The sense and nonsense of Alarm system performance KPIs[1]

What are meaningful values?

Abstract

Alarm system performance KPI's have been around since the release of EEMUA 191. The Bransby & Jenkinson survey performed in 1998 concluded that one alarm per ten minutes was considered very likely to be acceptable. Since then, these KPI's have been starting to live their own lives. One alarm per ten minutes was quickly translated to six alarms per hour. ISA 18.2 upon its release in 2009 stated that about 150 alarms per day would be acceptable as a KPI. IEC 62682 in 2014 states about 144 alarms per day would be a good target value. ISA 18.2 – 2016 omitted this KPI, along with two other KPI's. This paper explains why; and why one alarm per ten minutes cannot be translated into so many alarms per hour or day.

Introduction

The alarm system performance KPI's date from the UK HSE report CRR 166 of 1998, following the Milford Haven refinery incident in 1994, in which was concluded that a rate of one alarm per operator per ten minutes was generally seen as acceptable and not a major cause for concern. This report proposes measuring the alarm rates, as a good and simple measure of the workload imposed by the alarm system [CRR98166 page 31]. The report already states that some measure of the variability of the rate may be useful, e.g. peak rate in any ten-minute period [CRR98166 page 31]. These figures were proposed in the original EEMUA Publication 191 of 1999.

EEMUA 191 [EEMUA 191, Third Edition, p.96] further specifies that when considering the usability of an alarm system, there are two main situations to be considered:

- Plant in steady state operation
- Plant in upset/abnormal condition

The alarm issues associated with these two states are different, hence it is sensible to set benchmark values for each situation and consider improvement progression for each situation separately. The publication specified that after an inquiry at many control rooms, the average of less than one alarm per ten minutes in steady state was very likely to be acceptable, one per five minutes was considered manageable, one per two minutes likely to be over-demanding and more than one per minute very likely to be unacceptable. [EEMUA 191, Third Edition, page 96].

The EEMUA Publication also specified that in the first ten minutes following a major plant upset, under ten alarms (per operator) should be manageable, but maybe difficult if several alarms require a complex operator response (we get back to this point further down this paper). Twenty to a hundred alarms per operator is hard to cope with and more than a hundred alarms per operator is excessive and very likely to lead to the operator abandoning the use of the system. [EEMUA 191, Third Edition, page 97].

[1] KPI: Key Performance Indicator

In the first ANSI/ISA 18.2 standard the following KPI’s for the performance of an alarm system were formulated based on the KPI’s originally proposed in EEMUA 191:

Alarm Performance Metrics Based upon at least 30 days of data		
Metric	**Target Value**	
Annunciated Alarms per Time	Target Value: Very Likely to be Acceptable	Target Value: Maximum Manageable
Annunciated Alarms Per Day per Operating Position	~150 alarms per day	~300 alarms per day
Annunciated Alarms Per Hour per Operating Position	~6 (average)	~12 (average)
Annunciated Alarms Per 10 Minutes per Operating Position	~1 (average)	~2 (average)
Metric	**Target Value**	
Percentage of hours containing more than 30 alarms	~<1%	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	
Maximum number of alarms in a 10 minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur.	
Stale Alarms	Less than 5 present on any day, with action plans to address	
Annunciated Priority Distribution	3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% “highest” Other special-purpose priorities excluded from the calculation	
Unauthorized Alarm Suppression	Zero alarms suppressed outside of controlled or approved methodologies	
Unauthorized Alarm Attribute Changes	Zero alarm attribute changes outside of approved methodologies or MOC	

Figure 14 – Alarm Performance Metric Summary

In the 2016 version of the standard, the table was updated to the following:

Table 7 – Recommended alarm performance metrics summary

Alarm performance metrics based upon at least 30 days of data		
Metric	**Target value**	
Annunciated alarms per time	Target value: very likely to be acceptable	Target value: maximum manageable
Annunciated alarms per hour per operator console	~6 (average)	~12 (average)
Annunciated alarms per 10 minutes per operator console	~1 (average)	~2 (average)
Metric	**Target value**	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	
Maximum number of alarms in a 10-minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur.	
Stale alarms	Less than 5 present on any day, with action plans to address.	
Annunciated priority distribution	3 priorities: ~80% low, ~15% medium, ~5% high or 4 priorities: ~80% low, ~15% medium, ~5% high, ~<1% highest Other special-purpose priorities) excluded from the calculation	

Four entries were omitted:

- Percentage of hours containing more than thirty alarms.
- Annunciated alarms per day per operating position.
- Unauthorized alarm suppression.
- Unauthorized alarm attribute changes.

Why this change?

The operator

It must be remembered that these benchmarks were set to make sure the alarm rate should not exceed that which the operator is capable of handling, as the operator's role typically involves many different activities and responsibilities. It states that the time required for other activities of the operator often imposes severe limits on what alarm handling workload is acceptable [EEMUA 191, Third Edition page 4].

In the light of the above mentioned KPI's, it would be that with a rate of one alarm per ten minutes, the operator can spend up to ten minutes on dealing with each alarm.

ANSI/ISA 18.2 specifies the operator's workflow as follows:

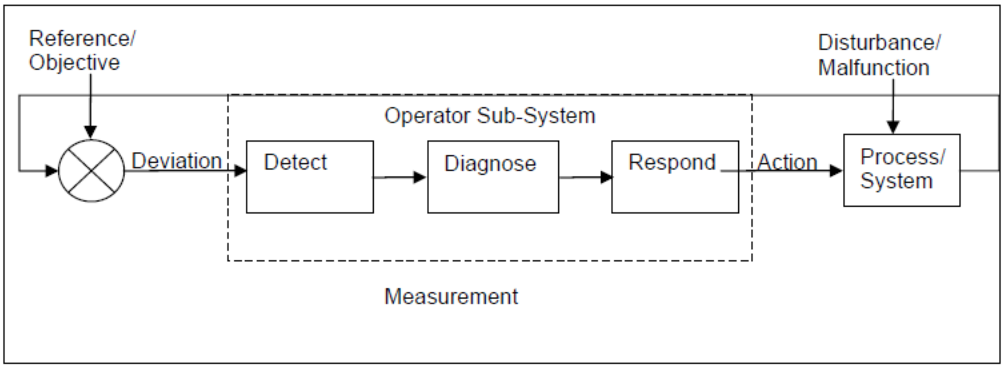
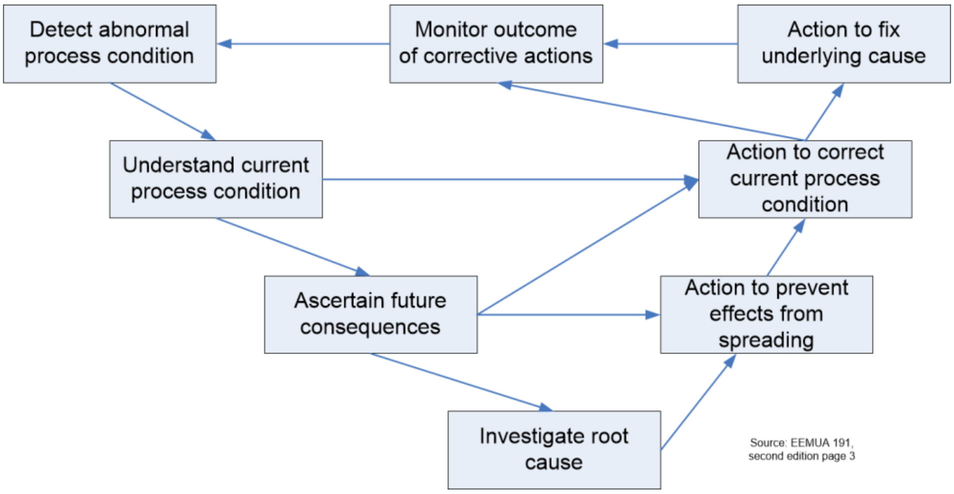


Figure 7 – Feedback Model of Operator Process Interaction

The alarm system detects and annunciates an abnormal condition, malfunction or process deviation which requires human intervention. According to figure 7, the operator must, after becoming aware there is a problem which requires his action, diagnose the problem, formulate a response and put the response into action. His actions should influence the process or system in such a way the situation returns to normal.

EEMUA 191 Second Edition specifies (on page 3) the operators workflow as follows:



The operator must understand the current process conditions (is the process in steady state, upset, shutdown, start-up etc.). He must act to correct the current process conditions; he has to have an understanding of the future consequences and needs to eventually take actions to prevent the effects from spreading. He must know, or investigate the root cause of the problem and he might need to take actions to fix the underlying root cause. He also needs to monitor the outcome of all his corrective actions. [EEMUA 191 Third Edition pages 33-34].

How much time does an operator have to act? It depends on the situation and the state of the process. For operations in the normal operating window, ANSI/ISA 18.2 provides the following overview:

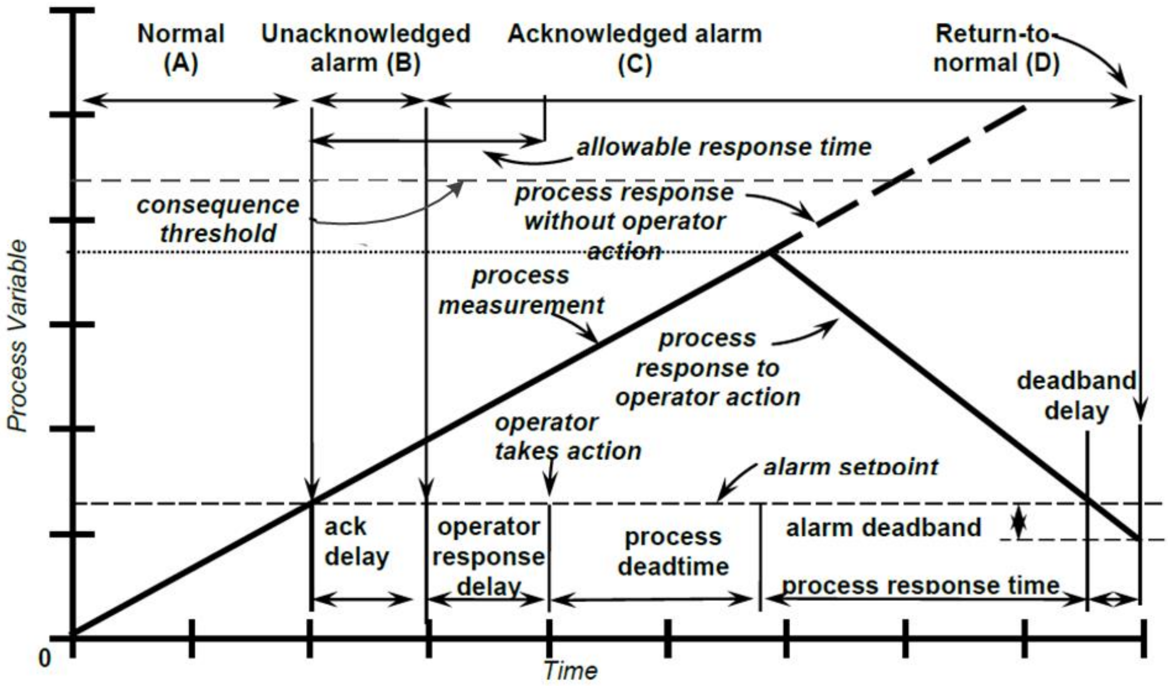


Figure 4 - Alarm response timeline

From the figure, it can be derived that the operator's attention starts after he acknowledges there is an alarm (there is a problem) and ends when the alarm disappears (and the problem is gone, hopefully). So, the alarm response time is the sum of the operator response delay, the process deadtime, the process response time and eventually the dead-band delay. This is the alarm response timeline. The operator has less time: he only has the time to act between the alarm annunciating and the time the process variable hits the consequence threshold, minus the time he starts working on the alarm (the ack delay) and minus the time the process will respond to his actions (the process deadtime). Ten minutes sounds like a good average, that's why it was likely to be acceptable that one alarm per ten minutes per operator is a manageable situation. But is it for every alarm?

If the alarm system is properly configured, then for most alarms, the consequence of not responding or not having enough time to respond will result in a trip of the corresponding device, machine, unit or installation.

Unfortunately, most alarm systems are poorly configured, whereby the first alarm popping up will be of low priority and the consequence of not responding to it is a higher priority alarm. In this case there is no consequence (commercial, environmental or safety) of missing the low priority alarm. This simply promotes the attitude of "it doesn't matter if I don't respond, there'll always be another alarm".

Eventually, the safety instrumented systems or functions of the emergency shutdown system will kick in and will typically generate numerous alarms which are likely to overwhelm the operator and detract him from limiting the effects of the tripped equipment. But then the plant or unit is in upset condition – hopefully the most critical processes have been shut down and the equipment brought to a safe state. An alarm at the trip point also makes little sense, what is the operators action here? It is too late for him to respond.

Proper alarm configuration requires only annunciating those alarms which will require operator action, for example, to restart the device, machine, unit or installation, or to prevent the effect of the issue proliferating. Having multiple alarms for the same situation makes no sense and has the sole effect of increasing the operators stress levels.

For new alarm systems, the time to deal with an alarm must be calculated (based on the expected rate of change of the process variable) or estimated – implying hypothetical reasoning. An alarm without a documented action or actions is very likely to be an unnecessary alarm and therefore unacceptable. If there is only one single action to perform, such action can usually be automated and hence the alarm (the candidate alarm) should not be configured and maintained anymore.

Coming back to the meaningfulness of the average rate per hour KPI: for a green-field plant, the average estimated response time, measured over all the configured alarms will define the average alarm rate KPI. Example: if the estimated average response time is twenty minutes, then the KPI should be set at one alarm per twenty minutes. That can only be done when the estimated operator response time for each configured alarm is documented in the Master Alarm Database.

For existing alarm systems, (where the control system does not allow group or page acknowledgement) the time that an alarm returns to normal, or its active state, can be measured.

For example, *on average* the alarms generated in a certain mode (steady state or upset state) will have *an average* time to return to normal. If this average time is five minutes and the operator has no other tasks to perform, then one could propose that one alarm per five minutes is acceptable.

But these calculations rely on the assumption there being no alarms which disappear without being acknowledged (often the case with fleeting alarms) or where the acknowledgement is done after the alarm has returned to normal. There should also be no alarms which are acknowledged but not returned to normal over the period the calculations take place. In other words, there should be no stale alarms, no fleeting alarms and no chattering alarms considered in such average response time calculations. That is one of the reasons why these performance KPI's 'Quantity of chattering and fleeting alarms' and 'Stale alarms' are listed in table 7 of the standards.

It should also be considered if the operator must perform all the required tasks by himself, in front of his operator console, or if he has to rely on another engineer to perform outside actions as part of the alarm response. The operator could start working on the next alarm, whilst his engineer is implementing the actions out on the plant to rectify the first alarm.

But here poses another problem: if the next alarm would require the maintenance person in the field to go to another part of the plant, that would be impossible. What should the control room operator need to do in such a situation? Proper task analysis for each alarm is required and proper workload estimation for each involved person recommended.

Good to remember: estimated (theoretical) operator alarm response time values should be proposed in the Alarm Philosophy and should be used in the Master Alarm Database; average alarm response time values should be available from the monitoring and assessment tools. The audit process could evaluate the measured response time against the theoretical response time and propose changes to the alarm response times proposed in the Alarm Philosophy and/or adjust the estimated alarm response time in the Master Alarm Database. The table below illustrates how such "Maximum time to respond" is very often proposed in an Alarm Philosophy.

Maximum Time to Respond	Severity of Consequences			
	Insignificant	Low	Medium	High
> 30 Minutes	Event	Low Priority	Low Priority	Low Priority
10 to 30 Minutes	Event	Low Priority	Low Priority	Medium Priority
3 to 10 Minutes	Event	Low Priority	Medium Priority	High Priority
< 3 Minutes	Event	Medium Priority	High Priority	High Priority

Example: During an alarm system Audit, it is concluded the operators need at least 10 minutes to avoid a trip following a high priority alarm. Consequently, the Master Alarm Database can be updated accordingly and should keep track of the rationale behind this update.

Realistic KPIs

The sites target annunciated alarm rates should be documented in the alarm philosophy, on condition they are achievable. If one is confronted with an alarm system generating on average one alarm per minute, suggesting an average of one alarm per ten minutes might be unrealistic and unachievable in one audit cycle.

Hence the recommendation is to perform a benchmark (initial audit) to determine the current performance of the alarm system, followed by the creation of an alarm philosophy, or an update of the alarm philosophy with realistic achievable goals. If the alarm philosophy specifies one alarm per two minutes as a first objective, then, when you have one alarm per minute, you have achieved a 100% improvement. The next audit can provide evidence that this objective has been achieved and the average rate can be updated to, for example, one per three minutes.

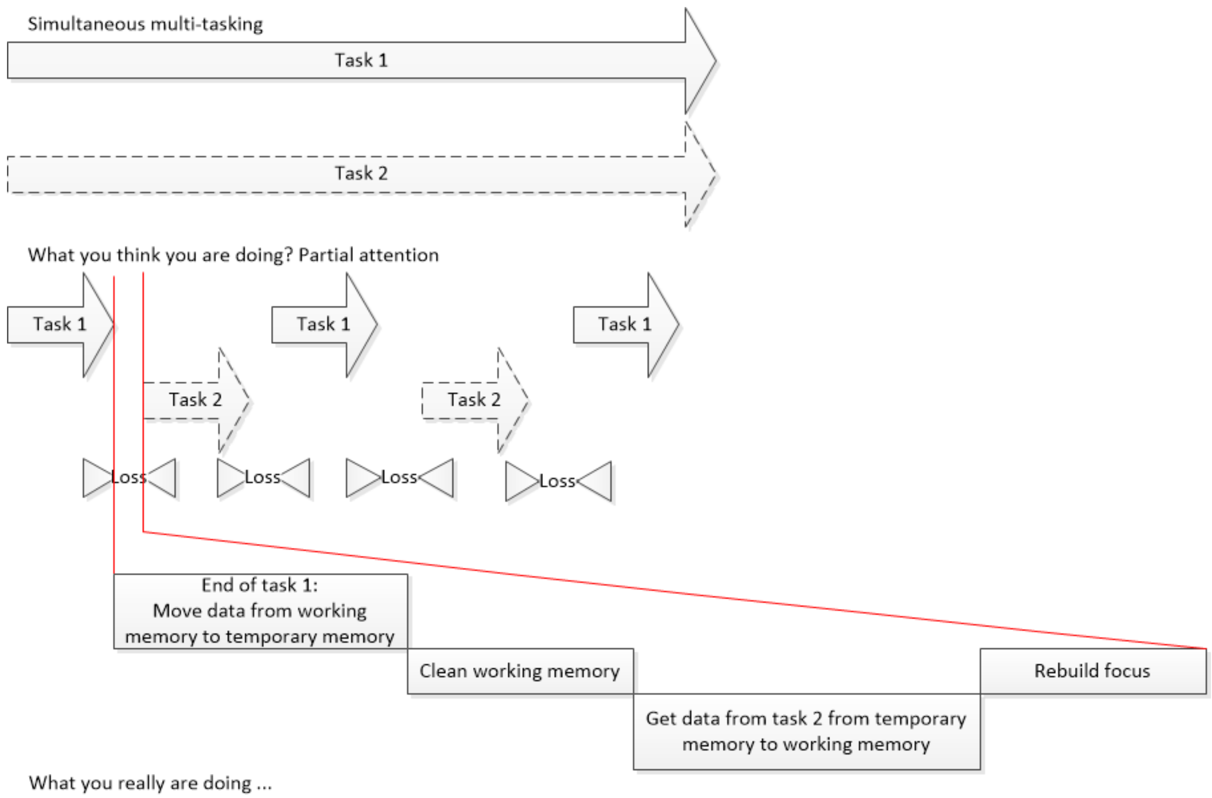
It illustrates the importance of having an alarm philosophy and an audit process in place: if you don't have your site alarm philosophy, the performance of your alarm system will be compared against the KPIs set forth in the standards and guidelines.

The danger of averaging

One alarm per ten minutes cannot be converted to six alarms per hour and certainly not extrapolated to 144 alarms per day. Everybody should understand that if a person can perform one task in an average time frame, he is not going to keep this level of performance for the entire day. Usain Bolt can run 100m in less than 10 seconds. This does not mean he can run a Kilometer in 100 seconds. And he probably cannot run it six times in a row without any recuperation.

The six alarms can all occur within five minutes of an hour. Likewise, the 144 alarms of a day can all occur in (less than) an hour.

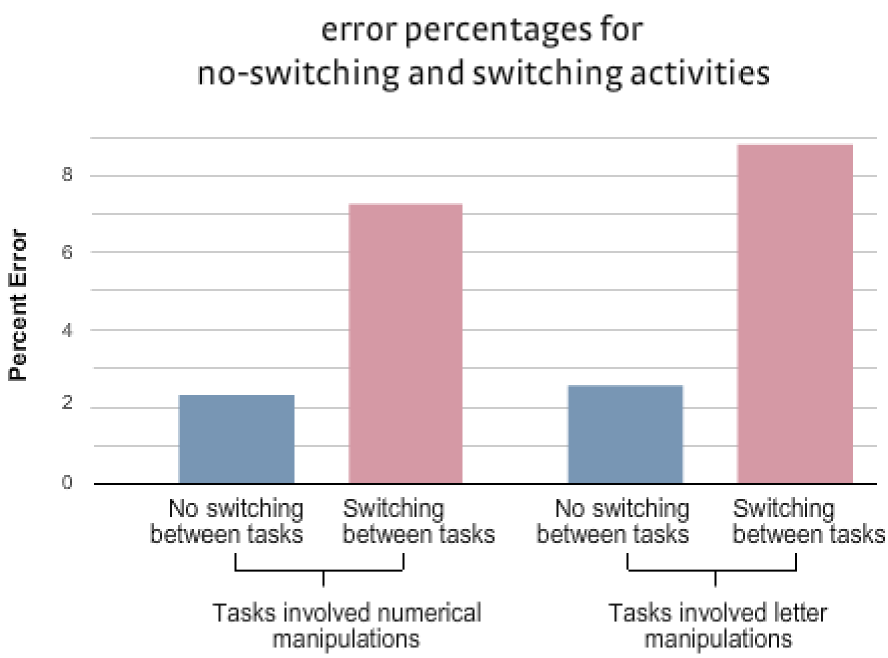
Confronted with multiple alarms at the same time, the operator must switch his attention between these alarms and perform actions appropriate for each alarm. Recent psychological studies [Brainchains, Compernolle et al] have provided evidence that multi-tasking negatively impacts the performance of a task, i.e. more time is required to perform the divided tasks than if the tasks were to be completed serially. If an alarm initiates the start of a task – and it should – then the number of alarms annunciated provides an indication of how many tasks the operator should perform. The following figure illustrates this.



Source: Brainchains, Prof. Dr. Compernolle Theo, pages 43 - 48

Psychology delivers evidence that the sum of completing two tasks simultaneously increases the time of completion of both tasks (significantly) and is greater than the sum of the time to complete both tasks sequentially.

Furthermore, neurological research has pointed out that switching between tasks, increases the chance on errors and mistakes significantly, as illustrated in the graph below.



Source: Brain Rules, Dr. Medina John

The problem with the (equal) distribution of the annunciation of alarms over a day has made the standard committee decide to remove the daily KPI "Annunciated Alarms per day per operating position" from the list, as well as the "percentage of hours containing more than 30 alarms".

It must be remembered that the KPI was created to provide a measure for a manageable workload for an operator and there are – hopefully - no control rooms where operators work 24 hours per day. Translating the calculation from one alarm per ten minutes to six per hour (on average), in my opinion, nonsense.

Unauthorized actions

The two entries "Unauthorized alarm suppression" and "Unauthorized alarm attribute changes" were also removed from the list of alarm performance metrics.

There is in the 2016 version of ANSI/ISA 18.2 an obligation to monitor alarm attribute changes and there is a recommendation to detect uncontrolled suppression of alarms.

Measuring the unauthorized actions has nothing to do with the alarm system performance. It is rather a separate process which should monitor that the changes made to the alarm attributes or suppression are authorized and recorded. This should be done first in your Master Alarm Database and then applied to the control system, not the other way around.

Some of the unauthorized suppression methods (cutting wires, silencing the horn, putting coins on the keyboard) cannot be detected by a software application or the control system and by consequence cannot be traced in the alarm historian.

Therefore, it was decided that these should be part of the audit process and no longer part of the alarm system performance metrics.

Conclusions

The alarm philosophy is the place to specify alarm system key performance indicators which make sense and are achievable in <u>your</u> plant.

Specify the interval

Rather than specifying an amount of alarms per operator, per hour, per shift or per day, more attention should be given to the interval of annunciated alarms. An interval should be long enough to read and understand the message, to acknowledge that human intervention is required and to have time to perform the required actions. That makes sense.

The occurrence of multiple alarms annunciated at the same time with little or no interval often point to the same problem. Under the assumption that a set of alarms generated in a short amount of time point to the same problem or root cause, and the situation can be returned to normal with a limited set of actions, one could argue that there is no need for multiple alarms. Consequently, it is recommended to replace all those alarms with one single alarm using advanced logic, with meaningful information, diagnostics and proper advice.

Specify meaningful values in your Alarm Philosophy

Take the opportunity to specify meaningful values per mode of operation. In start-up or shut-down mode, these values could be different from steady state.

Remember that not all plants and installations run 24x7 for a long period like a refinery, a compressor station or a base load power generation plant. These were the type of industries where the operators were interviewed to come to this famous one alarm per ten minutes paradigm. If your plant only runs day-shifts, it might be wise to specify different values for day or manned operation and night or unmanned operations. If there would be a start-up shift, an operations shift, a clean-up shift and a no-operations shift, four classes of values could be specified.

If you don't specify anything in your alarm philosophy or if you don't have an alarm philosophy, the performance of your alarm system will be measured against general accepted good practice values, like the ones specified in IEC 62682 of ISA 18.2. That might make no sense.

If you have a plant where you have 300 alarms per hour (on average one every 12 seconds), your operators will be happy to see these go down to one alarm every 30 seconds. That could be an achievable goal for the first year you have your alarm philosophy in place. The next audit process could reveal how the operators cope with this rate and with this input, a new rate can be proposed, for example one alarm every 45 seconds. That makes sense, doesn't it?

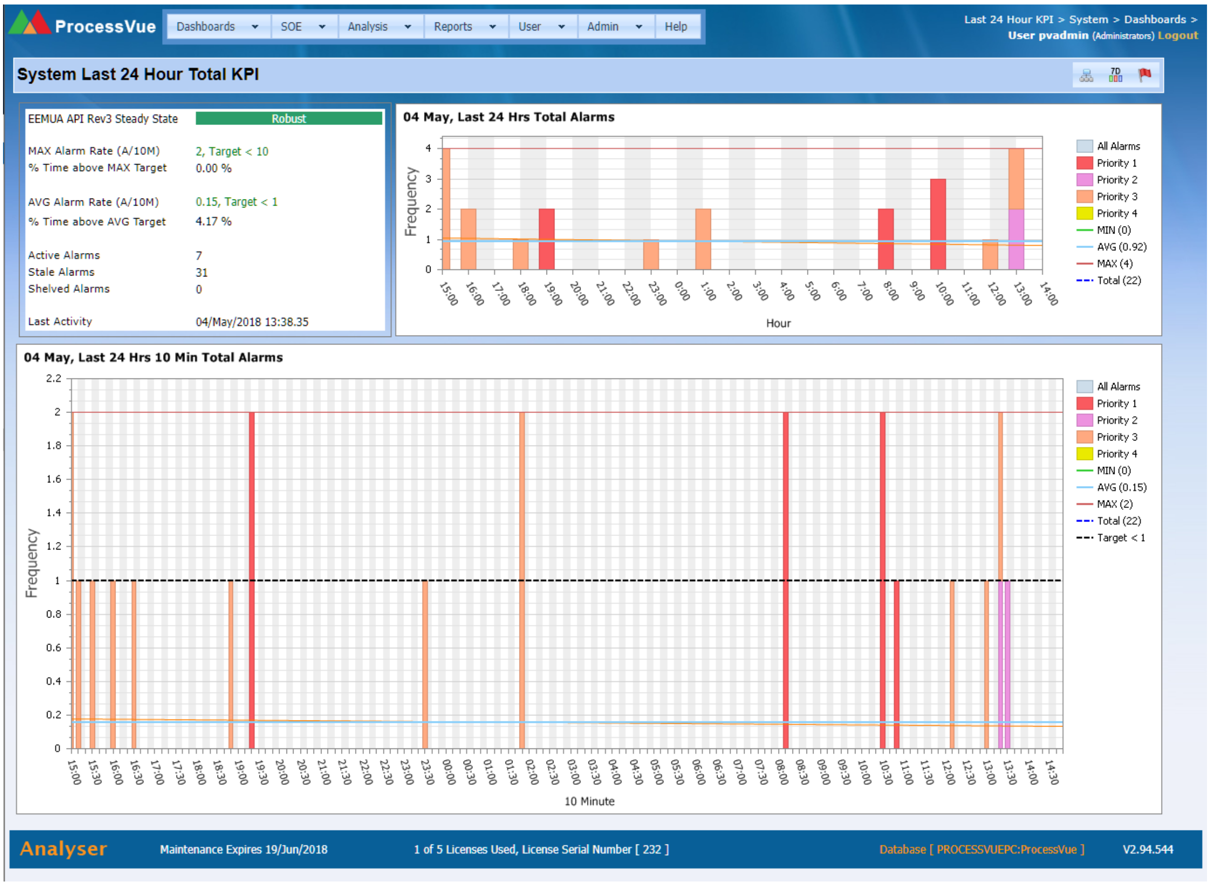
Just specifying six alarms per hour on average when you are dealing with 300 on average, might make everybody think it is unachievable and by consequence de-motivate the staff working on an alarm system improvement and put them under unnecessary pressure.

Choose the right tool

Given all the above, it makes sense to specify an alarm system performance measuring tool or report generator which supports all that is proposed above.

Rather than drawing lines in graphs on average alarms per hour or per day per operator, it is recommended that the tool can present the data in a way the operator is confronted with them, i.e. in number of alarms per time frame you specified in your alarm philosophy.

When an hourly analysis does not report any excess of the average alarm rate, the ten-minutes analysis reveals ten-minute time frames (as illustrated in the screenshot below) where the operator receives more than one alarm and is forced to either choose one (the one with the highest priority) or to start multi-tasking (when the alarms have the same priority). Rationalization can investigate if these alarms are redundant or not (point to the same problem), and if they are, improve the alarm system to, for example, suppress one alarm in favor of the other alarm, or come up with a new alarm with better diagnosis in the alarm text.



Source: ProcessVue Analyser

It makes sense to give the KPIs, the prioritization methods and the alarm set point configuration methods you specify in your alarm philosophy a proper review and make sure there is consistency and achievable values are defined, enabling the operator to respond to abnormal situations, deviations and failures in your plant.

References

EEMUA Publication 191 First Edition, Second Edition, Third Edition
ANSI/ISA 18.2 – 2009 and 2016
IEC 62682 – 2015
Brainchains, Prof. Dr. Theo Compernolle MD, ISBN 9789401417457, pages 43-53
Brain Rules, Dr. J. Medina, ISBN 978-0983263371
The Management of Alarm Systems, HSE 1998, M.L. Bransby & J. Jenkinson
MAC Solutions - ProcessVue Analyser (www.processvue.com)

About the author

Lieven Dubois (°1957) studied first electronic engineering and then software engineering in Belgium. He got involved in alarm management in the 1990s, where he introduced a real-time expert system to assist operators in dealing with abnormal situations.

Lieven started contributing to the ISA 18.2 Technical Report 4 on Advanced Alarming in 2009 and is now voting member of ISA 18.2 Alarm Management Committee. He was elected co-chair of Working Group 8 preparing a technical report on Alerts, Prompts, Notifications and Events.

Lieven was also involved in the preparation of the International Electro-Technical Committee (IEC) 62682 standard and the ISA 18.2 2016 edition. He is a qualified ISA IC39 alarm management course instructor.

Lieven is co-author of several papers about the application of real-time Artificial Intelligence technology, in particular to the domain of Alarm Management. He is a multilingual presenter on Alarm Management and Situational Awareness at several seminars, workshops and conferences, among others at the triennial IFAC HMS conferences in Valenciennes 2010 and Las Vegas, 2013.

M.A.C Solutions (UK) Ltd. UNITS 6 & 7 KINGFISHER BUSINESS PARK,
ARTHUR STREET, REDDITCH, B98 8LG. UK.

WEB: www.processvue.com
EMAIL: sales@processvue.com

Telephone : +44 (0)1527 529774