The 'new' EEMUA 191

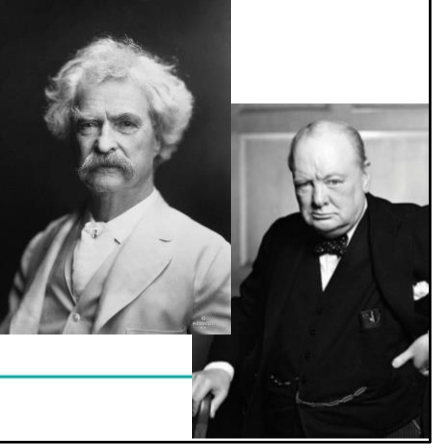
Andy Brazier
Lead Author of EEMUA 191 4th Edition
AB Risk Limited

Why is it better? What has changed? What has stayed the same?

Re-write objectives

- Better structure – less repetition
- More consistent
- More succinct
- Graphical representations
- Provide templates / example procedures
- Link with EEMUA 201
- Updates to standards - e.g. IEC 62682

"I didn't have time to write a short letter so a wrote a long one instead"



Engineering Equipment and Materials Users Association ©

EEMUA Alarm Management Seminar October 2024

I have referred to the 3rd Edition of 191 extensively since its publication. My conclusion was that the answers to most of the pertinent questions were covered, but often difficult to find. Some content was duplicated, but in some cases there were some significant inconsistencies.

Making it more succinct was an objective and the result is a reduction from 250 to 200 pages. It is still a substantial document, but some of it is now templates and examples which should be useful resources, beyond simple guidance.

As Mark Twain, or was it Winston Churchill, once pointed out it takes a lot of effort to write a shorter document.

Another driver for the update was in issue of edition 3 of EEMUA 201 in 2019 and updates to the standards, in particular 62682.

Re-write team

- Writing - Edward & me
- Detailed comments – Elaine Skilling, Asger Schiemann & Nic Butcher
- EEMUA industry review group

– Martin Anderson	Humanfactors101
– Linn Iren Vestly Bergh	Havtil
– Marek Bialy	Perenco
– Dave Board	Yokogawa
– Ian Brown	ProcessVue
– Ruud Pikaar	Ergos Human Factors Engineering
– Marleen Stieler	NAMUR WG2.9
– David Strobhar	Beville
– Scott Turner	Emerson Process Management Ltd
– Steve Willetts	Formerly of British Gas

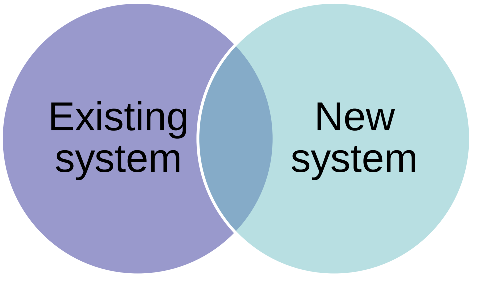
I acted as lead author for the re-write, but Edward has been very heavily involved throughout.

Elaine from HSE, Asger from Lloyds Register and Nic Butcher from ONR made extensive comments throughout several drafts. And a wider group from the EEMUA industry review group made a significant contribution.

I have to say at this stage that we did not address every comment made. The guide has a very wide audience and it was clear that certain industries have their own issues and solutions.

Alarm management requirements – all situations

- Understand role of alarms and issues if poor
- Regulations, standards, policies to apply
- Have a good philosophy document
- Resources and competencies



The guide is intended to assist you on your alarm management journey. But it can't do it for you.

Whatever your situation, whether looking to improve an existing system or introduce a new one you need to understand the role of alarms and what the consequences can be of tolerating a poor system.

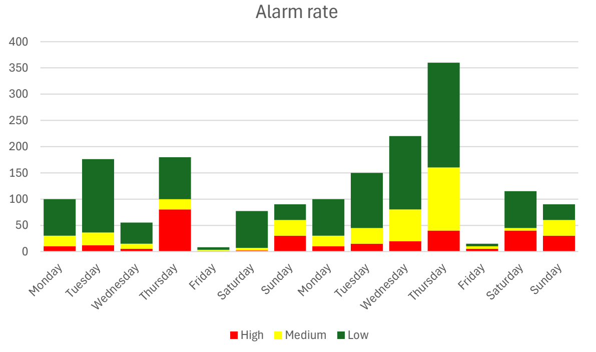
You have to understand which regulations, standards and local policies that apply to your site.

You must have a good alarm philosophy. There are many aspects of alarm management where there is no right or wrong solution. You may have specific requirements and compromises may be required. We have included a template for a philosophy in the guide, but you have to adapt it to your requirements.

Finally, you need resources, including people with appropriate competencies.

Working with an existing system

- Performance measures
- Good data
- Rationalise if required
- Other methods of improving performance
- Business case for change
- Management of Change



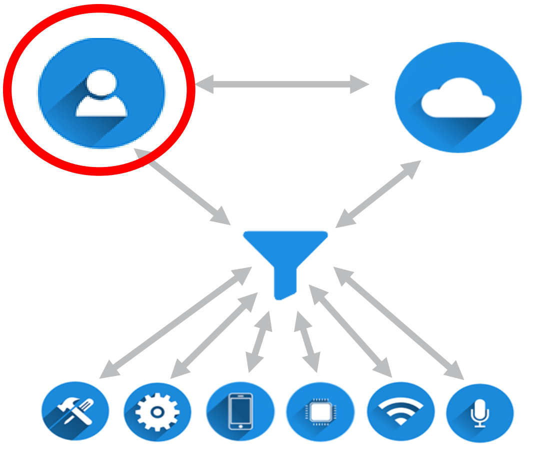
If you are working with an existing system you need to have a way of evaluating current performance in order to identify where improvements are required. Data about steady state is not sufficient, and be aware that operators may be receiving alarms from multiple systems.

Depending on current performance you may need to undergo a full rationalisation, looking at every alarm configured on the system. We have included an example rationalisation procedure in the guide that you may wish to amend to be consistent with your philosophy document.

You will need to secure resources, especially time for employees and maybe external support and hardware upgrades. And any changes you make need to be properly managed.

Working with a new system

- Focus on system performance and human factors
- Competent resources
- Procure a suitable system
- Alarm data base
- Formal rationalisation study



Engineering Equipment and Materials Users Association ©

EEMUA Alarm Management Seminar October 2024

If you are implementing a new system your requirements are a bit different.

You need the project team to recognise that the system's performance will be judged on how well it supports the human operators, not how good the hardware and software is put together. We have included a template for a human factors integration plan in the guide.

You need to make sure the people tasked with developing the alarms understand the requirements. This is something that has gone wrong so many times. An instrument engineer does what they have always done.

When buying a system you need to make sure it has the facilities you need to manage alarms.

Someone has to be responsible for generating and implement the alarm database, and this has to be handed over to operations.

In most projects I would expect a formal rationalisation study to take place. This is still not standard in lots of places.

New guide - same messages

- Alarm definition
- Design principles
- Operator response
- Incentives to improve performance
- Most alarms handled by BPCS

An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response

As I said previously the previous edition of 191 was mostly correct and up to date. The definition of an alarm has not been changed – the key message being that all alarms require a timely response from an operator.

The incentives to improve, especially related to safety remain the same. Recognising that the trend towards having more alarms has had a negative impact.

The guide reflects the fact that most alarms are handled by a basic process control system. These are viewed as low integrity systems, and although formal credit may not be taken in safety studies, they do contribute to overall risk management.

Untouched content

- Core principles – usability, safety, performance monitoring, investment in engineering
- Alarm system lifecycle – IEC 62682
- Types of alarm – absolute, deviation, system etc.
- Principles of alarm set point determination
- Technical design of instrumentation
- Alarm display options – annunciator, list, graphical
- Logical processing, grouping, suppression etc.

As a quick overview, here are examples of content from the 3rd edition that has been copied virtually untouched into the 4th. It may appear in a different place and some minor edits may have been made.

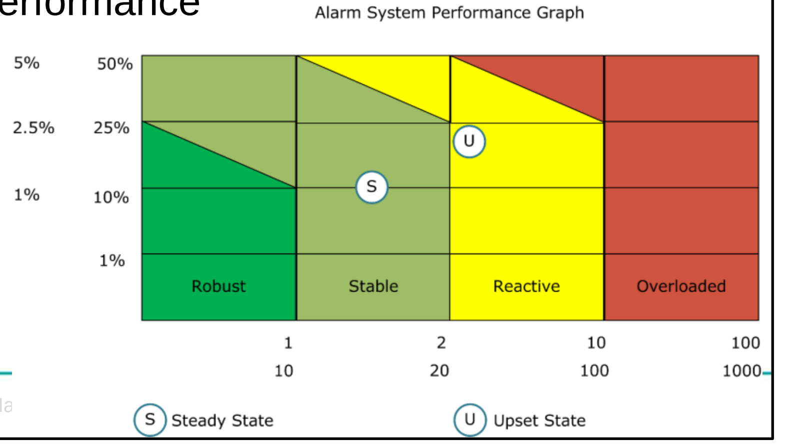
This includes core principles, system lifecycle from IEC 62682, types of alarm, method of choosing set points and technical aspects of instrumentation design.

The guide still covers alarms presented on annunciator panels, although most alarm systems are now electronic using alarm lists along with indications shown on graphical displays.

Options for logical processing have stayed the same.

Untouched content

- Avoiding repeating alarms
- Evaluation & monitoring metrics
- Techniques to improve performance
- Questionnaires
- Specification checklists
- Intelligent fault detection

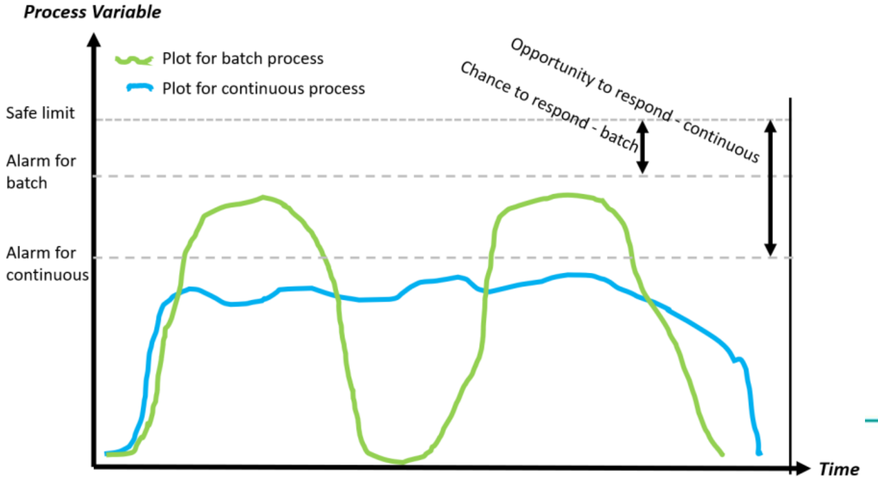


Also method of avoiding repeating alarms, evaluating and improving performance have remained. The guide still refers to alarm systems being robust, stable, reactive or overloaded.

Questionnaires and specification checklists have been carried across and information about intelligent fault detection has been retained, although we suspect that the technology is likely to change in the future.

Batch & distributed systems

- May not be special cases



Engineering Equipment and Materials Users Association ©

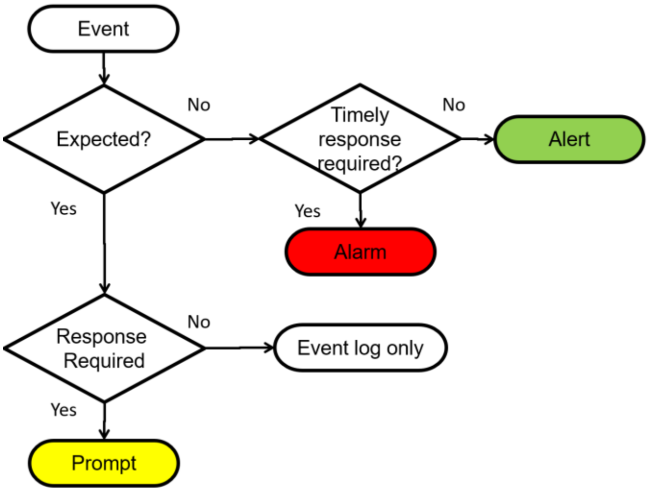
The previous edition of 191 included quite a lot of content related to managing alarms for batch and distributed processes. The implication was that they were special cases that require different approaches.

This plot illustrates that there can be challenges of setting alarm points for batch vs continuous plants. However, the safety limits rarely change according to the status of the batch and when examined the content in the previous edition was really referring to alerts and prompts, but using the term alarm incorrectly.

But a continuous process does not operate all of the time. It has to be started up and shutdown from time to time. They are not as different as they appear, and could be viewed as a very long batch.

Similarly geographically distributed systems do create some issues but most process plants are distributed to some extent. You may need to set some specific rules for alarm management for a distributed plant but the underlying principles are essentially the same.

Alarms, alerts, prompts & events



Engineering Equipment and Materials Users Association ©

EEMUA Alarm Management Seminar October 2024

One thing we have worked hard on with the new edition is to use clear definitions of alarm and non-alarm, and to use them consistently throughout.

This is really important and useful because being able to classify a signal as an alert or prompts is often a very effective way of reducing challenges with alarm management.

Alerts give information to an operator that may be useful for their situational awareness. The key point is that they do not need to respond, but can if they are able to.

An prompt is a trigger for an operator to respond but it should not be time critical and failure to respond does not have any safety implications. Usually the process is held in a safe hold position. The typical uses are for batch processes and automated sequences such a compressor start-up. One thing that has caused confusion in the past is the prompts can sound like an alarm.

Events are typically a record of everything including alarms, alerts and events. They are most use as an offline diagnostic tool, typically via a data historian.

Highly Managed Alarms (HMA)

- Create a higher reliance on operator response to avoid an undesirable outcome
- More than reducing demand on an engineered system
  - HMA-S: Safety
  - HMA-E: Environment
  - HMA-A: Asset
  - HMA-Q: Quality
  - HMA-C: Customer

There is quite a lot of interest in certain circles about a class of alarm that may be considered the most critical. They have been referred to as safety or safety related alarms, and often just described as critical. In my experience most people have been a bit baffled by the terminology and the underlying principles. We seemed to spend a lot of time discussing them, which is ironic because the main objective is to avoid using them wherever possible.

One of the problems with referring to safety alarms is that some are critical but not for safety. Also, it was noted that IEC 62682 was using the term Highly Managed almost interchangeably. The outcome was to recommend that HMA for different reasons should be identified.

HMA-S may be mapped onto safety alarms identified from functional safety studies. Also, they may be discussed with your safety regulator. But this approach means you can apply the principles to things that are important to your business.

Credit for alarms & operator response

EEMUA

- Refer to IEC 61508 & IEC 61511
- Response is more that acknowledging / silencing
- Time required to:
  - Realise an alarm requires attention
  - Identify the alarm
  - Diagnose the alarm
  - Decide how to respond,

Misplaced conservatism about alarm response times places higher reliance on other protection layers, resulting in increased complexity and potentially reducing the incentive to implement good alarm management

Following on, the people interested in taking credit for alarms in their functional safety studies would probably have liked more details on this aspect in the guide. We concluded that it was quite a niche application and really a functional safety issue. The advice is to refer to the appropriate standards.

It did lead to an interesting discussion about time required for operators to respond to alarms. A key message is that this is not concerned with just acknowledging or silencing an alarm, and really it requires a reasonable assessment of how long a proper response really requires.

We found ourselves stuck between a view that experience shows operators can handle many alarms and credit cannot be taken for alarm response in safety studies because human cannot be relied on.

Human factors

- People are fallible
- People have remarkable capabilities

Human activity	HMI requirement
Detect	Alarm status clearly indicated to the operator, standing out from all other information presented by the HMI.
Diagnose	Alarm identification is clear. Information required to determine why it has occurred readily available and easy to interpret correctly.
Respond	Access to controls required to respond. Information required to confirm successful response readily available. Clear indication of escalation (i.e. unsuccessful response).

People are fallible. They can be imprecise in their actions, they forget things, misinterpret data and lose attention. Also, people can choose not to respond to an alarm.

On the other hand, people have remarkable capabilities that have proven difficult to replicate with even the most sophisticated technology. They are particularly good at recognizing visual patterns and noticing very minor changes. They can take account of information from many different sources, allowing them to understand what is happening, even if it is something that they have never encountered before or been trained to handle. When an operator notices an alarm has occurred they will look for data to help them understand what is happening, which highlights the importance of recognizing alarms as part of the overall HMI. They will also be considering information given at shift handover, e-mails and reports received (possibly months previously), direct observations (sounds, vibrations and smells), environmental conditions (weather, time of day). These other sources of information are clearly outside of the scope of alarm system design but understanding human factors can help develop a system that supports the operator to act reliably.

The table summarises how a good HMI can support operators. It highlights why human factors knowledge during design is so valuable.

Audible indications

- Notice an alarm
- Do not startle
- Up to 4 different alarm sounds
- None for alerts (also prompts)

Audible sounds are used widely to indicate to operators that alarm has occurred and requires their attention. The sound has to be loud enough to be heard. Previous guidance suggested 10 decibels above background but this is now considered stressful.

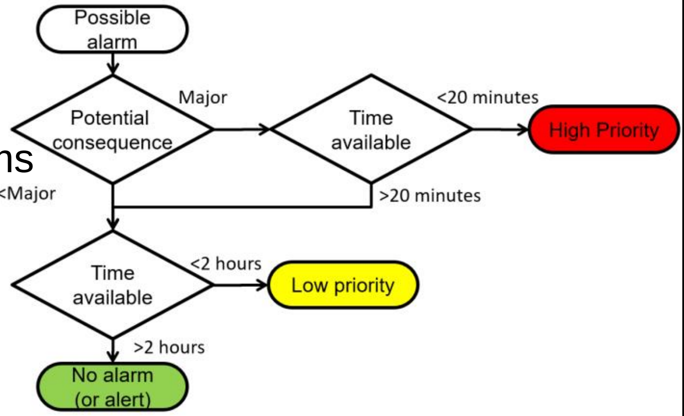
We did get some comments saying that the audible indication can be at the same level as background if the sound is different. Also, some studies suggest that people can differentiate a large number of different sounds. However, in practice I not so sure and 191 suggests up to four different sounds can be used.

To be honest, if you have good alarm management you really only need one sound because it will be heard infrequently and the operator will always be able to respond.

One piece of clarity in the new edition. Alerts will not normally need an audible indication. Similarly for prompts but if you do use one it should be much less prominent than the alarm sound.

Prioritisation

- All alarms are important & responded to immediately
  - Based on priority and time to respond
- Priorities guide an operator's resources when multiple alarms occur
  - Not to determine whether it can be ignored
- Define prioritisation method in alarm philosophy



The underlying principles of prioritisation have not changed but I think it worth reiterating the purpose.

All alarms are important and should be responded to. One potential issue with this is when more than one alarm occurs at the same time. And this is where prioritisation is supposed to help.

It guides the operators to decide which to deal with first. But to be clear, a low priority alarm does not mean it can be ignored, ever. But its response may be delayed if a higher priority alarm occurs.

There is some guidance in 191 about how to prioritise alarms but you really need to develop your own methods and include this in your alarm philosophy document. I would say that some of the methods in the previous edition were open to a lot of interpretation and could result in alarms being prioritised that should not have been alarms.

Alarm rationalisation

- Not just prioritisation
- Delete unnecessary alarms
- Procedure – see appendix 5

- Other appendices
  - Human Factors Integration Plan (HFIP)
  - Alarm philosophy
  - Review checklists

One topic that has received more attention in the guide is alarm rationalisation. This is a formalised study that looks at how the system is arranged. It is not just about prioritising existing alarms but very importantly deleting unnecessary alarms. This is a new term introduced to differentiate from nuisance alarms, which are defined in the standard as alarms that occur excessively. The difference is an unnecessary alarm does not satisfy the requirements to be an alarm and should be deleted. A nuisance alarm is an indication that part of the system needs to be fixed.

For an existing alarm system you may not need to conduct alarm rationalisation if performance is reasonably good. I would say that a formal study should be part of any significant project that will introduce a new alarm system. We have included an example procedure in the appendices.

Whilst talking about appendices, some new ones that I hope you will find useful include an example human factors integration for projects, an example alarm philosophy document and some checklists that you can use when evaluating a system.

- www.eemua.org

- ANY QUESTIONS?