# Appendix D - Design Standards: BMS Critical Alarms

## Table of Contents

## Scope

This design guide deals with the installation and configuration of the BMS to handle the monitoring of critical equipment and the subsequent alarm processing.

The design guide consists of five sections covering the following content.

- Critical alarm processing
- Equipment alarm connection points
- Alarm counts and totalisers
- Graphical interface and userviews
- Alarm testing

## Purpose

The purpose of this guide is to create a degree of uniformity in the installation and presentation of critical alarms so that operators are able to quickly identify the present incidence of alarms and to monitor the frequency at which they occur. It is also intended that this will help to streamline the process of alarm testing.

## Related Guides and Standards

The following documentation should be referenced in conjunction with these appendices:

1. Appendix C – BMS User Interface R1.1
2. Appendix E – Categories and Priorities R1.1

# 1. Critical Alarm Processing

## Critical Alarm Definition

Critical alarms are generated for monitored plant or equipment where timely intervention can mitigate the risk of potential harm to persons, damage to equipment or the ruination of laboratory samples and experiments. Critical alarms monitored by the BMS are passed to a dedicated alarm handling system which is used to alert UQ security staff.

Common types of critical alarm which are monitored at UQ are summarized in the following table:

| Critical Alarm | Monitored plant or equipment |
|---|---|
| Low Oxygen / Gas leak detection | Gas detectors typically located in gas stores or laboratories with equipment which utilise gas supplies. The gas sensors are monitored by a gas detector panel which generates local alarms which are monitored by the BMS. |
| Laboratory gas supply | A pressure switch located in the gas supply line triggers an alarm when the pressure drops below the required supply pressure. Action may be required to protect laboratory equipment and experiments that rely on the supply. |
| Freezers, Fridges and Incubators | Controlled temperature storage vessels with alarm contacts to alert that the internal temperature is no longer within the required range with potential damage to the vessel contents. |
| Cold rooms and Freezer rooms | Controlled temperature storage rooms with independent temperature and plant fault monitoring. Action may be required to relocate critical samples to an alternative storage. A typical cold room alarm setting would be >10°C for 15 minutes. |
| Process air and vacuum plant | System pressure and plant fault monitoring warning of the loss of process air or vacuum systems with a subsequent risk of failure of dependent laboratory equipment. |
| Reverse osmosis water supply | Water quality and plant fault monitoring warning of the loss of reverse osmosis water with a subsequent risk of failure of dependent laboratory equipment. |
| Chilled water supply | Chilled water temperature and chiller plant fault monitoring warning of loss of cooling capability to building equipment. A typical CHW temperature alarm setting would be >12°C for 15 minutes |
| Animal House Conditions | There are strict requirements for the temperature and humidity conditions under which animals are kept and any loss of conditions needs to be responded to quickly. |
| Laboratory Containment or Quarantine | Laboratories with physical containment, clean room or quarantine status require tight room pressure control to meet the terms of operation of the facility. Any loss of room pressure or faults in the associated mechanical plant are critical. |
| Power generators | Some buildings rely on the continuity of power supply provided by back-up power generators. Any generator fault condition or fuel system alarm needs to be dealt with in a timely manner to ensure back-up power is always available. |

## Hardware Components

There are several hardware components required to propagate the critical alarm from the monitored equipment to the security alarm handling system. The local alarm contact connects to a BMS I/O module which is monitored by a BMS Network Engine (NAE) located in that building. This NAE sends the alarm to a second dedicated BMS Network Engine which is interfaced to an alarm handling system in the security office.

The integrity of the alarm system is dependent on the reliable functioning of each component including the campus Ethernet backbone on which the BMS network engines are dependent. → Every point of connection is a risk of failure and should be proven on a regular basis via a rigorous test regime. Every component is reliant on a secure power supply and the monitoring software must include the provision to detect and alert to a loss of communications which effectively nullifies the alarm monitoring.

The following diagram captures the hardware components involved with the arrow symbol representing the directional flow of the alarm through the system:

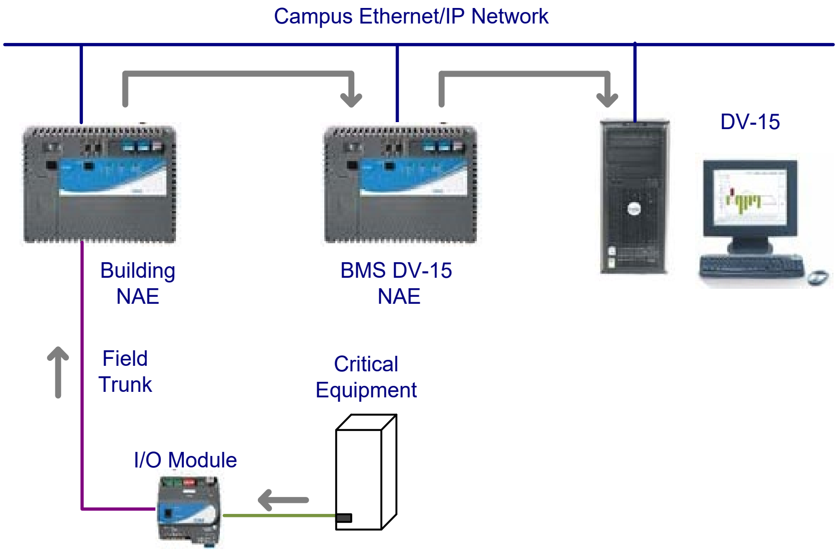



*Fig 1: Alarm propagation through each hardware component*

## Software Configuration

For each alarm the BMS network devices require a number of software components. It is important that the BMS software is configured to a consistent design standard to help avoid programming anomalies and to simplify troubleshooting. The software elements which require configuration are as follows.

| | |
|---|---|
| Building NAE: | BMS Alarm Input |
| Building NAE: | BMS Alarm Interlock |
| Building NAE: | BMS Alarm Global Data Object |
| DV-15 NAE: | DV-15 Multi-state Alarm Object |
| DV-15 NAE: | Building NAE Reliability check |

## BMS Alarm Input

The alarm input connection to the BMS is typically an open/closed contact. These should be configured such that the open contact state is the alarm state. Thus, if the alarming device fails, loses power or the cable connection to the BMS is damaged or disconnected, then the BMS input will default to the alarm state. The BMS input state text would typically be Alarm-Normal. If the BMS input is analogue then the alarm is configured in software and there is no fail safe state.

The input database tag reference should include the building number, the room number and an incremented integer to uniquely identify the item of equipment. The object name should clearly depict the type of critical alarm and where it is located. The object description should reference the associated alarm object in Metasys-DV15 so it is obvious when viewing the input that this is a critical alarm and can be easily traced to the alarm interlock. An example of tag reference, object name, description and state text for a BMS critical alarm input would be:-

| | |
|---|---|
| Tag Reference: | 0060-EA-729-1 |
| Object Name: | 60 Room 729 Freezer 1 |
| Description: | St Lucia 0060 Rm 729 Freezer Alarm 1 |
| States Text: | Alarm / Normal |

The following table summarises the object name and description for different types of critical alarm using Gehrmann (building 60) as an example:-

| Critical Alarm | Object Name | Description |
|---|---|---|
| Freezer Alarm | 60 Room 729 Freezer 1 | St Lucia 0060 Rm 729 Freezer Alarm |
| Cold Room | 60 Cold Room 302 Temp | St Lucia 0060 Rm 302 Cold Room |
| Low Oxygen | 60 Room 127 Low Oxygen | St Lucia 0060 Rm 127 Low Oxy Level |
| Gas Supply | 60 Room 630 Nitrogen Supply | St Lucia 0060 Rm 630 Nitrogen Supply |

## DV-15 Multi-State Objects

The key component of the BMS-DV15 interface is a multi-state object that reflects the current status of each critical alarm. The state of this object is updated to DV-15 in the security office whenever the value changes. The object has 4 states and utilizes a customized state text called DV15 Alarm:

| | |
|---|---|
| State Text 0: | Normal |
| State Text 1: | Alarm |
| State Text 2: | Unreliable |
| State Text 3: | Out of Service |

The object category is also customized using custom category 11 which has been allocated for DV15 Alarms.

| | |
|---|---|
| Object Category: | DV15 Alarms |

The object name is critical and should capture the campus, building and room number and alarm description. If the alarm covers multiple rooms then use the floor number (e.g. 0064-L5).

Object Name: St Lucia 0064 Rm 526 High CO2 Level

It is vital that this object name becomes the BACnet object name when discovered by DV-15. For this to happen a flag must be set in the object focus window called “Username is BACnet Obj Name”. This flag must be set to True otherwise the full item reference will be passed as the alarm name to DV-15.

| | |
|---|---|
| **Display** | |
| Number Of States | 4 |
| States Text | DV15 Alarm |
| **BACnet** | |
| Object Name | GATTON 8167-105 Energex Incomers Open |
| User Name Is BACnet Obj Name | True |
| Object Identifier | MV:3024943 |
| Out Of Service | False |

This flag must be set to True

The object description should match the BMS alarm input tag reference so that it becomes clear which field input triggers the alarm.

### Building NAE Alarm Folders

Each building NAE has a folder called DV15 Alarms (tag reference Alarms) with sub-folders for Interlocks, global data and alarm counts. All components of the critical alarm logic in the building NAE reside in one of these sub-folders. The naming of the alarm interlocks should mimic the MV alarm object so that they can be readily transposed to a common userview and can be independently monitored when Metasys-DV15 is down or being upgraded.

### BMS Alarm Interlock

A software interlock is used to monitor the alarm input or multiple inputs. It includes an alarm object that adds a time delay to filter out transient alarms and a trend object to record the changes in value. This time delay will vary from a few seconds for low oxygen alarms to 20 minutes for freezer equipment alarms. When the interlock returns to false it has an action to cancel the report delay on the alarm returning to normal. The object name for the Interlock should match the tag reference for the associated MV object in Metasys-dv15 using the SecAlarmXX numbering system.

### BMS Alarm Global Data Object

A Global data object is used to write the alarm object state from the interlock to the MV object in Metasys-DV15 at command priority 10. The global data object responds to change of value and also has a 2 minute refresh. Alarms are therefore processed on change of state and if there is a loss of communication between network elements then the system will restore the correct alarm state. The global data object also recognizes if the alarm input is unreliable and writes the unreliable state to the MV object as a fail command.

### Building NAE Reliability Check

A Global data object and interlock in Metasys-DV15 captures the offline state of each building NAE. If the NAE is detected as offline then a second interlock is used to command all alarms from that NAE to the unreliable state. A time delay of 15 minutes is applied to allow for reboots, downloads and temporary power cycles of the building NAE. The reliability interlock operates at priority 9 and takes precedence over the priority 10 commands from the building NAE. When the NAE is back on line the priority 9 command is released.

## BMS Alarm Time Delays

Time delays are included in the alarm interlock alarm objects to filter out transient and nuisance alarms. The following table lists some typical alarms with the recommended time delay.

| Critical Alarm | Time Delay | Reason for Delay |
|---|---|---|
| -80 Freezer Alarm | 20 minutes | Transient alarms due to door being open for too long. Allow testing of alarm input without triggering DV15 |
| Cold Room | 15 minutes | Transient alarms due to door being open for too long. |
| CHW Supply | 15 minutes | Transient alarms due to load changes and chiller staging |
| Room Conditions | 5 minutes | Transient alarms due to control response to condition changes or duty-standby changeover |
| Plant faults and alarms | 1 minute | Transient alarms to filter out temporary fault conditions |
| Low oxygen alarms | 10 Seconds | Minimum Delay |

## BMS-DV15 Alarm Folders

The Metasys-DV15 NAE has alarm folders allocated for each campus and sub-folders for each building within the campus.


*Fig 2: Security alarm folders allocated for each campus*

All critical alarm MV objects reside in the corresponding building folder. The building folder tag reference is a four digit building number. The object name includes the same number plus the building name.

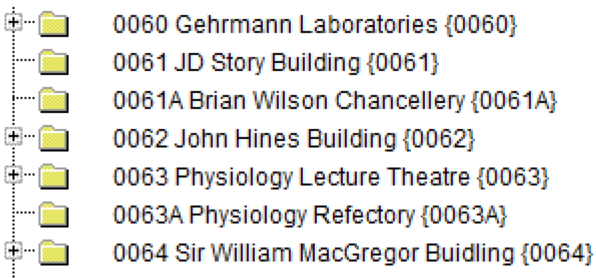



*Fig 3: Alarm folders allocated for each building*

The building folder has a sub-folder to contain the NAE offline interlocks for each NAE which serves the building. There is also an alarm counts sub-folder to contain building alarm totals. This is covered in more detail in section 3.

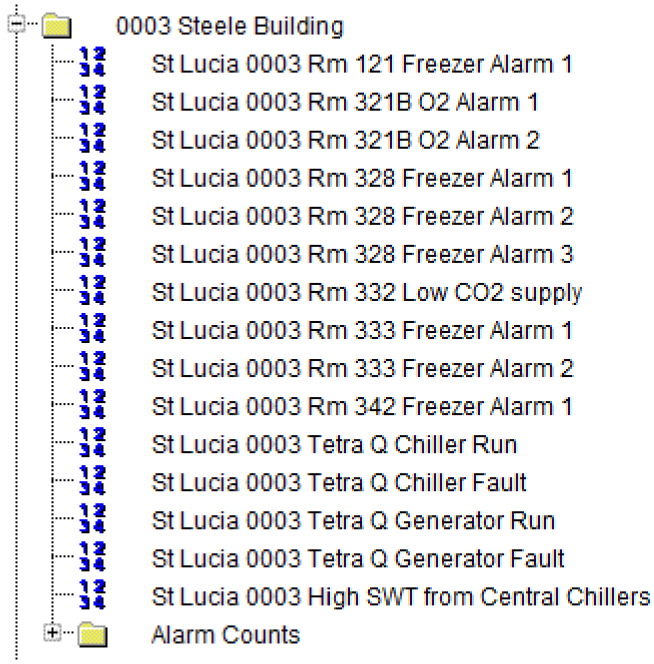



*Fig 4: Multi-state objects and folders for alarm processing*

## Item References

It is important that the tag references follow a strict convention for processing within the DV-15. The tag reference and folder names concatenate to provide a reference string which is interpreted by the DV-15. In the above example the folders and tag reference for Room 526 CO2 alarm combine to produce: Programming/Security Alarms/St Lucia/0064/SecAlarm01.

## Disabled Alarms

If a critical alarm is temporarily not required due to equipment failure or re-location then steps should be taken to prevent unintended activation of the alarm. These steps include:

| | |
|---|---|
| Alarm MV Object: | Change the alarm name to include the word - "Disabled" |
| | Add the words "Temporarily Not in Use" to the description |
| Alarm Interlock: | Disable the alarm object in the alarm interlock and add the words "Alarm Disabled to the interlock name |
| | Add the words "Temporarily Not in Use" to the description |

The Security Tech Office should be notified that the alarm has been disabled. By changing the alarm name, the DV15 alarm text verification will fail and the alarm will no longer be viable. If the alarm is rediscovered then it will stand out that it is a disabled alarm.

When the alarm is reinstated the alarm text and interlock links have to be re-established and the Security Tech Office notified. The alarm must then be re-tested end-to-end to confirm its operation.

## Obsolete Alarms

If a critical alarm is no longer required and is unlikely to be re-instated then the alarm should be made completely non-operational and the Security Tech office notified. The following changes should be made on the BMS:

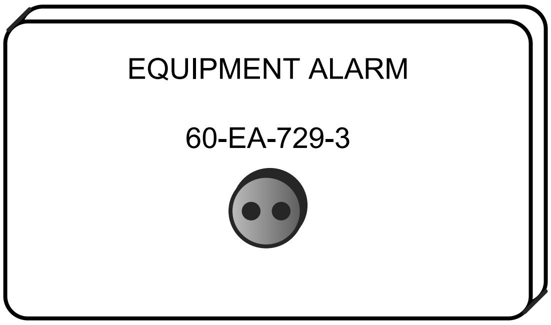
| | |
|---|---|
| Alarm MV Object: | Change the alarm name to the term - “Spare Alarm”<br><br>Add the words “Not in Use” to the description |
| Alarm Interlock: | Delete the link to the alarm input<br><br>Add the words “Not in Use” to the interlock name and description |
| Alarm Input: | Remove the DV15 alarm reference from the description and add the words “Spare Input”. |

## 2. Equipment Alarm Connections

The reliability of the alarm handling system is improved by minimizing potential points of failure at the connection point. Daisy-chaining multiple items of equipment to a single BMS alarm input adds a complexity which can result in alarms being masked by other equipment already in the alarm state or disconnected due to equipment failure. For this reason it is strongly advised that any critical laboratory equipment that requires monitoring has a dedicated connection to the BMS and is treated as a single entity throughout the software configuration resulting in a DV-15 alarm reference unique to that item of equipment.

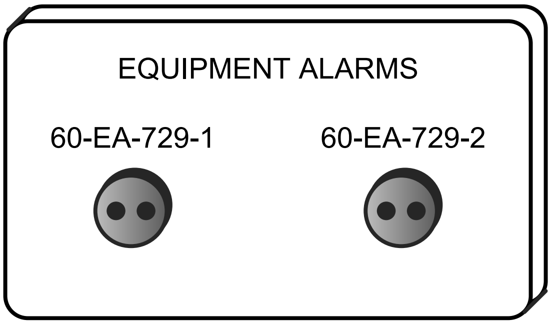
### Alarm Connection Points

The physical connection point is a 2-PIN DIN socket mounted on a clearly labelled wall plate. The label text is printed on 12mm high labels and placed above the socket. The text must be the same as the tag reference used for the BMS alarm input. This consists of the building number, the room number and an incremented integer to uniquely identify the item of equipment within the room. For example, the third equipment alarm in Gehrmann room 729 would appear as: 60-EA-729-3.




More than one connection point may be provided on a single wall plate given the following provisos:

1. Each connection point must have a dedicated BMS input.
2. The label text must clearly differentiate between the inputs




The equipment being monitored is connected to the wall socket via a female connector plug. A 2-core cable is soldered to the plug with the other end connecting to the volt-free terminals which form the alarm contacts on the monitored device.

If the alarm contacts have a normally open / normally closed option then normally closed should always be used. This means that if the cable or connection fails in any way then the contacts will be interpreted as being open circuit and the BMS will default to the alarm state. This also means that if the equipment needs to be disconnected or taken out of service then a blank plug will be required to connect to the wall socket in lieu of the equipment to avoid a nuisance alarm being generated at the security alarm handling system.

If the alarm contacts are to be shared with other alarm handling systems, such as direct dial-outs, then a slave relay will be required such that each system can operate in parallel.

## Out of Service Plugs

If a freezer is taken out of service then steps should be taken to prevent unnecessary alarms being sent to the DV-15 alarm handling system. Each room or floor which houses equipment alarm connection points should be supplied with dummy connectors which create a closed circuit to the BMS input.

When a freezer is known to be faulty or is going to be taken out of service then the equipment should be disconnected from the wall socket and this dummy connector, or Out of Service Plug, connected in place. The out of service plug should have an isolation tag attached that allows the equipment owner to record the time, date and reason that the monitored equipment has been disconnected. This holds the alarm in a permanently normal state and prevents wasted time chasing up alarms that are no longer relevant.

## Freezer Dial-Out Systems

Modern -80 freezers are becoming increasingly sophisticated and have integral alarm dial-out systems. These provide an additional monitoring capability which may occur in parallel but should not be considered as replacement of the BMS monitoring.

A crucial aspect of forwarding alarms to the security office is related to duty of care. By involving security staff in the alarm response they inherently become aware that research staff or students will be attending the building, probably out of hours, and they can take appropriate action to ensure their safety.

# 3. Alarm Counts and Totalisers

## Alarm Counts

The critical alarm monitoring across the St Lucia campus is extensive and some method is desired to provide a picture of the current alarm status at any one time. This is achieved by providing a live count of the number of alarms which are current for each building. There are also checks to detect if the alarms for any building are unreliable. The alarm counts and checks are presented on a summary graphic which gives an instantaneous picture of the health of the critical alarm monitoring for each building across the campus. Below is an extract from the graphic showing that there is one alarm current in the Goddard building, all alarms are presently reliable for the buildings shown and that the Steele building has the worst record for alarm reliability.

| Building | Initiators | Alarms | Unreliable | Unreliable Total |
|---|---|---|---|---|
| Steele | | 0 | No | 26 |
| Richards | | 0 | No | 3 |
| Pamell | | 0 | No | 1 |
| Goddard | | 1 | No | 7 |
| Michie | | 0 | No | 5 |

*Fig 5: Graphical extract showing active alarm counts per building*

The alarm data can be summarized as follows:

| | |
|---|---|
| Status: | Green when no alarm is active in the building |
| Alarms: | The number of critical alarms which are currently active |
| Unreliable: | The alarm status is not known for one or more alarms |

Thus, for each building there is an indication of how many alarms are current or whether the alarm state cannot be determined due to device communication issues.

It is imperative that the alarm counts and checks are updated whenever a new alarm is added to the system. The analog data objects which represent the alarm count should include a BMS alarm object such that the graphic display turns red when the value is greater than zero. The binary data objects which represent the unreliable checks should include an alarm and a totalizer object to increment each time the check returns as true. Also, for all objects the last twenty five changes in value should be captured as trend data and written to the repository at 20.

An alarm counts sub-folder is created under each building folder in Metasys-DV15. Within this sub-folder are the unreliable checks and the alarm totals. If a critical alarm is the first one added for the building then the folders, calculations and summary alarm graphic will all need to be updated. Where a building has multiple NAEs the alarm count and unreliable interlocks will be required for each NAE. It is advisable to limit the interlock to 20 alarms.

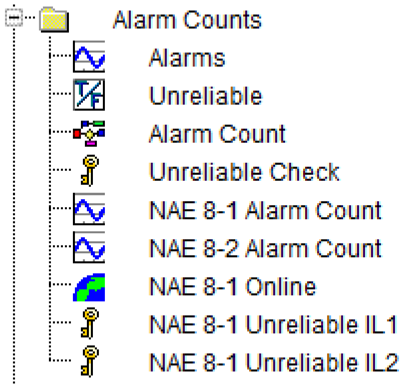



*Fig 6: Folder structure for Metasys-DV15 alarm counts*

An alarm counts sub-folder is also created for each building NAE alarm folder. Within this sub-folder are the calculations which generate the alarm counts, the AV objects which store the values and the Global Data object that writes the NAE total to Metasys-DV15.

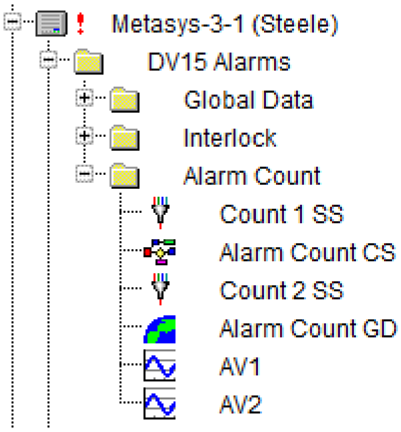



*Fig 7: Folder structure for building NAE alarm counts*

## Userviews

The alarm summary graphic gets all of its information from Metasys-dv15 which interfaces to the security alarm handling system. If this device is offline then there will be no alarms forwarded to DV15 and no back-up BMS summary of the buildings with alarms.

As a fall back during this rare event, a Security userview has been built which includes folders containing the alarm input interlocks from the building NAEs. As these exist in the distributed network engines around the campus, the alarm input state is still available when Metasys-DV15 is down. The alarm object included with the alarm interlock produces a red exclamation mark which can guide the user to where the current alarms are.

The critical alarm folders in the building and security userviews are linked to the Metasys-DV15 alarm folders such that they automatically update with each new alarm.

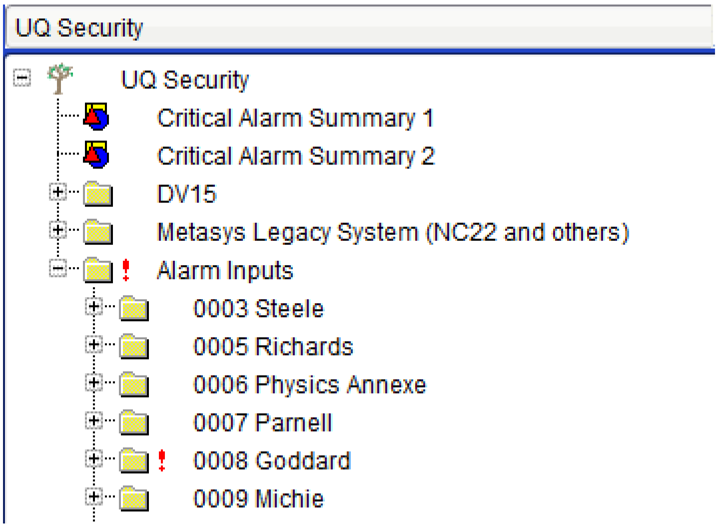



*Fig 8: UQ Security userview*

## Alarm Priorities and Event Viewer

The alarm objects created for the MV objects and alarm input interlocks should be created with the alarm and normal priority set to 1 and 2 respectively. In the circumstances that DV15 or Metasys-DV15 are down the event viewer can be used as a back-up alarm monitoring system. The priority is important because these filter to the top of the Metasys Event Viewer and are therefore not masked by the many other alarms in the system.

## 4. Alarm Testing

The integrity of the critical alarm handling system is dependent on frequent testing to check that all hardware and software components involved are functioning normally. There are 3 testing regimes to be considered:

| | |
|---|---|
| End-to-End Testing: | A comprehensive test from alarm initiation to security office screen |
| BMS Testing: | A local test from alarm initiation to the BMS alarm input interlock |
| Self-Testing: | A local test carried out by the equipment owner |

In each case the alarm input is initiated at the equipment being monitored. For equipment alarms this may be as simple as removing the connection plug from the wall socket. For this reason, it is important when installing freezers and similar equipment that there is free access to the wall socket.

### End-to-End Testing

This test should be carried out at least once a year and is the only test which genuinely proves that all aspects of the alarm handling system are functioning normally and can be relied upon. The test requires the involvement of two technicians, one to attend the monitored equipment and initiate the alarm and the other to witness the generation of the alarm on the security office DV-15 Screen.

An unfortunate aspect of the test is the time delay between alarm initiation and propagation which for -80 freezer alarms is typically 15 to 20 minutes. This either means long waiting periods during the testing or changing the delay time to something more manageable. For the latter, the testing procedure must include a step which ensures that the time delay is restored to its original value.

Part of the testing should include a check of the building alarm total to ensure it correctly reflects the number of active alarms at any one time. The opportunity should be taken to check any alarms which have abnormally high unreliable counts which may be explained by poor connections or faulty equipment.

### BMS Alarm Input Testing

The advantage of this test is that it only requires one technician and does not involve waiting for lengthy time delays or changing the time delay values to avoid delays. This means that it is quicker and cheaper to execute the testing and can be considered on a more frequent basis. The main shortfall is that only the BMS alarm input logic is tested.

The methodology requires the technician to carry a laptop or tablet that is connected to the BMS. The alarm input is overridden by the technician who then witnesses the change of state on the alarm interlock in the building NAE. Once the test is deemed successful, the alarm input is released and the alarm interlock returns to normal before the time delay has expired. In this way, there is no generation of alarms to the security office thus avoiding the disruption this causes.

### Self-Testing

This test regime can be carried out by the owner or manager of the monitored equipment. For -80 Freezers the test involves unplugging the equipment from the wall socket which is connected to the BMS and waiting for a confirmation call from security.