Science and Technology Facilities Council

ISIS Neutron and Muon Source

isis.stfc.ac.uk

THPV016

Developing an Alarm Philosophy for the EPICS Control System at ISIS

S.A. Medley, I.D. Finch, S. Malinowski, ISIS Neutron and Muon Source, Didcot, United Kingdom
M. Romanovschi, University of Manchester

ICALEPCS 2021

ISIS Control System Alarms

The ISIS Neutron and Muon Source has been operating for over 35 years. In this time, the number of alarms shown in the main control room (MCR) has steadily increased as new equipment (and associated channels) has been added to ISIS during various upgrades.

The result is that there are now hundreds of alarms frequently displayed to the MCR operators, particularly during shutdown periods when many machine systems are powered off.

Figure 1 shows a typical example of the large quantity of alarms displayed when ISIS is in shutdown, the majority of which are not valid when the machine is not running.

When so many alarms are shown at once, the alarms which are important during shutdown are easily overlooked by the operators.

The upcoming migration from the Vista Control Systems product Vsystem to EPICS provides the right opportunity and framework for a 'fresh start' to review and rationalise the alarms,

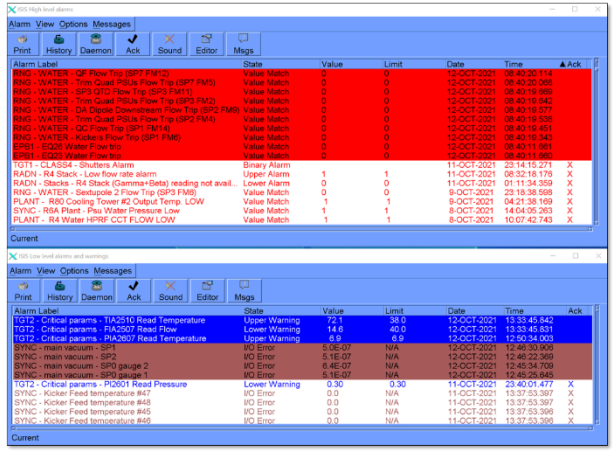

Figure 1: *The ISIS control system alarm screen uses the Vista Control Systems product Valarm. The top screen shows higher priority alarms, whereas the bottom screen shows lower priority alarms (referred to as 'warnings') and I/O errors.*

Alarm Philosophy: IEC 62682 Standard

The IEC 62682 / ISA 18.2 industrial standard on *Management of Alarm Systems for the Process Industries* describes internationally recognised good engineering practice for control system alarm management.

Through our review of ISIS control system alarms, we are striving to adhere to the good practice principles outlined in the IEC 62682 / ISA 18.2 standard.

The standard is centred on the concept of the Alarm Management Lifecycle – see Figure 2. The starting point is the Alarm Philosophy document, which establishes the basic definitions, principles and processes to design, implement and maintain the alarm system.

As ISIS is not a new facility and already has an extensive set of existing alarms, an Alarm Philosophy is being developed based on ongoing feedback from the operators on how the usability of these alarms can be improved.

The criteria outlined in the Alarm Philosophy will then be applied to rationalise the existing alarms and carefully manage the addition of new alarms.

The alarm rationalisation will be implemented during the migration of the control system from Vsystem to EPICS, resulting in EPICS control system alarms which are more useful and relevant to the ISIS operators.

After this initial implementation, the Alarm Philosophy principles will then be used as the basis for regular alarm reviews, as part of the ongoing process of the Alarm Management Lifecycle.

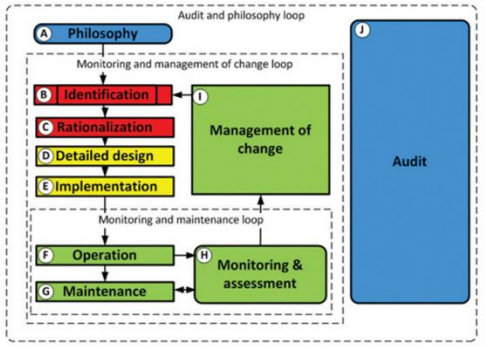

Figure 2: *The Alarm Management Lifecycle as per IEC 62682 / ISA 18.2 (source: isa.org). The Alarm Management Lifecycle is an ongoing process of continuous improvement to ensure that control system alarms remain up to date and useful.*

Alarm Identification and Prioritisation

Figure 3 shows the IEC 62682 definition of an alarm. We have agreed to adopt this definition at ISIS in our Alarm Philosophy for EPICS.

During the alarm rationalisation, we will apply this definition to each of our existing Vsystem alarms, warnings and I/O errors. Any which do not meet the criteria for a valid alarm will be removed. In principle, this initial rationalisation should reduce the quantity of alarms.

An important element of the alarm definition is the *response*, i.e. the action undertaken by an operator. For many of the alarms at ISIS, the operator response consists of contacting the relevant equipment owner so that they can take further action.

Alarm Priority: *the relative importance assigned to an alarm within the alarm system to indicate the urgency of response.*

IEC 62682 states that alarms should be prioritised based on the severity of the consequences and the time available to take corrective action. For many of the control system alarms at ISIS, the direct and most severe consequence is beam downtime. It follows that the approximate timescale until the beam stops should be used to define the allowable response time (and hence urgency) of the alarms.

Figure 4 shows a proposed set of alarm priorities based on these two factors (severity and urgency), developed in conjunction with ISIS operators. The aim is to replace the existing scheme of higher priority alarms and lower priority warnings with just one alarm screen, where each alarm is assigned one of the three new priority levels.

However, the feasibility of implementing a three-level priority system for alarms on EPICS process variables (PVs) needs to be investigated.

> **Alarm**: *an* ***audible*** *and/or* ***visual*** *means of indicating to the* ***operator*** *an* ***equipment malfunction, process deviation,*** *or* ***abnormal condition*** *requiring a* ***timely response.***

Figure 3: *IEC 62682 definition of an alarm.*

Priority	Time (approximate) until beam will stop if no operator intervention
High	Beam has already stopped, or is about to stop imminently
Medium	1-2 hours
Low	Several hours – operators should aim to resolve before end of their shift

Figure 4: *Proposed alarm priorities for ISIS based on feedback from the operators.*

Alarm Suppression

Alarm suppression: *any mechanism to prevent the indication of an alarm to the operator when the base alarm condition is present.*

At ISIS, we intend to implement alarm suppression in two different ways:

Designed Suppression: *alarms are suppressed based on operating conditions or states.*

At ISIS, designed suppression will be used for automatically suppressing a specified set of alarms when ISIS is in a shutdown period.

Shelving: *a mechanism, typically initiated by the operator, to temporarily suppress an alarm, with engineering controls to unsuppress the alarm.*

At ISIS, alarm shelving will be a feature available to operators, who will be able to specify the amount of time alarms are suppressed for. Engineering controls can include automatic unsuppression of an alarm once it clears, and unsuppresssion of all alarms in specified scenarios.

It is not yet determined whether the data required for automatic suppression can be captured in the standard EPICS PV structure.

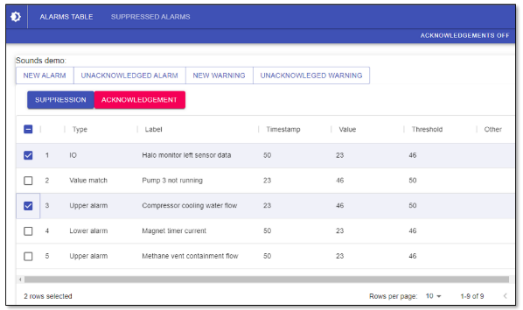

Figure 5: *RONA, the new web-based alarm viewer software currently under development at ISIS.*

We are prototyping the user interface aspect of alarm suppression using RONA, a new web-based alarm viewer currently under development at ISIS. RONA displays the same alarm information as Valarm, however because the software is being developed in-house at ISIS, it is much more easily customisable. This makes RONA an ideal test bed for demonstrating our proposed new alarm features to the operators, to gather their feedback before final decisions are captured in the Alarm Philosophy and implemented in EPICS.

Figure 5 shows the RONA user interface and demonstrates how alarm shelving would work in practice. Operators select alarms from the list and press the 'suppression' button, which moves the selected alarms from the alarms table to the separate tab for suppressed alarms. The suppressed alarms will still be visible on this tab, but as they are no longer taking up space on the main screen, it will be easier for operators to focus on the more important alarms.

Science and Technology Facilities Council

ISIS Neutron and Muon Source

ISIS Control System Alarms

The ISIS Neutron and Muon Source has been operating for over 35 years. In this time, the number of alarms shown in the main control room (MCR) has steadily increased as new equipment (and associated channels) has been added to ISIS during various upgrades.

The result is that there are now hundreds of alarms frequently displayed to the MCR operators, particularly during shutdown periods when many machine systems are powered off.

Figure 1 shows a typical example of the large quantity of alarms displayed when ISIS is in shutdown, the majority of which are not valid when the machine is not running.

When so many alarms are shown at once, the alarms which are important during shutdown are easily overlooked by the operators.

The upcoming migration from the Vista Control Systems product Vsystem to EPICS provides the right opportunity and framework for a 'fresh start' to review and rationalise the alarms,

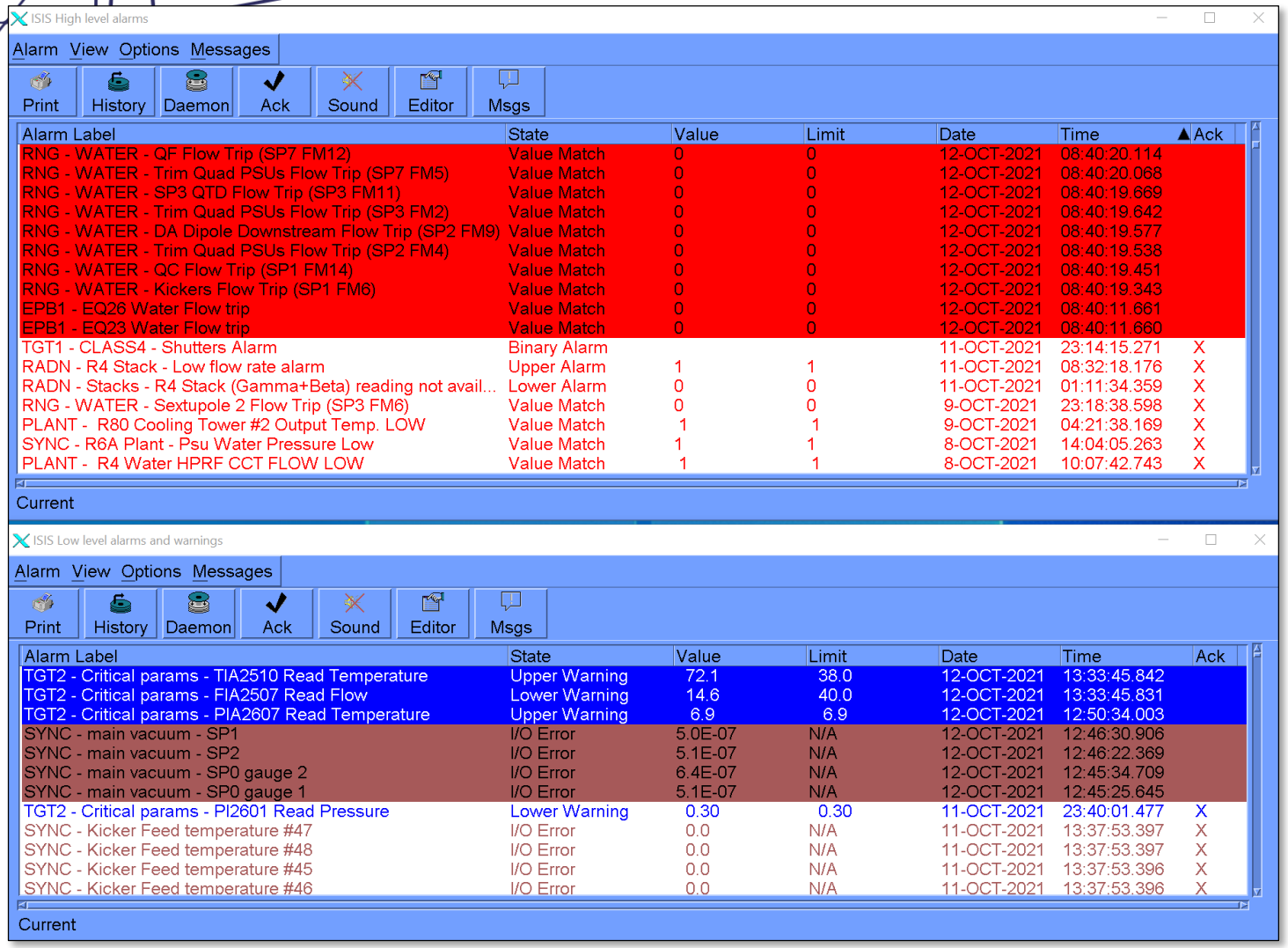

Figure 1: *The ISIS control system alarm screen uses the Vista Control Systems product Valarm. The top screen shows higher priority alarms, whereas the bottom screen shows lower priority alarms (referred to as 'warnings') and I/O errors.*

Science and Technology Facilities Council
ISIS Neutron and Muon Source

Alarm Philosophy: IEC 62682 Standard

The IEC 62682 / ISA 18.2 industrial standard on *Management of Alarm Systems for the Process Industries* describes internationally recognised good engineering practice for control system alarm management.

Through our review of ISIS control system alarms, we are striving to adhere to the good practice principles outlined in the IEC 62682 / ISA 18.2 standard.

The standard is centred on the concept of the Alarm Management Lifecycle – see Figure 2. The starting point is the Alarm Philosophy document, which establishes the basic definitions, principles and processes to design, implement and maintain the alarm system.

As ISIS is not a new facility and already has an extensive set of existing alarms, an Alarm Philosophy is being developed based on ongoing feedback from the operators on how the usability of these alarms can be improved.

The criteria outlined in the Alarm Philosophy will then be applied to rationalise the existing alarms and carefully manage the addition of new alarms.

The alarm rationalisation will be implemented during the migration of the control system from Vsystem to EPICS, resulting in EPICS control system alarms which are more useful and relevant to the ISIS operators.

After this initial implementation, the Alarm Philosophy principles will then be used as the basis for regular alarm reviews, as part of the ongoing process of the Alarm Management Lifecycle.

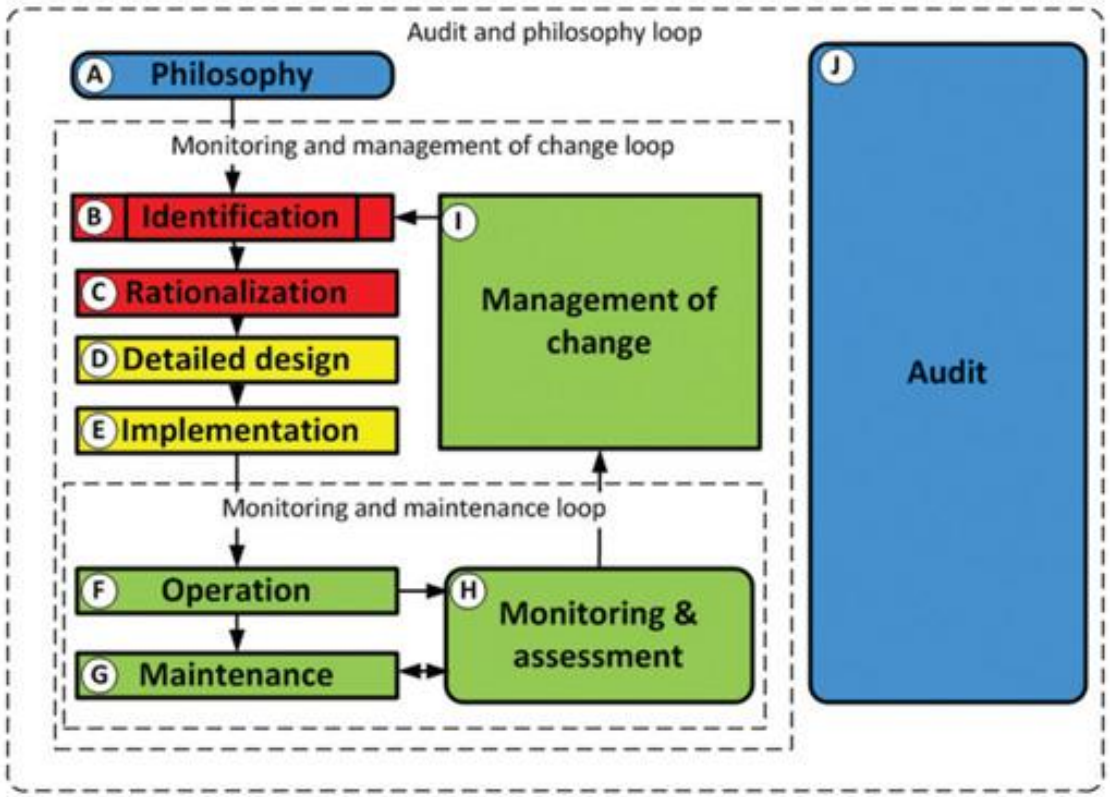

Figure 2: *The Alarm Management Lifecycle as per IEC 62682 / ISA 18.2 (source: isa.org). The Alarm Management Lifecycle is an ongoing process of continuous improvement to ensure that control system alarms remain up to date and useful.*

Science and Technology Facilities Council
ISIS Neutron and Muon Source

Alarm Identification and Prioritisation

Figure 3 shows the IEC 62682 definition of an alarm. We have agreed to adopt this definition at ISIS in our Alarm Philosophy for EPICS.

During the alarm rationalisation, we will apply this definition to each of our existing Vsystem alarms, warnings and I/O errors. Any which do not meet the criteria for a valid alarm will be removed. In principle, this initial rationalisation should reduce the quantity of alarms.

An important element of the alarm definition is the *response*, i.e. the action undertaken by an operator. For many of the alarms at ISIS, the operator response consists of contacting the relevant equipment owner so that they can take further action.

Alarm Priority: *the relative importance assigned to an alarm within the alarm system to indicate the urgency of response.*

IEC 62682 states that alarms should be prioritised based on the severity of the consequences and the time available to take corrective action. For many of the control system alarms at ISIS, the direct and most severe consequence is beam downtime. It follows that the approximate timescale until the beam stops should be used to define the allowable response time (and hence urgency) of the alarms.

Figure 4 shows a proposed set of alarm priorities based on these two factors (severity and urgency), developed in conjunction with ISIS operators. The aim is to replace the existing scheme of higher priority alarms and lower priority warnings with just one alarm screen, where each alarm is assigned one of the three new priority levels.

However, the feasibility of implementing a three-level priority system for alarms on EPICS process variables (PVs) needs to be investigated.

Alarm: *an **audible** and/or **visual** means of indicating to the **operator** an **equipment malfunction, process deviation,** or **abnormal condition** requiring a **timely response**.*

Figure 3: *IEC 62682 definition of an alarm.*

Priority	Time (approximate) until beam will stop if no operator intervention
High	Beam has already stopped, or is about to stop imminently
Medium	1-2 hours
Low	Several hours – operators should aim to resolve before end of their shift

Figure 4: *Proposed alarm priorities for ISIS based on feedback from the operators.*

Science and Technology Facilities Council

ISIS Neutron and Muon Source

Alarm Suppression

Alarm suppression: *any mechanism to prevent the indication of an alarm to the operator when the base alarm condition is present*.

At ISIS, we intend to implement alarm suppression in two different ways:

Designed Suppression: *alarms are suppressed based on operating conditions or states*.

At ISIS, designed suppression will be used for automatically suppressing a specified set of alarms when ISIS is in a shutdown period.

Shelving: *a mechanism, typically initiated by the operator, to temporarily suppress an alarm, with engineering controls to unsuppress the alarm*.

At ISIS, alarm shelving will be a feature available to operators, who will be able to specify the amount of time alarms are suppressed for. Engineering controls can include automatic unsuppression of an alarm once it clears, and unsuppresssion of all alarms in specified scenarios.

It is not yet determined whether the data required for automatic suppression can be captured in the standard EPICS PV structure.

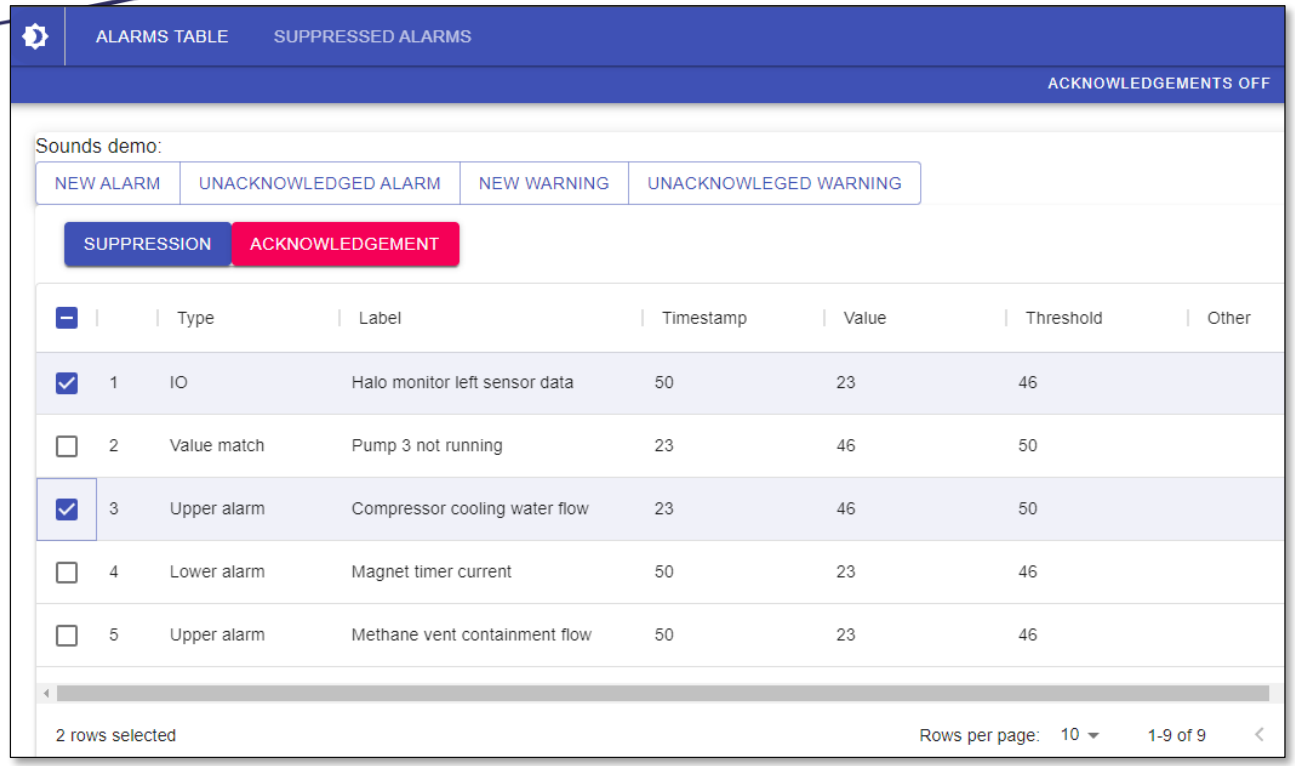

Figure 5: *RONA, the new web-based alarm viewer software currently under development at ISIS.*

We are prototyping the user interface aspect of alarm suppression using RONA, a new web-based alarm viewer currently under development at ISIS. RONA displays the same alarm information as Valarm, however because the software is being developed in-house at ISIS, it is much more easily customisable. This makes RONA an ideal test bed for demonstrating our proposed new alarm features to the operators, to gather their feedback before final decisions are captured in the Alarm Philosophy and implemented in EPICS.

Figure 5 shows the RONA user interface and demonstrates how alarm shelving would work in practice. Operators select alarms from the list and press the ‘suppression’ button, which moves the selected alarms from the alarms table to the separate tab for suppressed alarms. The suppressed alarms will still be visible on this tab, but as they are no longer taking up space on the main screen, it will be easier for operators to focus on the more important alarms.