Guidance for optimising operator plant situational awareness by rationalising control room alarms

energy institute

GUIDANCE FOR OPTIMISING OPERATOR PLANT SITUATIONAL AWARENESS BY RATIONALISING CONTROL ROOM ALARMS

1st edition

July 2016

The Energy Institute (EI) is the chartered professional membership body for the energy industry, supporting over 23 000 individuals working in or studying energy and 250 energy companies worldwide. The EI provides learning and networking opportunities to support professional development, as well as professional recognition and technical and scientific knowledge resources on energy in all its forms and applications.

The EI's purpose is to develop and disseminate knowledge, skills and good practice towards a safe, secure and sustainable energy system. In fulfilling this mission, the EI addresses the depth and breadth of the energy sector, from fuels and fuels distribution to health and safety, sustainability and the environment. It also informs policy by providing a platform for debate and scientifically-sound information on energy issues.

The EI is licensed by:

- the Engineering Council to award Chartered, Incorporated and Engineering Technician status;
- the Science Council to award Chartered Scientist status, and
- the Society for the Environment to award Chartered Environmentalist status.

It also offers its own Chartered Energy Engineer, Chartered Petroleum Engineer and Chartered Energy Manager titles.

A registered charity, the EI serves society with independence, professionalism and a wealth of expertise in all energy matters.

This publication has been produced as a result of work carried out within the Technical Team of the EI, funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost-effective, value-adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and internationally.

For further information, please visit **http://www.energyinst.org**

The EI gratefully acknowledges the financial contributions towards the scientific and technical programme
from the following companies

BP Exploration Operating Co Ltd
BP Oil UK Ltd
Centrica
Chevron
CLH
ConocoPhillips Ltd
DCC Energy
DONG Energy
EDF Energy
ENGIE
ENI
E. ON UK
ExxonMobil International Ltd
Kuwait Petroleum International Ltd
Maersk Oil North Sea UK Limited
Nexen
Phillips 66
Qatar Petroleum
RWE npower
Saudi Aramco
Scottish Power
SGS
Shell UK Oil Products Limited
Shell U.K. Exploration and Production Ltd
SSE
Statkraft
Statoil
Talisman Sinopec Energy (UK) Ltd
Tesoro
Total E&P UK Limited
Total UK Limited
Tullow Oil
Valero
Vattenfall
Vitol
World Fuel Services

However, it should be noted that the above organisations have not all been directly involved in the development of this publication, nor do they necessarily endorse its content.

ISBN 978 0 85293 914 7

Published by the Energy Institute

The information contained in this publication is provided for general information purposes only. Whilst the Energy Institute and the contributors have applied reasonable care in developing this publication, no representations or warranties, express or implied, are made by the Energy Institute or any of the contributors concerning the applicability, suitability, accuracy or completeness of the information contained herein and the Energy Institute and the contributors accept no responsibility whatsoever for the use of this information. Neither the Energy Institute nor any of the contributors shall be liable in any way for any liability, loss, cost or damage incurred as a result of the receipt or use of the information contained herein.

Hard copy and electronic access to EI and IP publications is available via our website, **https://publishing.energyinst.org**.
Documents can be purchased online as downloadable pdfs or on an annual subscription for single users and companies.
For more information, contact the EI Publications Team.
e: **pubs@energyinst.org**

Contents

Pages

Foreword 5

Acknowledgements 6

1 Introduction 7
1.1 Aim 7
1.2 Who should use this publication? 8

2 Introduction to alarms and situation awareness 9
2.1 What are alarms for? 9
2.2 Alarm design principles 10
2.3 Alerts VS alarms 10
2.4 Situation awareness. 11
2.4.1 Inputs to situation awareness 11
2.4.2 Elements of situation awareness. 11

3 Wider issues affecting alarm management and rationalisation 14
3.1 The nature of an existing alarm system 14
3.2 Different operating contexts 14
3.3 Other inputs to situation awareness. 15
3.4 Alarm floods 15

4 Alarm performance targets 17
4.1 What is the right number of alarms? 17

5 Individual alarm usability assessment 19
5.1 Background 19
5.1.1 Why reducing alarm numbers by itself is not sufficient 19
5.1.2 Improving process system performance 19
5.2 Overview of approach to usability assessment 20
5.2.1 The review team composition. 20
5.2.2 Resources required for the review. 20
5.2.3 Proactive and reactive assessment 21
5.3 Stage 1: Alarm prioritisation 21
5.4 Stage 2: Usability assessment of individual alarms 22
5.4.1 Introduction 22
5.4.2 Structure of analysis 23
5.4.3 The alarm usability assessment tool 23
Table 2: Stage 1 Perception of alarm signal. 24
Table 3: Stage 2 Maintaining alarm salience until acceptance 30
Table 4: Stage 3 Diagnose the cause of the alarm. 32
Table 5: Stage 4 Plan the alarm response 35
Table 6: Stage 5 Respond to the alarm 37
5.4.4 Using the outputs of the alarm review 40

Annexes

Annex A References 41
A1 References 41
A2 Further reading 41

Contents continued...

Pages

Annex B Glossary of terms and acronyms 42
B1 Terms 42
B2 Acronyms 44

Annex C Alarms in the context of safety instrumented functions (SIFs) 45

Annex D Worked example 46

FOREWORD

Alarm rationalisation is often seen as the process of reducing the number of control room alarms that present to a control room operator (CRO), during normal and abnormal operating conditions, down to levels that are manageable, in that the CRO is able to respond to each alarm appropriately, timely and correctly, without the need for disengaging 'nuisance' alarms or resorting to other means. EEMUA 191 *Alarm systems: A guide to design, management and procurement* is a common standard many organisations work towards.

However, Energy Institute (EI) members have raised concern that conducting an alarm rationalisation is not a straightforward exercise, particularly when considering the human factors (HF) aspects of alarms, namely that alarms should be optimised to support CROs maintain situation awareness of the happenings of the plant. Whilst EEMUA 191 does contain guidance to help do this, additional guidance has been sought to help ensure that, in particular, high-priority alarms can be assessed against HF principles.

The EI Human and Organisational Factors Committee commissioned *Guidance for optimising operator plant situational awareness by rationalising control room alarms,* to do just this. This publication can be seen as a companion guide to EEMUA 191 to support organisations working towards the alarm targets set out in EEMUA 191. It provides:

- brief introductions to alarms and situation awareness;
- concise guidance on aspects of alarms that should be considered, other than the number of alarms, particularly in relation to situation awareness;
- brief overview and guidance in relation to EEMUA 191 alarm metrics, and
- a practical tool to help assess the usability of individual alarms.

The alarm usability assessment is the main deliverable of this publication. It is a simple tool, with accompanying guidance, allowing high-priority alarms (or problematic alarms) to be assessed against a simple five-stage model of how a CRO acknowledges, interprets and responds to alarms. Use of the tool will allow organisations to understand and prepare to make improvements to individual alarms and, in some cases, to the alarm system as a whole. This should be seen as a complementary approach to just simply reducing alarm numbers.

The information contained in this document is provided for general information purposes only. Whilst the EI and the contributors have applied reasonable care in developing this publication, no representations or warranties, expressed or implied, are made by the EI or any of the contributors concerning the applicability, suitability, accuracy or completeness of the information contained herein and the EI and the contributors accept no responsibility whatsoever for the use of this information. Neither the EI nor any of the contributors shall be liable in any way for any liability, loss, cost or damage incurred as a result of the receipt or use of the information contained herein.

The EI welcomes feedback on its publications. Feedback or suggested revisions should be submitted to:

Technical Department
Energy Institute
61 New Cavendish Street
London, W1G 7AR
e: technical@energyinst.org

ACKNOWLEDGEMENTS

Guidance for optimising operator plant situational awareness by rationalising control room alarms was developed by Jamie Henderson (Human Reliability Associates Ltd.) and produced by the EI Human and Organisational Factors Committee (HOFCOM). At time of publication, HOFCOM members included:

Tony Atkinson	ABB
Ed Corbett	HSL
Alix Davies	EDF Energy
Bill Gall	Kingsley Management Ltd.
Peter Jefferies	Phillips 66 (Vice-Chair)
Stuart King	EI (Secretary)
Eryl Marsh	HSE
Richard Marshall	Essar Oil UK
Rob Miles	Hu-Tech Risk Management Services Ltd (Chair)
Simon Monnington	BP plc
Helen Rycraft	IAEA
Jonathan Ryder	ExxonMobil Corporation
Rob Saunders	Shell International
Gillian Vaughan	EDF Energy
Mark Wilson	ConocoPhillips
Razif Yusoff	Shell International

Management of this project and technical editing were carried out by Stuart King (EI).

Formatting was carried out by Jack Keaney (EI).

The EI also wishes to acknowledge the following individuals who contributed to the development and/or review of this project:

Andrew Fewster	HSE
John Burnett	RWE
Andy Geddes	Scottish Power
Peter Rutherford	BP plc

Affiliations are correct at the time of contribution.

1 INTRODUCTION

1.1 AIM

The aim of this publication is to provide accessible guidance to individuals interested in improving existing control room alarm systems or designing new ones. It summarises and organises relevant available guidance on how to conduct an alarm rationalisation (to reduce the number of alarms) and discusses why factors other than the number of alarms should be considered when attempting to improve alarm system performance.

Specifically, the publication aims to help operating companies answer three questions:

- What factors should be considered when trying to improve control room operator (CRO) situation awareness?
- Are there an acceptable number of alarms?
- Do the high-priority alarms maximise the probability of successful CRO response?

To help answer these questions:

- Section 2 introduces the topics of alarms and situation awareness.
- Whilst alarm system improvements often focus on the number of alarms, section 3 aims to raise awareness of some of the other factors that influence CRO situation awareness, and to encourage their consideration when undertaking alarm system design or improvement. From the perspective of a CRO, alarms provide just one input to 'knowing what is going on around you' – sometimes called situation awareness (Flin, et al., *Safety at the sharp end*).
- Section 4 discusses alarm rationalisation and the use of alarm metrics in order to determine the number of alarms that should be in place. Whilst rationalisation is often referred to in the context of existing alarm systems, more properly it should be considered to be a part of an alarm management life cycle (e.g. as described in ISA/ANSI, *Management of alarm systems in the process industries*), performed initially as part of the system design, where proposed alarms are compared with criteria outlined in an alarm philosophy. However, often when organisations seek to improve the performance of their existing alarm systems they use the term rationalisation to mean the reduction of alarm numbers to move closer to benchmark values. Typically, such interventions are performed as engineering processes, where software is used to aggregate data on alarm system performance, allowing comparison with benchmark targets (e.g. more than one per minute in a steady state is unacceptable). Consequently, less useful alarms, such as those that provide duplicate information, may be removed, or have their priority downgraded.
- Whilst reducing the overall number of alarms is useful, individual alarms should be designed to support CROs in identifying and acting upon threatening situations. Section 5 describes a process, and provides a practical tool, for conducting an alarm usability assessment of individual high-priority alarms. To this end, some of the guidance provided in EEMUA 191 *Alarm systems: A guide to design, management and procurement* has been organised into a tool to help users complete a human factors assessment of individual alarms.

It should be noted that EI *Guidance for optimising operator plant situational awareness by rationalising control room alarms*, in particular the usability assessment tool in section 5, draws heavily on the information presented in EEMUA 191, which is a fairly common standard that many organisations use. Information provided in the other relevant documents may be equally useful, such as IEC 62682 (*Management of alarm systems for the process industries*) and ANSI/ISA S18.2 (ISA, *Management of alarm systems in the process industries*). However, to make it as easy as possible for users of this publication to find further information, a decision was taken to draw primarily on one source. Therefore this publication can, in part, be seen as a companion guide to EEMUA 191.

1.2 WHO SHOULD USE THIS PUBLICATION?

This publication is intended to be used by individuals with responsibility for designing, maintaining and improving alarm systems (e.g. safety engineers, process engineers, plant operators and supervisors). The primary focus is the influence of human factors (HF) on alarm handling, rather than system engineering aspects, therefore, users of this publication should not require any specific technical background.

2 INTRODUCTION TO ALARMS AND SITUATION AWARENESS

2.1 WHAT ARE ALARMS FOR?

An alarm is a signal generated by a process control system to indicate that there is a problem that requires prompt CRO action or attention. It is triggered when a process parameter reaches a pre-defined point.

The alarm signal can be visual, auditory, or both, and is intended to draw the CRO's attention to the changed state of a specific process parameter. This can help the CRO to take action to keep the plant within pre-planned operating limits, and provide insights into the current process conditions.

EEMUA 191 (P.17) characterises alarms as one of a series of layers of protection against (personal, process, environmental, economic, etc.) risks.

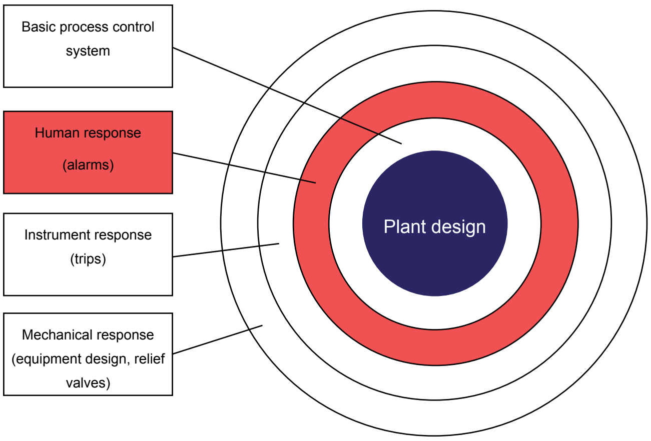
Basic process control system
Human response (alarms)
Instrument response (trips)
Mechanical response (equipment design, relief valves)
Plant design

Figure 1: Alarms as a layer of protection in a process system (adapted from EEMUA 191, P.18)

Alarms allow CROs to respond to developing process situations. In many cases, alongside the information provided by the human-machine interface (HMI), alarms give the CRO time to bring a situation under control before automated trips can take effect. This flexibility can have significant benefits. Firstly, from a production perspective, avoiding the use of trips can have significant time and cost benefits, as restarting a system following a trip is often a lengthy exercise. Secondly, from a safety and environmental perspective, by successfully responding to an alarm the CRO reduces the demands on the trip system.

In some situations there may be no associated trip or automated control measure. This means that the CRO response to an alarm is the last line of defence and therefore of even higher importance. See Annex C for more information on relevant issues when an alarm is part of a safety instrumented function (SIF).

2.2 ALARM DESIGN PRINCIPLES

EEMUA 191 lists a number of key design principles for alarms; including the following:

- The purpose of an alarm system is to direct the CRO's attention towards plant conditions requiring timely assessment or action.
- Each alarm should alert, inform and guide.
- Every alarm presented should be useful and relevant to the CRO.
- Every alarm should have a defined response.
- Adequate time should be allowed for the CRO to carry out a defined response.
- The alarm system should be explicitly designed to take account of human limitations.

EEMUA 191 contains much detail about alarm design, related management systems, alarm configuration, performance monitoring, and purchasing alarm systems. Embedded within this detail are a number of important HF principles for maximising the usability of high-priority alarms. Section 5 draws out these principles and aims to provide users with a tool for assessing the adequacy of high-priority alarms against EEMUA 191 guidance, using a simple HF framework.

Issues for alarm improvement and design – navigating the content of EEMUA 191

Whilst EEMUA 191 provides extensive guidance on the design and management of effective alarm systems, its very comprehensiveness, and the way it is organised, can make it difficult to use on an occasional basis. For example, there is extensive guidance regarding specific design principles for individual alarms, mixed with more general guidance on managerial and organisational arrangements that should be in place for alarm systems. This can make it difficult to ensure that individual alarms meet all the requirements of the guidance. Section 5 addresses this issue by organising some of the information from EEMUA 191 into a tool.

2.3 ALERTS VS ALARMS

Alerts are similar to alarms in that they also provide an indication of some change in the progress or operation of the system. However, they may not necessarily require immediate acknowledgement or action on the part of the CRO. Whereas an alarm notifies a CRO of an unwanted excursion, an alert may advise of a to-be-expected event (EEMUA, P.14). For example, an alert may advise a CRO that a particular process has reached a notable stage, such as a vessel reaching the target temperature for production to begin.

EEMUA 191 outlines some key differences between alarms and alerts (P.15):

- Alarms have limits that should not normally be violated.
- An alarm should always be acted upon immediately (unless a higher priority alarm exists).
- Ignoring an alert should not place a demand on a safety system (without first triggering an alarm).

- Alerts can be configured on an ad hoc basis to suit the control strategy of the CRO (i.e. alert set-points can be changed). Alarm set-points should not be operator configurable.
- Alerts should be suppressed in abnormal situations.

The application of alerts in an alarm system entails careful management otherwise they may contribute to problems of alarm flooding.

Issues for alarm improvement and design – differentiating between alarms and alerts

One way of reducing alarm numbers is to reclassify alarms as alerts on the basis that they do not have a defined response (EEMUA 191, P.3, for example, states that 'every alarm should have a defined response'). Whilst this is a useful rule of thumb, there may be situations (as mentioned in the associated caveats in EEMUA 191) where no physical action is required, but an alarm provides information to the CROs that allow them to make better decisions as a scenario develops. Therefore, care should be taken when removing an alarm, or reclassifying it as an alert, on the grounds that no physical response is required, to ensure that CROs' situation awareness is not adversely affected.

2.4 SITUATION AWARENESS

2.4.1 Inputs to situation awareness

EEMUA 191, particularly when discussing safety-related alarms (P.19), takes a predominantly engineering view of the CROs role in the alarm system, describing them as one component amongst many, with limited discussion of the wider operating context and its influence on decision-making.

Alarms provide just one input to situation awareness or 'knowing what is going on around you' (Flin, et al., *Safety at the sharp end*), and the choices made by a CRO will be informed by a broad range of information (e.g. shift handovers, graphical information from control displays, communications from other plant operators, CCTV feeds, weather information, and the CRO's own knowledge and understanding of the plant). The potential impact of this upon alarm rationalisation is discussed further in section 3. However, as a precursor to that discussion, 2.4.2 provides a brief introduction to the concept of situation awareness.

2.4.2 Elements of situation awareness

Three elements of situation awareness are:

- gathering information;
- interpreting information, and
- anticipating future states.

Information from alarms will be one input to the information gathering stage, but the way that this information is collected will be influenced by CRO's experience, preconceptions and understanding of the current state of the system. For example, if they believe that the part of the plant where the alarm is originating is offline, or if they have recent experience of the alarm being spurious, they may be less likely to attend to it promptly (Flin, et al., *Safety at the sharp end*, pp.22–31).

Issues for alarm improvement and design – the impact of control room design on situation awareness

Physical factors, such as the design of the control room, and the related visibility of relevant process unit information, override panels, fire and gas detection systems, and permit boards, will all affect how a CRO makes sense of an incident. For example, the investigation into the Milford Haven refinery explosion (HSE, *The explosion and fires at the Texaco Refinery*) suggested that the failure of CROs to develop an overall understanding of the incident contributed to the outcome. This may have been addressed by a well-designed process overview. Therefore, successfully addressing HF in the design of control rooms will have a significant impact on CRO situation awareness. For more information, see relevant standards for control room design such as ISO11064 (*Ergonomic design of control centres*) and EEMUA 201 (*Process plant control desks utilising human-computer interfaces*).

If an alarm system is well designed, it may aid the second element of situation awareness: interpretation of the gathered information. For example, first-out/first-up alarms on an annunciator panel may present themselves differently to subsequent alarms, to indicate where a problem originated. Again, a CRO's experience will have a significant bearing on their interpretation of a problem; people are known to be good at matching patterns of information in current situations to their prior experiences in order to determine what is happening. A related concept is the notion of mental models, where CROs update their understanding of the process as information, including alarms, is presented to them. These capabilities are what enable experienced CROs to cope with sub-optimal alarm systems and situations such as alarm floods, where too many alarms are presented to be realistically addressed in a short period of time. An experienced CRO's mental model will include their own acquired understanding of the relative value of different alarms, and consequently they will be able to focus on more important information. Less experienced CROs will have poorer mental models, and will spend longer evaluating the information they receive.

However, relying on a CRO's experience in these situations is dangerous for several reasons. In addition to the obvious problem of a CRO's mental model being incorrect, there is the well-known phenomenon of confirmation bias – where a person actively seeks information to support their initial diagnosis, and excludes conflicting information. A poor alarm system may encourage these types of human error.

The final element of situation awareness is to anticipate what is likely to happen in the future. There is a close relationship between this element and the previous two, and, as previously mentioned, there is a danger of reinforcing earlier misunderstandings. For example, based on previous interpretation, a CRO may incorrectly look for further alarms in a particular area of plant.

Issues for alarm improvement and design – understanding the contribution of alarms as one input to situation awareness

Some alarms, that appear to be candidates for removal or downgrading to alert status on the basis of their individual characteristics (e.g. because they duplicate information presented elsewhere), may have a wider importance that is not immediately apparent. This is particularly the case with alarms that have been in place for a number of years and may have formed part of a CRO's mental model (e.g. the early occurrence of an alarm may trigger a CRO to check for other symptoms of a specific problem, allowing them to maintain the process within safe parameters). Therefore, caution should be taken when proposing alarm removal, to ensure that situation awareness is not undermined.

The alarm usability assessment tool (presented in section 5), focuses on the technical aspects of an alarm system, with the primary aim of improving the usability of the system. However, by making improvements to usability, a collateral benefit should be to improve CRO situation awareness (e.g. by better supporting information gathering, interpreting, and anticipation of future states).

In addition, organisations undertaking alarm rationalisation should be conscious of broader issues such as situation awareness (and the others discussed in section 3) when undertaking alarm rationalisation. This is because the success of alarm rationalisation, or indeed any process that changes the way tasks are performed, risks being undermined by its rote application (i.e. without due consideration of the specific context of application, and the potential impact on human factors considerations).

3 WIDER ISSUES AFFECTING ALARM MANAGEMENT AND RATIONALISATION

3.1 THE NATURE OF AN EXISTING ALARM SYSTEM

In some older systems, it may be technically difficult to reduce numbers of alarms. Therefore, even if low-priority nuisance alarms have been identified, the design of the alarm system may make removing the alarm very difficult. Even where it is possible, site change-management procedures may make the removal of a single alarm a labour intensive process. Therefore, in such situations, and whilst it may not be the best approach to take from a HF perspective, interventions to improve alarm management may need to focus more on training CROs in identifying and responding to given scenarios. For example, CROs may be trained not to respond to every specific alarm, but instead to use alarm patterns to identify symptoms of scenarios, that will trigger pre-defined responses aimed at bringing the situations under control.

There may also be some features of alarm systems that are not covered by the available guidance. For example, in some systems, CROs may have to establish that two alarms agree before taking action.

Issues for alarm improvement and design – limits imposed by the design of the existing alarm system

The design of some, typically older, alarm systems may make it difficult to rationalise alarms in the manner suggested by EEMUA 191. In these situations, other strategies may need to be adopted to improve the probability of successful CRO response (e.g. scenario-focused training).

3.2 DIFFERENT OPERATING CONTEXTS

A related issue is that there are many different operating contexts in which alarms are employed, and the nature of the specific operating context under consideration may define the extent to which the principles set out in EEMUA 191 (and organised in section 5) can be applied. For example, a simple oil terminal may have a relatively low number of high-priority alarms when compared to a nuclear processing plant. The former situation, where it is realistic for the CRO to identify, interpret and act on individual alarms, is well addressed by the guidance in section 5. However, the latter situation, where the CRO may have to rely more on strategies such as pattern matching to determine the likely cause of the developing scenario, may be less well addressed. Ideally, where this is the case, steps will be taken to reduce alarm numbers, but this may not always be possible (see 3.1).

Issues for alarm improvement and design – taking account of different operating contexts

The nature of the operating environment may affect an organisation's ability to reduce alarm numbers in the manner suggested by EEMUA 191 and in section 4 of this guidance. Therefore, existing CRO response strategies should be evaluated prior to embarking on an improvement programme (e.g. do they seek to identify and respond to every alarm individually or do they concentrate on using alarms to identify scenario-types, and respond accordingly?).

3.3 OTHER INPUTS TO SITUATION AWARENESS

The information that a CRO receives from alarms is just one input to their overall understanding of a developing situation. As previously mentioned, they will update their mental model of the current status of the process based on the alarms they are presented with, but also using other information (e.g. communications from colleagues, CCTV, display screens, shift logs).

Issues for alarm improvement and design – other sources of information

The availability of relevant information sources should be considered when undertaking alarm improvements, and, in particular, when trying to optimise the usability of individual alarms. For example, having been notified of a developing situation by an alarm, the CRO may seek to confirm this event by checking CCTV and obtaining confirmation from a field operator. This may have an impact on the amount of time required between an alarm sounding and action being taken. From a design perspective, for important alarms, consideration could be given to automatically providing specific HMI displays that provide all of the required information (e.g. trends) and buttons to deal with the situation.

3.4 ALARM FLOODS

Whilst a CRO may be able to identify and respond to alarms relatively easily during normal periods of operation, the more significant challenge is to manage alarms during upset conditions, where a CRO might be presented with a large number of alarms in a short period of time.

The number of alarms presented in an upset condition is one of the key measures typically used in alarm reduction programmes (see section 4). A well-managed alarm improvement programme should, over time, reduce the extent and severity of alarm floods through alarm removal and reclassification. However, if this is the only action taken, there is a danger that the focus of this analysis will be solely on less important, but frequently occurring, alarms with little or no consideration of the characteristics of higher priority-alarms.

A different approach to management of alarm floods is to improve the usability of alarms in upset conditions (e.g. by using dynamic suppression, filtering by priority – EEMUA 191 provides more detailed guidance on the types of technical measures that can be employed to improve the presentation of alarms during upsets). Improving the usability of an alarm should influence a CRO's experience of that alarm, including during times of upset. To support the process of improving alarm usability, section 5 includes a consideration of some of the factors that might be addressed to improve individual alarm performance.

These should be seen as complementary approaches. Using alarm system metrics to target and, where possible, eliminate so called bad-actors will reduce overall alarm numbers. However, examining and improving the usability of high-priority alarms should also improve the CRO's experience of these alarms and, in so doing, improve reliability of response. It is also probable that changes to alarm usability will help to reduce the frequency with which they occur.

Issues for alarm improvement and design – relationship of alarm improvement programmes to alarm floods

A systematic process of alarm reduction, particularly when used in conjunction with other technical approaches such as dynamic suppression and filtering, should, over time, improve a CRO’s experience of alarm floods by reducing the load on the CRO during upset conditions. Furthermore, a detailed alarm usability review, such as that described in section 5, examines design features of the alarm system which, if optimised, should improve CROs’ ability to respond in periods of high alarm load.

4 ALARM PERFORMANCE TARGETS

4.1 WHAT IS THE RIGHT NUMBER OF ALARMS?

By defining targets for alarm performance, sites can monitor and analyse the reasons for failing to meet performance targets, and take action to improve performance (e.g. by removing bad-actors). Software is available to support these analyses.

In order to set performance targets, benchmark figures should be used. One commonly used source of information are the benchmark figures set out in EEMUA 191. If adhered to, these should lead to manageable CRO workload. Often, sites use these benchmarks and measures as key performance indicators (KPIs) to assess the performance of their own alarm system, and to identify areas for improvement. Some of the key measures are summarised in Table 1.

Table 1: Benchmark target for alarms from EEMUA 191

Nature of target	Measure/target	Demands on CRO
Acceptable average alarm rate whilst a plant is in steady state (P.96,100) This is the alarm rate over a time period (e.g. an hour or a shift) and provides an insight into CRO workload. A high rate indicates that CROs will spend much of their time responding to alarms, rather than monitoring and controlling the system. No more than a third of a CRO's time should be spent on alarm analysis and rectification (P.95).	More than one alarm per minute	Very likely to be unacceptable
	Two alarms per two minutes	Likely to be over-demanding
	One alarm per five minutes	Manageable
	Less than one alarmper 10 minutes	Very likely to be acceptable
Percentage of time outside acceptable average alarm rate (p.99,100) (one alarm per 10 minutes) Where the long-term average alarm rate provides an insight into CRO workload, this measure indicates the duration of elevated workloads as a proportion of overall time in control of the process.	A target of less than 10 % spent outside acceptable average alarm rate	
Number of alarms during an upset (P.97,101) This is the short-term workload for a CRO following a plant upset. It is measured over a 10 minute period and may be most relevant to continuous processes. The term alarm flood is often used to describe a situation where a CRO struggles to respond to the number of alarms being presented. It is defined here as more than 10 alarms in a 10 minute period.	More than 100 alarms	Excessive and likely to result in CRO abandoning the system
	20–100 alarms	Hard to cope with
	Under 10 alarms	Should be manageable

Table 1: Benchmark target for alarms from EEMUA 191 (Continued)

Nature of target	Measure/target	Demands on CRO
Percentage of time upset rates are outside acceptable target (P.99, 101) (under 10 alarms per 10 minutes) This is a measure of the proportion of time, during upset conditions, where the alarm rate is outside the target number of less than 10 alarms in a 10 minute period.	A target of less than 1 %	
Alarm priority distribution (P.98) This provides an insight into the risk profile of the alarm system and gives an alternative indication of probable CRO workload. If a disproportionately large number of the total alarms are assigned critical- or high- priority, this may suggest fundamental issues with the system safety, or that a large number of alarms have been incorrectly prioritised. Moreover, a large proportion of critical- and high- priority alarms may also result in high workload levels during an upset.	High-priority 5 % target	
	Medium-priority 15% target	
	Low-priority 80 % target	
	About 20 critical alarms in total	
Average number of standing alarms (P.99, 102) High numbers of standing alarms may interfere with a CRO's ability to use an alarm system, as well as indicating a possible failure to properly maintain the plant.	A target of less than 10 for average number of standing alarms	
Average number of shelved alarms (P.99, 102) These are alarms related to systems that are redundant or out-of-service.	A target of less than 30 for average number of shelved alarms	

The measures and benchmarks set out in Table 1 offer a means for assessing the usability of an alarm system. Typically, once an organisation has reviewed its alarm system against these benchmarks, it will use the results to try and improve performance. This may be done, for example, by examining the top ten most frequently occurring alarms, and removing them, if possible, or reconfiguring them to make them more useful. Sometimes this is done as a one-off project, but for a more sustained approach to alarm management, the outputs from the rationalisation process are analysed on a regular basis (e.g. quarterly) in order to identify areas for improvement.

5 INDIVIDUAL ALARM USABILITY ASSESSMENT

5.1 BACKGROUND

5.1.1 Why reducing alarm numbers by itself is not sufficient

Whilst comparing alarm system performance against benchmark values will be likely to improve the performance of an alarm system over time, it may mean that specific issues with individual high-priority alarms are not addressed.

For example, having identified an alarm that occurs too frequently, an organisation may decide to change the alarm trigger set-point to a higher temperature, pressure or flow rate, meaning that it occurs less frequently. However, other features of the alarm that will influence the probability of a successful response may not have been addressed (e.g. alarm presentation, appropriateness of alarm type, information about response, differentiation from other alarms).

Furthermore, such an approach is reactive. Many problem alarms (also known as bad-actors) identified in this way may not be the most important alarms in the system. Whilst bad-actors may distract the CRO, directing improvement strategies solely at these alarms means that the performance of more important alarms may not be evaluated. The highest priority alarms will typically be those that occur with the lowest frequency. Therefore, a rationalisation process that focuses solely on frequently occurring alarms might mean that important factors affecting the usability of high-priority alarms are never formally assessed.

Issues for alarm improvement and design – assessing the usability of high-priority alarms

Focusing improvement efforts solely on alarm rationalisation (by evaluating performance against benchmark targets) may mean that the performance of infrequently occurring, high-priority alarms is neglected. Ensure that some analysis effort is devoted to ensuring that high-priority alarms give CROs the best chance of a successful response (e.g. by allowing sufficient time to act, providing training in required responses, ensuring that alarm information is clear).

A complementary approach, such as that set out in the remainder of this section, is to carry out a review, to systematically analyse the characteristics of the most important alarms to ensure that they best support CRO performance. This proactive, risk-based, strategy complements the more reactive rationalisation approach set out in section 4. It aims to identify issues with the potential to affect successful CRO response to individual alarms, and deficiencies that contribute to the overall number of unnecessary or unwanted alarms (hence addressing alarm flooding).

5.1.2 Improving process system performance

In some cases, before attempting to reduce alarm numbers, it may be worth examining process performance in general. The generation of alarms, and hence the performance of the alarm system, is closely linked to the performance of control loops, and the ability of the process plant to consistently operate within limits. It will be difficult for alarm reduction programmes to improve alarm performance if the process performance is poor. In these situations, CROs will spend a great deal of their time and effort compensating for a poorly designed, or executed, process system that will, in turn, undermine their ability to react effectively to process problems. Conversely, a well-designed interface will aid the CRO in anticipating and heading-off process deviations before an alarm is triggered, thus reducing the overall alarm load.

5.2 OVERVIEW OF APPROACH TO USABILITY ASSESSMENT

The usability assessment is a team-based, risk-based approach to review and assess the usability of individual alarms. Alarm usability is the degree to which the alarm supports a CRO in successfully responding to the process condition notified by the alarm. For example, if the alarm allows the CRO sufficient time to act, is differentiated from other less important alarms, and has a clearly defined response, then the probability of a successful response will be higher than if this were not the case.

It is a two-stage process. The first is to prioritise the existing alarms; most organisations will have their own ways of doing this, but different possible approaches are discussed in 5.3. Whilst the second stage, the evaluation process (5.4), is relatively quick, the effort applied should be directed at the most important alarms to maximise the benefit.

5.2.1 The review team composition

It is likely that the review team will include similar individuals to those already involved in periodic site alarm reviews:

- An experienced CRO – Involvement of a frontline operator is essential for this process. These individuals have the detailed knowledge and understanding of the alarm system needed for the review. If possible, more than one individual should participate, to enable sharing of experience and discussion of opinions.
- Alarm system engineer/manager – This individual will have a detailed understanding of the capabilities of the alarm system. It is possible that the review will lead to recommendations to change the functionality of the alarm system. It is therefore important that there is input from someone who understands the alarm system deficiencies identified during the review and who can recommend practicable improvements to the system which will address the identified issues.
- Site safety engineer/process safety specialist – This individual can offer additional insights during the alarm analysis process and outline how the outputs of the review process affect, or are affected by, wider site risk analyses (e.g. risk analysis findings from hazard and operability assessments (HAZOPs), hazard identification studies (HAZIDs), layer of protection analyses (LOPAs) and safety integrity level (SIL) assessments).

It may also be useful to involve someone with a background in HF issues in the review team to ensure that issues such as those raised in section 3, such as potential impact on situation awareness, are considered.

5.2.2 Resources required for the review

- Access to the alarm system (or simulator) – Some of the areas explored in the detailed alarm usability assessment will be most easily answered by interacting with the alarm system itself. For example, establishing the information that is displayed to the CRO when an alarm activates. Some organisations will have simulators that mimic the properties of the actual plant which could be used as an alternative.

- Alarm database document (where this exists) – If the organisation has a detailed database summarising the properties of individual alarms (e.g. purpose, alarm types, set-points, required responses), this will be an invaluable resource, as many of these issues are explored during the detailed alarm usability assessment. If such a document does not exist, the analysis could be used to help develop one.
- Related safety analyses – For example, if a site has undertaken LOPA, that has considered individual alarms, these documents should be referred to in the review process to ensure that any proposed alterations take account of all relevant issues.

Issues for alarm improvement and design – relationship to risk management

When undertaking alarm rationalisation, the purpose of alarms should be considered in the context of wider risk management. For example, one organisation consulted during the development of this publication had undertaken a process of rationalisation and removed or reclassified a number of alarms based on the input of experienced CROs. However, a subsequent process safety risk assessment meant that a number of these alarms had to be reinstated, as they were needed to contribute to specified layers of protection. This illustrates the importance of having a balanced review team (including both CROs and process safety specialists), and of documenting the purpose of alarms for reference when any future changes are proposed.

5.2.3 Proactive and reactive assessment

The usability assessment tool has been designed primarily for proactive use. The intention being that high-priority alarms will be identified using a prioritisation process (see 5.3) and then analysed. However, the process could also be used reactively, to analyse, for example, a bad-actor alarm that has been identified in an alarm rationalisation exercise, or a specific alarm that has been identified in an incident investigation. It may also be used as a checklist to inform the design of an alarm system, to ensure that proposed high priority alarms meet usability requirements.

5.3 STAGE 1: ALARM PRIORITISATION

The first stage of the usability assessment is to prioritise the alarms in terms of importance. Every process plant is likely to have its own criteria for prioritising alarms. Outcomes that alarms help to protect against might include process safety issues, such as unsafe temperatures or pressures, but could equally include production issues, such as spoiling of a product, or environmental issues, such as high levels in effluent storage. All of these are important in their own way, so an organisation might, for example, have a risk assessment matrix that enables different types of outcomes to be compared.

It should be noted that prioritisation should only support a CRO, in times of high alarm activity, to decide which alarms should be dealt with first, not which alarms can be ignored (EEMUA 191, P.29). In other words, all alarms should require an action of the CRO. If they do not, then their status as an alarm should be reviewed.

If the existing alarm prioritisation is considered reasonable (i.e. it provides an accurate and reliable reflection of alarm importance), then it may also form the basis for deciding which alarms should be subjected to the detailed alarm review that follows. For example, a site may decide that all of their alarms categorised as high priority should be subject to the usability review. Or they may decide that high-priority alarms that protect against a process safety hazard should be reviewed first. Prior to carrying out the usability analysis on a specific alarm, it should be checked to ensure that it has been correctly prioritised and requires a CRO response.

If a site is unhappy with their existing alarm prioritisation, EEMUA 191 Appendix 3 gives examples of four different methods for alarm prioritisation (Table 2).

Table 2: Different approaches to alarm prioritisation (from EEMUA 191, Appendix 3)

Type of prioritisation	Description/notes
Priority matrix	A score is given to the alarm event, based on an assessment of the hazard involved, and multiplied by another score for 'time until consequence is realised', to give an overall priority index for each alarm.
Summation of consequences	The safety, environmental, and financial consequences of missing an alarm are estimated, converted into common units, and added together. Each alarm is then weighted if it is considered to be time critical. The outputs can then be used to rank order the system alarms.
Taking maximum consequence	Each alarm is assessed according to safety, environmental, and financial consequences using heuristic rules (e.g. small = negligible risk of failure to respond resulting in injury). Then the maximum assessed consequence from the three categories (i.e. safety, environmental and financial) is used to give the alarm priority.
General alarm assessment	A sequential set of customisable flowcharts covering general (e.g. is there sufficient time to respond?), safety (e.g. is there danger of death if action is not taken?), environmental (e.g. is the outcome a release within the boundary fence?), and financial (e.g. is the outcome damage to equipment or a process upset with a cost of £x?) factors.

5.4 STAGE 2: USABILITY ASSESSMENT OF INDIVIDUAL ALARMS

5.4.1 Introduction

The tool presented in this section is designed to facilitate the usability assessment of individual alarms. The aim is to maximise the probability of successful response by ensuring that each alarm adheres to good HF principles, and, consequently, supports the CRO in responding to the alarm and maintaining good ongoing situation awareness of the current state of the plant.

As this section deals with individual alarms, issues related to alarm flooding, which will clearly have an impact on CRO performance, are not addressed here, however these issues have been discussed in section 3.

5.4.2 Structure of analysis

The usability assessment tool is a series of statements designed to assess some of the important factors that will affect the probability of a successful CRO response to an alarm. The tool is organised according to a simple model of human performance (Figure 4).

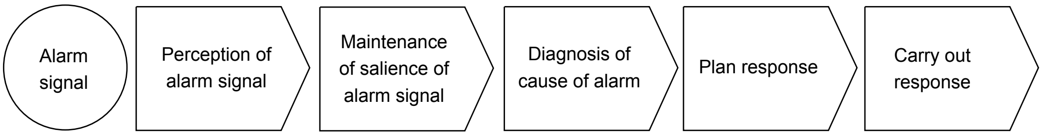
Alarm signal
Perception of alarm signal
Maintenance of salience of alarm signal
Diagnosis of cause of alarm
Plan response
Carry out response

Figure 4: Model for usability analysis tool

These are the main stages of a CRO's response to an alarm. The CRO first has to recognise the alarm, work out what has caused it, then plan and execute a response. The design of the alarm, and the way it has been implemented, can affect the ability of the CRO to successfully complete any one of these stages.

5.4.3 The alarm usability assessment tool

The tool involves a detailed assessment of each alarm, therefore it should normally be reserved for use only on the most important alarms (see 5.3 for discussion of alarm prioritisation). The team should take each individual alarm identified during the prioritisation and answer yes or no for each of the statements shown in the tables. The red-shaded area indicates a usability issue. The more answers that are in the red-shaded areas, the greater the number of usability issues that have been identified for that alarm. For red responses, the team should consider whether improvements to the alarm are required.

Some statements (marked with an asterisk (*)) are properties of the alarm system as a whole, rather than of an individual alarm. Therefore, if several alarms are being assessed, it may only be necessary to evaluate these statements once. In many cases, these alarm system properties may be described in an organisation's alarm philosophy document (if one exists). As such, if they are found to be deficient in the evaluation then the alarm philosophy document may need to be updated (or created).

Table 2: Stage 1 Perception of alarm signal

Stage 1 – Perception of alarm signal

A CRO has to first notice the alarm and recognise that it needs acting upon. There are a range of factors that may affect the ability of the CRO to do this, including the clarity with which the alarm is presented (e.g. is it differentiated from other less critical alarms) and their expectations (e.g. if the alarm in question has a history of false alarms).

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
1.1 The alarm signal is presented at the point where the process crosses from the normal to upset operating condition (i.e. not too early or not too late)		🟥	(P.1–3, P.36, P.40) B. The alarm is useful and relevant	A good alarm signal will occur at the point at which action needs to be taken (i.e. not too early or too late). Alarms that occur too early, in terms of the boundary between normal and upset conditions, will be spurious. Alarms that occur after the boundary with upset operation has passed may be unsafe, leaving too little time for safe CRO response.	Reassess the specific alarm set-point to determine why the alarm signal is occurring at an incorrect point (either within the boundary of the normal operating envelope or too close to the process trip) and consider moving the set-point. CAUTION: any changes to the set-point should be assessed to ensure that sufficient time is still available for a response. If this is not possible, this may be a sign of a more complex problem, for example, a conflict between production and safety demands, and the overall system philosophy should be reviewed.
1.2 The alarm set-point is regularly exceeded in normal operation	🟥		(P.13, P.15) B. The alarm is useful and relevant	Routinely exceeding an alarm set-point suggests that either the set-point is incorrect (e.g. as a result of failure to amend a set-point following a change to the process, forcing the CROs to exceed the set-point to maintain the process – a 'situational non-compliance') or there is a routine violation of procedures (e.g. as a result of lack of understanding of the criticality of the alarm).	Reassess the specific alarm set-point to establish why the set-point is being exceeded. If acting on the alarm means that the process cannot be run effectively then the system philosophy should be reviewed. If the set-point is correct and there is still evidence of routine non-compliance (i.e. continuing to operate without acting on the alarm) then the underlying reason for this should be determined. If the set-point is being violated because of a misunderstanding of the criticality of the alarm then this should be communicated to the operating team.

Table 2: Stage 1 Perception of alarm signal (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
1.3 The alarm prioritisation identification (e.g. tag and colour coding) on the distributed control system (DCS) matches the assigned prioritisation in the alarm risk assessment		🟥	(P.30–31) D. The alarm tag is appropriately prioritised within the DCS	If the DCS tag/colour coding does not match the risk assessment prioritisation it leads to the possibility of either a critical alarm being missed (high-priority, risk-assessed alarm categorised low on the DCS) or a low-priority alarm acting as a distraction/hindrance to more critical process control (low-priority alarm in the risk assessment categorised as high on the DCS).	Change the presentation of the DCS alarm priority to reflect its priority within the alarm risk assessment.
1.4 The alarm is operator configurable (i.e. presents the option of having a variable set-point)	🟥		(P.30–31) D. The alarm tag is appropriately prioritised within the DCS	Configurable alarms are those where the CRO has the freedom/authority to programme their own (variable) set-points to suit their preferences when using the system. This approach is more suited to alerts and should be avoided for critical alarms. Self-configuration of alarms presents the possibility of potentially inappropriate set-points (which lead to nuisance alarms or alarms being ignored) or unsafe set-points (which do not allow sufficient time for alarm response).	Any alarm that is self-configurable should be reassessed to verify whether it can be downgraded to 'alert' status. If it needs to be an alarm, the aim should be to remove the ability to change the set-point. If this is not practicable, then there should be robust controls regarding the configuration process (e.g. it can only be altered at the end of a batch, using a key system, requiring independent checks).

Table 2: Stage 1 Perception of alarm signal (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
* **1.5** Where alarms are duplicated on different displays: the categorisation, prioritisation and coding is identical and the alarm can be accepted by a single CRO action		🟥	(P.73) D. The alarm tag is appropriately prioritised within the DCS	Once an alarm has been categorised and prioritised, this information should be the same wherever that alarm is presented within the system. Inconsistencies will increase the likelihood of CRO confusion.	Ensure that, where the alarm is duplicated on different displays, it is presented consistently.
* **1.6** The highest criticality alarms are visually distinct from other classes of process alarms and alerts		🟥	(P.78) E. Only safety-related alarms have been assigned the highest priority	Where possible (e.g. where it does not contribute to visual clutter), the highest criticality alarms should look different to other, less critical, alarm categories to assist their identification. If this is not the case, at times of high alarm load, critical alarms may be missed or overlooked by a busy CRO.	Ensure that the most critical alarm categories are visually distinct from other classes of alarm. Often this can be achieved using colour coding in the DCS.
* **1.7** The highest criticality alarms are audibly distinct from other process alarms and alerts		🟥	(P.71, P192) E. Only safety-related alarms have been assigned the highest priority	Where possible (e.g. where it does not present a nuisance), the highest criticality alarms should sound different to other, less critical, categories of alarm to assist their identification. This will help draw the CRO's attention to that alarm signal. If high-criticality alarms are not audibly different, at times of high alarm load, critical alarms may be missed or overlooked by a busy CRO.	If possible, assuming this does not create additional distraction/irritation to CROs, provide a different sound for the most critical alarms. Ideally, the alarm should be at least 10 dB higher than background noise.

Table 2: Stage 1 Perception of alarm signal (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
1.8 Other alarms that provide the same process upset information, occur at the same time as the alarm being assessed (e.g. a 'pump stopped' alarm and a pump discharge low-flow alarm)	🟥		(P.182) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment/ action	There are occasions when a CRO may be notified of the same fault by two (or more) different alarms. For example, a 'pump stopped' alarm and a pump discharge low-flow alarm may provide the same information to the CRO (i.e. they are both caused by the pump stopping). This will increase overall alarm load on the CRO.	If information is duplicated across alarms, consider whether both are necessary. If they are both necessary, consider whether it is possible to use the system logic to group (or hide) alarms that provide the same information during an event. Some alarm systems have a 'first-up' indication that shows the CRO which alarm occurred first, to help with diagnosis.
* **1.9** At times of high alarm load the CRO can apply a high-priority alarm filter (this applies to chronological alarm lists not graphical displays)		🟥	(P.29, P.41) E. Only safety-related alarms have been assigned the highest priority	Such a filtering capability allows the CRO to display only the most critical alarms on the list. This should make it easier to identify critical alarms during upsets and also reduce the level of interruption posed by lower priority alarms. (Note: most lists of alarms are displayed chronologically; this statement does not apply to graphical alarm presentation, e.g. on the DCS process mimic).	If such a facility does not exist, investigate whether it is possible to provide a high-priority alarm filter. If this course of action is taken, ensure that alarms that are to be filtered out are not immediately important for process control.

Table 2: Stage 1 Perception of alarm signal (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
1.10 The alarm type is appropriate to the fault condition to which it relates (e.g. absolute, bit pattern, calculated, deviation, rate-of-change, etc.)		🟥	(P.24) A. The alarm type is appropriate to the requirements of process control	For CROs to have confidence in the alarm system (and for the alarm system to reliably indicate to the CRO the exact nature of any unsafe process changes), each alarm should correctly represent the true nature of the process upset. Therefore, the alarm type should be appropriate to the process parameter being controlled. Different types of alarms serve different purposes. For example, an absolute alarm arises when a set parameter is crossed, a rate-of-change alarm will occur when the speed with which process parameters are changing exceeds a predetermined value. For example, in a given system, the process temperature (e.g. 100 °C) may be less critical than the speed with which the temperature is rising (e.g. two degrees every five seconds), hence a rate of change alarm would be more appropriate. Other types of alarms include bit pattern, calculated and deviation.	Ensure that the alarm type is appropriate to the process parameter being controlled.

Table 2: Stage 1 Perception of alarm signal (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
*** 1.11** If the alarm is an electrical, control and instrumentation (EC&I) alarm (e.g. associated with hardware/ software faults): the presentation of the alarm is distinct from regular process alarms		🟥	(P.25) A. The alarm type is appropriate to the requirements of process control	EC&I alarms warn of problems with the control system rather than the process itself (e.g. associated with software faults). Alarms that indicate hardware/ software faults are valuable (for example, an indication that a pressure controller is inoperable). However, these alarms are likely to be associated with problems that the CRO cannot immediately address/rectify. Therefore, these alarms, where possible, should be presented separately to process alarms.	Ensure that electrical, control and instrumentation alarms are displayed separately from process alarms.
Total red responses for alarm perception:			**Notes:**		

Table 3: Stage 2 Maintaining alarm salience until alarm acceptance

Stage 2 – Maintaining alarm salience until alarm acceptance

Having recognised the alarm, the alarm should remain apparent to the CRO throughout the upset, until it is resolved. This statement set assesses the qualities of the alarm that will help to maintain the CRO's attention, or, conversely, that may increase the probability of it getting lost amongst other alarms.

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
* **2.1** The alarm remains on view to the CRO for the entire time that it is active		🟥	(P.22) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment/action	Where possible, high-priority alarms should remain visible until the cause of the alarm has been addressed. For example, on an alarm list, high volumes of alarms may mean that high-priority alarms are pushed off the bottom of the display. This may mean that the alarm is forgotten by the CRO at times of high alarm load. Also consider the possibility that, on a DCS display, the alarm list may become hidden within other process control screens.	Where possible, ensure that the alarm remains visible until it has been addressed. This may be achieved, for example, by keeping high-priority alarms at the top of a list of alarms.
* **2.2** If the alarm is no longer applicable, it automatically clears from the alarm list		🟥	(P.191) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment/action	When the process change that caused the alarm returns to normal, the alarm automatically clears from the alarm list. This prevents the CRO from having to manually clear an alarm that is no longer active, contributing to workload during busy periods.	Investigate whether the alarm can be configured to automatically reset, eliminating the need for manual resets.
* **2.3** When the alarm is accepted, the alarm state clearly changes		🟥	(P.193) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment / action	The alarm state should be clearly indicated; it should be immediately apparent if the alarm has yet to be accepted (e.g. unaccepted = flashing indicator, accepted = steady indicator, reset = cleared from display). Upon acceptance, there is a clear visual change to notify the CRO that the alarm status has changed. If the alarm's signal does not change state this may be confusing; requiring the CRO to spend more time reviewing alarm lists.	Ensure that alarm presentation is such that it is immediately obvious to the CRO what the current status of an alarm is.

Table 3: Stage 2 Maintaining alarm salience until alarm acceptance (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
* **2.4** During times of high alarm load, it is possible to separately silence the alarm and then later accept it on the display		🟥	(P.195) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment/action	It should be possible for the audible signal to be silenced, whilst retaining a visual signal that the alarm is active. Alarms that have to be accepted to silence the audible warning, present the risk that the CRO could simply accept the alarm to silence it, then forget about it.	Consider whether the system can be adapted such that there are separate 'silence' and 'accept' functions. If the system needs to be reconfigured, ensure that CROs are appraised of the new operating conditions. It may be useful to only allow the use of a mute button at times of high alarm load.
* **2.5** The alarm re-annunciates after a certain time delay		🟥	(P.229) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment / action	After the passing of a predetermined time, if the alarm has not been responded to, the alarm signal is presented again. This ensures that, at times of high alarm load, the most critical alarms remain apparent to the CRO.	Consider re-annunciating the alarm after a predetermined time delay if the alarm is not attended to. (Note: this feature should be used sparingly, and for the highest priority alarms, as it may present an unnecessary distraction if used for too many alarms.)
Total red responses for maintaining alarm salience:			**Notes:**		

Table 4: Stage 3 Diagnose the cause of the alarm

Stage 3 – Diagnose the cause of the alarm

The alarm system should support the CRO in understanding why an alarm has occurred. The following factors will affect the ability of the CRO to understand what is happening.

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
3.1 The alarm only arises during appropriate phases of operation		🟥	(P.34, P.62) B. The alarm is useful and relevant	An alarm should only annunciate at the appropriate time. For example, a rate of change alarm that is useful during start-up (e.g. during filling or pressurisation of a vessel) may be a nuisance if it occurs at other times.	Where possible, ensure that the alarm only occurs during relevant operating phases.
3.2 The alarm message (alarm information) is clearly understandable and assists the CRO in diagnosing the cause of the upset		🟥	(P.3, P.193) H. The alarm alerts, informs and guides the CRO to make the correct response	The alarm message should assist the CRO in identifying the cause and location of the upset. Ambiguous, abbreviated, and incomprehensible alarm messages may cause confusion and hamper response. Poor alarm messages may force CROs to rely more heavily on other sources of information for diagnosis (e.g. the graphical display).	Provide an informative alarm message that is clear, helpful and easy to understand.
3.3 The current value of the alarmed variable is clearly indicated		🟥	(P.192) H. The alarm alerts, informs and guides the CRO to make the correct response	Failure to clearly present the process parameter that is currently in alarm is likely to delay diagnosis. The exact value of the process parameter that has gone into alarm (for example, the vessel level/vessel pressure) should be indicated.	Improve presentation of the process variable that has gone into alarm.
3.4 The alarm message uses terms and values with which the CRO is familiar		🟥	(P.3, P.193) H. The alarm alerts, informs and guides the CRO to make the correct response	Use of different units in alarm displays to those commonly used in other contexts (e.g. verbal communication) may lead to confusion. For example, if CROs understand vessel capacity by means of tonnes then this metric should be used rather than cubic metres. It may require CROs to make conversion calculations which, under pressure, will be prone to error.	Revise the alarm messages to use terminology and values familiar to the CRO.

Table 4: Stage 3 Diagnose the cause of the alarm (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
3.5 Interpretation of the alarm message relies on CROs having to learn tag names or numbers	🟥		(P.193) H. The alarm alerts, informs and guides the CRO to make the correct response	Alarm messages that require CROs to learn obscure abbreviations or memorise alphanumeric sequences may lead to confusion and delay. CROs should not have to memorise tags, or learn abbreviations to interpret an alarm.	Revise the wording of the alarm message/alarm tag to that the message is clear and comprehensible to all CROs. Note: if changes are being made to existing alarm tags/messages, ensure that all CROs are aware of the change and understand any new naming/numbering conventions to be used.
3.6 The alarm message is presented in a manner consistent with other alarms (e.g. variable, qualifier, status)		🟥	(P.193) H. The alarm alerts, informs and guides the CRO to make the correct response	If the alarm message uses naming or numbering conventions that are different to other alarms in the system (e.g. different presentation of process variable, qualifier, status information) this may lead to confusion.	Revise the alarm messages to ensure they are consistent with other alarms.
3.7 It is possible to navigate quickly and easily from the alarm list to the operational graphic for that alarm. (i.e. the alarm can be viewed in context)		🟥	(P.75, P.195, P.229) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment/ action	In complex systems (e.g. with many display screens for separate control loops), when an alarm arises it is possible that the specific control graphic associated with that alarm will not be visible. In such instances, the first indication that a process parameter has gone into alarm will be the occurrence of the alarm tag somewhere on the active DCS page (e.g. the alarm banner) or an additional alarm reference occurring on the alarm list. Navigation from this tag to the relevant control graphic should be quick and simple.	Ensure that the CRO can navigate quickly from the alarm display indication to see the alarm in context.

Table 4: Stage 3 Diagnose the cause of the alarm (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
3.8 The display interface is configured such that all information relevant to the specific plant failure which caused the alarm is quickly accessible		🟥	(P.41) G. The alarm directs the CRO's attention towards plant conditions requiring timely assessment/ action	All contextual information associated with the alarm should be available as this will help with diagnosis.	Ensure that all contextual information associated with the alarm is available to help with diagnosis.
3.9 The alarm presents information that defines what the problem is by means of descriptive text or by graphical display		🟥	(P.3) H. The alarm alerts, informs and guides the CRO to make the correct response	The text (alarm tag) associated with an alarm is likely to be one of the first sources of information that the CRO uses to identify the problem. This information, together with any associated graphical representation of the process, will be used by the CRO to diagnose the cause of the alarm (and possibly the available response options).	Where possible, ensure that the alarm describes the problem identified by the alarm using text or graphical displays.
* **3.10** It is possible to accept this alarm while accepting multiple other alarms simultaneously (e.g. accept a page of alarms without reviewing the individual context and establishing a course of action)	🟥		(P.195) H. The alarm alerts, informs and guides the CRO to make the correct response	Multiple acceptance of alarms is the practice of accepting and, in effect, silencing a number of separate alarms in one action. This allows a page of alarms to be accepted without reviewing the individual context of each alarm and establishing the correct/necessary course of action for each alarm.	If this option is available, consider whether the blanket acceptance of alarms may lead to important issues being missed. This is potentially more of an issue in steady state operations. In abnormal situations, a CRO will already be alert to a developing issue.
Total red responses for diagnosing alarm cause:			**Notes:**		

Table 5: Stage 4 Plan the alarm response

Stage 4 – Plan the alarm response

Having recognised the alarm, and determined the probable cause, the CRO should decide upon an appropriate course of action. It is possible that there may be multiple ways to recover the process, however not all will be safe, effective or timely. The following factors will affect the ability of the CRO to decide upon an appropriate response to the alarm.

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
4.1 The consequences of not responding to the alarm are well understood by the CRO. (Information is provided in the DCS or written documentation is available to this effect)		🟥	(P.49) I. The alarm has a defined response	At times of stress or high alarm load, CROs may be inclined to ignore or delay response to certain alarms in an attempt to address what they perceive to be the most critical alarms. Information should be available regarding the process implications associated with the alarm and consequences associated with failing to respond.	Ensure that information regarding the consequences of not responding to the alarm is available to the CRO (e.g. through training, procedures and competence management).
4.2 The CRO is trained in the management of the specific plant failure indicated by the alarm		🟥	(P.68) I. The alarm has a defined response	As the highest criticality alarms should occur infrequently, in emergency situations CROs are likely to be presented with alarms that are either unfamiliar to them or that they have never encountered before. In such circumstances, CROs will need to work out a course of action using any available information (e.g. procedures, previous experience with similar alarms). This may result in a slow response or mistakes. CROs should be familiar with, and understand how to respond to, the highest priority alarms within the system.	Ensure that CROs receive training in responding to the highest priority alarms. (Note: this training should be used to complement accurate point-of-use alarm response guidance.)

Table 5: Stage 4 Plan the alarm response (continued)

Statement	**Response**		**EEMUA 191 reference**	**Further information**	**Possible action**
	y	**n**			
4.3 Guidance is presented on the display (or available in point-of-use alarm response manuals) regarding the actions to be taken in the event of an alarm		🟥	(P.229) H. The alarm alerts, informs and guides the CRO to make the correct response	Guidance could be available on the DCS, or in point-of-use alarm response manuals. Failure to provide sufficient guidance to CROs, presents the possibility of misdiagnosed alarms or delayed alarm response. For complex alarm systems that have large numbers of alarms (including alarms that infrequently occur), it is unrealistic to assume that CROs will remember the correct response to each alarm.	Identify the guidance that is required to support CROs in diagnosing and responding to alarms. This information should be provided either directly via the control system (and be easily accessible) or via point-of-use written alarm response manuals.
Total red responses for planning alarm response:			**Notes:**		

Table 6: Stage 5 Respond to the alarm

Stage 5 – Respond to the alarm

The final stage in alarm response is to execute the planned response. This involves the CRO taking action to bring the process back under control. Often, during serious process upsets, this alarm response will be undertaken during a time of high CRO workload. It is also likely that the most critical process alarms will be those that occur less often and are therefore least familiar to the CRO. Therefore, it is vital that sites have prescribed responses for each alarm, that there is sufficient time to carry these out, and that CROs are aware of the required course of action.

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
5.1 When the alarm sounds it is possible to ignore it until later	🟥		(P.4) B. The alarm is useful and relevant	If a CRO can delay the alarm response, it is possible that competing tasks will arise that could distract the CRO from returning to that alarm. If this is the case, it may be that the alarm signal arises too far in advance of the point at which a response is required. The alarm set-point may be inappropriate or the signal may have been incorrectly classified as an alarm.	Re-examine the purpose of the alarm in terms of process control. Review the set-point to determine whether the alarm signal is being generated at the correct point in the process.
5.2 Feedback regarding the success of the alarm response is readily available on supplementary displays (the alarm information directs the CRO to this information to verify success of response)		🟥	(P.3) H. The alarm alerts, informs and guides the CRO to make the correct response	Failure to provide sufficient feedback regarding the success of alarm response may cause uncertainty and confusion on the part of the CRO. This could result in CROs spending unnecessary time investigating whether their corrective actions have been successful.	Where possible, provide indication that an action has been successful. For example, it may be possible to ensure that the alarm remains active (and observable) until the process parameters associated with the alarm have improved. If there is known to be a delay in the return of the process to a safe state after executing the alarm response, this should be made clear to the CRO either by means of training or via supporting alarm response manuals/ documentation.

Table 6: Stage 5 Respond to the alarm (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
5.3 The alarm has a defined response (recorded in an alarm database)		🟥	(P.3, P.84) I. The alarm has a defined response	At times of stress or elevated workload, asking a CRO to determine a safe alarm response increases the probability of error. Therefore, wherever possible, the desired response to a critical alarm should be predetermined. There should be clear guidance regarding the steps that should be taken to recover to a safe state. This response should be recorded in the alarm database.	Identify and document the required control response necessary to recover the process to a safe state. So far as is possible, the response should be standard to reduce the need for CROs to make decisions regarding potential alternative control strategies. This information should be available to all CROs either within the process control system or in point-of-use written manuals. CROs should be trained in the execution of this alarm response.
5.4 The alarm response is simple, obvious and invariant		🟥	(P.84) I. The alarm has a defined response	Ambiguity regarding the required response to an alarm means a CRO must choose the correct course of action from a number of possible courses of action when under pressure. Whilst it is possible that numerous control options may be available, the most simple or reliable (whichever is most appropriate for the nature of the alarm) should be documented. If there are a variety of available alarm responses that differ depending on process conditions, efforts should be made to provide clarity regarding which response to execute.	Provide clear, simple and (where possible) invariant alarm-response information. Ensure that any room for misinterpretation or variability in response is eliminated.

Table 6: Stage 5 Respond to the alarm (continued)

Statement	Response		EEMUA 191 reference	Further information	Possible action
	y	n			
5.5 The alarm occurs early enough for the CRO to correct the fault but not so early that the CRO purposefully delays response to a later, more appropriate time		🟥	(P.4) There is adequate time available for the CRO to carry out the defined response	Timing of the alarm is important. If the alarm signal occurs too late it may be difficult/impossible for the CRO to effect a reliable alarm response. However, if the alarm signal is presented too early the alarm may be accepted but the response delayed – during which time the alarm may be forgotten/overlooked. The alarm signal should be presented at the most appropriate time to facilitate a safe and reliable response.	Assess the time that is required to effect a successful alarm response. Ensure that the alarm set-point is appropriate such that the alarm does not occur so early that response can be delayed, but occurs early enough to provide adequate time for response in all foreseeable process conditions.
Total red responses for responding to alarm:			**Notes:**		

5.4.4 Using the outputs of the alarm review

Each usability report provides a record of the assessment for the alarm under review. The output highlights areas where the alarm (and potentially the alarm system) is deficient. This can then be used to determine possible improvements.

Where statements have been answered negatively (i.e. in the red-shaded box), the usability assessment provides general guidance (in the 'possible action' column) as to how these specific features of the alarm in question could be improved. However, it may be the case that more appropriate, site-specific recommendations can be identified by the review team which can be carried forward.

There may be occasions where it may not be possible to implement specific recommendations. If this is the case, reasons why it is not possible to address the issue should be recorded.

A number of the usability statements within the tool are marked with an asterisk (*); these are features that are properties of the entire alarm system, rather than a feature specific to individual alarms (i.e. if the usability statement is applicable for the alarm under review, it should also be applicable for all other alarms within the system). For example, an alarm automatically clearing from the alarm list when no longer applicable is likely to be a feature of the system rather than the individual alarm. If such statements have been assessed negatively, improvements will likely have broader benefits, but may be more difficult to change.

ANNEX A
REFERENCES

A.1 REFERENCES

The Engineering Equipment and Materials Users Association (EEMUA) – http://www.eemua.org
EEMUA 191, *Alarm systems: A guide to design, management and procurement*, Edition 3
EEMUA 201, *Process plant control desks utilising human-computer interfaces: a guide to design, operational and human-computer interface issues*

Energy Institute (EI) – http://www.energyinst.org
Guidance on quantified human reliability analysis (QHRA)

Various authors
Flin, R., O'Connor, P. & Crichton, M. (2008) Safety at the sharp end: A Guide to Non-Technical Skills. Ashgate: Aldershot.

Health and Safety Executive (HSE) – http://www.hse.gov.uk
The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994: A report of the investigation by the Health and Safety Executive into the explosion and fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24 July 1994

International Electrotechnical Commission (IEC) – http://www.iec.ch
IEC 62682, *Management of alarm systems for the process industries*

International Society of Automation (ISA) – http://www.isa.org
ISA/ANSI-18.2-2009, *Management of alarm systems in the process industries*

International Organization of Standardization (ISO) – http://www.iso.org
ISO 11064-1, *Ergonomic design of control centres. Principles for the design of control centres*

A.2 FURTHER READING

International Electrotechnical Commission (IEC) – http://www.iec.ch
IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE, or E/E/PES)*, Parts 1–7
IEC 61511, *Functional safety –Safety Instrumented systems for the process industry sector*, Parts 1–3

ANNEX B
GLOSSARY OF TERMS AND ACCRONYMS

B.1 TERMS

alarm An automatically generated auditory and/or visual signal that provides indication of a process event requiring prompt CRO attention and/or action.

alarm usability A judgement of the functionality of the alarm in terms of ease of use to the CRO. This is a broad term that encompasses how easily and effectively the alarm is identified, diagnosed and responded to and how reliable it is to the CRO as a support to effective process control

alarm flood An alarm rate exceeding 10 alarms in a 10 minute period (typically during a plant upset).

alert An automatically generated auditory and/or visual signal that provides indication of a particular noteworthy event. Alerts are distinguishable from alarms as they may not require any CRO response. (For example, a signal that indicates that a routine process cycle has completed.)

bad-actors Spurious, unnecessary or fleeting alarms offer little or no benefit to the user in terms of providing meaningful notification of serious process changes, but contribute to overall high alarm levels.

confirmation bias The human tendency to seek, and interpret, information in a way that confirms an initial analysis, while giving less consideration to other possibilities.

continuous process A manufacturing system that, once started, has an indefinite process cycle (assuming product inputs remain available). It may operate for many weeks or months, and creates a continually available product stream. Compare a batch process where the process cycle has a defined start and end point.

human factors The study of systems and processes to ensure that they take account of the strengths and weaknesses of the people using them.

layers of protection A model/design of process safeguarding whereby control is achieved by means of a variety of (independent) measures. Generally these protection layers are a combination of procedural, instrumented and mechanical measures that contribute to overall process control. Alarms would be one potential layer of protection in such a model.

mental models An individual's internal model of reality used to anticipate future events (see also situation awareness).

rationalisation Whilst rationalisation is often referred to in the context of existing alarm systems, more properly it should be considered to be part of an alarm management life cycle, and performed initially as part of the system design, where proposed alarms are compared with criteria outlined in an alarm philosophy. However, often when organisations seek to improve the performance of their alarm systems they use the term rationalisation to mean the reduction of alarm numbers to move closer to benchmark values.

shelved alarms Alarms that are (temporarily) prevented from operating within the alarm system. Shelved alarms will not arise even when the process conditions deviate to the point where the alarm signal should be generated. Shelved alarms will only re-enunciate when they are purposely reinstated.

situation awareness An individual or team's understanding of what is going on around them.

standing alarms An alarm that persists as the process state that generates the alarm signal has not changed (or cannot be changed).

B2. ACRONYMS

ANSI	American National Standards Institute
CCTV	closed-circuit television
CRO	control room operator
DCS	distributed control system
EC&I	electrical, control and instrumentation
EEMUA	The Engineering Equipment and Materials Users Association
E/E/PE	electrical/electronic/programmable electronic
EI	Energy Institute
HAZID [study]	hazard identification [study]
HAZOP [assessment]	hazard and operability [assessment]
HF	human factors
HMI	human-machine interface
HOFCOM	Human and Organisational Factors Committee
ISA	International Society of Automation
ISO	International Organization of Standardization
KPI	key performance indicator
LOPA	layer of protection analysis
PFD	probabilities of failure on demand
SIF	safety instrumented function
SIL	safety integrity level

ANNEX C
ALARMS IN THE CONTEXT OF SAFETY INSTRUMENTED FUNCTIONS (SIFS)

A safety-related alarm is an electrical/electronic/programmable electronic (E/E/PE) system as defined in the functional safety standards (IEC, 61508 and IEC, 61511). It is part of a safety instrumented function (SIF) designed to protect against a hazard. A SIF is assigned a required safety integrity level (SIL) rating as part of a risk analysis, in order to achieve a tolerable risk. SIFs with claimed probabilities of failure on demand (PFD) of 0,1-0,01 are classified as SIL 1, those with PFDs of 0,01 or below are SIL 2 or greater.

EEMUA 191 recommends that in no circumstances should a claim be made for a PFD of below 0,01 (i.e. SIL 2-rated SIFs) that requires a CRO action in response to an alarm (P.19). However, there is more debate as to whether SIL 1-rated SIFs (i.e. PFD for the overall safety function of 0,1-0,01) can include a CRO response (i.e. a response to an alarm). EEMUA 191 makes some recommendations for basic requirements to be fulfilled as a prerequisite for making such a claim (e.g. alarm remains on view, CRO response is simple, the alarm should be obvious). Completing the usability assessment in section 5 may also assist with this, however, caution should always be exercised whenever any claim involving a CRO response is made.

One reason for this is because it can be difficult to confidently assign a PFD to a CRO action (e.g. EI, *Guidance on quantified human reliability analysis (QHRA)*). However, there may be situations where an automated response introduces additional risks, and where a CRO response, prompted by an alarm, is preferable. Determining whether or not this is a reasonable approach is outside the scope of this publication. However, if a decision has been taken to include a CRO response in a SIL 1-rated SIF, then it should be ensured that the CRO has the best possible chance to respond to the alarm, which will mean optimising human factors issues that may affect performance. Section 5 of this publication provides one way of evaluating the characteristics of individual alarms.

ANNEX D
WORKED EXAMPLE

The following worked example illustrates how the detailed usability review may be applied to an individual high-priority alarm.

Alarm review project: Plant 1 HP column **ISSUE 14**			
Alarm name: HP Column low-temperature alarm			
Alarm tag/reference: HPLT1			
Statement	**Response**		**Analyst comments**
	y	**n**	
1. Perception of alarm			
1.1 The alarm signal is presented at the point where the process crosses from the normal to upset operating condition (i.e. not too early or not too late)		🟥 ✓	The alarm arises on cold days and is often inhibited, otherwise it would generally always be active. The alarm set-point (12 °C) is not considered to represent a critical transition in the process (this is evidenced by the fact that the procedure actively requires it to be exceeded by running the process below 12 °C).
1.2 The alarm set-point is regularly exceeded in normal operation	🟥 ✓		The ambient temp. is frequently below the trip point due to exposed location of instrumentation. Therefore the alarm has to be overridden. During times of low ambient temperature it serves no process safety function.
1.3 The alarm prioritisation identification (e.g. tag and colour coding) on the distributed control system (DCS) matches the assigned prioritisation in the alarm risk assessment	✓	🟥	
1.4 The alarm is operator configurable (i.e. presents the option of having a variable set point).	🟥	✓	The alarm is not operator configurable.
* **1.5** Where alarms are duplicated on different displays: the categorisation, prioritisation and coding is identical and the alarm can be accepted by a single CRO action	NA	🟥 NA	

Alarm review project: Plant 1 HP column **ISSUE 14**			
Alarm name: HP Column low-temperature alarm			
Alarm tag/reference: HPLT1			
Statement	**Response**		**Analyst comments**
	y	**n**	
1. Perception of alarm			
*** 1.6** The highest criticality alarms are visually distinct from other classes of process alarms and alerts	✓	🟥	
*** 1.7** The highest criticality alarms are audibly distinct from other process alarms and alerts	✓	🟥	The alarm signal is distinct, however, given that it often occurs during ambient conditions (offering no process control value) it is regularly overridden.
1.8 Other alarms that provide the same process upset information occur at the same time as the alarm being assessed (e.g. a ‘pump stopped’ alarm and a pump discharge low-flow alarm)	🟥	✓	No other alarms which mean the same thing arise with this alarm.
*** 1.9** At times of high alarm load the CRO can apply a high-priority alarm filter (this applies to chronological alarm lists not graphical displays)	✓	🟥	
1.10 The alarm type is appropriate to the fault condition to which it relates (e.g. absolute, bit pattern, calculated, deviation, rate-of-change, etc.)	✓	🟥	This alarm arises when a designated temperature has been reached and also if there is a dramatic rate of change in temperature (set-point 12 °C and falling).
*** 1.11** If the alarm is an electrical, control and instrumentation (EC&I) alarm (e.g. associated with hardware/software faults): the presentation of the alarm is distinct from regular process alarms	NA	NA	
TOTAL RED responses for alarm perception	2		

energy institute

Energy Institute
61 New Cavendish Street
London W1G 7AR, UK

t: +44 (0) 20 7467 7100
f: +44 (0) 20 7255 1472
e: pubs@energyinst.org
www.energyinst.org

This publication has been produced as a result of work carried out within the Technical Team of the Energy Institute (EI), funded by the EI's Technical Partners and other stakeholders. The EI's Technical Work Programme provides industry with cost effective, value adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and beyond.

9780852939147

ISBN 978 0 85293 914 7
Registered Charity Number: 1097899