

Developing an Alarm Philosophy for the EPICS Control System at ISIS THPV016



isis.stfc.ac.uk

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

Z

Q

0 Ž

0

C

00

E

σ

4

Ø

1

ard

σ

ta S

Ś

N

(0)

N

0

C

111

<u>ion</u> E

S

S

1

0

0

5

S

ICALEPCS 2021

Audit

S ntro Alarm 0 \mathbf{C} em ഗ $\mathbf{\Omega}$

atio

S

oriti

P 0

0

ati

C

ntifi

Ō

arm

2

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,

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 syste 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 wi 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.

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

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.

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.

					ACKNOWLED	GEMENTS OFF
	UNACKNOWLED		UNACKNOWLEGE	DWARNING		
	Туре	Label	Timestamp	Value	Threshold	Other
1	10	Halo monitor left sensor data	50	23	46	
2	Value match	Pump 3 not running	23	46	50	
3	Upper alarm	Compressor cooling water flow	23	46	50	
4	Lower alarm	Magnet timer current	50	23	46	
5	Upper alarm	Methane vent containment flow	50	23	46	
	LARM PPRES 1 2 3 4	LARM UNACKHOWLED PPRESSION ACKNOWL Type Type UNACKHOWL ACKNOWL ACKNOWL ACKNOWL UPRESSION UNACKHOWLED ACKNOWLED	LAMM LUNACHION(EDGED ALARIX MEDITY MAINING VETURESUICE ACREMENT MEDITY MAINING I Type I Libel I IO Main month int Sensor data 2 Main metht Pump 3 not running 3 Upper atem Compressor costing user from 4 Lower atem Magnet Sting current	LAIMIN UNACCHORM/EDGED ALAMIN MEW NAUNNA UNACCHOR/EDGED ALAMIN I Type I Account EDGED ALAMIN I Treastamp I Type I Label I Treastamp I JD Hale monthr wit sensor data 50 1 2 Value match Fung 3 and running 23 23 3 Upper atom Compressor counting water flow 23 4 Lower atom Mages three current 50	LAMM UNACONCIVILEDEED ALARIX NEW YMMENNES UNACONCIVILEDEED ALARIX NEW YMMENNES UNACONCIVILEDEED MINING I ACONCIVILEDEED MINING Immestamp Immestamp Value I Type I Lebel Immestamp Value I IV Hale month with sensor data 60 23 I Value match Pump 3 not running 23 46 I Upper atem Compressor conting satier flow 23 46 L Lower atem Magnet timer current 50 23	LABINE UNACCHORELEGED HAMM MEW NAMINA UNACCHORELEGED HAMMING I Type LABIE I Tirestamp Value I Tirestamp I Type LABIE I Tirestamp Value I Tirestamp I Dir Habe monthr vet sinsor data 00 23 46 2 Value math Fung 3 and running 23 46 50 3 Upper atom Compressor cooling safer flow 23 46 00 4 Lower stamm Tanges titree current 60 23 46

Management of

change

Monitoring &

assessment

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

Audit and philosophy loop

Monitoring and management of change loop

Monitoring and maintenance loop

D Detailed design

(E)Implementation

F Operation

G) Maintenance

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



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,

🗙 ISIS High level alarms					—	
Alarm View Options Messages						
🦸 🛓 📓 🗸 🗙 😭						
	- *					
	Msgs					
Alarm Label	State	Value	Limit	Date		Ack
RNG - WATER - QF Flow Trip (SP7 FM12)	Value Match	0	0	12-OCT-2021	08:40:20.114	
RNG - WATER - Trim Quad PSUs Flow Trip (SP7 FM5)	Value Match	0	0	12-OCT-2021	08:40:20.068	
RNG - WATER - SP3 QTD Flow Trip (SP3 FM11)	Value Match	0	0	12-OCT-2021	08:40:19.669	
RNG - WATER - Trim Quad PSUs Flow Trip (SP3 FM2)	Value Match	0	0	12-OCT-2021	08:40:19.642	
RNG - WATER - DA Dipole Downstream Flow Trip (SP2 FM		0	0	12-OCT-2021	08:40:19.577	
RNG - WATER - Trim Quad PSUs Flow Trip (SP2 FM4)	Value Match	0	0	12-OCT-2021	08:40:19.538	
RNG - WATER - QC Flow Trip (SP1 FM14)	Value Match	0	0	12-OCT-2021	08:40:19.451	
RNG - WATER - Kickers Flow Trip (SP1 FM6) EPB1 - EQ26 Water Flow trip	Value Match Value Match	0	0	12-OCT-2021 12-OCT-2021	08:40:19.343 08:40:11.661	
EPB1 - EQ20 Water Flow trip	Value Match	0	0	12-0CT-2021	08:40:11.660	
TGT1 - CLASS4 - Shutters Alarm	Binary Alarm	0	0	11-OCT-2021	23:14:15.271	X
RADN - R4 Stack - Low flow rate alarm	Upper Alarm	1	1	11-OCT-2021	08:32:18.176	x
RADN - R4 Stack - Low now rate alarm RADN - Stacks - R4 Stack (Gamma+Beta) reading not avail.		0	0	11-OCT-2021	01:11:34.359	x
RNG - WATER - Sextupole 2 Flow Trip (SP3 FM6)	Value Match	0	0	9-OCT-2021	23:18:38.598	x
PLANT - R80 Cooling Tower #2 Output Temp. LOW	Value Match	1	1	9-OCT-2021	04:21:38.169	x
SYNC - R6A Plant - Psu Water Pressure Low	Value Match	1	1	8-OCT-2021	14:04:05.263	x
PLANT - R4 Water HPRF CCT FLOW LOW	Value Match	1	1	8-OCT-2021	10:07:42.743	x
ISIS Low level alarms and warnings Alarm View Options Messages Image: State of the state	P					
Print History Daemon Ack Sound Editor	Msgs					
Alarm Label	State	Value	Limit	Date	Time	Ack
TGT2 - Critical params - TIA2510 Read Temperature	Upper Warning	72.1	38.0	12-OCT-2021	13:33:45.842	
TGT2 - Critical params - FIA2507 Read Flow	Lower Warning	14.6	40.0	12-OCT-2021	13:33:45.831	
TGT2 - Critical params - PIA2607 Read Temperature	Upper Warning	6.9	6.9	12-OCT-2021	12:50:34.003	
SYNC - main vacuum - SP1	I/O Error	5.0E-07	N/A	12-OCT-2021	12:46:30.906	
SYNC - main vacuum - SP2	I/O Error	5.1E-07	N/A	12-OCT-2021	12:46:22.369	
SYNC - main vacuum - SP0 gauge 2 SYNC - main vacuum - SP0 gauge 1	I/O Error	6.4E-07	N/A	12-OCT-2021	12:45:34.709	
	I/O Error	5.1E-07	N/A		12:45:25.645	
			0.00	AA OOT COOL		
TGT2 - Critical params - PI2601 Read Pressure	Lower Warning	0.30	0.30	11-OCT-2021	23:40:01.477	X
TGT2 - Critical params - Pl2601 Read Pressure SYNC - Kicker Feed temperature #47	Lower Warning I/O Error	0.30 0.0	N/A	11-OCT-2021	13:37:53.397	Х
TGT2 - Critical params - Pl2601 Read Pressure SYNC - Kicker Feed temperature #47 SYNC - Kicker Feed temperature #48	Lower Warning I/O Error I/O Error	<mark>0.30</mark> 0.0 0.0	N/A N/A	11-OCT-2021 11-OCT-2021	13:37:53.397 13:37:53.397	X X
TGT2 - Critical params - PI2601 Read Pressure SYNC - Kicker Feed temperature #47 SYNC - Kicker Feed temperature #48 SYNC - Kicker Feed temperature #45	Lower Warning I/O Error I/O Error I/O Error	0.30 0.0 0.0 0.0 0.0	N/A N/A N/A	11-OCT-2021 11-OCT-2021 11-OCT-2021	13:37:53.397 13:37:53.397 13:37:53.396	X X X
TGT2 - Critical params - Pl2601 Read Pressure SYNC - Kicker Feed temperature #47 SYNC - Kicker Feed temperature #48	Lower Warning I/O Error I/O Error	<mark>0.30</mark> 0.0 0.0	N/A N/A	11-OCT-2021 11-OCT-2021	13:37:53.397 13:37:53.397	X X X X
TGT2 - Critical params - PI2601 Read Pressure SYNC - Kicker Feed temperature #47 SYNC - Kicker Feed temperature #48 SYNC - Kicker Feed temperature #45	Lower Warning I/O Error I/O Error I/O Error	0.30 0.0 0.0 0.0 0.0	N/A N/A N/A	11-OCT-2021 11-OCT-2021 11-OCT-2021	13:37:53.397 13:37:53.397 13:37:53.396	X X X

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.

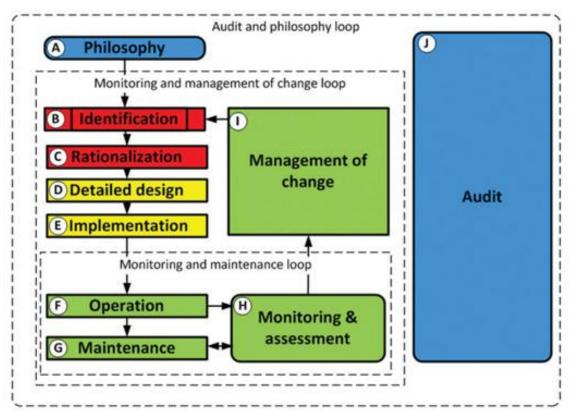


Figure 2: The Alarm Management Lifecycle as per IEC 62682 / ISA 18.2 (source: isa.org). The Alarm Management Lifecycle is an ongoing process of continuous improvement to ensure that control system alarms remain up to date and useful.



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: 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.

Alarm Suppression

							ACKNOWLE	DGEMENTS OFF
ound	s dem	0:						
NEW	NEW ALARM UNACKNOWLEDGED ALARM NEW WARNING		UNACKNOWLEGED WARNING					
s	UPPRI		OWLEDGEMENT					
		Туре	Label		Timestamp	Value	Threshold	Other
~	1	IO	Halo monitor le	ft sensor data	50	23	46	
	2	Value match	Pump 3 not running		23	46	50	
~	3	Upper alarm	Compressor co	Compressor cooling water flow		46	50	
	4	Lower alarm	Magnet timer ci	urrent	50	23	46	
	5	Upper alarm	Methane vent c	Methane vent containment flow		23	46	

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.