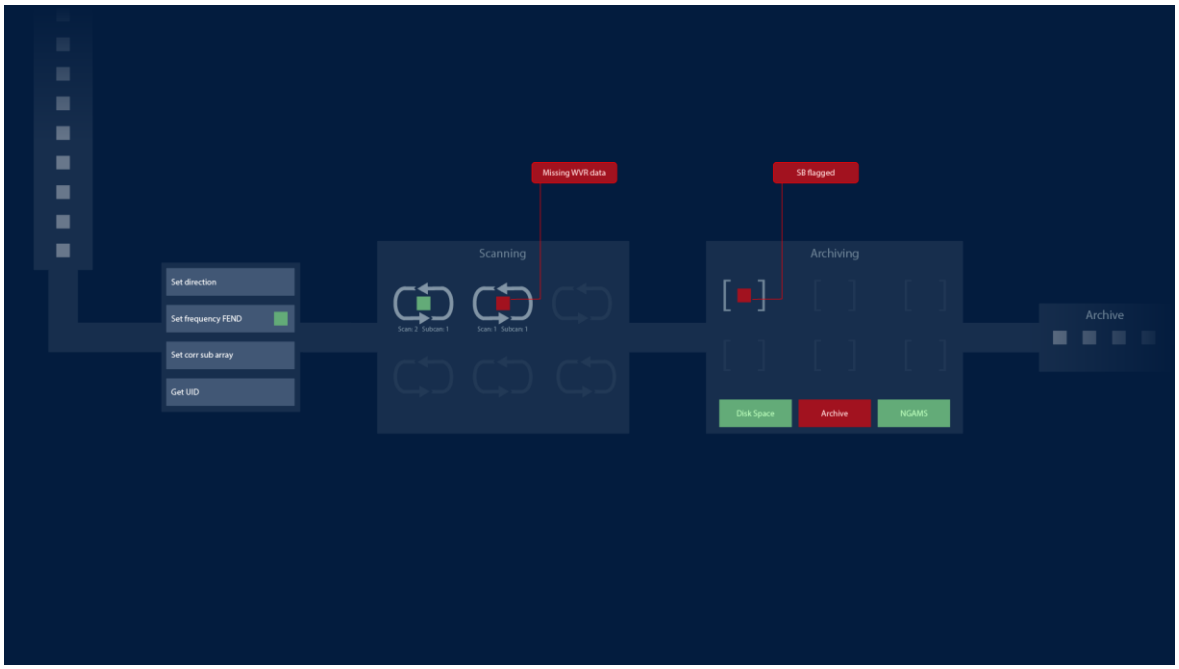


Figure 10 - Process oriented view of the observation process

Generic panels that can be configured from a predefined set of widgets using a built in configuration editor have not been drafted as part of this study. But the general principle can be derived from the ESA example shown in Figure 11.

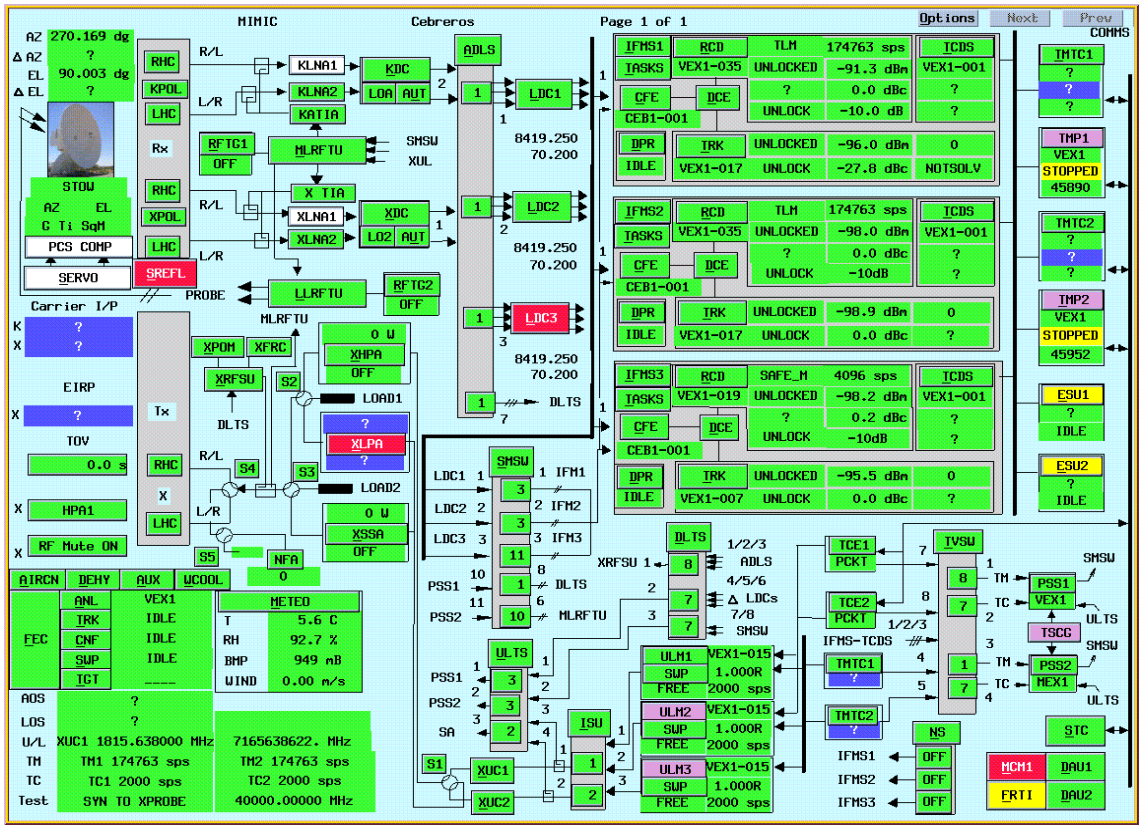


Figure 11 - Generic configurable view (ESA ground station example)

This example may look much less appealing (and perhaps dated) at first sight, but one should not forget that these displays have been refined over many iterations to display the optimal amount of information on a single screen in a way that is very intuitive to the trained and experienced operator. The complexity of ESA ground stations is generally comparable to ALMA, so this visualisation provides a reasonably good approximation.

5.1.3 Detail Displays

While the panels described in the previous sections allow for the status and alarm display from a broad system wide overview to a reasonably detailed subsystem level, with rapid drill in capabilities, the final step for investigating an alarm cause or abnormal status will always be a detail display that shows the properties of a particular component in detail.

For such detail displays a tabular representation will be best. Part of these details will be information about the component itself, including:

- Name
- Type
- Description, including serial numbers and other identification
- Status (e.g. enabled/disabled, error, warning, etc.)
- Location of the component and access information
- Link to available documentation

For each of the component's values the displayed information must include the following:

- Name
- Description
- Current value with timestamp
- Maximum value measured with timestamp
- Minimum value measured with timestamp
- Error boundaries
- Warning boundaries

The full scope and design of these panels will need to be done as part of the next step of the project. It will be very important to design a generic display paradigm that is suitable for all of the components, providing a consistent user experience.

5.2 Alarm Monitoring and Handling

The most important aspect here is that the integrated alarm system's sole purpose is to notify the operators of alarm conditions and abnormal statuses of observatory components. The operators' only interaction with this system is to acknowledge alarm conditions, including providing information about how the alarm has been addressed. The work to address any such condition is done in separate operator interfaces provided by the various systems. The alarm condition or abnormal status will never be cleared by the operator using the integrated alarm system, only the components themselves can clear the . It is a pure monitoring system that shows the status of components as they are reported.

5.2.1 Alarm vs Abnormal Status

It is important to be very clear on the definition of an *alarm* as opposed to an *abnormal status*.

Abnormal status for a component means that one or more of its reported and monitored values are out of the normal range.

An *alarm* means that a component has entered into an abnormal status and the operator has not yet acknowledged this situation. Acknowledging the alarm means that the alarm notification itself will be cleared, but not that the abnormal status will be cleared at the same time. Likewise if a component reports an alarm because of an abnormal status and the status returns to normal, either through user action or by itself, the alarm notification will not be cleared automatically either.

Note that an *abnormal* status does not always imply that a component is broken or out-of-order. Alarms can be defined to warn the operator of an upcoming maintenance date of a component, or to indicate a slight deviation from regular measurement, which could hint towards an upcoming problem.

5.2.2 Abnormal Status Reporting

The status of components will be reported through colour coding, also taking into account special requirements of colour-blindness.

In the simplest case the configuration could be *green* for reporting a normal status and *red* for an abnormal status. This will be sufficient for components that report a simple *on/off* or some other binary status. More typically there will be at least a distinction between an *error* and a *warning* status. More levels of status reporting through different colours should be avoided as it could easily lead to confusion rather than more clarity.

There is, however, a need to also report the validity of values and alarms, as well as to clearly mark components that are not monitored, e.g. because they are turned off, not used, not installed or undergoing maintenance. This leaves us with the following colour coding[1]:

- *Green*: component in validated normal operational state
- *Yellow*: component in validated warning state
- *Red*: component in validated error or abnormal state
- *Blue*: value of component unknown or invalid
- *Plum*: alarm of component raised, but not validated
- *Grey*: component is not configured, or in maintenance mode

The colour coding of a non-aggregated component is therefore very simple. For components that represent an underlying hierarchy of subcomponents, the propagation rules must be specified as part of the integrated alarm system configuration. The default behaviour will be that an aggregated component shows the most severe status of any of its subcomponents, i.e. in the order: *red, yellow, plum, blue, green, grey*. However, it will not be possible to simply use this default for all cases. One example is the failure of one of the ALMA power generation turbines, when the other two are still fully functional. The failed turbine will be marked red, but the power station as a whole only in yellow to

[1] Note that a final colour scheme still needs to be defined. These colours are only used as an example here.

indicate a warning. In the same example if one of the turbines is put into maintenance mode (grey), the power station as a whole will remain green as fully functional. But two of the three turbines being in maintenance mode might well be indicated as a warning in the power station because of the lack of redundancy.

5.2.3 Alarm Reporting

Any alarm will be indicated through the blinking of the component reporting the alarm, which optionally may be complemented with a configurable warning sound. The blinking will be propagated from the individual component reporting the alarm to all its container components that are on display on any of the visible panels. The warning sound will only be played on the observatory overview panel to avoid confusion.

The blinking notification will be shown at the most detailed applicable level of any of the display panels. E.g. an alarm from a particular gauge on one of the power turbines would see this gauge blinking if we are showing a detailed display of the turbine. On the power station overview (see Figure 8) only the turbine with the gauge reporting the alarm would be blinking, while in the system overview panel (see Figure 5) the icon representing the entire power station would be blinking.

The blinking will continue until the alarm has been acknowledged or shelved by the operator. This is true even if the alarm condition disappears from the system. It may be worth considering automatically acknowledging such alarms, whose initial alarm condition has been resolved, after a defined period of time. In any case such alarms must be logged, with a clear indication of the automatic acknowledgement.

5.2.4 Tabular Alarm Reporting

All alarms will also be reported in a table view, similar to the one currently being provided by the ACS alarm system (see Figure 12).

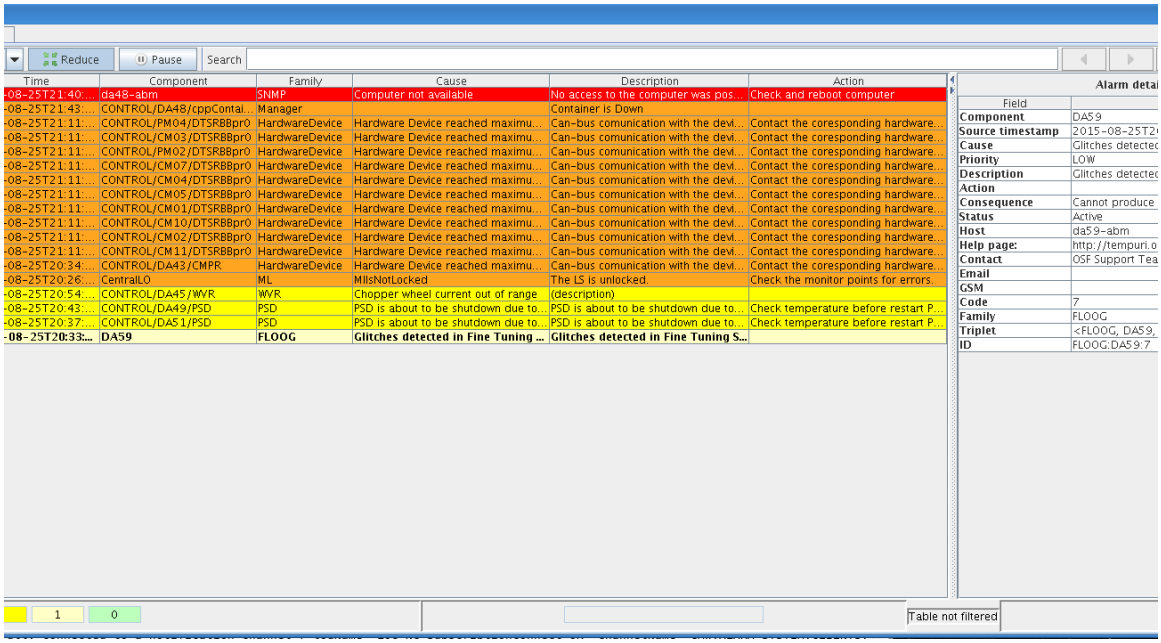


Figure 12 - Tabular alarm reporting (ACS alarm panel)

5.2.5 Clearing of Alarms

Every alarm needs to be acted upon by the operators. The actual action to resolve an alarm, or rather the underlying abnormal condition, is not part of the integrated alarm system's scope. It will, however, display contextual information and instructions to the operator on how to react to each particular alarm. The integrated alarm system allows the operator to clear (i.e. acknowledge or shelve) an alarm, which is only a confirmation that the alarm has been seen and the appropriate action has been taken or initiated.

Alarms can only be acknowledged or shelved from the main operator station in the ALMA control room. This will be controlled through a login-in requirement. It will be a strict requirement for the operator to provide clear comments on how each alarm has been addressed.

Operators must be able to view and clear alarms from any of the displays, including the tabular display. Since it is possible that a higher level display showing an alarm is actually a summary of two or many more separate alarms reported by contained components, the alarms must be presented in such a way that the operator gets a quick and easy overview of the situation and can take the appropriate action in the correct order.

5.3 High-Level Architecture

The following diagram (Figure 13) shows a conceptual layout of the architecture envisioned for the integrated alarm system:

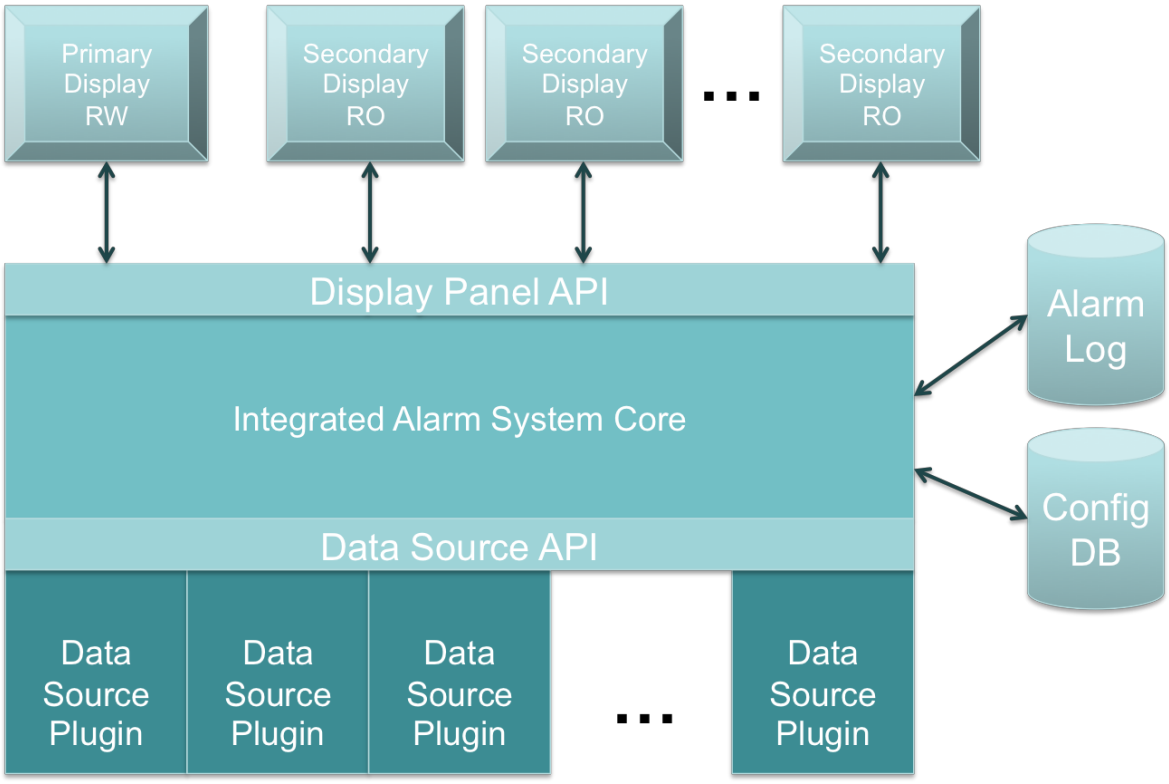


Figure 13 - Integrated alarm system high-level architecture

There will be a single instance of the integrated alarm system core, which centrally processes all the incoming data and alarms and makes them available to an arbitrary number of display panels, of which only one will be the designated primary operator

interface to clear alarms. All other displays will be read-only. There will be a single API through which all displays access the integrated alarm system, not only to receive monitoring and alarm data, but also to access configuration information, including the layout of display panels.

The integrated alarm system will provide a data source API and a plugin architecture, which allows it to receive the monitoring and alarm information from any number of data sources, which will be very heterogeneous. All data source specific handling will be performed by the specialised plugins. Internally to the integrated alarm system every monitored component will be represented in a homogeneous data model.

There will be two conceptual databases to store the relevant information: one for storing all the configuration information, and one for storing a complete log of alarms and abnormal conditions, including operator action and comments. Both these conceptual databases may be implemented as a set of distinct databases, based on practical considerations.

A detailed architecture will be designed as part of the development project. It may deviate from this very conceptual architectural layout.

5.4 Observatory Monitoring Model

As described in more detail in the ESA report [RD10] the requirements for visualising a complex and heterogeneous set of monitored elements, in conjunction with the inherently hierarchical design of the ALMA observatory, leads to a structured hierarchical model to represent the system internally. The conceptual design of such a model and its relationship to the displayed information is visualised in Figure 14.

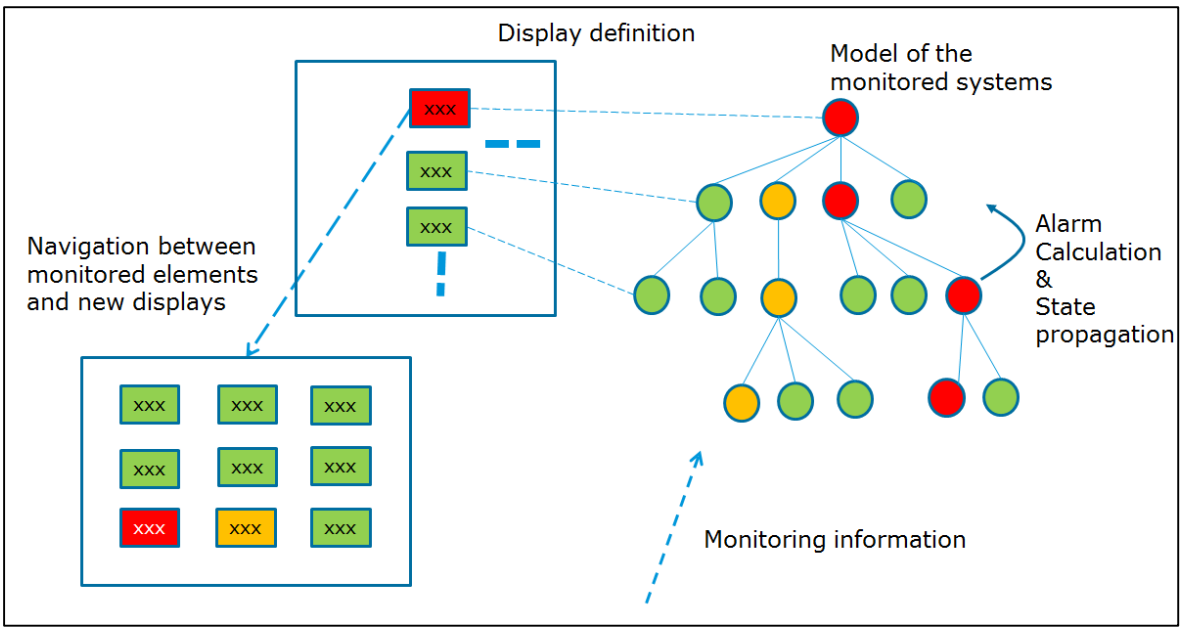


Figure 14 - Observatory monitoring model

The most important aspect here is that every displayed component directly refers to a node in the hierarchical model. Every such node represents either a physical device (including software components) or a logical one, typically summarising the status of all its descendants. All alarm and status calculations, including propagations, are done at the

model level, and never in the display. This will be the only way to ensure a consistent representation in all active displays.

Each node in the model carries at least the following information:

- Value
    - Value Validity
- Alarm
    - Alarm Validity
    - Alarm acknowledgement state
- Maintenance mode
- Operational status, e.g. start-up, initialisation, shutdown, etc.

Even in the case where certain fields are not applicable, e.g. no maintenance mode available, or no possible alarm condition, it is of utmost importance that every node provides the same complete interface, in this case providing some default or *not-applicable* values. This will allow every display to visualise every node in the hierarchy and makes generic, configurable displays possible.

Each node in the model that has subcomponents will also require some logic for summarising the status of all its descendants and how alarms will be propagated. While it will not be possible to have a single algorithm that fits all cases, care must be taken to abstract common code as much as possible through a clever class inheritance hierarchy.

5.5 Configuration Systems

The integrated alarm system needs to be configurable at several levels. We do not only anticipate increased use by different groups at the observatory and perhaps the executives, which requires the definition of new (secondary) display panels, but also that the monitoring model will regularly be extended and refined, and that new data sources will be added as new systems are being developed and commissioned or in fact systems get decommissioned or replaced by different ones. All these configuration tasks must be possible without the need to make changes at the code level of the integrated alarm system.

5.5.1 Model Configuration

The observatory monitoring model must be fully configurable outside the code base of the alarm system. It may be advisable to keep such configuration in a human readable format, e.g. in JSON format. This has the added benefit that, at least in the early deployment phase, the model can be simply created and edited with a text editor. The creation of smart custom editors could then be left to a later stage, when the requirements are clear. Moving to a database representation would also be easily possible, without changing the actual data interchange format.

5.5.2 Display Configuration

The integrated alarm system must provide a smart WYSIWYG editor to create and maintain all display panels. This includes both generic panels and highly customised ones, using smart HCI templates. The main focus must be on reusability of each and every panel in multiple independent displays. This implies that also every display

hierarchy will be named and reusable, with the possibility to clone and modify, while not endangering the integrity of defined displays through user access control.

5.5.3 Data Source Configuration

As mentioned in section 5.3 above the integrated alarm system will provide the ability to have any number of data sources through a plug-in architecture. While each of these plug-ins will have a highly specialised interface to the actual data source, their interfaces to the alarm system core will be identical, allowing the rapid addition (and removal) of plug-ins. There will be no need to change plug-ins at run time, but it must be possible to deploy a new or updated plug-in through a simple configuration change followed by a simple restart of the alarm system. This limitation is possible because the integrated alarm system will not be suitable for safety critical alarms. Requiring a full 24/7 uptime would require significant additional effort in design, implementation and most of all testing of the alarm system.

Since such a flexible architecture leads to the possibility of (temporary) misconfiguration, it is also important that the whole system is resilient to such events. Such situation should be reflected in the displays as the values and resulting alarms for these components not being valid, but never should the malfunctioning or misconfiguration of a plug-in stop the entire integrated alarm system from malfunctioning. The alarm system must also be able to report internal alarms, e.g. the malfunctioning of a particular plugin, or some misconfiguration.

5.6 External Interfaces

The integrated alarm system relies on many different and mostly incoherent interfaces to external systems to collect monitoring and alarm information from. Some of these interfaces are described in varying level of detail in the appendix in section 7. As already mentioned in previous sections, various plug-ins will need to be designed and developed that interface with these data sources and collect the required information in a uniform way for the integrated alarm system to process.

The integrated alarm system will have no direct “back-links” to any of the monitored systems on the programmatic level, e.g. to open a configuration panel of the OMC for the operators to address a particular alarm situation. The only permissible “back-link” will be through fully qualified URLs to either open documentation or web applications in a web browser.

6 Conclusions

This study has identified the core requirements for an integrated alarm system and, with the inclusion of relevant external expertise and experience from the European Space Agency (ESA) and INRIA, a high-level design concept has been produced. The system suggested for development will be a powerful, generic and extensible alarm system that not only addresses the needs of the array operators, but also allows other groups, such as engineering or science operations to improve their situational awareness and operational efficiency and effectiveness.

During the course of this study it has become very clear that the need for an integrated alarm system is an undisputed priority for the ALMA observatory. Encouragement for this study and to push forward with the actual development has not only been received from all the ALMA partners, but also from the science community. Namely the European Science Advisory Committee (ESAC) has stated in their recommendations from the February 2016 face-to-face meeting: “ESAC was pleased to hear that the ESO (internal) study on an ‘Integrated Alarm System for ALMA Observatory’ was selected and looks forward to receiving a report at its next face-to-face meeting. ESAC applauds ESO for this pro-active approach to improve the observatory efficiency.”

We therefore recommend the creation of a European ALMA development project to design, implement and deploy an integrated alarm system for ALMA at the earliest possible date. We anticipate a total project duration of approximately two years and a total FTE count of 3.1 FTEs to be required. The project can be broken down as follows, where T_0 is the project start date:

Start	Duration	FTE	Who	Activity
T_0	24m	In-kind	Head of ICT-EU	Project management, contracts, etc.;
T_0	3m	0.2*	ESO ISM	Detailed requirements and design;
T_0+3m	3m	0.2*	ESO ISM	Implementation of alarm system core, including data model, plugin architecture and data source API;
T_0+6m	6m	0.5	JAO LSM	Implementation of data source plugins at OSF in a TBD priority order; requires frequent interaction with engineering and key stakeholders for the to be monitored systems.
T_0+6m	6m	0.4*	ESO ISM	Implementation of display panel API, sample display panels, configuration system, logging system;
T_0+12m	9m	0.75	JAO LSM	Implementation of display panels**
T_0+12m	6m	0.4*	ESO ISM	Preparation of integration tests and deployment processes; refinement of data models, behaviour, etc.
T_0+18m	3m	0.2*	ESO ISM	User documentation; pilot installation at OSF, refinements
T_0+21m	3m	0.2* 0.25	ESO ISM JAO LSM	System deployment, including full implementation of the observatory data model in collaboration with array operators, engineering and science operations.

T_0+24m	~			Alarm system in operation.
Totals	**24m**	**1.6** **1.5**	**ESO ISM** **JAO LSM**	

* Based on a total availability of 0.8 FTE/year

** Could be done in collaboration with INRIA

This very coarse project break down will be more detailed, once the in-principle agreement to push forward this project has been reached.

After delivery and acceptance of the integrated alarm system, the regular maintenance and configuration will become part of the regular tasks of the array operators and software support staff at the OSF. Secondary displays will be configured and maintained directly by their users, e.g. engineering or science operations staff. There is, however, the need to budget for regular software maintenance, providing bug fixes and updates. Using the formula that 10% of the total effort to build a software product will be required on an annual basis to support it, we can deduce an annual FTE requirement of approximately 0.3 FTE. This support would be best done at the OSF.

Detailed costing of the project and its maintenance will be provided to the relevant parties in a separate document.

7 Appendix A - Description of Alarm Sources

As shown on page 7 of the study proposal [AD1], we have identified the following alarm sources:

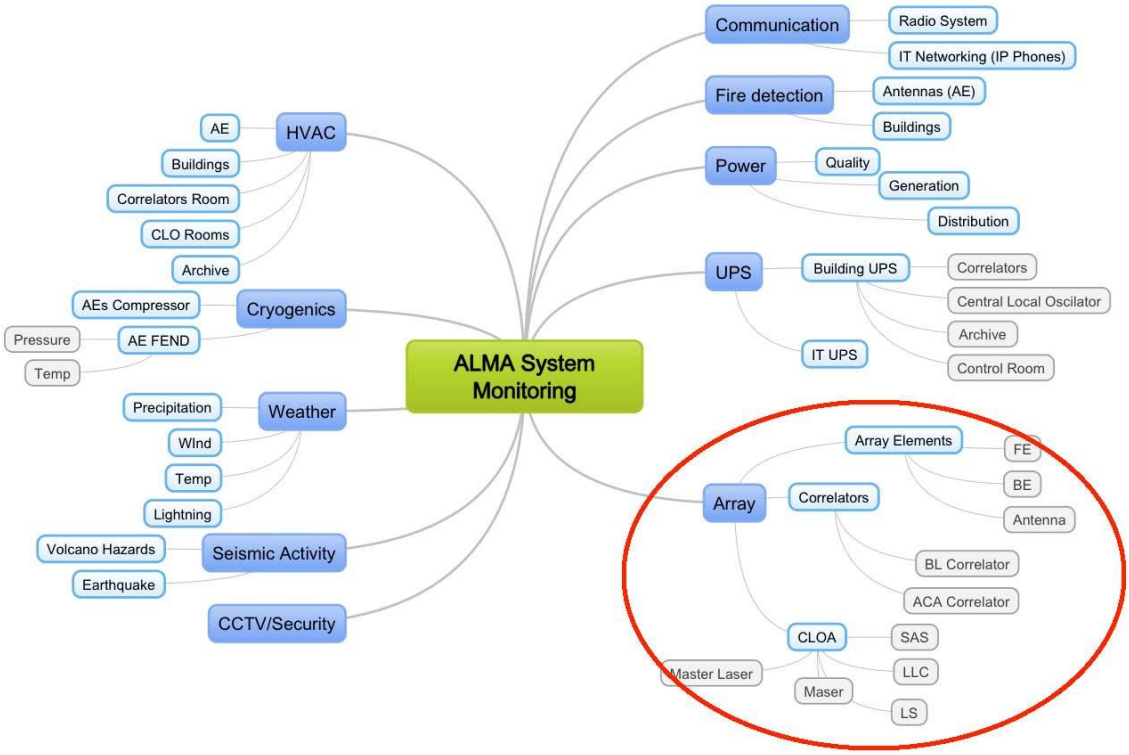


Figure 15 – ALMA Alarm Sources

In a very simplistic view of the system, the green box in the centre is the **integrated alarm system**, which is the main topic of this study, while the dark-blue boxes around it are the various **alarm sources** described in this section. Ideally each alarm source should have an external interface through which it can publish alarms to the central integrated alarm system.

The detailed breakdown for each of the alarm sources is only documented herein as far as it adds to the understanding of the data formats and interfaces. More detailed information present in other documentation is provided in referenced documentation.

In the following the alarm sources are listed in no particular order.

7.1 Array - ACS Alarm System

The section refers the **Array** part of Figure 15.

7.1.1 Overview

The ALMA Common Software (ACS) alarm system collects, reduces and presents alarms generated by various alarm sources to operators. The alarms collected by this alarm

system are limited to those generated by the ALMA software during a running ACS session.

ACS provides a set of APIs to allow developers to publish alarms without dealing with the details of the underlying alarm system implementation. Monitor points, associated to so-called BACI properties, can be configured so that alarms are automatically produced under certain circumstances, for example if the value of a monitor point is greater than a given threshold.

The alarm server collects the alarms received by the sources and applies the reduction rules retrieved from the knowledge base to present to the operators a compact view of the active alarms to facilitate the identification of the root cause of a problem.

A detailed description of the ACS alarm system is part of ACS documentation and can be found in [RD3]

The architecture of the ACS alarm system is composed of three layers. At the bottom, the sources produce the alarms that are sent to alarm server in the middle layer. The alarm server receives all the alarms and then generates an enriched and reduced view of the active alarms. This view of the active alarms is sent to the third level, the alarm clients, e.g. the alarm panels used in the control room.

7.1.2 Alarm Sources and Triplets

ACS alarms are identified a by a triplet in the format of ***<family, member, code>***. Family and member have the purpose to identify the source of an alarm: the family groups all the sources of a given type and the member identifies which particular instance of the family is actually producing the alarm. The code specifies which particular alarm is produced. This schema is particularly useful when having big sets of identical components (the family), each of which can produce the same set of alarms depending on the possible failure types. The possible alarm codes, i.e. the alarm types, are the same for each instance of the family. For example, ACS generates an alarm if a container crashes. In this case the family, grouping all the containers is named *Container*, the member can be the name of the crashed container that is unique at run time, for example *LoggerContainer*. The failure, the crash is identified by the integer *0*: the triplet for this particular alarm would be *<Container, LoggerContainer, 0>*. All the alarms, i.e. the triplets produced by sources must be configured in the static database, the TMCDB.

In a distributed software environment, there is no limitation imposed on the source that produces an alarm, so we can think of having software tools in charge of checking the integrity of other components, either hardware or software, and produce alarms if needed.

A source submits an alarm with a simple call like:

```
containerServices.getAlarmSource().raiseAlarm("Antenna","DA45",1);
```

The ACS infrastructure is in charge of routing the triplet to the alarm server for processing. The triplet is published in a CORBA notification channel and the alarm server is subscribed to the same channel. Alarms are published in form of XML strings and grouped to reduce the number of messages. The following XML snippet (there is no schema at the present) describes the format of alarms published by sources in the notification channel:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
 <ASI-message ...>
   <source-hostname>HOST</source-hostname>
   <source-timestamp>YYYY-MM-DDTHH:MM:SS.nnn</source-timestamp>
```

```
   <fault-states>
    <fault-state family="FF" member="MM" code="0">
      <descriptor>ACTIVATE</descriptor>
      ...
    </fault-state>
    ...
   </fault-states>\n')
 </ASI-message>\n'
```

A source can send an alarm directly to the alarm server, a CORBA servant whose IDL provides the method `submitAlarm` for this purpose:

```
void submitAlarm(in alarmsystem::Triplet myTriplet,
                 in boolean active,
                 in string sourceHostName,
                 in string sourceName,
                 in ACS::Time sourceTimestamp,
                 in CosPropertyService::Properties alarmProperties)
                 raises (...);
```

7.1.3 Alarm Server

The alarm server collects all the alarms produced by the sources and identified by the triplets, i.e. it has a view of all the active alarms in the ALMA software. Usually a failure in one component produces a chain of failures in the same and other dependent components. At run time a failure often produces a burst of alarms that would make it very difficult for an operator to understand what is really happening in the system.

The ACS alarm server has a knowledge base of the dependencies between the alarms configured in the static database (TMCDB). Knowing the dependencies between the alarms and the active alarms at a given moment, the alarm server can identify the root cause of a chain of failures. Alarm clients like the ACS alarm panel present to the operator only the root cause of a chain of failures, hiding the non-relevant alarms, so that the operator can quickly initiate the appropriate counter action.

The dependencies between alarms are defined by a set or reduction rules that describe the dependencies between triplets. There are two kinds of reduction rules that can be combined:

- The *node reduction* is a linear dependency between two alarms; when it is known that a failure in component A triggers a failure in component B, this reduction rule allows to mask the failure of B and present to the operator only A as the root cause of the chain of alarms.
- The *multiplicity reduction* allows reducing the number of certain alarms. When it is known that a failure in one component triggers a failure in a set of other components, the multiplicity reduction allows hiding all these failures and present to the operator a single alarm describing the failure.

The alarm server starts as part of ACS services and terminates when ACS is shut down. The alarms are not persisted i.e. when the alarm service shuts down, the alarms it contains are lost. When the ALMA software starts, components initialize the devices and send alarms in case of problems creating a new, typically empty set of alarms for the alarms server to manage.

While the actual alarm sources only send a triplet to submit an alarm, the alarm server sends to its clients an enriched data structure containing information to allow the operators to understand the nature of the alarm, what caused the problem and how to fix it, amongst other information. The triplet of the alarm is used as a unique identifier to access the static database to retrieve the proper data structure for the clients.

Alarms can be categorised before being sent to the clients. One can for example define one category for ACS alarms, one for the control system alarms, and so on. Alarm clients can decide if they want to receive alarms for all the categories or only for a subset of the existing categories. The alarm server sends the alarms to the clients by publishing them as XML strings in one notification channel for each category. An alarm can be published in one or more categories, or notification channel, as configured in the TMCDB.

The schema for the alarms published by the alarm server to the clients is available in *AcsAlarmSystem.xsd* in the ACS *acsalarmidl* module.

7.1.4 Alarm Clients

ACS provides a Java API to

- be notified of alarms generated by sources; and
- be notified of alarms sent by the alarm server to the clients

Alarm source subscribers connect to the notification channel, where the triplets submitted by the sources are published.

The API hides CORBA details and consists only of a few lines of code: instantiate a `SourceClient` object, add a listener to be notified when a triplet has been published and finally call the connect method to start receiving events:

```
SourceClient sc = new SourceClient(containerServices);
sc.addSourceListener(listener);
sc.connect();
```

The listener receives alarms in form of triplets and XML strings.

The `AlarmCategoryClient` allows receiving callbacks when the alarm server publishes an alarm to the clients, following the same paradigm of the source client. This client offers a few more methods to deal with the reduction rules.

The `alarmPanel` is the operator GUI. It shows the alarms provided by the alarm server, hiding the reduced ones to minimize the number of alarms displayed in the table and to simplify the identification and quick resolution of the root cause of a problem. The panel is read-only in the sense that the operator cannot take any action on the displayed alarms. An active alarm becomes inactive when the failure has been fixed and the source clears the alarm. The `alarmSenderPanel` allows to set/clear alarms passing their triplet at any time.

The alarm panel is a Java Swing application that encapsulates a `SimpleClient` to connect to the ALMA software at run time. It is tied to the ACS alarm system in the sense that it deals with triplets and reduction rules whose format is peculiar to the ACS alarm server. The alarm panel can be modified to run outside of the ALMA software connecting to the alarm system with CORBA calls; a feature already implemented by the `AlarmCategoryClient`.

At the present the `alarmPanel` is the best option to receive alarms and present them to the operators, taking into account reduction rules. At the same time it needs several improvements.

7.1.5 Alarm Configuration

The configuration of alarms is part of the static database, the TMCDB. The *tmcdb-explorer* application has a dedicated area for configuring the alarm system.

Alarms are documented by *family* because all the alarms belonging to the same *family* have the same cause, description and solution. In the same way the *members* can all fail in the same way producing the same set of fault codes.

Considering the fact that ALMA contains a great number of equal devices (*members* in this context) for which the documentation would simply be a copy and paste from one member to another, the ACS alarm service can automatically infer the documentation of a specific triplet from its *family* and *code* (with some limitations).

Reduction rules as well as the optional association between alarms and categories are also stored in the TMCDB.

7.1.6 Running the Alarm Server Outside of ACS

At the present the life cycle of the alarm server is tied to that of ACS. The server starts together with other ACS services and shuts down when the ACS session terminates. The configuration is read at start-up from the configuration database.

The ACS alarm server is a CORBA servant that depends on the CORBA Notification Service to receive triplets from sources and to send alarms to the clients, the TMCDB to read the configuration and the logging service.

It is in principle feasible to make the alarm server independent from an ACS session and let it run 24/7 provided that:

- The CORBA Notification Service is started before the alarm server; if properly configured in the TMCDB, ACS sources and clients should be able to connect to the notification service independently of who started it.
- The alarm service can be extended to be able to read the alarm configuration from the TMCDB independently of the CDB ACS service. As an alternative, the alarm configuration could be moved into a dedicated database and a new configuration editor provided (not to be done from scratch but starting from what is currently in the tmcdb-explorer)
- A mechanism is provided to update the configuration without restarting the service
- Alarms are persisted

The alarms that are active when an ACS session terminates should all be cleared until a new session starts. This could be realized by enabling the alarm service to detect if an ACS session is running or ensure that a clean shutdown of the ALMA software is always performed. There is no practical reason to extend the life of the ACS alarm server outside of the boundary of an ACS session if there are no alarms to show unless we decide to let the alarm panel show also alarms generated by external sources (i.e. non ALMA.).

7.1.7 Feed an External Alarm System with Array Alarms

It is in principle easy to start a client that gets triplets generated by ALMA sources or alarms published by the alarm server and feed that information into another alarm system. ACS already provides clients for that. They need some adaptation but should not be a great effort.

The biggest problem is what to do with ALMA software alarms that are active when an ACS session terminates. At the present the ACS session is killed to save time during a full system restart. A clean shutdown would, in fact, increase the time of a full system restart.

The new alarm system that receives alarms from the array should also be aware of the reduction rules unless we want to use the mechanism provided by this external alarm server.

7.2 UPS

7.2.1 Overview

ALMA uses two different types of UPS systems:

- General Electrics SG Series UPS 10-600 kVA three phase 400 Vac [RD6] at the AOS
- Emerson Chloride 80-NET [RD5] at the OSF

7.2.2 Description of Alarm Sources

7.2.2.1 General Electrics SG Series UPS

The General Electrics UPS offers an optional SNMP plug-in card that allows the UPS to communicate over a LAN with compatible remote systems. See page 10 of [RD6] for details.

7.2.2.2 Emerson Chloride 80-NET

The Emerson UPS offers hardware connectivity through **ManageUPS NET**. It ensures the monitoring and control of the networked UPS, through the TCP/IP protocol. This permits the integration of the Chloride UPS with Building Monitoring and Automation Systems via MODBUS RTU, MODBUS/TCP or JBUS protocols. See pages 9-10 of [RD5] for details.

7.3 Power

7.3.1 Overview

The ALMA power system is composed of three major components:

- Turbomach power turbines at the OSF (see [RD8])
- General Electrics F35 Multiple Feeder Protection System (Switch Gears) at the AOS (see [RD7])
- Micom power distribution substations at the OSF and AOS

All these systems are operated and monitored by dedicated teams outside the OSF control room. Remote monitoring and alarm notification to the OSF control room is not currently in place.

7.3.2 Description of Alarm Sources

7.3.2.1 Turbomach Power Turbines

Originally a fully featured SCADA system to monitor and control the power plant was in the project scope, but it was de-scoped when it was decided not to provide it for other parts of the power distribution system. Nevertheless all major components have been procured to support it and therefore they come with communication features.

Normally the various power subsystems are supposed to communicate with SCADA terminals coming from the same manufacturers, not through open networks with third party computers. And the intention was always to keep this network physically separated from any other on security grounds.

As shown in [RD8], the power turbines are equipped with an Ethernet interface through which they communicate with a (somehow customized) PC that acts as terminal. Physically one could use that Ethernet to access the data, but this may be a proprietary protocol and the manufacturer is not keen on disclosing the relevant information.

7.3.2.2 Switch Gears

Remote monitoring is available via TCP using the Modus RTU protocol. See Appendix B of [RD7] for the node mapping.

7.3.2.3 Power Distribution Substation

Remote monitoring is available via the IEC61580 protocol. The exact monitor points are self-discovered via the protocol.

7.4 HVAC

7.4.1 Overview

There are building HVAC systems in the AOS technical building and OSF technical facility. There will most likely be a similar system in the residencia.

No information provided.

7.4.2 Description of Alarm Sources

Remote access to the HVAC system is provided via the BACnet IP protocol. See [RD9] for details.

7.5 Fire Detection

7.5.1 Overview

There are fire detection and suppression systems in the AOS technical building and OSF technical facility. There will most likely be a similar system in the residencia.

No information provided

7.5.2 Description of Alarm Sources

Remote access to the HVAC system is provided via the BACnet IP protocol. See [RD9] for details.

7.6 Communication

ALMA is currently in the process of implementing a digital radio system, which should allow us to monitor the system remotely. No detailed information is currently available.

7.7 CCTV/Security

The site surveillance system is currently in the (early) requirements definition phase.

7.8 Seismic Activity

A monitoring system for seismic activity is not yet available.

7.9 Weather Stations

7.9.1 Overview

There are eleven sets of weather stations deployed at the ALMA observatory:

ID	Weather Station	Location	Status
1	**MeteoTB1**	AOS Technical Building	Decommissioned
2	**MeteoTB2**	AOS Technical Building	Active
3	**MeteoOSF**	OSF Holography Tower #2	Active
4	**MeteoItinerant**	AOS Itinerant Wind Meter	Active; wind only
5	**Meteo201**	Near antenna pad W201	Active
6	**MeteoCentral**	Central Weather Station	Active
7	**Meteo309**	Near antenna pad S309	Active
8	**Meteo410**	Near antenna pad P410	Active
9	**Meteo131**	Near antenna pad A131	Active
10	**Meteo129**	Near antenna pad A129	Active
11	**Meteo130**	Near antenna pad A130	Active

Table 1 - ALMA Weather Stations

Each of them provides the following measurements:

a. Humidity
b. Ambient temperature
c. Dew point
d. Wind direction

e. Wind speed

f. Air pressure

Each of these monitoring points are sampled at a frequency of 1Hz. The sampled data is saved in the production archive and a web interface is available to show the current values and plots of these measurements. See http://weather.aiv.alma.cl.

The current measurements of each weather station can be retrieved using this web service:

`http://weather.aiv.alma.cl/ws_weather_jsonf.php?getCurrentWeatherData`

The corresponding WSDL is available via

`http://weather.aiv.alma.cl/ws_weather_jsonf.php?wsdl`

```
<definitions xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-
  ENC="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:tns="http://weather.aiv.alma.cl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  targetNamespace="http://weather.aiv.alma.cl/">
<types>
  <xsd:schema targetNamespace="http://weather.aiv.alma.cl/">
    <xsd:import namespace="http://schemas.xmlsoap.org/soap/encoding/"/>
    <xsd:import namespace="http://schemas.xmlsoap.org/wsdl/"/>
  </xsd:schema>
</types>
<message name="getCurrentWeatherDataRequest">
  <part name="id" type="xsd:integer"/>
</message>
<message name="getCurrentWeatherDataResponse">
  <part name="return" type="xsd:string"/>
</message>
<portType name="getCurrentWeatherDataPortType">
  <operation name="getCurrentWeatherData">
    <input message="tns:getCurrentWeatherDataRequest"/>
    <output message="tns:getCurrentWeatherDataResponse"/>
  </operation>
</portType>
<binding name="getCurrentWeatherDataBinding"
  type="tns:getCurrentWeatherDataPortType">
  <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="getCurrentWeatherData">
    <soap:operation
soapAction="http://weather.aiv.alma.cl/ws_weather_jsonf.php/getCurrentWeatherData
" style="rpc"/>
      <input>
        <soap:body use="encoded" namespace="http://weather.aiv.alma.cl/"
          encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
      </input>
      <output>
        <soap:body use="encoded" namespace="http://weather.aiv.alma.cl/"
          encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
      </output>
    </operation>
  </binding>
  <service name="getCurrentWeatherData">
    <port name="getCurrentWeatherDataPort"
      binding="tns:getCurrentWeatherDataBinding">
      <soap:address location="http://weather.aiv.alma.cl/ws_weather_jsonf.php"/>
```

```
    </port>
  </service>
</definitions>
```

An example of Python client using this web service is shown below. The `getCurrentWeatherData(ID)` method requires a single parameter, which indicates the ID of the weather station.

```
>>> import suds
>>> wsdl = "http://weather.aiv.alma.cl/ws_weather_jsonf.php?wsdl"
>>> ws = suds.client.Client(wsdl)
{"weather
id":1,"timestamp":1.3659279691e+17,"status":"true","serialNumber":"D2320029D18100
15","sensors":[{"sensor
name":"humidity","unit":"percentage","value":52.2384986877},{"sensor
name":"temperature","unit":"celsius","value":-5.21969985962},{"sensor
name":"dewpoint","unit":"celsius","value":-13.516500473},{"sensor name":"wind
direction","unit":"degree","value":254},{"sensor name":"wind
speed","unit":"m\/s","value":1.4},{"sensor
name":"pressure","unit":"hPa","value":554.787475586}]}
```

7.9.2 Description of Alarm Sources

During operations of the observatory weather conditions must be monitored in order to stow and shutdown antennas to protect them and to avoid permanent damage in equipment and antennas.

In summary, the list of alarms are to trigger survival stow are

i. Ambient temperature < -20° Celsius.

ii. Wind speed > 20 m/s

iii. Precipitation: *rain*, *snow* or *icing*

Currently weather alarms are sent to this email address: cfg_notification@alma.cl

The official document that describes this procedure can be found at

http://edm.alma.cl/forums/alma/dispatch.cgi/f.operationsd/showFolder/100123.

The logic of these alarms described in this document is implemented within the weather station software and the results are displayed in the weather interface. There is no programmatic interface to retrieve those alarms so far, but it is simple to implement a web service similar to that for the current measurements. The data format is open to be defined according to the requirements of the operations and this project. The weather station software is in-house software developed by JAO.

7.10 Cryogenics

7.10.1 Overview

The Cryogenics system analyses information points from the cryostat and compressor, and sends alarms notifications if the information points exceed certain limits defined by the cryogenic team. The cryogenic team is in charge of the cryostat and compressor devices, both vital to maintain the correct functioning of the ALMA frontend receptors. They have defined several information points and their tolerance limits for normal operations.

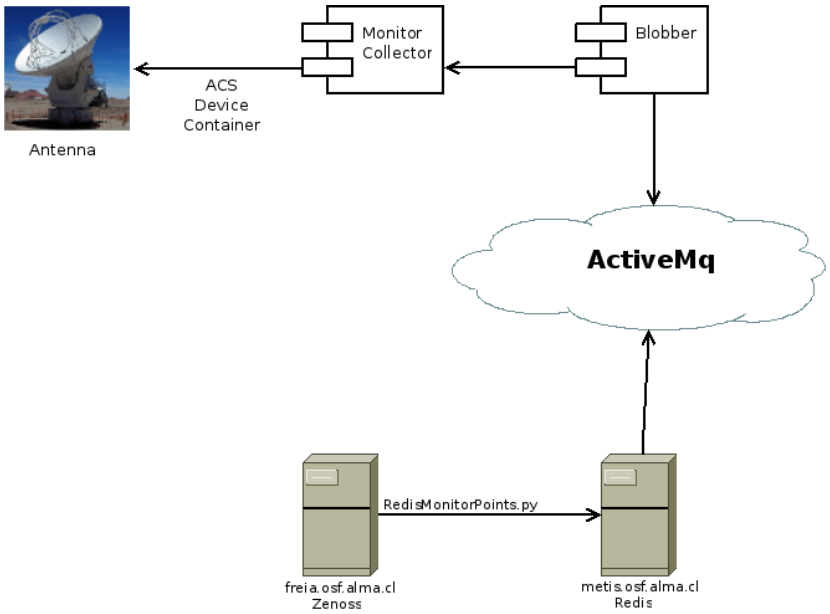


Figure 16 - Cryogenics monitoring system

The information points for the Cryostat and Compressor are received from the *Redis*[2] application running on *metis.osf.alma.cl*. This information is processed by a *Zenoss*[3] application running on *freia.osf.alma.cl.* The Zenoss application is responsible to send alarm notifications if the information points are above the tolerance limits defined for the devices.

Table 2 shows the information points that are currently analysed for each active frontend assembly.

Information Point	Device	Tolerance Limit	Comments
4K Cryo Cooler (TEMP0_TEMP)	Cryostat	< 5 K	
4K Plate near link #1 (TEMP1_TEMP)	Cryostat	-	Derived from TEMP0
4K Plate near link #2 (TEMP2_TEMP)	Cryostat	-	Derived from TEMP0
4K Plate far side #1 (TEMP3_TEMP)	Cryostat	-	Derived from TEMP0
4K Plate far side #2 (TEMP4_TEMP)	Cryostat	-	Derived from TEMP0
15K Cryo Cooler (TEMP5_TEMP)	Cryostat	< 21 K	
15K Plate near link #1 (TEMP6_TEMP)	Cryostat	-	Derived from

[2] See http://redis.io
[3] See http://www.zenoss.com

			TEMP5
15K Plate far side #1 (TEMP7_TEMP)	Cryostat	-	Derived from TEMP5
15K Shield Top (TEMP8_TEMP)	Cryostat	-	Derived from TEMP5
110K Cryo Cooler (TEMP9_TEMP)	Cryostat	-	
110K Plate near link #1 (TEMP10_TEMP)	Cryostat	-	Derived from TEMP9
110K Plate far side #1 (TEMP11_TEMP)	Cryostat	-	Derived from TEMP9
110K Shield Top (TEMP12_TEMP)	Cryostat	-	Derived from TEMP9
COMPRESSOR_DRIVE_INDICATION_ON	Compressor	1 (= On)	

Table 2 – Cryogenics Information Points

7.10.2 Description of Alarm Sources

The cryogenics systems of all active ALMA antennas are constantly monitored and any deviation from the allowed values must be brought to operator attention for immediate action. Any resulting alarms are currently sent to the cryogenics team via email to a group email address. Only power failures are also sent via email to the array operators, so they can notify the cryogenics team outside their regular working hours.

Currently all cryogenics alarms are sent to: ade-ig-cryogenic@lists.alma.cl.

Power alarms are also sent to: znalarms@alma.cl.

The official document that describes this procedure can be found at:

https://ictwiki.alma.cl/twiki/bin/view/SoftOps/CryostatTrendAnalysisAlarmDashboard

There is no programmatic interface to retrieve those alarms so far. The data format is open to be defined according to the requirements of the operations and this project. The Cryostat Trend Analysis and Alarm Dashboard software is in-house software developed by JAO.

--- End of document ---

esoc

European Space Operations Centre
Robert-Bosch-Strasse 5
D-64293 Darmstadt
Germany
T +49 (0)6151 900
F +49 (0)6151 90495
www.esa.int

DOCUMENT

Report for an Integrated Alarm System for the ALMA Observatory

European Space Agency
Agence spatiale européenne

Title **Report for an Integrated Alarm System for the ALMA Observatory**	
Issue Final	**Revision** B
Author **Petros Pissias, petros.pissias@esa.int**	**Date** 28/04/2016

Table of contents:

1 INTRODUCTION

1.1 Purpose

This document is a report for a new Integrated Alarm System for the ALMA Observatory. It explains the current status and goals of the new system. Moreover, it formulates high level requirements and outlines some considerations for the software design.

1.2 Scope

This report focuses on capturing the requirements for the new system and also investigates potential design approaches.

1.3 Document Overview

Section 1 - Introduction (this section) provides the purpose, scope and this document's overview.

Section 2 – Applicable and reference documents, provides the list of applicable and reference documents.

Section 3 – Terms, definitions and abbreviated terms, provides a list of acronyms and terms used throughout this document.

Section 4 – Current monitoring and alarm system, provides a summary of the current monitoring and alarm system of the ALMA observatory .

Section 5– Requirements for the new integrated alarm system, describes high level requirements for the new integrated alarm system.

Section 6 – Technical considerations, describes some technical considerations that should be taken into account for the design of the new integrated alarm system.

Annex A – Workshop Discussion, presents the notes taken during the workshop discussion with the ALMA staff.

Annex B – Potential Technology re-use, presents ESA and non-ESA software for potential evaluation and re-use.

2 APPLICABLE AND REFERENCE DOCUMENTS

2.1 Applicable Documents

Ref.	Document Title	Issue and Revision, Date
[AD-1]		
[AD-2]		
[AD-3]		

2.2 Reference Documents

Ref.	Document Title	Issue and Revision, Date
[RD-1]	Integrated Alarm System for the ALMA Observatory (Plan) – ESO 271448	December 2015, version 1
[RD-2]	Integrated Alarm System for the ALMA Observatory (Design Report) – ESO 281186	January 2016, version 1.3
[RD-3]	Alarm system guidelines	Oct 23 2010.
[RD-4]	ACS Alarm System	2010-01-13, version 1.8
[RD-5]	Monitoring, Control and Automation of the ESA Ground stations	DASIA Conference 2011
[RD-6]	High Level Presentation of EUD	http://www.esa.int/Our_Activities/Operations/gse/EUD
[RD-7]	ESA EGS-CC website	http://www.egscc.esa.int/

3 TERMS, DEFINITIONS AND ABBREVIATED TERMS

3.1 Acronyms

Acronyms	Description
ALMA	Atacama Large Millimeter/submillimeter Array
AND	Alpha Numeric Display
ESOC	European Space Operations Centre
HVAC	Heating, ventilation, and air conditioning

3.2 Definition of Terms

Terms	Description

4 CURRENT MONITORING AND ALARM SYSTEM

As indicated in [RD-1] the control centre of the ALMA observatory uses a combination of tools in order to perform the monitoring and alarm management of the ALMA Antenna Array. Moreover, the current system does not include information from other domains, such as the power plant, HVAC system and others, which is considered to be an important input in order for the operators of the control centre, in order to have information on the status of all main systems of the ALMA facility.

The needs for a new Integrated Alarm System are outlined in [RD-1] and not re-iterated in this document. However, some of the limitations of the current monitoring and alarm systems are presented below:

- Parts of the monitoring of the user interface are not fully aligned with the monitored systems.
    - This refers to the array monitoring of the control system. While the system offers advanced capabilities such as semantic zooming and provides the means to have an overview at various levels of the entire antenna array, it is not updated to fully reflect the monitored equipment and thus it does not provide fully accurate monitoring of each individual antenna.
- Variety of tools
    - A number of monitoring and alarm tools have been developed in order to complement the monitoring of the ALMA facility and the ALMA Antenna Array. These tools are not tightly integrated and thus the operators have to check several displays and tools in order to judge if there is an issue they need to react to.
- Ad-hoc colour coding
    - The various tools deployed in the control centre do not follow a strict colour coding and thus the operators need to adjust to the conventions of each tool. A strict colour coding is considered very important in order to intuitively understand the current state of the system in cases where the operator needs to act urgently.
- Configuration Information Missing
    - The main control system does not cover configuration information in a way that is compatible with the day-to-day operations. This type of information is not monitored, but is information entered manually and describes complementary aspects of the monitored systems. For example:
        - Antenna Status (if an antenna is in maintenance)
        - Expected Observation Type for each antenna
        - …

This information, which is very useful in order to judge if a reported alarm is critical, is not integrated with the main control system, but it will be integrated near future.

- Complex Alarm Condition Evaluation
    - With the current systems it is not possible to define complex alarm conditions depending on the overall state of the system. Each individual subsystem may generate alarms which are received and further processed, even potentially reduced, by the Alarm System as described in [RD-4]. However, a subsystem, nor the alarm system, has the necessary information in order to judge if the currently reported alarm is significant at the system level. Thus, the system that generates the alarms at the system level should have access to the necessary information that enable it to define alarm conditions that depend on the state of the monitored systems. For example an antenna subsystem might report an alarm because a specific receiver is not present. This is correct from the point of view of the subsystem but at the system level, under the current operational context, this might not be considered an alarm (because for example the current observation mode does not use this receiver).

5 REQUIREMENTS FOR THE NEW INTEGRATED ALARM SYSTEM

5.1 Introduction

This section outlines some key ideas, concepts and requirements around the new Integrated Alarm system. They were derived from discussions with the ALMA staff and operators of the current control facility (See Appendix A) as well as from [RD-1] and [RD-2].

The primary function of the system will be to show a high level status & alarm information of all the main systems of the ALMA observatory:

- ALMA Antenna Array
- Control Centre
- Power Plant
- …

allowing the operator to identify the area of the root problem in case of a non-nominal situation.

In the system displays, each element will summarize the overall status of a system or subsystem via an appropriate colour coding that will be defined. Once an element shows an abnormal status, the operator will be able to navigate to a new display (i.e. drill down) in order to see the status of the sub-elements and identify the root cause of the problem. Depending on the complexity of the monitored element, it might be necessary to have several levels of displays showing more details of each element. For example by navigating 3 times: "ALMA Antenna Array → Antenna 43 → Cooling System" the system will present a display showing the status and monitored information from the specific Cooling System element.

A conceptual example of such displays and navigation between them is shown in the Figure below.

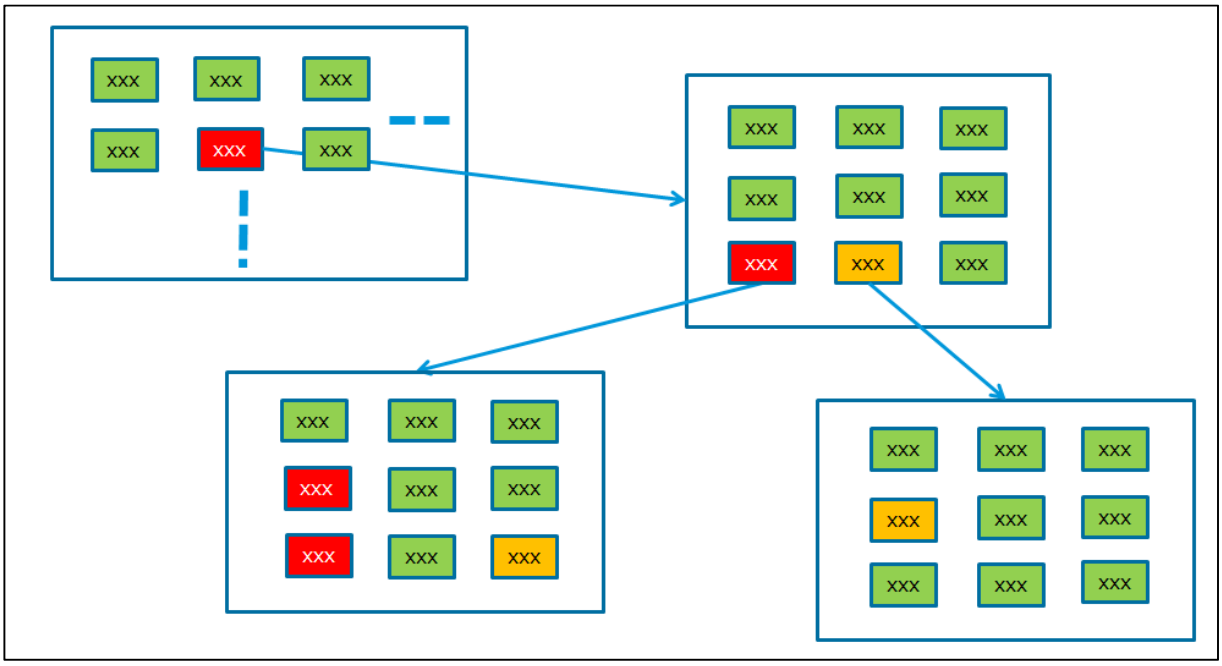


Figure 1. Conceptual Display Visualisation and Navigation

The example above should not be taken as the expected representation of the display format (i.e. boxes with colours). The representation of the displays (i.e. if they will contain graphics, tables, boxes, …) will be defined at a later stage of the Project. The diagram is present to express the following needs :

- There is a need to define several displays that show information related to the monitored systems.
- There is a need to display elements which summarize an overall status of other elements (For example, an antenna element should summarize the information from all the antenna subsystems - conceptually, this relationship of elements can be visualized as a Tree where each parent summarizes the state of its children).
- The monitored elements need to display information (related to their value or overall state)
- There needs to be navigation between elements of a display and a new display (i.e. by clicking at a monitored element a new display will open).
- There needs to be different colour coding to express different states of the monitored elements.

Some of the monitoring displays (for example a top level status display, or a high level mimic display) will need to be always visible, in order for the operator to always see the overall status of the system.

The displays shall be configurable (via a configuration tool) which will enable arranging their appearance, navigation and behaviour. Regardless of the architecture of the Integrated alarm system, the configuration tool is targeted to the following:

- Definition of displays and navigation between elements and displays
- Definition of the behaviour of the elements in each display
    - Behaviour includes all the information that is needed in order to identify if an element is in a non-nominal condition. This implies that the configuration tool must have access to the available monitoring and alarm information in order to be able define the behaviour of its elements according to conditions based on this information.

Depending on the operational needs for the configurability of the displays, the complexity and features of the configuration tool shall be adapted. If, for example, the displays and behaviour of the display elements is not expected to change often, then the effort for developing the configuration tool should be traded-off with the expected effort for the manual configuration of the displays and the behaviour of the display elements.

A complementary display, showing more information for each element which is in a non-nominal status (for example more information on the reason on why this element is in a non-nominal status) will enable having more detailed information and also provide an overview of the elements which are not nominal.

Moreover, the system shall enable 2 modes of interaction. A mode where an operator may perform control actions (i.e. acknowledge an alarm) and a mode where an operator may only observe.

The following sections summarize a set of requirements capturing the core functionality of the system. Each requirement is expressed by the information in the description as well as the information in the comment.

5.2 Assumptions and limitations

SW Requirement ID	Description	Qualifier
MON.LIM.001	The software and hardware shall be compliant with the baselines defined in [TBD]	Mandatory
comment		
[TBD] will define the allowed operating system, third party software and hardware platforms.		
Justification		
In order to be in line with the general software and hardware baselines of ALMA.		

5.3 Functional Requirements

SW Requirement ID	Description	Qualifier
MON.GEN.001	The System shall show a top level status of all monitored systems summarizing their health state.	Mandatory
comment		
This includes all systems that will be monitored (Power Plant, Weather Stations, ALMA Antenna Array, …). The top level status of each system shall summarize the status of all elements that belong in the monitored system.		
Justification		
Core functionality		

SW Requirement ID	Description	Qualifier
MON.GEN.002	It shall be possible to navigate from an element of a display to a new display.	Mandatory
comment		
The new display may be shown in a predefined position by replacing an existing display or be a new display completely. The arrangement of displays shall reflect the physical or logical structure of the monitored systems (i.e. by navigating to a new display from the “Antenna Array Element”, it should contain all Antenna elements and other relevant information.		
Justification		
Core functionality. Intuitive root cause identification by “drilling-down”.		

SW Requirement ID	Description	Qualifier
MON.GEN.003	The system shall present a display with all elements that are in non-nominal status.	Optional
comment		
This display shall contain all elements (in a table format (TBC)) which are in non-nominal status. Each element shall provide all available information for the reason of the non-nominal status (i.e. reason that triggered an alarm). This display shall contain only the elements which triggered a non-nominal status and not the elements that are in non-nominal status as a result of summarizing the state of other elements (i.e. if the cooling system of Antenna 43 is in alarm, then the summarizing element “Antenna Array” should not be included in this list).		
Justification		
Additional information for root cause identification. Summary of all active alarms at system level.		

SW Requirement ID	Description	Qualifier
MON.GEN.004	The behaviour of each element shown in displays shall be configurable based on the incoming monitoring and alarm information.	Mandatory
comment		
This is expected to be done offline as part of the configuration of the system. Incoming monitoring information is considered all the input to the Integrated Alarm System which includes all necessary information from all the other monitoring and alarm systems that will be integrated. For example, it shall be possible to define the alarm conditions of an element based on received alarms and monitoring information.		
Justification		
Core functionality. Needed in order to be able to define complex alarm conditions based on the state of the monitored systems.		

SW Requirement ID	Description	Qualifier
MON.GEN.005	It shall be possible to define elements on displays based on properties of other elements.	Mandatory
comment		

These are often referred to as "synthetic parameters" or "custom parameters". For example it shall be possible to define a parameter which has a value which is a combination of values or other properties of other elements. The elements which are referenced might also be "synthetic parameters" themselves.

For example, we should be able to define a parameter which has a value defined as an expression of values of other parameters:

```
Parameter A = (Parameter B + Parameter C) / 2
```

As a real example taken out of the configuration of one of the ESA ground stations, Parameter /MCM1/LDC1/204, which is defined in the context of a Down Converter, calculates a *Derived L-Band* frequency by taking into account the validity and values of other parameters.

The actual definition using the algorithmic language of the system is presented below just for reference to a sample algorithm:

```
      Value select
  Algorithm   UNDEFINED
                      when VALID (/MCM1/LDC1/201.VALUE)= FALSE

              9040 - /MCM1/LDC1/201.VALUE
                      when VALID (/MCM1/LDC1/206.VALUE)= TRUE AND
          /MCM1/LDC1/205.VALUE = "X-BAND";

              /MCM1/LDC1/201.VALUE - 22400 - /MCM1/LDC1/206.VALUE
                      when VALID (/MCM1/LDC1/206.VALUE)= TRUE AND
          /MCM1/LDC1/205.VALUE = "KA-BAND";

              UNDEFINED otherwise

          Endselect
```

Justification
This is needed in order to be able to define custom monitored elements combining information from other

elements.

SW Requirement ID	Description	Qualifier
MON.GEN.006	It shall be possible to access configuration information.	Mandatory
comment		
This is not information that is being monitored. It is configuration information entered by the operator or retrieved via a configuration system. For example the operating mode of an observation, configuration status of an antenna or other information that is important to the system but is not being monitored. This information shall be usable in defining the behaviour (i.e. alarm conditions) of elements.		
Justification		
Enable using configuration information for the determination of the state of monitored elements.		

SW Requirement ID	Description	Qualifier
MON.GEN.007	It shall be possible to determine if the systems are monitored reliably.	Mandatory
comment		
This shall be visualized accordingly to the associated elements in displays. For example if because of a network issue, or because of an error with a device being monitored, the Integrated alarm system cannot obtain reliably a value or alarm information, this should be reflected in the related elements that base their behaviour on the input information.		
Justification		
Ability to know if the system can reliably monitor the relevant systems.		

SW Requirement ID	Description	Qualifier
MON.GEN.008	It shall be possible to manage and visualize non-nominal states according to a well-defined workflow	Mandatory
comment		
This includes concepts such as alarm acknowledgement, alarm shelving and alarm severity states as defined in [RD-2] ad [RD-3]. However the overall alarm states and workflow shall be defined in detail in the next phase of the project. The ability to acknowledge or shelve multiple alarms utilizing the hierarchical nature of the system shall also be explored (for example by acknowledging an alarm at a system level, all the underlying alarms will be acknowledged)		
Justification		
Core functionality. Alarm management and presentation.		

SW Requirement ID	Description	Qualifier
MON.GEN.009	It shall be possible to use equipment templates for the configuration of the system.	Mandatory
comment		
This is needed in order to ease the configuration of the system. There shouldn't be the need for example to individually define all Antennas, but it should be possible to use as template the configuration of the elements for one Antenna to define another.		

Justification
Ease of configuration

SW Requirement ID	Description	Qualifier
MON.GEN.010	All non-nominal behaviour shall be archived	Mandatory
comment		
This refers to all non-nominal information such as alarm conditions, inability to monitor a system etc.		
Justification		
Incident investigation, system performance metrics		

5.4 Software Maintainability Requirements

SW Requirement ID	Description	Qualifier
MON.MAINT.001	It shall be possible to add new monitored elements by configuration	Mandatory
comment		
This assume s that the monitoring interface is already implemented. If for example a new equipment is added to an Antenna, or if there is a need to monitor an additional equipment which is not already monitored (but with the system being interfaced already) then this shall be possible by configuration without a new release of the software.		
Justification		
Configurability and ease of software maintenance.		

5.5 Performance and Budget Requirements

SW Requirement ID	Description	Qualifier
MON.PER.001	It shall be possible to calculate the overall state of the monitored systems within 2 seconds.	Mandatory
comment		
This time is calculated up-on receiving monitoring information. If for example we receive a new set of monitoring information from one of the monitored systems, it shall be possible to calculate all alarm conditions and states of all elements and reflect them to the user interface.		
Justification		
Monitoring reliability		

SW Requirement ID	Description	Qualifier
MON.PER.002	It shall be possible to monitor 50.000 information elements.	Mandatory

comment
Information elements are all individual monitoring and alarm information monitored from other systems. For example a value of a sensor is 1 information element and the information that an equipment is in alarm condition is 1 information element.
Justification
Monitoring scalability.

SW Requirement ID	Description	Qualifier
MON.PER.003	It shall be possible to define 10.000 “synthetic parameters”	Mandatory
comment		
Synthetic parameters are custom parameters that base their value on properties of other parameters.		
Justification		
Monitoring scalability.		

6 TECHNICAL CONSIDERATIONS

The following section does not strictly stay at the requirements level but also considers, at least at a conceptual level, some design aspects of the Integrated Alarm System.

6.1 Summary states of monitored elements and display navigation

The combination of the following requirements :

- to be able to define custom displays showing information from monitored elements
- to be able define elements which summarize the state of other elements

hints to a conceptual design where we have a structured hierarchical model of the monitored systems (which defines the hierarchy of the systems at a logical or physical level) and display definitions that visualize elements of this model.

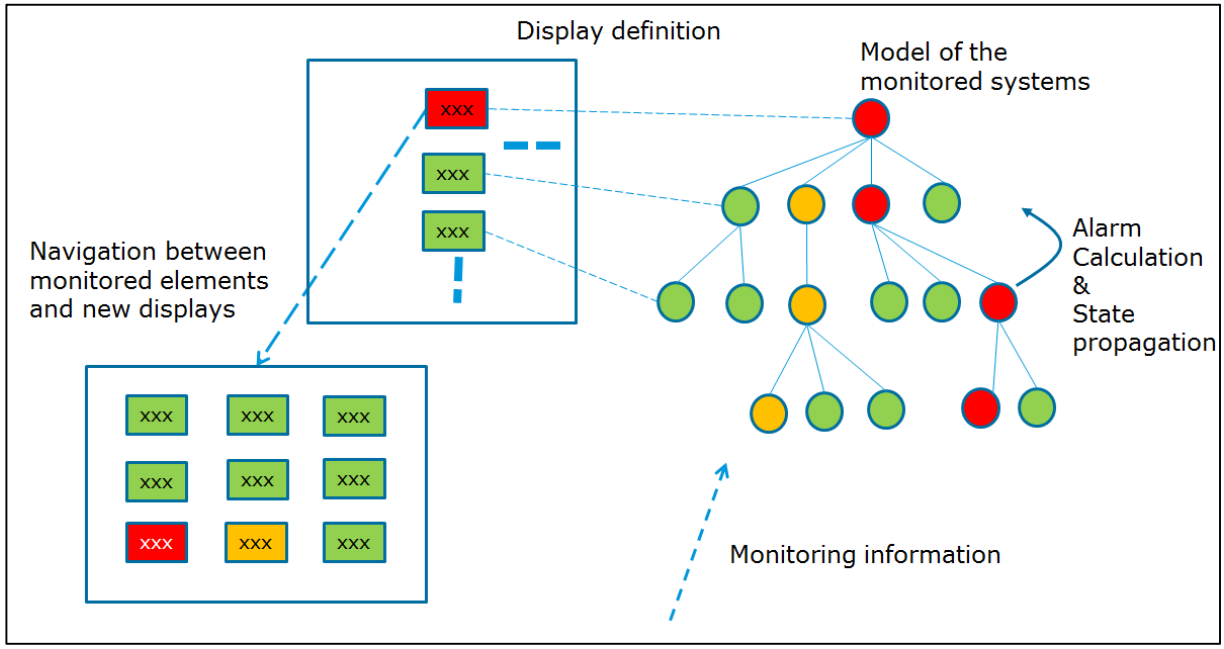


Figure 2. Conceptual Design

Following this concept, we can define a tree structure which reflects the logical or physical representation of the elements we monitor. This structure defines a containment relationship between parent and child nodes (i.e. the parent node contains its children) which follows either the logical or physical representation of the systems we monitor.

For example, the top level element may be the “ALMA site” which contains among others the children “Antenna Array”, “Correlator”, “Weather Stations” and the “Power Plan”. The “Antenna Array” will contain all 68 Antennas and any other elements of the Antenna Array.

Each of the Antennas will contain children which represent the major subsystems of each Antenna and each of these subsystems will contain elements which represent the status of the subsystem (i.e. monitored parameters, alarm statuses, etc).

6.1.1 Monitoring Model

Using this representation, containment relationships modelled with a Tree structure, we can thus define a model (either physical, logical or a combination of both) which reflects the state of the elements we monitor. The elements of such a structure can be categorized into two major categories, Container elements and Leaf elements as shown in the Figure below.

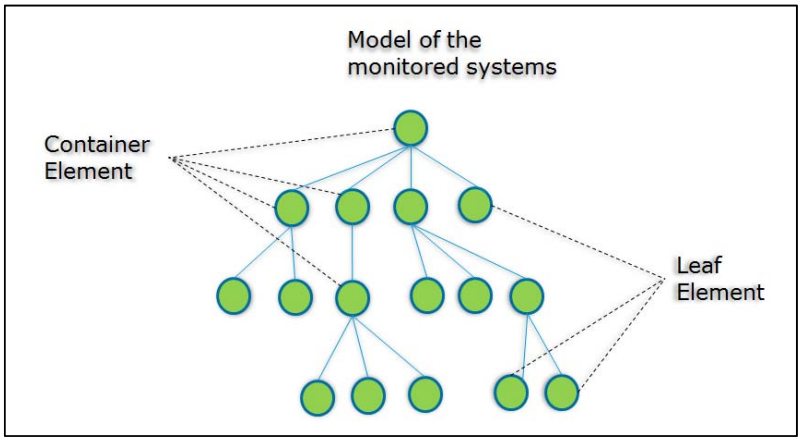


Figure 3. Element Types

Container elements are any elements which have children. Leaf elements are any elements that do not have any children (i.e these are the leaf elements of the Tree structure). Leaf elements usually base their value and state on incoming monitoring information (this typically includes values from sensors or information related to alarms) and represent elements of the system(s) being monitored. Container elements on the other hand aim to summarize the state of their contained elements. Depending on the implementation of the system, the *state* of an element may include additional information but in principle, it should describe if the specific element is in a non-nominal situation and if it can be reliably monitored.

Containers may naturally contain other containers and thus a common representation of all elements (Containers and Leaf elements) in the model is desirable, in order to have clear rules for summarizing the state of a group of elements to a container. Thus containers should have the same properties as leaf elements.

In such a model, there are two basic approaches in summarizing the state of a group of elements:

- Follow a most critical approach (i.e. alarm > warning > …) where the container has the most critical state of its contained elements.

- Allow elements to carry multiple (i.e a Set) of properties. So if a container contains 200 elements and 3 of them are in state “alarm” 2 of them in state “warning” and 4 of them cannot be properly monitored (state “unknown”), then the container will have all these states [“alarm”, “warning”, “unknown”] as its state.

Both approaches have advantages and disadvantages and should be investigated during the detailed design of the project.

6.1.2 Values and states of elements

So far using this generic model we can have elements which have their properties associated to information being monitored and elements which have properties summarising the state of their contained elements. In this paragraph, some aspects of the values and states of elements are explored.

The Integrated Alarm System will collect information from various sources

- ALMA Control System
- Power Plant
- Weather Stations
- Alarm System of the Control System
- …

In principle, this information is either reflecting properties of various equipment (for example a temperature reading, power level or operating frequency) or reflecting the state of various equipment (for example, alarm information).

This input information, named the “*Monitoring Information*”, reflects our knowledge of the system(s) that are being monitored. This information is then used as input in order to specify the Properties (for example the value and alarm state) of the leaf elements of the model based on logic which is expressed in a formal way. An example is shown in the Figure below:

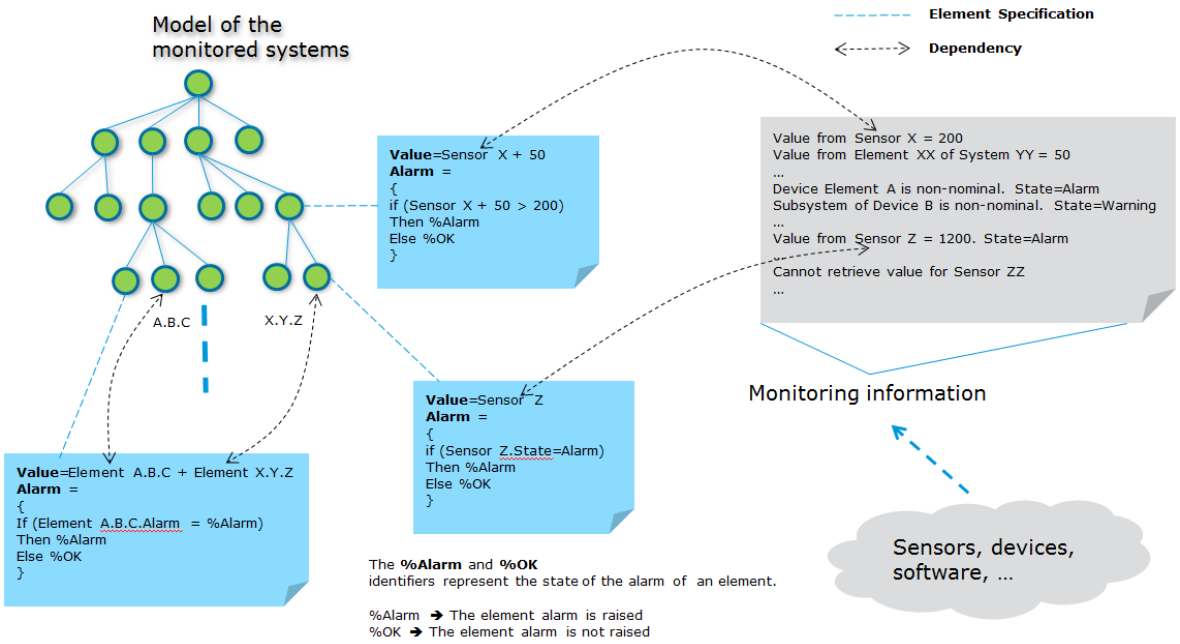


Figure 4. Model behaviour definition

While the "Model of the monitored systems" is structured using the hierarchical concepts explained previously, the "Monitoring information" which is in information obtained by sampling the environment may be structured differently. While its structure is not important, it is important that we can reference this monitoring information in elements of the "Model of the monitored systems". The leaf elements of the model typically use this Monitoring information in order to specify their behaviour.

For example the 2 elements on the right side of the tree in the figure above use values and alarm information retrieved from the "Monitoring information" to determine their value and alarm state (this information is *Sensor X* and *Sensor Z* which represent monitored values and *Sensor Z.State* which represents the alarm state of the monitored sensor). The logic of the value and alarm of each element is expressed in pseudo-code.

There might be cases where we want to define an element without a value and with only an alarm, for example if we just want monitor an alarm triggered from an external system. In such cases where we would not like to show a value of the associated element to the operator, we could use a default or no value at all.

Moreover, elements of the model can refer to other elements of the model thus giving the possibility to aggregate information with custom elements (these are usually also referred to as synthetic or virtual parameters). Such an example is the bottom left element in the figure above, where it specifies its behaviour (its Value and its Alarm specification) based on properties of 2 other elements of the model (it references the elements *A.B.C* and *X.Y.Z* – the naming of the elements is chosen arbitrary just to illustrate the functionality). In this case, *A.B.C.Alarm* refers to the alarm state of element *A.B.C* and uses intentionally a

different notation (*.Alarm*) than the previous example where we used "*Sensor Z.State",* in order to indicate that in this example we refer to one of the properties of an element of the model itself, while in the previous example "*Sensor Z.State"* references monitored information from the environment which might be structured and accessed differently.

This enables having behaviour which depends on the overall state of the monitored system(s) and gives the full flexibility of defining alarm conditions which reflect more accurately the operating needs. For example, an antenna might be missing a receiver, which at the antenna subsystem level is considered an alarm. However under some operating conditions this sensor is not needed and thus the alarm should not be raised at system level. If part of the "Monitoring Information" is the current operating mode and the alarm state of the relevant antenna subsystem then we can define an alarm condition, associated with the reflective element of the model that only raises an alarm under the correct conditions.

It is often not possible to judge at a subsystem level if an alarm should be raised at the system level, as the information of the overall system is not visible to the subsystem itself. This model enables defining custom conditions based on the state of the entire system, taking into account all relevant information and thus will enable having more accurate conditions for alarm generation.

The monitoring model thus has dependencies on the monitoring information and various elements of the model have dependencies on other elements. Cyclic dependencies between elements are not allowed as they form a logical contradiction (i.e. if the value of Element A is based on the value of Element B and vice versa, this is a logical error).

6.1.3 Monitoring Availability and Logical Expressions

Monitoring availability is another aspect of each Element of the model (it can be considered a separate property). It reflects the reliability of the monitored information used to calculate the value or alarm of an Element. More accurately, it reflects the reliability of the monitoring information up on which the Element depends. For example, if we have an Element of the model which depends on the value of a sensor, but we cannot read the value of the sensor, or the sensor reports that the current value is not meaningful under the current operating context, then this needs to be reflected in the Element of the model. This property is often referred to as "Validity" of the element and is essentially a qualifier of the value of the Element.

The actual definition of an element validity (i.e. the values it may have and their semantics) will be defined at a later stage in the project according to the detailed needs, however it is important to note that this property of an Element needs to be taken into account in the logic expressed to define the behaviour of the elements.

For example, if the value of an Element is defined as "Value of Element A.B.C + 50" and the value of Element A.B.C is not valid (i.e. cannot be measured), then this needs to be reflected in the outcome of the expression "Element A.B.C + 50". Thus expressions are operations with 2-dimensional objects (with one dimension being the value and another

dimension being the validity). In principle, a validity of the expression must be calculated form the validities of the underlying terms that form the expression using rules that will be defined.

This raises the issue that also some alarms might not have a valid validity (i.e. cannot be calculated), which is a direct consequence of alarms basing their behaviour on properties which themselves may not be calculated.

For example if we have a parameter *Temperature*, which reflects the value of a temperature sensor and another parameter *WeatherStationA* which will show an alarm if the value of the *Temperature* parameter is above 25 C, then what should be the alarm of the *WeatherStationA* parameter if we cannot measure the temperature (i.e. the *Temperature* parameter is not Valid) ? In principle the alarm of the *WeatherStationA* parameter is also invalid, as we cannot calculate it.

Thus, elements of the model (both containers and leaf elements) must include in their basic properties, which is the value and the alarm, information related to their validity:

- Value
    - Value Validity
- Alarm
    - Alarm Validity

The actual definition of the elements may vary, this chapter serves only as a guideline outlining the various complexities that need to be taken into account, in abstract terms.

6.1.4 Container Properties

By default containers have the role of summarizing the states (alarms, monitoring availability) of their contained elements, thus providing an overview of the entire tree under them. This is a powerful abstraction as a display may show an overview of the entire subsystem by only showing the state of a single container element. The way in which Containers summarize the properties of their contained elements is to be decided (as specified in section 6.1.1 Monitoring Model) but it should reflect the summary of all the properties of their contained elements.

6.1.5 Alarm Acknowledgement and Maintenance Mode

As specified in previous sections, from the incoming monitoring information it is possible to formally define custom conditions under which alarms are raised. Alarms are linked to elements of the model and are transient in nature as they depend on the current state of the system. An alarm might be triggered because a monitored value exceeded a limit and then disappear as the value goes back in limit. Moreover an alarm may be triggered by monitoring alarms delivered from the monitored systems and then may be cleared as the monitored systems stopped reporting the alarm.

For an operator it is important to distinguish the following alarm cases:

- New Alarm → a new alarm is raised in the system
- Acknowledged alarm → an alarm has been acknowledged
- Nominal → no alarm condition

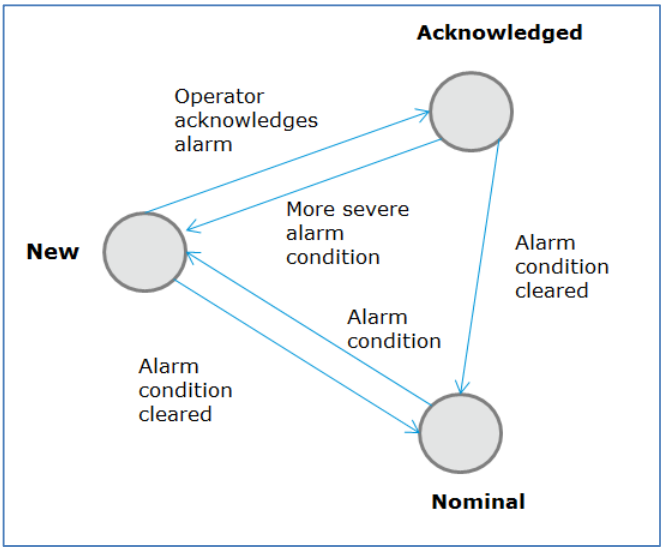


Figure 5. Alarm Acknowledgement State

This property, the alarm acknowledgement state, needs also to be presented to the operator. For example a new alarm might be blinking and be accompanied with a beeping sound until it is acknowledged. An acknowledge of an alarm on a container should also acknowledge all un-acknowledged alarms of all contained elements, thus an operator may quickly acknowledge multiple alarms in parts of the system.

Sometimes it might be desirable to shelve or switch-off some alarms for a predefined period. This can be achieved by setting part of the model in “maintenance mode”. If a Container is set to be in maintenance mode, then all of its contained elements should also automatically be set into maintenance mode. When an element is in this mode, it will not report alarms. This property of elements (if they are in maintenance mode) should also be presented to the operator.

As a conclusion of this chapter, the required information that needs to be associated with elements of the model in order to include all the discussed features is presented:

Element

- Value
  - Value Validity
- Alarm
  - Alarm Validity
  - Alarm acknowledgement state
- Maintenance mode

These properties rely on the model and not on the user interface, so if for example a user acknowledges an alarm, then the alarm is acknowledged in all displays for all users.

Depending on the element configuration some properties might be optional (for example a parameters that is used only for monitoring purposes and does not raise an alarm should not have the Alarm and Maintenance mode properties).

6.1.6 Monitoring Displays

The monitoring displays visualize elements of the model without further logic. This is illustrated in Figure 2, where displays simply show selected elements. The colour coding for visualizing all properties of a specific element will need to be defined.

As an example, in the current ground station monitoring and control system at ESOC [RD-3] the colour coding (element background) is as follows:

- Alarm (Red for severe, Yellow for warning)
- Value not valid (Light Blue, Dark Blue depending on the type of invalidity)
- Alarm not valid (Plum)
- Element in Maintenance mode (white)
- Alarm Ack State (Element Blinking & beeping sound on unacknowledged alarm)

In the Mission Control System domain, the default colour coding for monitoring displays is similar:

- Alarm (Red for severe, Yellow for warning)
- Value not expected (Orange) [This is a special kind of alarm and is called “status consistency check” in the domain terminology].
- Value not valid (Grey)
- Alarm Ack State (Element Blinking & beeping sound on unacknowledged alarm)

As a general remark, the number of different colours should be kept reasonably small, maintaining a balance between the different states the operator needs to visually distinguish and the need to have a visually intuitive interface.

With displays being capable of visualizing elements of the model and the ability to navigate from an element to a new display the core functionality of the Integrated Monitoring System is covered.

For example, the top level elements of the model represent the major systems being monitored and since the model aggregates information hierarchically these elements represent the entire status of each system. For each of these elements a new display will be configured and linked which will show one level of detail more and the process will be repeated until all the information is arranged in monitoring displays.

This is a very flexible way of showing the combination of alarm and monitoring information as we can define a display associated with an element (i.e. when drilling down) which also shows relevant information from neighbouring subsystems which will help the operator determine the root cause of the fault.

6.2 Configuration System

The configuration system will be responsible of

- Organizing all the input monitoring information it will receive
- Enabling the definition of the monitored system based on a hierarchical model based on the logical or physical representation of the monitored systems
- Define the behaviour of each element of the model based in the input monitoring information
- Define a number of displays
- Define navigation between elements of the displays and other displays

In order to enable the ease of configuration, it is desirable to utilize import formats (either custom or using industry standards) which describe the monitoring information from each monitored system. The formal definition of the available monitoring information in standard formats, which will be imported by the configuration tool, is considered beneficial as it also allows better configuration management and versioning of the available input information. This monitoring information definition (i.e. similar to the SNMP MIB file) acts also as a formal interface between the monitored systems and ensures consistency and configuration responsibilities across systems.

The output of the configuration system will be the configuration that will be used at runtime by the online system in order perform its function.

As stated in section 5.1, the need and complexity of the configuration system shall be evaluated based on the expected need for configurability of the displays and the behaviour of the displayed elements.

Depending on the operational concept, it might be desirable to give the ability to the operator to perform some of the configuration actions “online”, for example to provide the ability to the operator to define and show a display of selected elements in the online system, without the need to have the display definition configured offline. At ESOC, for example, for ground stations monitoring the current operational concept is to define the available displays of the system offline and not be able to change them online or to create new ones online. However, this heavily depends on the structure and organisation of the operations team and should not necessarily be taken as a reference.

6.3 External Interfaces

The system will need to monitor several non-standard systems such as

- Weather stations
- Building Management Systems
- Power Plant
- ALMA Antenna Array
- …

For each system an appropriate interface will need to be developed in order to retrieve the required monitoring information. Typically the external interfaces have an impact to the configuration system, as it will need to support potentially different types of systems and will need to provide information to the online system about the specific interfaces of each monitored system.

Regardless of the specific formats and interfaces of the monitored systems the input information can be abstracted to 2 fundamental types of information:

- Sensor information (i.e. a Parameter Value, such as 100 Celsius, or 70 Ghz)
- State information (i.e. Alarm / non-nominal information)

Thus, regardless of the specific interfaces, input information can be abstracted to structured information of these 2 types, which enables the configuration system to define the behaviour of the online system using this “normalized” information in a more abstract way, avoiding specific behaviour and conditions for specific interfaces. This implies that all input information will need to be translated to this common internal abstract format for further processing.

A. WORKSHOP DISCUSSION

In order to derive user requirements and outline a potential technical solution, a workshop took place where several ideas where discussed. The following sections outline the points that were discussed and their conclusions.

Identification of displays / monitored elements

The first step is to identify via a top – down approach the required information that the displays shall present. All the top level systems and all the layers of their sub elements will need to be identified.

Decision Point: Will the displays be configurable via a configuration system or "hard-coded" and changeable via a new software release? This point is very important for the design of the system. If the structure of the monitored elements and subsequent displays is expected to be stable then a hard-coded solution may be considered.

Conclusions:

- ⇨ Create the structure up to the desired level.
- ⇨ Structure will be configurable. Displays will be configurable.
- ⇨ There should be templates for the configuration.

Identification of alarms

What information is needed in order to judge if we have an alarm ?

For each of the "**leaf**" elements of the display Tree, we need to identify **all** potential sources that may raise an alarm.

Confirmation: This will include existing alarms available from the ALMA alarm system, linked to the monitored elements, also monitoring information from the ALMA Array Control System (i.e. key parameters from selected elements) and monitored and alarm information from all other monitored systems.

- ⇨ Some of the alarms have already information about the root cause.
- ⇨ Information from other sensors is desirable

Discussion: The incoming alarm information will be evaluated (i.e. not by default an alarm to be raised on the element). Alarms on a leaf element will be raised via specific rules that are linked to the element (i.e. if I have an active alarm X and value Y = "ZZZ") . In simple cases where no further logic is needed, the incoming alarms will be directly linked to a Leaf element.

- ⇨ The alarm conditions would need to be configurable. From the ALMA software this will likely be simple because the alarms are already trusted and provided but in the general the condition under which an element would go into alarm, should be configurable. The actual configuration method (limits, or how to choose the conditions) would be decided.

The leaf elements alarm status will be propagated all the way to their container elements.

Additional Alarm Display

Discussion: Is there a need for a tabular view (like the current system) of all active alarms ? In my view this is useful as well because one can have a high level overall view and at the same time all the individual active alarms on a side display.

- ⇨ The list of the active alarms is not desirable. But the list of conditions that raised an alarm is desirable. So form an alarm you will be able to see the conditions that triggered the alarm.

Display Monitoring Information

Discussion: Will the displays also display monitoring information? By monitoring information, I mean information that is useful in order to give an indication of the problem (i.e. include also some temperatures on the Cryogenics display, etc). Note that we will need potentially to monitor some information if we want to have rules for the alarms based on this information.

- ⇨ Show all parameters that are related in the calculation of the alarm.
- ⇨ For each alarm there will also be a link to web browser to indicate the action for the operator.

Alarm handling

The alarm handling should be discussed. In particular the following:

- What will be the states for an alarm (new, acknowledged, shelved, …)
- ⇨ Alarms that go back to nominal should be logged. The log will be an operator log. Might be integrated with another tool (the shiftlog)
- ⇨ Some alarm conditions are complex. For example if there is high wind for more 12 seconds, then the antenna should be stopped. This type of alarms should also be handled. In this case the alarm condition would not be only related to the wind speed, but to other parameters that will be triggered.
- ⇨ There are already existing requirements for the alarm handling.
- ⇨ Alarms should be context sensitive (i.e. be able to define the alarm conditions based on the current state of the system. For example if a subsystem is in a specific configuration an alarm should not be raised).
- ⇨ The information from the configuration tool should be accessible.

Maintenance mode

Will it be possible to set a subsystem (and all of its contained elements) into maintenance mode ? If yes, the relevant elements will be colour coded appropriately.

- ⇨ The maintenance will be read form the configuration tool. If something is in maintenance it will be color coded.
- ⇨ Alarm shelfing will cover alarms that we are not interested in. Shelved Alarms should be colour coded as well.
- ⇨ In maintenance needs some thinking. Because it might be tjat some other users need to have a different view sso it might beeded to be seen differently on each client.

Indication of monitoring

We shall also have an indication if the monitored elements are correctly monitored (i.e. grey out if we cannot monitor them).

- ⇨ Agreed.

Alarm and colour coding propagation rules

The Colour coding of each element shall distinguish different alarm states and the indication of monitoring and if a system is in maintenance mode. Propagation of alarms shall be done following a most critical approach (new > acknowledged > shelved). The combination of the information (For example, if an element contains 1 element it cannot monitor, 1 element that is in maintenance mode and 1 acknowledged alarm, how it shall be displayed ?)

- ⇨ Either configurable, or via standard rules, or to be able to show all information.

Configurability of Alarm rules definition

Will the rules for the alarm conditions for each leaf element be customizable ?

- ⇨ Yes

Custom Configuration Parameters

Will the system have the ability to have configuration parameters that influence the alarm rules ? (For example, to have a configurable mode of observation for the antennas, that will influence if an alarm is raised under conditions or not)

- ⇨ The primary configuration information will be accessible from the dashboard or a similar system.

Other functionality

- Archiving of alarm information ? ➔ the alarms should be archived. The target system would be decided.
- Multiple clients ? ➔ YES.
- Control privileges for each client ? ➔ There will be 2 classes of clients. 1 that has full control. And another only for monitoring which does not have any control.

- Different display definitions ? ➔ YES. We will be able to define custom displays on each client.

B. POTENTIAL TECHNOLOGY RE-USE

In this appendix, some ESA and non-ESA software is presented for potential evaluation and re-use. The availability of the software form ESA to ESO is a subject for further discussion and agreement between the two Agencies.

ESA Software

EGOS User Desktop (EUD)

EUD [RD-6] is an Eclipse-based application which is used as the standard user interface at ESOC in the domains of Mission Control Systems and Simulators and will be used in the next generation Ground Station Monitoring and Control Systems. The EUD is a generic user interface which can be adapted to communicate with different systems (called backend systems).

The EUD supports several displays/functionalities, which include:

- Message display: for visualizing log messages.
- User login: to handle session management.
- System control: to manage tasks within the backend system
- Parameter displays: to monitor parameters in the backend system.
- Action execution display: to run scripts targeting the backend system.

The EUD software release includes, apart from the EUD framework itself, the following products:

- The **EUD Test Product**, a tailoring of the EUD framework used for testing and validation

- The **EUD Backend Simulator Product**, an application that simulates a backend for the EUD, to which the EUD Test Product connects to.

- The **EUD MIMIC Designer** application, a stand-alone product for the creation and test of MIMIC Displays

Besides the displays that are provided with the EUD product, it is possible to extend the software by creating custom specialized displays.

Below some screenshots of the EUD are presented. This section is not intended to be a full presentation of the EUD product, it only targets to demonstrate its look and feel. It should be noted that the colours in the monitoring displays are customizable and the next Figures do not represent a standard colour coding, they are used to demonstrate the features of the software.

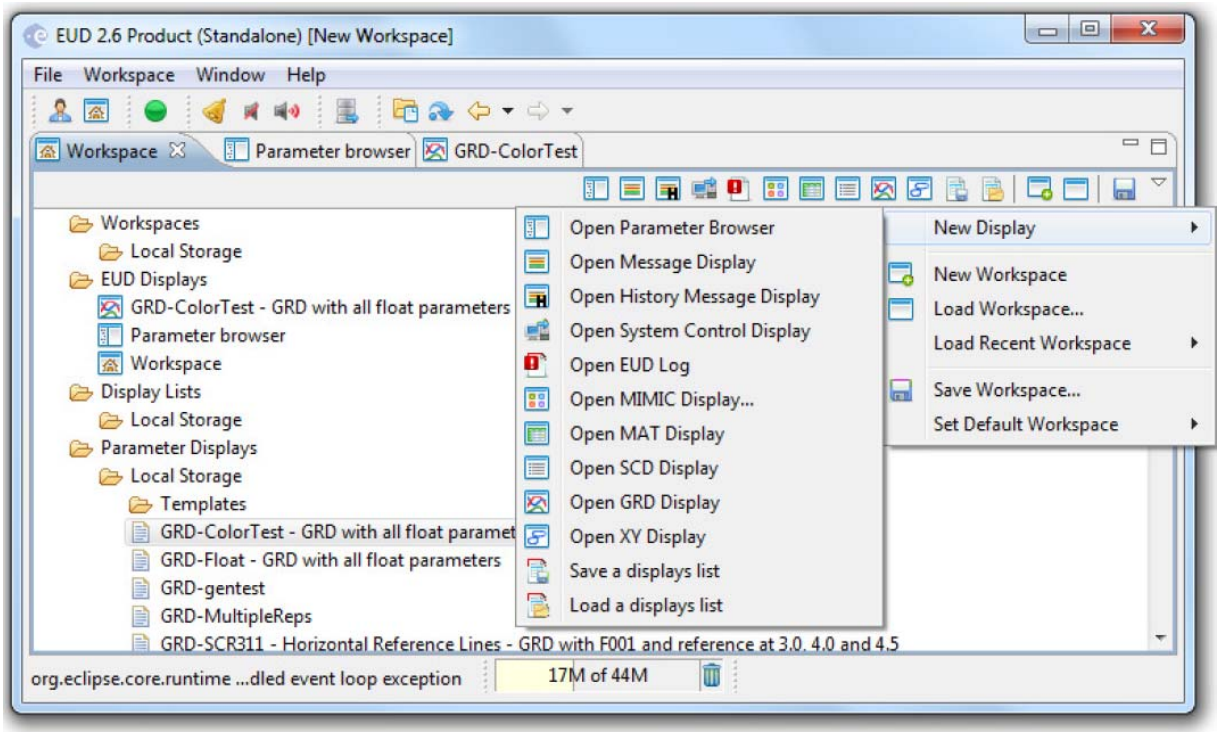


Figure 6. EUD Workspace View

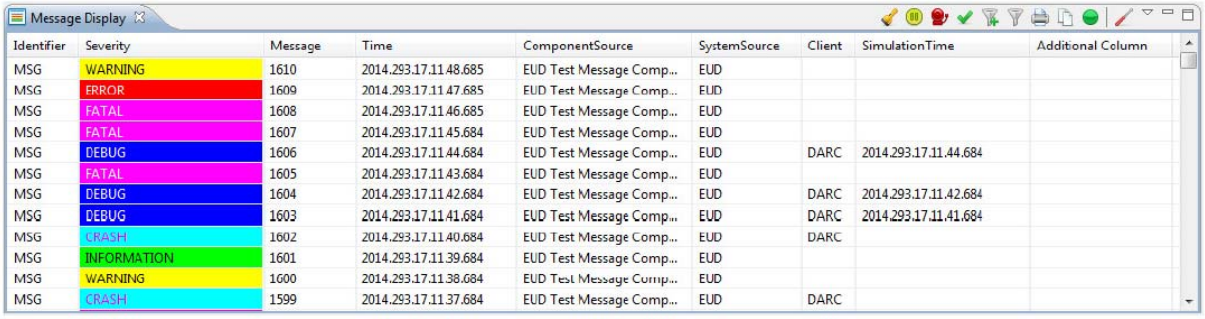


Figure 7. EUD Message Display

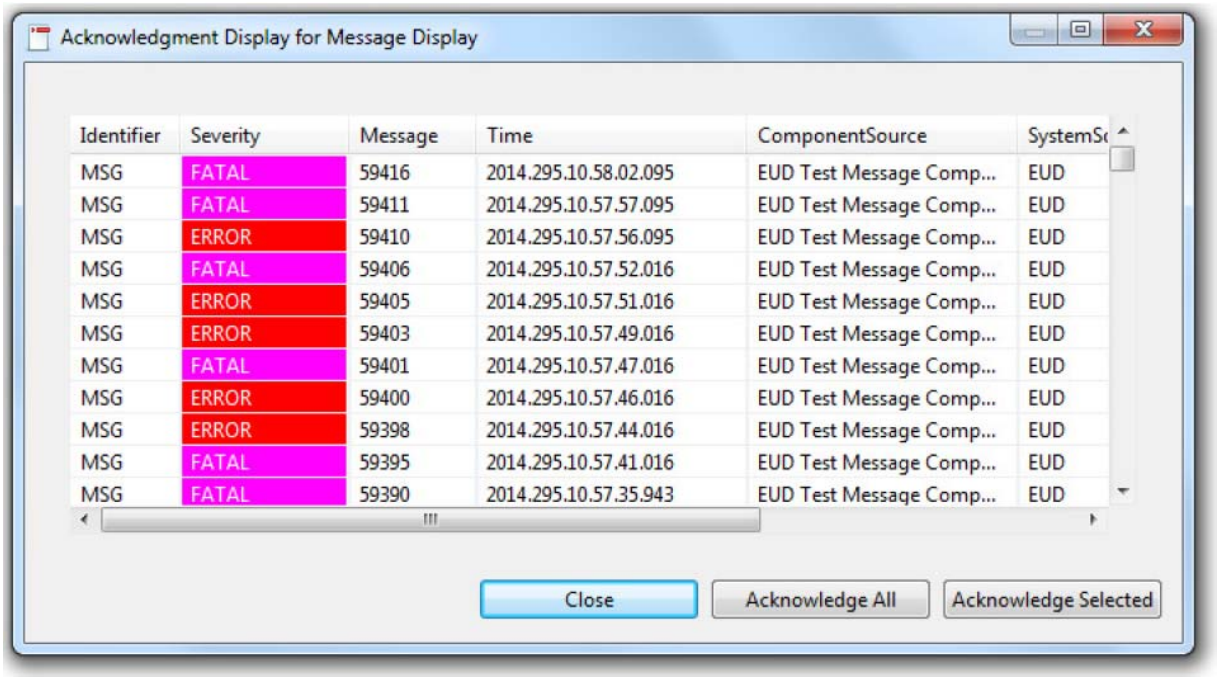


Figure 8. Separate Alarm Acknowledgement Display

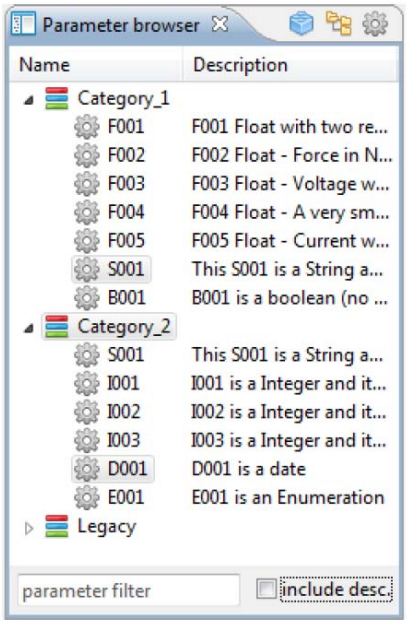


Figure 9. Parameter Browser Display

Figure 10. Parameter Matrix/AND Display

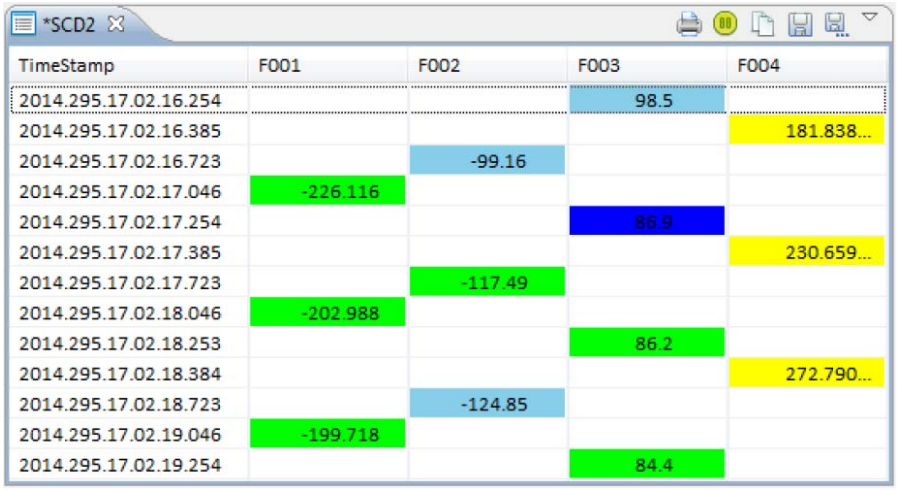


Figure 11. Parameter Scrolling Display

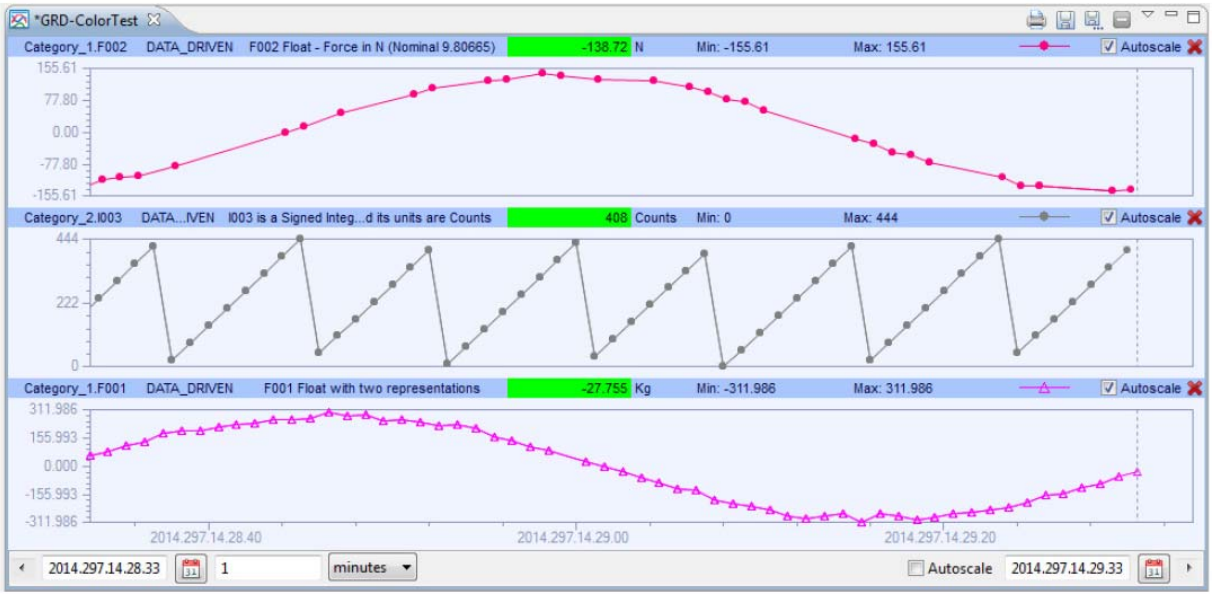


Figure 12. Parameter Graph Display

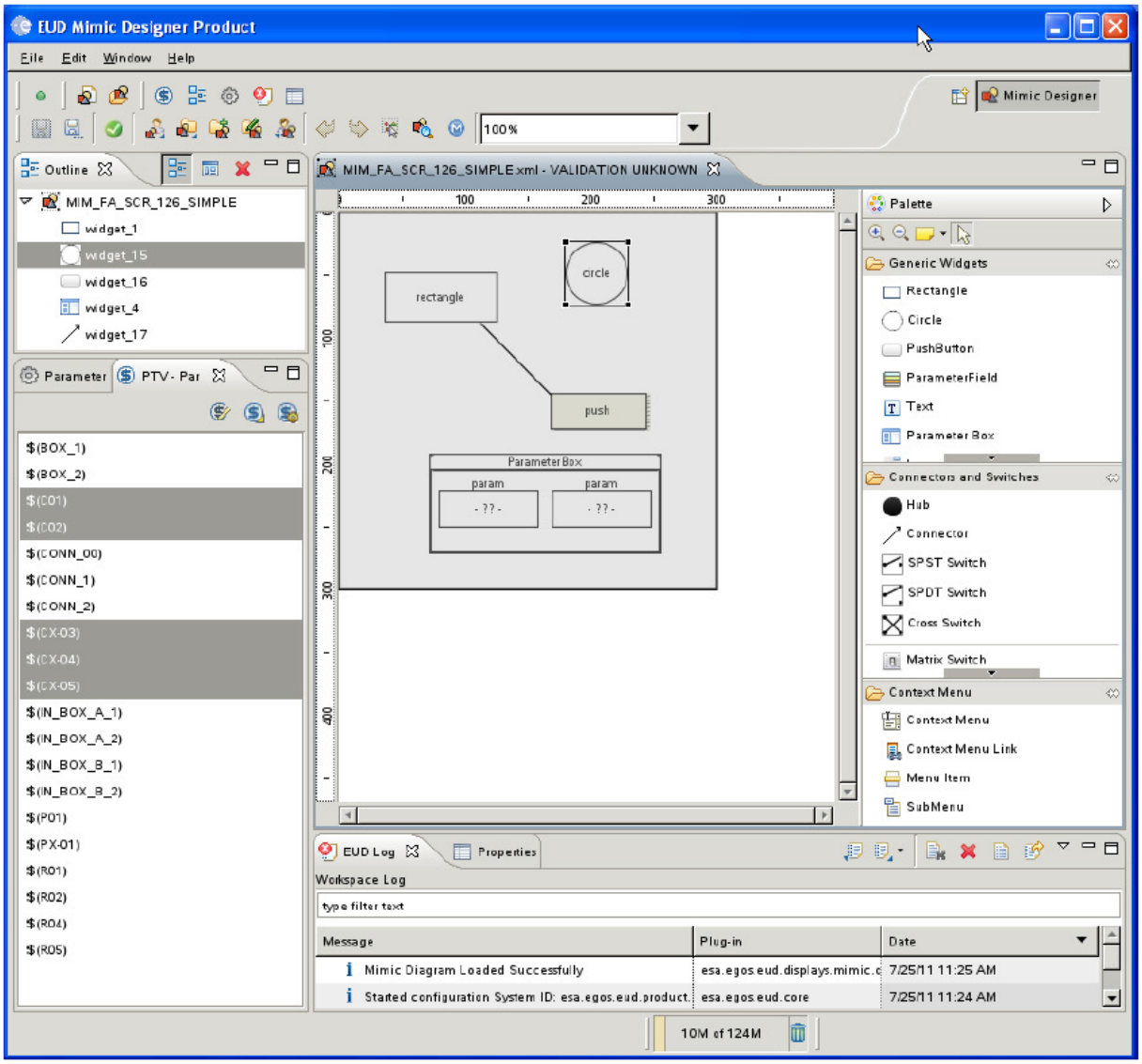


Figure 13. MIMIC Designer Display

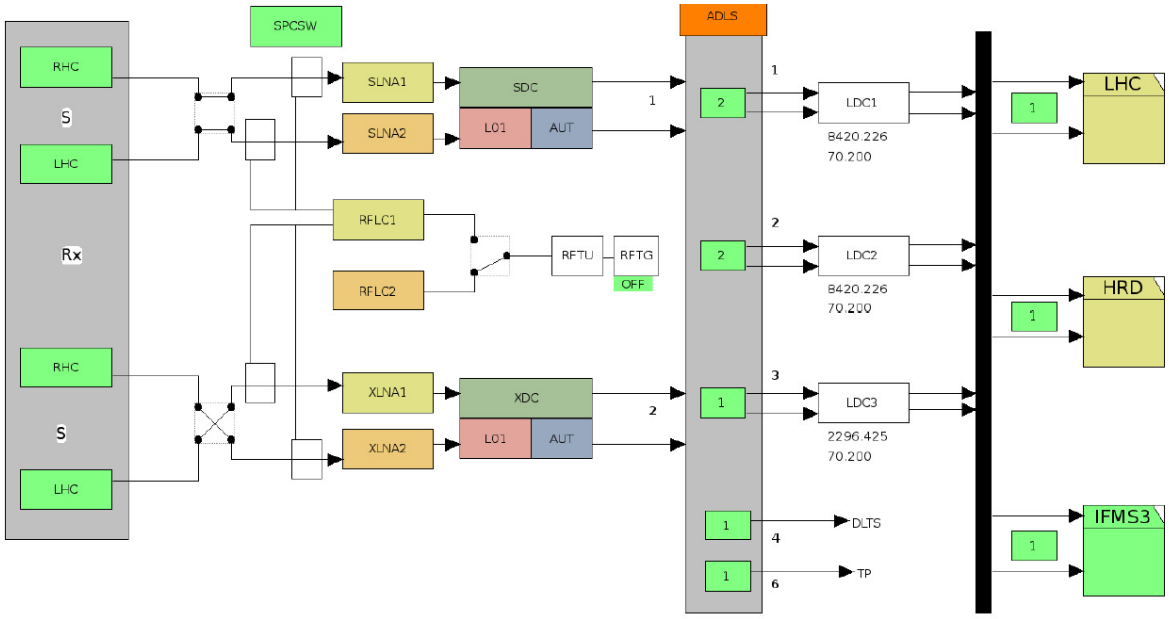


Figure 14. Sample MIMIC Display

European Software

EGS-CC

The European Ground Systems – Common Core (EGS-CC) [RD-7] is a European initiative to develop a common infrastructure to support space systems monitoring and control in pre- and post-launch phases for all mission types.

ESOC is planning to use the EGS-CC for its future ground systems, including its next generation ground station monitoring and control system. The system is currently under development and is provided here only as a reference for future evaluation.

COTS

These COTS are not presented as a recommendation for the implementation, but are noteworthy systems that may be investigated. They are not the outcome of a detailed market analysis, instead they are systems selected by the author of the report.

DataMiner

DataMiner (http://www.dataminer.co/) is currently being evaluated as part of a study at ESOC in order to be used as a system for providing an end-to-end overview for the ground elements that spacecraft missions use.

Zabbix

Zabbix (http://www.zabbix.com/) was evaluated in the context of a study at ESOC. Even though it was not selected for the study, it is noteworthy.

Technical Report
Integrated Alarm System UI Front-End Workshop

Written by	Organization Role	Date and Signature
Emmanuel Pietriga	Head of team ILDA (INRIA & INRIA Chile)	
Maria Grazia Prato	User Experience designer (INRIA Chile)	

Contents

1 Introduction

This work is situated in the context of the joint ALMA-INRIA effort to improve the Human-Computer Interaction (HCI) aspects of ALMA. This work started in 2009 and is summarized in [RD01,RD02].

Given the experience of INRIA on the design and development of user interfaces and the collaboration that has been carried with ALMA under the signed MoU (ALMA-INRIA 2012) as well as the deep knowledge of INRIA about ALMA operations, monitoring and control (OMC) plugins and software structure, ALMA has requested INRIA to provide its expertise to help design novel user interface front-ends for observatory-wide alarm management as part of the Integrated Alarm System effort [RD03].

This report summarizes the findings from the workshop held at the OSF on March 15-16, 2016 and describes UI front-end proposals using mockups.

Reference Documents

Ref.	Document Title	Doc. Number
[RD01]	E. Pietriga, P. Cubaud, J. Schwarz, R. Primet, M. Schilling, D. Barkats, E. Barrios, B. Vila Vilaro, Interaction Design Challenges and Solutions for ALMA Operations Monitoring and Control, invited paper, *Astronomical Telescopes and Instrumentation, SPIE*, pages 10:1-10:16, July 2012	http://dx.doi.org/10.1117/12.925180
[RD02]	E. Pietriga, G. Filippi, L. Veliz, F. del Campo, J. Ibsen, A Web-based Dashboard for the High-level Monitoring of ALMA, invited paper, *Astronomical Telescopes and Instrumentation, SPIE*, pages 1B:1-1B:12, June 2014	http://dx.doi.org/10.1117/12.2055235
[RD03]	Erich Schmid, Emilio Barrios, Bernhard, Lopez, Tzu-Chiang Shen, Alessandro Caproni, Integrated Alarm System for the ALMA Observatory	ESO-281186 v1.3
[RD05]	Petros Pissias, ESA, Monitoring, Control and Automation of the ESA Ground Stations	
[RD06]	Requirements for Array Infrastructure Operations Centre	ALMA-80.04.05.02-0001-A-SPE
[RD07]	Endsley M. R. and Jones D. G., editors. *Designing for Situation Awareness: an Approach to User-Centered Design*. CRC Press, Taylor & Francis, 2012.	ISBN 9781420063554
[RD08]	Green, T. R. G.; Petre, M. *Usability analysis of visual programming environments: A 'cognitive dimensions' framework.* Journal of Visual Languages and Computing 7: 131–174, 1996.	https://dx.doi.org/10.1006%2Fjvlc.1996.0009
[RD09]	Edward Tufte. *Beautiful Evidence*. Graphics Press, 2006.	ISBN 0-9613921-7-7

Acronyms

The acronyms and abbreviations used within this document are given below.

Acronym	Definition
ACS	ALMA Common Software
AOS	(ALMA) Array Operations Site
FEPS	Front-End Power Supply
HCI	Human Computer Interaction
HVAC	Heating, Ventilation, and Air Conditioning
IAS	(ALMA) Integrated Alarm System
INRIA	Institut national de recherche en informatique et en automatique
OSF	(ALMA) Operations Support Facility
PSA	Power Supply Analog
PSD	Power Supply Digital
PPS	Permanent Power System
PSU	Power Supply Unit
SB	Scheduling Block
SCO	(ALMA) Santiago Central Office
UI	User Interface
UPS	Uninterruptable Power Supply

2 Participants

- Emilio Barrios (ALMA, Array Operator Manager)
- Fernando del Campo (INRIA Chile, Software Engineer)
- Alessandro Caproni (ESO, Common Infrastructure ICT Lead)
- Arturo Hoffstadt (Joint ALMA Observatory, Software Engineer)
- Jorge Ibsen (Joint ALMA Observatory, Head of ALMA Department of Computing)
- Bernhard Lopez (Joint ALMA Observatory, Engineering Services Manager)
- Norikazu Mizuno (Joint ALMA Observatory, Array Maintenance Group Manager)
- Rolando Olivos (Joint ALMA Observatory, Infrastructure Maintenance Group)
- Emmanuel Pietriga (INRIA / INRIA Chile, Head of research team ILDA)
- Tzu-Chiang Shen (Joint ALMA Observatory, Software Group Manager)
- Luis Veliz (INRIA Chile, Software Engineer)

3 Methodology

The workshop was held at the OSF and involved the people listed in the previous section. We tried to get representatives of the various departments that are concerned with operations and have to handle the different types of alarms that will be managed through the Integrated Alarm System [RD03]. Brainstorming and discussion sessions with those end-users, as well as engineers in charge of the IAS' development, occurred on March 15th (morning) and March 16th (morning).

The output from these two workshop sessions (audio recordings and whiteboard snapshots) was then used by INRIA (Emmanuel Pietriga & Maria Grazia Prato) to inform the design of the UI front-end mockups delivered with this report.

4 Context and Scope

The goal of human-computer interaction (HCI) is to make computers easier to use, while augmenting users' capabilities; to enable them to deal with more complex problems and larger datasets, as efficiently as possible, in single-user or cooperative work contexts. More formally, HCI is about designing systems that lower the barrier between users' cognitive model of what they want to accomplish, and computers' understanding of this model. HCI is about the design, implementation and evaluation of computing systems that humans interact with. It is a highly multidisciplinary field, with experts from computer science, cognitive psychology, design, engineering, ethnography, human factors and sociology. In this broad context, INRIA's collaboration with ALMA has focused so far on the control room's user interfaces for operations monitoring and control [RD01], and the design and implementation of the ALMA Dashboard [RD02]. The purpose of the control room interfaces is to help users, in this case operators and astronomers on duty, better comprehend the status of the observatory and take informed decisions, using appropriate interaction and visualization paradigms.

From an HCI point of view, ALMA's control room is a mission-critical system. Central to such systems is the notion of situation awareness, i.e., how workers perceive and understand elements of the environment with respect to time and space, such as maps and data feeds from the field, and how they form mental models that help them predict future states of those elements [RD07]. One of the main challenges is how to best assist subject-matter experts in constructing correct mental models and making informed decisions. The alarm system is an essential source of information of the observatory, in the control room and beyond. The purpose of this work is to investigate how to improve upon the existing user interfaces that display alarms (ACS Alarm System, etc.), by reconsidering from the ground up how alarms should be conveyed to different audiences. The following sections report the findings from the workshop and contain mockup proposals for different user interface front-ends designed for the display of different types of alarms, and targeting different audiences.

One important element to clarify is that this workshop was specifically about the design of UI panels (front-ends from the perspective of the end-users). It takes into consideration facts related to the heterogeneity of alarms and alarm sources, and existing software architectures. But those essentially-technical elements were not the focus of attention during the workshop. Discussions were concentrated on the end-users' needs rather than on the current status of the hardware and software systems, their features (e.g. reduction rules, configuration through the TMCDB) and limitations. Indeed, the purpose of this workshop is to inform the overall design of the Integrated Alarm System (IAS). The workshop thus addressed mostly what is termed *Presentation & Handling subsystem* in the functional requirements listed in [RD03], and the resulting UI panel proposals take into account the user-centered requirements from Sections 3.2 and 3.4 found in [RD03]. Brainstorming discussions assumed for the most part that we are in

an ideal world, where all relevant alarms, data and sensors required to trigger those alarms exist, regardless of their actual availability.

5 General Approach

The general problem addressed during the workshop is that alarms come from many different sources, making it difficult to get an overview of all alarms and to form a clear mental model of what is happening. Too much time is spent navigating between different tools and correlating alarms and associated data to understand what is happening and take informed decisions. End-users would like to have a unified gateway to all alarms, with more visual, easy-to-comprehend depiction of the system's status. Having a unified gateway should be understood from the perspective of the end-user. This does not mean that the IAS should provide a unified way of managing alarms at the hardware/software back-end level. It rather means that the user interface front-end to alarms should provide end-users with a unified, single gateway to those alarms, no matter their actual source. Multiple independent alarm sources will continue to co-exist, but those sources can broadcast their alarms, the UI front-end listening to them and displaying them, organizing them in thematic panels, as described below.

Alarms managed through ACS are currently displayed through a single UI panel (Figure 1). Those alarms only represent a subset of all alarms that will eventually be managed through the Integrated Alarm System (IAS), but they are already quite varied, encompassing sources such as power supply units in antennas, water vapor radiometer, telescope-calibration-related alarms, the central local oscillator. All these alarms are presented in one unique, single-level list, forcing users to apply filters or search for specific entities to isolate specific items.

Having such a centralized, temporally-ordered list of all alarms can be useful in some situations, but fails to provide users with a contextualized view of alarms which, given the high level of heterogeneity in the types of alarms managed by this component, adds significant burden on users in terms of cognitive load. An OMC plug-in synchronization mechanism was designed and developed as part of the ALMA-INRIA HCI effort [RD01], that enables automatic filtering of the alarm panel based on selections made in other OMC UI panels, but this mechanism is not sufficient to address the overall problem.

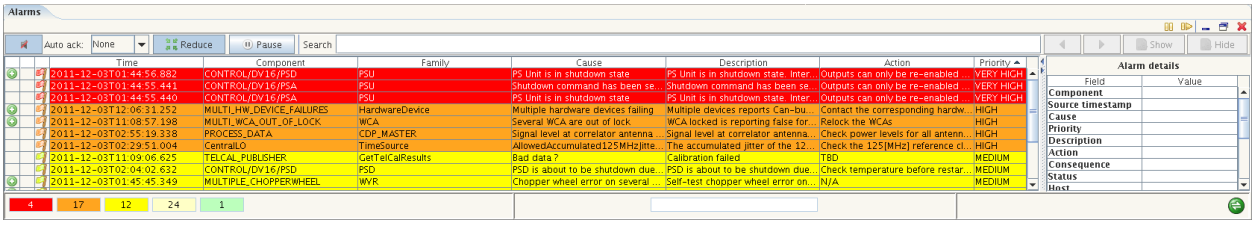


Figure 1: Alarm Panel (as an OMC plug-in)

Workshop participants quickly reached consensus that an alternative approach should be explored, as the above does not scale. Instead of presenting all alarms in a unique UI panel made of a uni-dimensional table fed with all alarms and letting users filter/sort/search that list manually, we considered the opposite strategy: design multiple thematic panels, that group alarms into coherent subsets. The rationale for this choice is based on the following elements:

- Only having to deal with subsets of alarms reduces the level of heterogeneity in any given panel, which thus reduces complexity.
- Designing panels for coherent subsets of alarms increases *closeness of mapping* [RD08], thus providing more opportunities to create visual representations of alarms and associated systems/components. Such visual representations are expected to better relate to the users' mental model of the system, and help them build that model in the first place. Thanks to such visual representations, alarms can be presented *in context*, helping users relate them to their source.
- Grouping alarms into panels reduces the need for filtering/sorting/searching the entire list.

It should be noted that this approach has the drawback that alarms are no longer all accessible from a single panel, but the above elements largely compensate for this, knowing that the number of different panels is currently limited to six, with multiple target audiences. Furthermore, users in need of a single generic entry-point to all alarms can still access them using the existing alarm panel illustrated in Figure 1.

One fundamental observation that informed the design of the UI panels described in the following sections is that there are two main types of alarms: **infrastructure-related alarms**, that correspond to specific components of the observatory, and **process-related alarms**, that correspond to specific steps in workflows and procedures. The overall design strategy that guides our proposals is based on the idea that the two types of alarms are fundamentally different and call for specific views, detailed in Sections *7. Infrastructure-centric Views* and *8. Process-centric Views*. For instance, an alarm related to a specific piece of equipment should be displayed in the panel that summarizes this part of the observatory's infrastructure, while an alarm related to an ongoing observation performed with a given array should be displayed in the panel summarizing this observation.

The following general considerations were raised during the workshop:

- The color scheme used for visually representing alarms should be coherent across UI panels, and should be chosen considering the fact that some users are color-blind. See Appendix F.
- The capability for UI panels to replay past alarms was mentioned on several times during the workshop, as a way to facilitate post-mortem analysis. This feature was not discussed in detail, as it is essentially, at this point, a question of enabling access to logged alarms rather than a matter of UI design.

For each of the following panels, the mockups aim at fitting all relevant information on one single screen, so as to enable monitoring of all alarms without resorting to virtual navigation. We use FullHD (1920x1080) as our baseline (minimum requirements).

6 Observatory Overview

The first alarm panel discussed during the workshop is aimed at providing an overview of the observatory's main elements. It is a high-level view, aimed at a broad audience. Its purpose is to provide an observatory-wide summary of the main systems, that makes it possible to quickly make an assessment of the current situation without deep technical knowledge about those systems. A second purpose of this overview is, for each of the alarms it features, to make it easy to identify what ALMA department is responsible for the corresponding component, and who is in charge at this moment (the person from this department who is on duty).

This view is predominantly static: the display gets updated in real-time, but users do not interact with it to get more detail. It is an alarm-oriented display that fits on one single screen, indicating at a high level of abstraction that something is wrong with one of the observatory's primary systems. Users who identify a problem from this overview display and seek additional information about the problem are expected to move to a workstation and access the relevant alarm UI panels to obtain detailed information.

The following high-level alarms have been identified. Each one of them is a simple two-state variable: either an alarm has been triggered (indicating a problem with this subsystem), or not:

- Power
- Communications:
  - Phones / radio
  - Network
- Weather (*)
- Observing System
  - Correlator
  - Science Array (**)
  - CLO
  - Data Archiving

(*) Indicates whether the observatory can operate or not
(**) Indicates the availability of the antennas that are part of the science array configuration for the current observation cycle.

For this synoptic display, a schematic representation of the above-listed subsystems is proposed, partly inspired by the ALMA Signal Path Visualization found in [RD03] and a diagram that can be seen in, e.g., the Array Operators Tips & Tricks tables at:
`https://wikis.alma.cl/bin/view/DSO/AogAlmaNewTroubleshootingMap`
A mockup of this panel is given in Appendix A.

7 Infrastructure-centric Views

The following alarms, associated with mission-critical pieces of equipment or environmental variables were identified (listed in no particular order):

- Array elements (including front-ends, receivers, etc.)
- Cryo units
- UPS
- Power generation and distribution, from turbines to switch gears.
- HVAC
- Fire alarm system
- Computing
- Network connectivity
- Weather station alarms, weather alarms
- AOS conditions (access roads, radio communications)

Those were grouped in three thematic panels, as detailed on the following pages.

7.1 Array Elements Alarm Panel

This panel features a set of antenna-related alarms. Given that geolocation information is not considered as an important piece of information in this context, a tabular representation is chosen for this visualization, as it is compact and enables visualizing numerous alarms for all alarms on one single panel without resorting to virtual navigation. The table is organized into multiple sets of columns, and one antenna per row, grouped by type (CM, PM, DA, DV) as was done in the ALMA Dashboard's compact view (Figure 2).

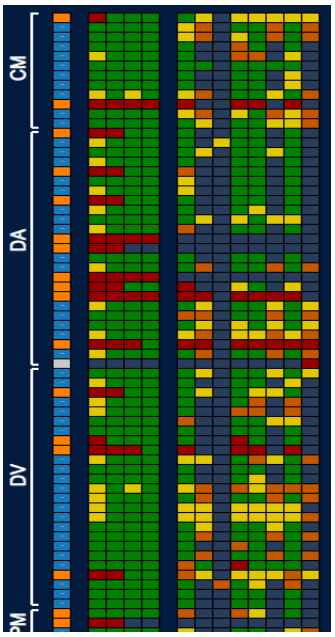


Figure 2: ALMA Dashboard Compact View

Columns are organized as follows:

- Cryo
  - Compressor
  - Pressure
  - Temperature (4K/15K/110K thresholds) – a conjunction of all 3 temperatures.
- HVAC
  - Generic alarm « something is wrong with the HVAC »
  - Complemented by cabin temperature alarm
- PSU (Power Supply Units)
  - PSA (Power supply Analog)
  - PSD (Power Supply Digital)
  - FEPS (Front-End Power Supply)
- UPS
  - AC Power
  - UPS Power
- Fire

Cells should be greyed out when a value cannot be read for a given amount of time, i.e., when the value has not been updated for a long period of time (duration to be determined).

A mockup of this panel is given in Appendix B.1. As the table can fit in approximately two thirds of the screen, the remaining screen real-estate can be used to show an optional map of the AOS that indicates the current location of the array element hovered by the mouse cursor in the table.

An augmented version of this table was discussed during the workshop, featuring sparklines [RD09] to indicate trends for numerical variables such as temperatures or pressure.

Appendix B.2 shows a variation on the above mockup, showing how such sparklines could be rendered.

7.2 Power Alarm Panel

This panel features alarms related to power generation and distribution, as well as related elements. It features two sections.

The first panel consists of a diagrammatic representation of the power generation & distribution network and displays alarms for the following components:

- Power Generation
  - Turbines (3)
    - On/off
    - Alarm
  - Fuel Tank Level
- Power Distribution
  - Hierarchy of switch gears. For each one :
    - On/off
    - Alarm
    - Associated UPS alarm
  - Flywheel (4)
  - Substations
    - AOS
    - OSF

Appendix C.1 shows a mockup of this alarm panel, featuring all above alarms, mainly using sunburst diagrams. The visualization emphasizes the hierarchical nature of the distribution network. On/off, Alarm and UPS are displayed in three juxtaposed sunburst diagrams, all showing the same hierarchy.

An alternative visualization was discussed based on a geovisualization of the AOS, possibly distorted so as to optimize screen real-estate use (see Figure 3), as is done in the OMC's Antenna Navigator [RD01] and Create Array X panels. This alternative has the advantage of showing the location of elements, but at the cost of legibility of the network, whose layout cannot be optimized beyond the spatial distortion applied to the entire area encompassing the array.

Figure 3: AOS Visualization without distortion (top) and with distortion (bottom). The one without distortion is more geographically accurate, while the one with distortion makes better use of the available screen real-estate, still preserving the main topological relationships between pads. The road network is represented only to provide users with additional orientation cues.

The second panel situates alarms related to the following pieces of equipment on basic floor plans of the corresponding buildings, to enable users to quickly identify the alarm source:

- Fire System
    - OSF technical building (only one alarm for all 150 sensors)
    - AOS technical building (only one alarm for all sensors)
- HVAC (related to fire alarm system)
    - Per technical building, per room (*)
        - On/off
        - Humidity level
        - Airflow
        - Temperature
    - Water tank level
- UPS
    - 3 @ AOS (technical building)
    - 1 @ AOS (electrical substation)
    - 4 @ OSF (technical building)
    - 1 @ PPS (permanent power system)

UPS alarms can be put on a separate panel or given the limited number of elements to display, on the same panel as the Fire and HVAC alarms.

(*) The following rooms were identified:

- AOS
    - ACA Corr,
    - BL Corr
    - CLO
    - Patch Panel
    - Computing
- OSF
    - Computing
    - Corr+CLO
    - Labs

Appendix C.2 shows a mockup of this alarm panel, featuring all above alarms (Fire + HVAC + UPS).

7.3 Weather Alarm Panel

This panel features alarms related to both weather conditions and weather stations. Because it displays alarms strongly related to the observatory's environment, a geovisualization is selected, albeit a very schematic one (as opposed to detailed representations such as, e.g., topographic maps or satellite imagery) only showing weather stations and their position relative to antenna pads and possibly roads, that can help users orient themselves. Pads are shown to help relate weather stations to the antennas in their vicinity. Here again, a distorted representation (Figure 3) can be considered to optimize screen real-estate use, as illustrated in the mockups.

The visualization features the following elements, for each of the 11 weather stations:

- Environmental alarms
    - Wind speed (>20m/s → shutdown, >30 m/s → VFR)
    - Temperature (< -20degC → shutdown)
    - Precipitation
- Hardware failures
    - Sensors (boolean)
    - Servers (boolean)
    - Power (boolean)
    - Network (boolean)

Individual items should be greyed out when a value cannot be read for a given amount of time, i.e., when the value has not been updated for a long period of time (duration to be determined).

Appendix D shows a mockup of this alarm panel.

8 Process-centric Views

Two process-centric views were considered: 1) the overall ALMA dataflow (starting with observation proposal submissions by PIs and ending with the archival of observation data); and 2) a subset of the dataflow, limited to the scheduling block (SB) execution lifecycle. The first one was quickly discarded as too broad with respect to the Integrated Alarm System. Discussions focused on the second as a good basis for the design of an alarm process-centric view.

8.1 SB Execution Alarm Panel

Alarms identified as relevant in the context of SB execution are of two types:

- alarms related to the execution of a specific scheduling block;
- alarms related to the supporting infrastructure.

Both types of alarms are mixed in a diagrammatic representation of the SB execution workflow. SBs are depicted as small glyphs (rectangles) that move from one step to the next in the workflow. Several SB glyphs can be at different positions in the diagrammatic representation of the workflow, symbolizing different observations currently being executed on different arrays. Each SB gets assigned a unique color in the visualization.

Alarms relating to the infrastructure are displayed on the corresponding device in the workflow. Alarms relating to the execution of a particular scheduling block are displayed close to the glyph symbolizing the SB in the workflow, using the same color.

This visualization not only shows alarms, but gives information about what the scheduler is currently doing (similar to some of the information displayed by the ArrayStatusGUI). This visualization should scale well, given that there should be 6 arrays maximum at any given time.

The diagrammatic representation of the workflow is composed of the following elements:

- Queue of candidate SBs
- Start of SB execution
    - Set direction of the array element → on source
    - Set frequency FEND → locking
    - Set corr sub array
    - Get UID
- Start scan (loop)
    - Subscan sequence
- End scan
- In parallel : Data Capture → Archive (wait for data capture flag) // NGAMS-client → NGAMS

The following alarms can be displayed:

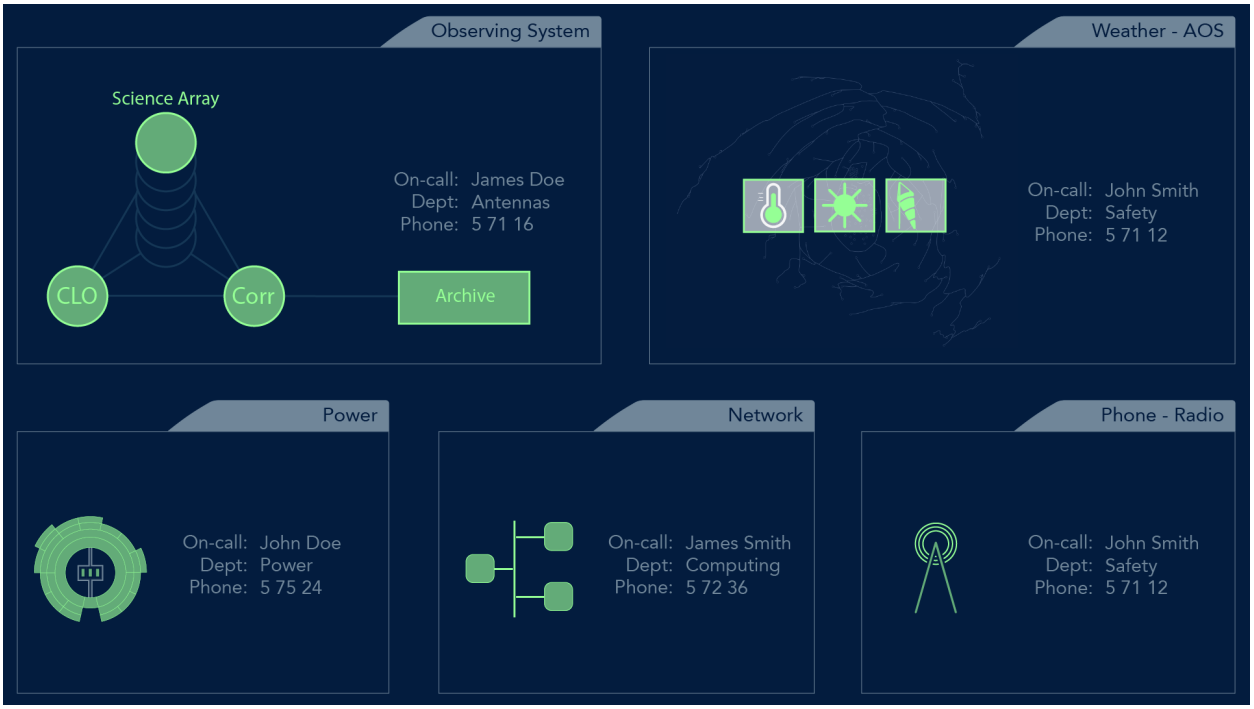
- For a given SB
    - Array not on source
    - Array not locking
    - ACD not in correct position
    - SB flagged
    - Possible a correlator-related alarm? (*)
    - Missing delay events
    - Missing WVR data
- Infrastructure
    - Archive disk space
    - Data capture
    - NGAMS

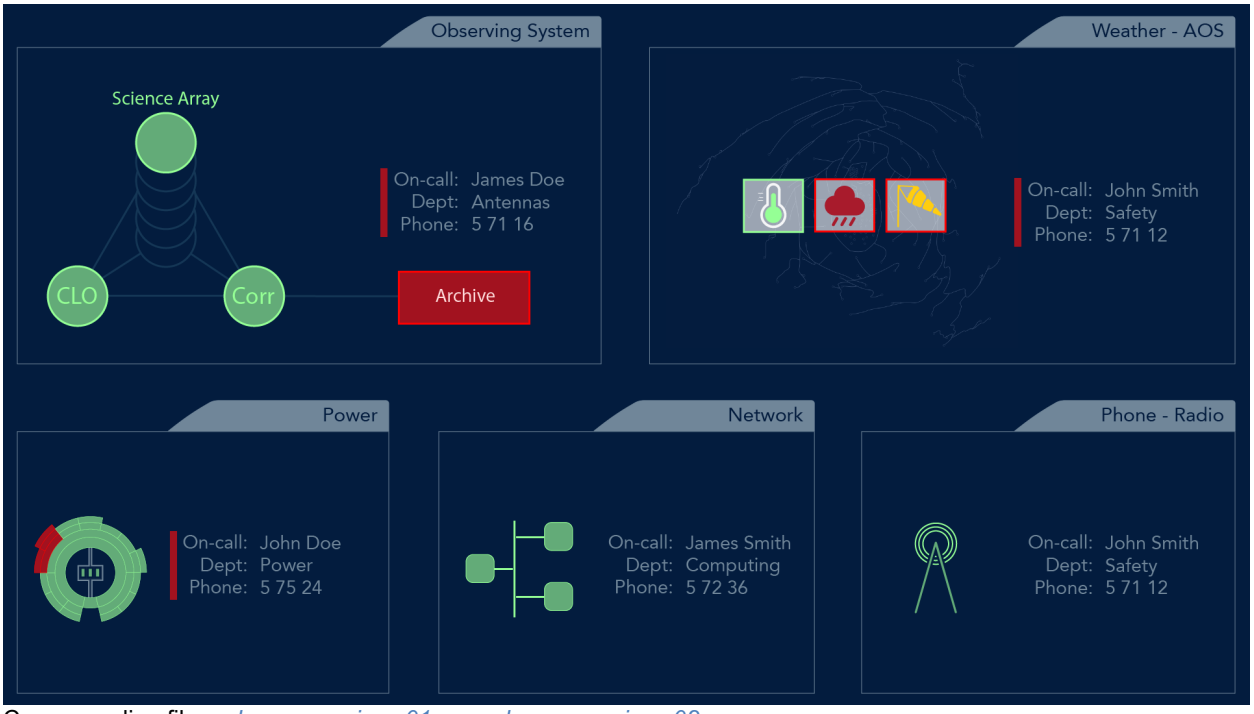
(*) This was raised as an issue to discuss at the Correlator Workshop later this year.

Appendix E shows a mockup of this alarm panel.

A. Observatory Overview Mockup

To help users relate this overview to the other, more detailed alarm panels (see Appendices B-F), we try to integrate as much of the visual representations from the detailed panels in the overview. The font size is deliberately set to a large value so as to make this panel readable from a distance.

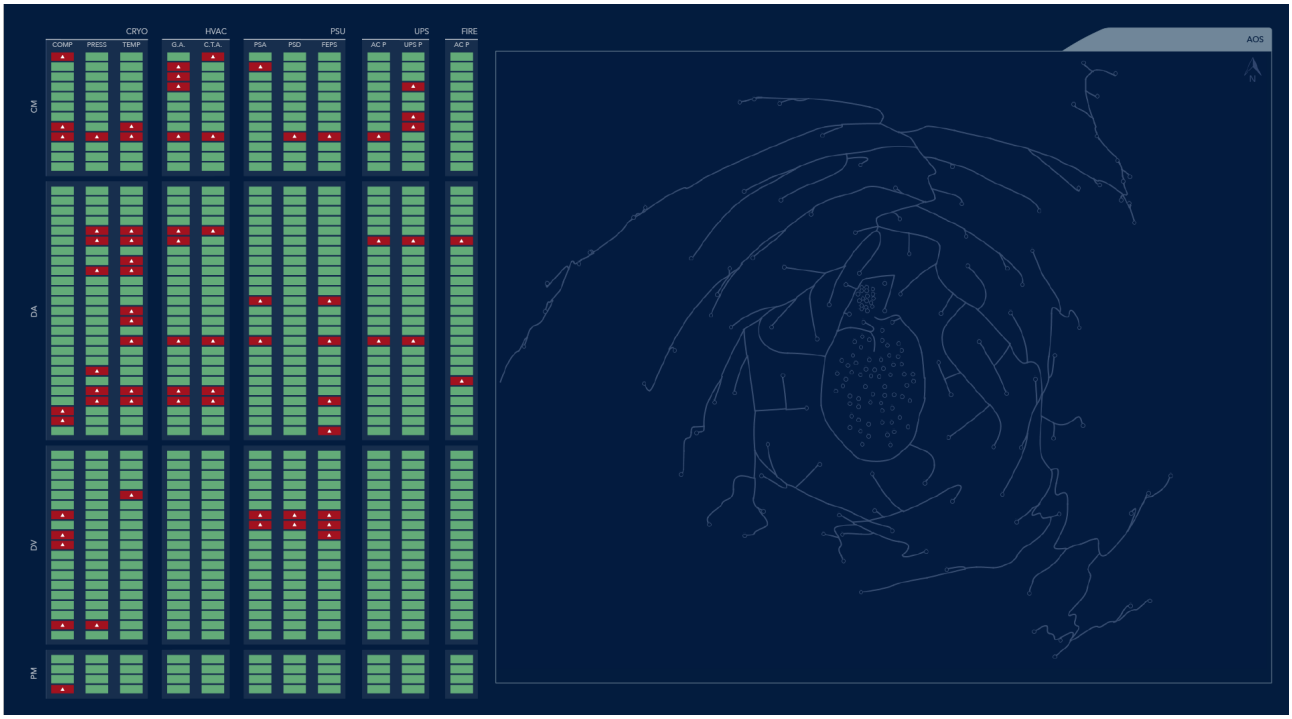


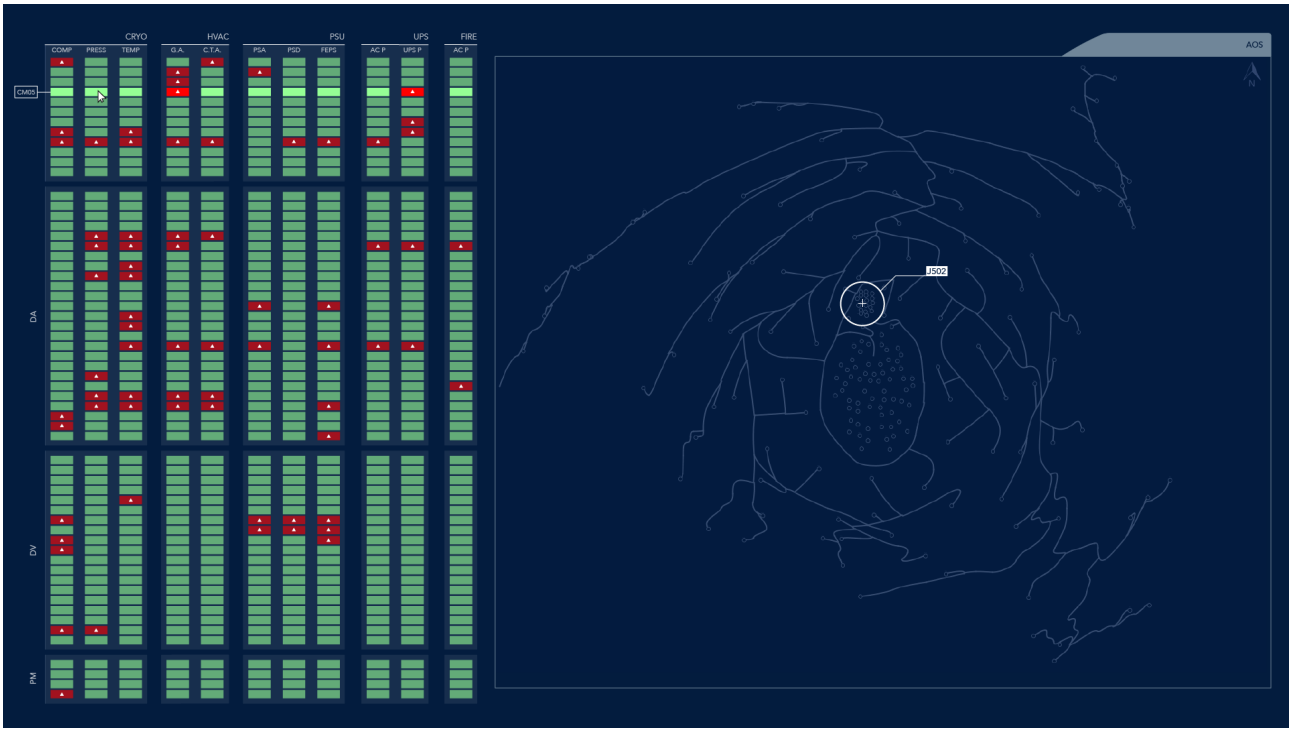


Corresponding files: *alarm_overview_01.png, alarm_overview_02.png*

B. Array Elements Alarm Panel Mockup

1. Default Design

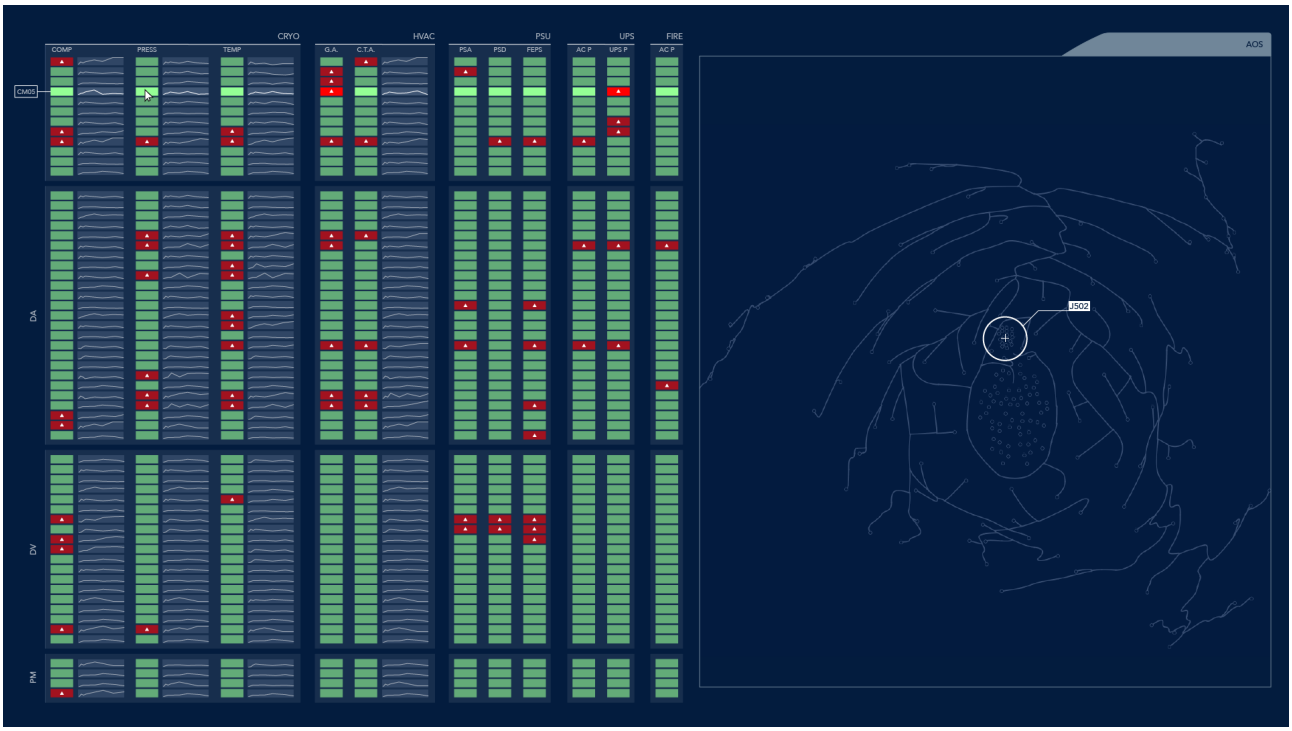




Corresponding files: *infrastructure_array_elem_default_01.png, infrastructure_array_elem_default_02.png*

2. Alternative Design with Sparklines

Variation on the default design, featuring sparklines representing the trend for numerical variables associated with some alarms such as temperatures going beyond/below a defined threshold.



Corresponding files: *infrastructure_array_elem_sparklines_01.png, infrastructure_array_elem_sparklines_02.png*

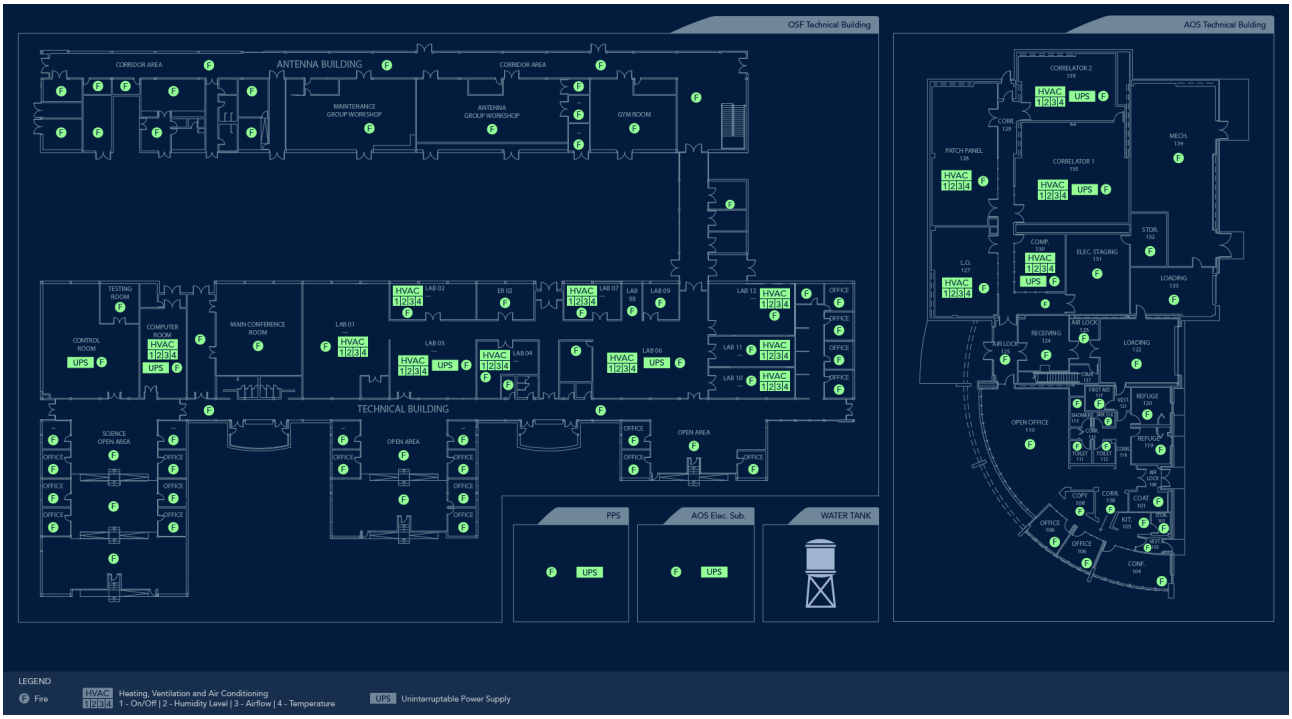
C. Power Alarm Panel Mockup

1. Power Generation and Distribution

Corresponding files: *infrastructure_power_ok.png, infrastructure_power_alarms.png*

2. Buildings (Fire, HVAC, UPS)

The first mockup shows the display when no alarm has been triggered. The second one shows the same panel with multiple fire, UPS and HVAC-related alarms triggered.



Corresponding files: *infrastructure_buildings_ok.png, infrastructure_buildings_alarms.png*

D. Weather Alarm Panel Mockup

The mockup uses the distorted AOS layout discussed in Sections 7.2, 7.3 and Figure 3. The alternative, geographically-accurate representation can also be considered depending on the actual location of weather stations. The locations used in the mockup are random, pending reception of the actual weather station coordinates.

Corresponding files: *infrastructure_weather.png*

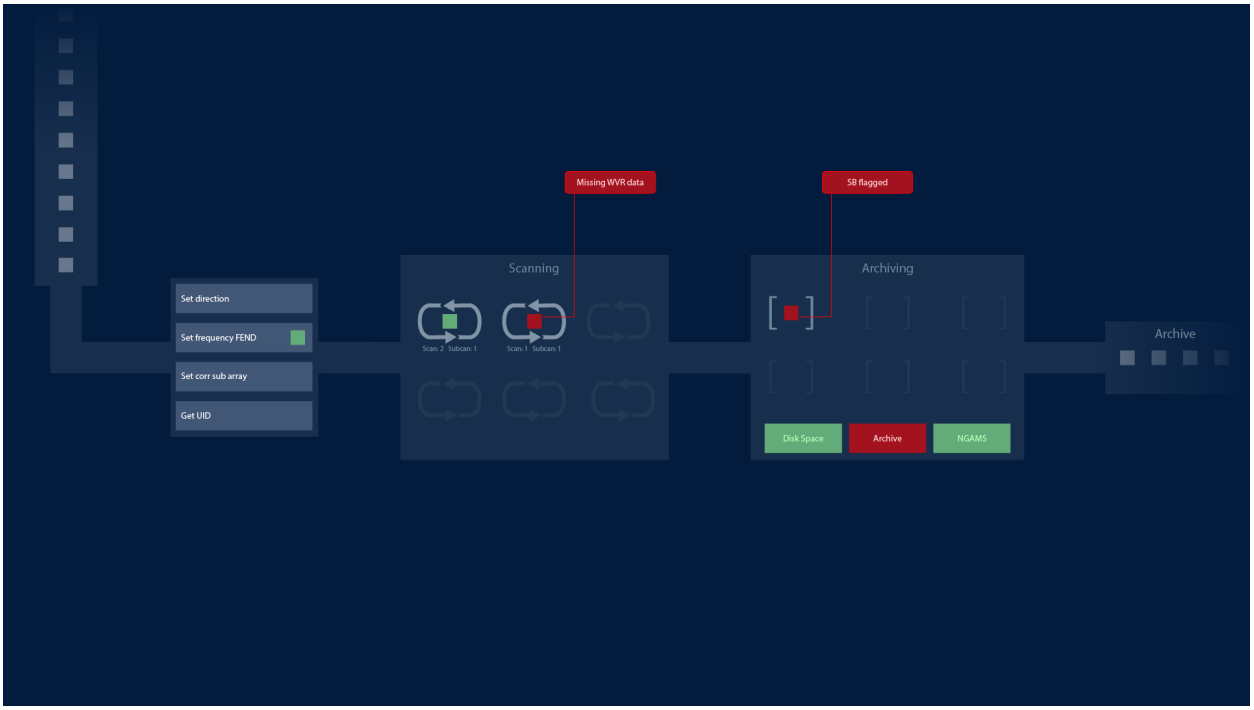
E. SB Execution Alarm Panel Mockup

This process-oriented view is conceptually different from all other mockups. It does not focus on particular equipment, but rather on the observation process. The main elements represented are execution blocks, that move throughout the workflow, as explained in Section 8.1.

The *Scanning* and *Archiving* components feature six placeholders for these execution blocks as it is anticipated that a maximum of 6 arrays can co-exist at the same time, and only one scheduling block can be assigned to an array at any moment. Execution blocks for all arrays are shown on one unique panel.

Blue squares on the left represent the queue of scheduling blocks to be executed next. Blue squares on the right are side are those that have been successfully executed and archived.

The upper part of the panel is mostly empty in the mockup, as it is reserved for displaying details about alarms related to the execution blocks (two of them are showing errors in this example). More detail can be added, and this should be defined as part of the next design iteration. Similarly, the lower part of the panel could hold additional contextual information.



Corresponding files: *process_sb_exec.png*

F. Alarm Color Scheme

The color scheme used to represent alarms has been designed taking into account color blindness. The two main colors used to represent alarm status differ not only in hue but also in saturation, trying to find a compromise between color mappings that are straightforward to understand and ease of differentiation for all users. The following figure shows a simulation of how it is perceived by different user categories.

Normal color vision | Color blindness – Protanopia | Color blindness - Deuteranopia