IChemE

IChemE Safety Centre Guidance

Lead Process Safety Metrics Alarm Rationalisation

released November 2021

Preface

This document is a supplement to the ISC Guidance Document *'Lead Process Safety Metrics – selecting tracking and learning 2015'*. This guidance note is used to provide context for alarm rationalisation which can be used for monitoring and managing the lead metric 'critical alarms per operator hour' and 'standing alarm' defined in the ISC guidance document under the human factors element.

This supplementary guidance document should be used to improve the understanding of various alarms, handling, monitoring, and meeting the target performance of the alarm management system. The document focuses on providing more clarity on the aspects and challenges in maintaining the alarm management system. This will allow for benchmarking and identification of good practice.

Acknowledgements

ISC would like to acknowledge the efforts of the following companies and people who formed the ISC Lead Metrics Working Group:

- Chevron – Eric McClellan
- Iresc Global – Sandeep Chaurasia
- Origin Energy – Les Airs
- PSRG – Robert Weber
- RAS Ltd – Carolyn Nicholls
- Safety Solutions, Australia – Garry Law
- Safety Solutions, New Zealand – Ross Benton
- Santos – Kim Pullon, Khek Wei Yong
- Snowy Hydro – Ben Nicholson
- Unilever – Liz Hallifax

Contact the ISC

safetycentre@icheme.org

Disclaimer

Definitions and terminology

The list of terms and definitions below represent the terminology used within this guidance document. They are reproduced using in combination the ANSI/ISA-18.2-2016 *Management of Alarm Systems for the Process Industry* [1] and the *EEMUA Guidance Document* [2].

Alarm	Signals which are annunciated to the operator, typically by an audible sound, some form of visual indication, usually flashing, and by the presentation of a message or some other identifier. An alarm will indicate a problem requiring operator action generally initiated by a process measurement passing a defined alarm setting as it approaches an undesirable or potentially unsafe valve. It may also indicate equipment status becoming unhealthy.
Alarm flood	Condition during which the alarm rate is greater than the operator can effectively manage (eg more than ten alarms per ten minutes) Note: it is removed when the rate drops below five alarms in ten minutes.
Alarm list	Display that lists annunciated alarms with selected information (eg date, time, priority, and alarm type).
Alarm philosophy	Document that establishes the basic definitions, principles, and processes to design, implement, and maintain an alarm system.
Alarm rate	Number of annunciated alarms, per operator, in a specific time interval.
Alarm rationalisation	Process to review potential alarms using the principles of the alarm philosophy, to select alarms for design, and to document the rationale for each alarm.
Alarm system management	Collection of processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems.
Annunciated alarms	Process and equipment alarm switches/control system logic may be used to trigger a special type of indicator device known as an alarm annunciator, which on dedicated alarm panels will be an array of indicator lights designed to secure a human operator's attention by blinking and sounding an audible buzzer when a process changes into an abnormal state. Annunciated alarms are those that have been activated to gain operator attention on the alarm panel or control room display. The alarm state may be then 'acknowledged' by an operator pushing a button or touching the alarm on the panel screen, causing the alarm to remain on (solid light) rather than blink or flash on the panel, and silencing the audible signal. The indicator light does not turn off until the actual alarm condition (the process alarm) has returned to its regular state.
Chattering alarm	Alarm that repeatedly transitions between active state and non-active state in a short period of time.
Fleeting alarm	Alarm that transitions between an active alarm state and a non-active alarm state in a short period of time without rapidly repeating.
Operator console	Interface for an operator to monitor and/or control the process, which may include multiple displays or annunciators, and defines the boundaries of the operator's span of control.
Shelved alarm	Temporarily suppresses an alarm, initiated by the operator, with engineering controls (eg time-limited) that unsuppressed the alarm. Note [2]: The operator is able to temporarily prevent an alarm from being displayed when it is causing a nuisance. A shelved alarm will be removed from the list and will not re-annunciate until un-shelved.
Stale alarm	Alarm that remains annunciated for an extended period of time (eg 24 hours). Note [2]: A standing alarm, which has been active for an extended period (eg 24 hours).
Standing alarm	An alarm is standing whilst the condition persists (raised and standing are often used interchangeably) [2].
Suppress	Prevent the annunciation of the alarm to the operator when the alarm is active. For example: shelve, suppress by design, remove from service.

Table 1. Definitions and terminology used in this document.

How to use this guidance

This guidance helps to identify suitable performance metrics relating to alarm rationalisation for an organisation. These metrics have been tested and used in different industries and have been found to provide value and help guide decision making.

Recommended steps on how to implement this guidance:

1. Determine the scope for implementation:
   - are the metrics to be applied across an entire organisation or an individual facility?
2. Map your current leading metrics to the list in table 2:
   - you may find you are already recording some of these metrics, or very similar ones.
3. Determine any gaps between your current metrics and the metrics outlined in table 2.
4. Where gaps are identified, determine if you have other metrics to cover them:
   a. where you have metrics covering the gaps, and they are useful, continue to record them;
   b. if the metrics covering the gaps are not useful, consider adopting the metrics in this guidance; and
   c. ensure that you have a comprehensive picture of the 'health' of your alarm and operator response barriers with the metrics that you are recording.
5. Develop an action plan to address the gaps identified:
   - review the implementation section of each metric to see how challenges can be overcome.

Scope of this document

The scope of the guidance document is to assist with how to approach alarm rationalisation, guided by leading metrics to achieve consistency across industries. This guidance is aimed at existing facilities.

The document provides a general context on alarm management and how to develop an alarm management philosophy to put in place the rationalisation structure.

The guidance provides options on approaches for rationalisation based on the use of metrics and provides a list of metrics. These metrics can be used across industries.

The alarm system management lifecycle

Alarm system management is the integration of instrumentation engineering and human factors (or 'ergonomics') to manage the design and implementation of an alarm system to increase its usability. Without alarm system management, the performance of any alarm system will deteriorate over time. Alarm system shortcomings cause a multitude of avoidable incidents which increase the risks to people, environment, and plant equipment, and also increase operating costs.

Improving alarm systems is not a one-off project, it has to continue through the lifecycle of the plant. Alarm changes should be controlled by management of change and effectiveness monitored as part of the safety management system.

ANSI/ISA-18.2-2016 Standard [1] outlines the alarm system management lifecycle as reproduced from the *EEMUA 191 guidance* [2] on figure 1, to demonstrate the different areas. Those circled in green are the focus areas in this guidance.

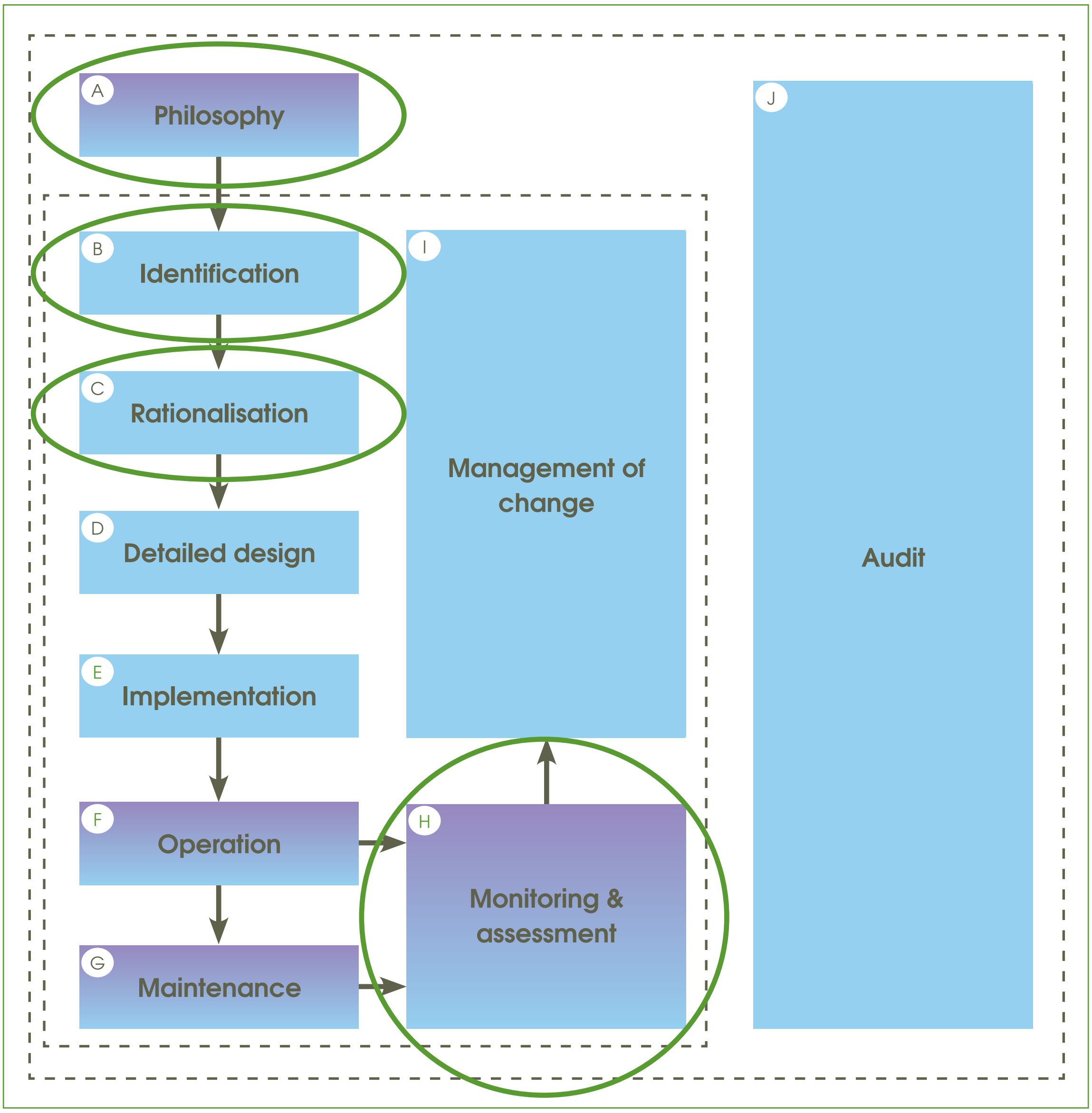

Figure 1. Alarm system management lifecycle (reproduced from *EEMUA 191 guidance* [2]).

Detailed discussion on alarm rationalisation lifecycle items

This document provides metrics that can be used to influence the approach to rationalising existing systems and so focuses on areas indicated as:

A – Philosophy

B – Identification

C – Rationalisation

H – Monitoring and assessment.

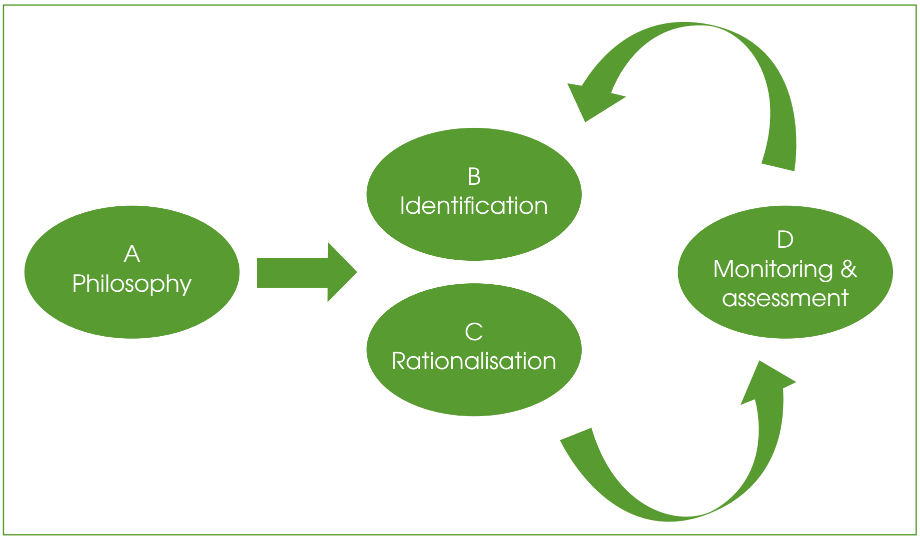

Figure 2. The feedback loop of the four areas (produced by the working group based on the *EEMUA 191 Guidance* [2]).

The monitoring step of the lifecycle becomes an important input into the rationalisation process. As you rationalise, there should be clear feedback in the metrics, showing improvements for the changes made. This continuous feedback loop is illustrated in the diagram above.

A – Philosophy

An alarm philosophy is the foundation of good alarm management, and it provides the basis of design and operation for a company's alarm systems. It covers all phases of the alarm management system (see figure 1). Without a clear and detailed alarm philosophy, where roles, responsibilities and monitoring are well defined, the alarm system will not be robust, and the performance of the system will not be effective and will continue to deteriorate over time.

Note: *ISA 18.2/IEC62682* suggests an alarm philosophy document contents list; *EEMUA 191* and the *Alarm Management Handbook* has further supporting information for content [3].

Only with a clear alarm philosophy setting the standards and outlining the requirements of the alarm system, can successful rationalisation be completed, and the alarm system performance then be measured against it.

Some common pitfalls emerge where there is no clear philosophy, these include:

- inconsistent nomenclature, particularly in systems which have expanded or modified over time;
- inconsistent alarm priority assignment; and
- multiple alarms due to both the alarm causes/inputs and effects being shown with similar priority.

B – Identification

Identification is the stage of alarm management where the possible need for an alarm or a change to an alarm is identified. For a new facility or large changes to the existing plant this should be done at the design stage and information about the need for alarms gathered from sources such as the hazard identification reviews and safety/risk studies or piping and Instrumentation diagram (P&ID) and related design reviews. For existing facilities, a tag/alarm database already exists, but it is often unclear how decisions were made as to why an alarm exists.

Obtaining the operator's feedback in the rationalisation process is important in ensuring effective alarms. *The HSE Information Sheet* [4] provides some good questions to ask operators.

C – Rationalisation

As per the *standard* [1], rationalisation is the process by which we select potential/existing alarms and review them to provide context and determine the appropriate configuration. To decide where to start rationalisation at an existing facility, a review of the performance of the alarm system is essential. Rationalisation includes the prioritisation of an alarm based on the method defined in the alarm philosophy.

Plant upgrades or after retrospective/Delta HAZOP review activities that introduce a large number of new alarms or review the safeguarding reasons for existing alarms, may be an appropriate time to consider an alarm rationalisation review.

Alarm rationalisation is a team effort, and a facilitator is needed for it to be effective. The team requires experts from a range of disciplines.

Alarm rationalisation approach

A full rationalisation of the entire alarm list can be very resource intensive, at the same time it also provides the most holistic way of standardising alarms across an operator console. Although essential for a new design, it may be acceptable for an existing facility to consider a 'bad actor' resolution approach. 'Bad actors' are alarms that repeat frequently and unnecessarily. These are considered the 'low hanging fruit' and will provide a large impact for a relatively small amount of effort.

Use a review of the alarm system metrics in table 1 to determine if the current configuration is acceptable (ie meeting target). If this is the case, a simple 'bad actor' alarm resolution may be sufficient.

If the configuration of the alarm system is deemed to be poor, or bad actor resolution has already been completed and metrics are still not meeting the suggested targets, then a more detailed rationalisation of the full alarm list should be carried out and/or implement the use of enhanced and advanced alarm methods.

One of the key indicators in determining if you have a good (acceptable) or a bad system is the annunciated priority distribution. If the distribution deviates significantly from the targets suggested in table 1, it can be detrimental to change priorities on an alarm-by-alarm basis (ie 'bad actor' resolution) and a fuller rationalisation will be needed.

It may also be possible to determine if there are issues in usability of the system through auditing.

Typical output from a rationalisation process is identification of a number of improvement recommendations which should be considered together for their combined effect.

It is possible to analyse the likely performance improvement effect of rationalisation proposed changes by considering the alarm performance of the past month or year and considering how that would look had the proposed changes already been in place.

Any agreed changes should be managed through a change approval process.

Where the recommendation is to carry out a large-scale alarm re-design, this should be managed in association with a robust hazard analysis and risk management process such as HAZOP, LOPA, bowtie review or similar. Any new or changed risk reduction credit taken for alarms and related operator response should be documented in these studies with reasoning aligned to the alarm rationalisation process.

H – Monitoring and assessment

To ensure that it is usable and effective, the alarm system performance should be assessed during commissioning and then regularly audited in operation. Performance monitoring will identify issues with alarms. This requires a real and continuing commitment by the senior facility management in consultation with operations and engineering.

EEMUA 191 [2] defines a 'robust' alarm system as:

- reliable during all plant modes including normal operation and plant upset;
- operators have a high degree of confidence in the alarm system and have time to read and understand all alarms.

Effective alarm monitoring needs to include metrics relevant to all plant states and may consist of measured values or could take the form of a survey or operator interviews.

Average alarms per hour (or other set time period) is a good starting point for monitoring normal plant operation, but operators do not really need alarms when the plant is stable. The time at which a robust alarm system becomes its most useful is during a plant upset and this is when most alarm systems fail.

This document splits the metrics into three categories:

- stable plant metrics;
- unstable plant metrics;
- configuration metrics.

Stable plant metrics

These metrics provide an indication of how well the alarm system operates under normal conditions. They help to establish if a system is only delivering relevant alarms to the operators. Stable metrics provide insight to the plant operator's mode of operation, it can show if the operators are able to be proactive, are reactive or overloaded. Poor performance of stable plant alarm metric is an immediate indication that operators will not believe the validity of all alarms coming in and develop habits of ignoring them.

Stable plant metrics are:

- average alarm rate per operator;
- standing alarms/stale alarms;
- shelved alarms.

Unstable plant metrics

These metrics provide an indication of how well the alarm system operates under unstable conditions. They help to establish the effectiveness of the alarm system when it is really needed. Unstable metrics provide insight into how quickly and efficiently an operator can assess the cause of plant upsets and take the appropriate corrective actions. Poor performance of unstable alarm metric is an indication that the operator is likely to be alerted to the problem but abandon the alarms in favour of finding the cause of the problem by some other means. A robust alarm system should direct the operator straight to the cause with as little noise as possible.

Unstable plant metrics are:

- peak alarm rate per operator;
- percentage of time in flood.

Configuration metrics

Configuration metrics are used for identification of bad actors to rationalise. If an alarm is configured poorly an operator will not trust it. Metrics can be used to recognise poor alarm configuration and identify the means by which to improve it. Configuration metrics provide insight as to how much an operator will trust an alarm system or normalise poorly performing alarms.

Configuration metrics include:

- frequently occurring alarms;
- chattering and fleeting alarms;
- alarm priority distribution (high, medium, low priority alarms see in table 2) for configured alarms and annunciate alarms over a defined period of time.

In table 2, a range of typically useful metrics are provided, along with a suggestion on how those metrics can be used to indicate what rationalisation approach may be appropriate. In most cases the starting point is bad actor resolution, but in a few cases, the metric is likely to be indicating a more serious problem, and full rationalisation should be carried out straight away.

Suggested metrics

Alarm performance metrics						
Metric	Performance category			Function/purpose of the metrics (around human factors)	Potential rationalisation methods	Reference
	Target	Sub-optimal	Poor			
Stable plant metrics						
Annunciated alarms per ten minutes per operator console	~1*	~2*	>2	It is expected that on an average basis, operator takes ten minutes to evaluate the situation, take corrective action and see the reversal of process parameter before they are ready to handle the next alarm. Continued higher alarm rate may require resources optimisation.	Bad actor resolution. If rates continue to be high – full rationalisation.	(*) IEC/ISA/EEMUA Steady state Peak load for long term
No. of stale alarms	<5* <10^	≤20	>20	Indication of violation of safe operating limit, poor maintenance, poor rationalisation.	Bad actor resolution of stale alarm list.	(*) IEC/ISA (^) EEMUA Steady state
Unstable plant metrics						
Maximum no. of alarm in a ten minute period	≤10*	≤20^	>20	It is prudent to expect more alarms during certain timing (eg regeneration, heating/cooling, backwashing, step changeover, ageing of the catalyst). Also, no. of alarms may vary due to external factor (eg day time, night time, rainy session). Max alarm rate on monthly basis may also provide indication of effective alarm system.	Bad actor resolution. If rates continue to be high – full rationalisation.	(*) IEC/ISA (^) EEMUA Abnormal/upset
Percentage of time the alarm system is in a flood condition[1]	<1%*	≤2.5%	>2.5%		Bad actor resolution. Implement enhanced and advanced alarm methods, see ISA 18.2 Section 12.	(*) IEC/ISA Abnormal/upset

[1] The performance category target suggested in table 2 is based on large scale process industry with centralised control room. For other industry and smaller plants, it may be appropriate to calibrate the table.

Configuration metrics						
Percentage contribution of the top ten most frequent alarms to the overall alarm load.	<1%*	≤5%*	>5%	80/20 rule, by targeting the 'low hanging fruit' we will resolve a large portion of the problem. This provides the greatest potential for ease in alarm load reduction with minimal effort.	Bad actor resolution.	(*) IEC/ISA Configuration
Quantity of chattering and fleeting alarms.	<1*	≤5	>5	Indicative of hardware faults, not applying default filtering parameters such as deadbands, and delays.	Bad actor resolution.	(*) IEC/ISA Configuration
Annunciated priority distribution.	3 priorities: ~80 % low, ~15 % medium, ~5 % high			The more of the highest priority alarms indicate either the plant is grossly unsafe *or* alarms are assigned wrong priority.	Full rationalisation.	(*) IEC/ISA/EEMUA Configuration

Table 2. Alarm rationalisation metrics[2].

[2] These benchmarks apply across process industries with centralised control rooms. Different industries with different systems will need to calibrate to their situation – and guidance such as EEMUA guides how to go about that.

References

[1] ISA 18.2/IEC62682 – American National Standard ANSI/ISA-18.2-2016 *Management of Alarm Systems for the Process Industries*. ISBN: 978 1 941546 86 4. USA, 2016.

[2] EEMUA 191 – *The Engineering Equipment and Materials Users Association: Alarm systems Guide to design, management and procurement* PUBLICATION 191 Edition 3. ISBN 978 0 859311 92 2. England, 2013.

[3] B. Hollifield, E. Habibi – *The Alarm Management Handbook* – PAS, Inc; 2nd edition. ISBN 978 0 977896 92 9. USA, 2010.

[4] HSE Information Sheet – *Better Alarm Handling Chemicals Sheet No. 6* (CHIS6). UK Health and Safety Executive. Great Britain, 2000.

Contact us for further information

UK
+44 (0)1788 578214
membersupport@icheme.org

Australia
+61 (0)3 9642 4494
austmembers@icheme.org

Malaysia
malaysianmembers@icheme.org

New Zealand
+64 (0)4 473 4398
nzmembers@icheme.org

www.icheme.org

Incorporated by Royal Charter 1957. The Institution of Chemical Engineers (trading as IChemE) is a registered charity in England and Wales (214379) and Scotland (SC039661). The Institution also has associated entities in Australia, Malaysia and New Zealand.

LC 0067_23