Alarm Enforcement … or not?

Introduction

Alarm Enforcement is the process of comparing Process Control System (PCS) alarm attributes with the authorised list of alarm attributes held within a site's Master Alarm Database (MADb), and restoring those which are found to be at variance to the values held within the MADb.

In this paper, we will discuss the pros and cons of this practice.

Is enforcement a requirement?

Alarm Enforcement is included in section 12 of the alarm management standards[1,2], which is an informative section. Unusually for a standard, section 12 cannot be considered to be normative, as it does not prescribe what 'shall be done'; but simply describes a number of features and functionalities not normally found on standard or legacy control systems which may be used to improve the management of alarms.

How is enforcement applied?

Enforcement can be accomplished by running a routine either manually on request, or at regular intervals (very often at shift change), which highlights those alarm attributes currently active in the PCS that are at variance with the information held in the MADb. Operators can elect to accept these variances or revert to the values captured in the MADb.

Why do we need enforcement?

The only reason one would want or need to restore the PCS alarm system parameters to those which are held within the MADb, is because the parameters contained in the PCS have been modified for some reason. There are effectively two cases which can be identified of why alarm system parameters have been changed:

- Authorised modifications to the alarm system parameters have been made in accordance with the Management of Change (MoC) procedure.
- Unauthorised, possibly undocumented changes have been made to the system, often as a result of tampering.

In a well-designed, managed and maintained alarm system; there should be no difference between the MADb and the alarm attribute values in the PCS, therefore, there should really be no need for Alarm Enforcement. Consider the following points:

System design

If the alarm system has been designed correctly; the right alarm, appropriately prioritised and with the correct setting, will be presented to the operator at exactly the right time no matter what the plant state is. No inappropriate alarms will be generated.

For all processes; alarms which are not required during particular plant modes (e.g. start-up, offline etc.) such as low flows or pressures will have been considered, and the logic to control them designed into the PCS.

In batch systems; alarms such as for example, agitator speed deviation, which may be critical during a cook phase to warn of the potential for a solid batch, may be of lesser or no importance during the initial charge, heat up and discharge operations, and the batch software will have been designed to manage this and other alarms appropriately for each phase.

Of course, even in well managed systems there may still be nuisance alarms generated by, for

[1] ISA 18.2 – Management of Alarm Systems for the Process Industries
[2] IEC 62682 – Management of alarm systems for the process industries

example, faulty transmitters or changing process conditions; but these should be dealt with by 'shelving' the alarm in accordance with the site's documented procedure (or alarm philosophy).

Management

In a well-managed system where an Alarm Philosophy and supporting related documentation has been implemented, a robust approach to auditing and assurance is followed, and ALL changes are managed and approved via the MoC process; there should be no differences between the alarm attribute values in the PCS and those held within the MADb. Of course, the MoC procedure must be designed to ensure all changes (temporary, permanent and emergency) are covered.

Maintenance

If all maintenance to process equipment is carried out appropriately; so that for example when a measurement device is calibrated, maintained or replaced, there is a rigorous process to ensure the instrument is ranged correctly and that all alarms generated from the device are tested and validated once the instrument is returned to service; then there will be no need for operations personnel to make unauthorised, compensatory changes to the alarm attributes as all will be as it should be, in accordance with the authorised attributes recorded in the MADb.

Culture?

In any walk of life, there are individuals or groups of individuals who believe the 'rules' don't apply to them and the process industries are no different. If everyone rigorously followed the rules, processes and procedures, then there would be no unauthorised, deviant alarm attributes within the PCS which need to be restored by Alarm Enforcement.

However, some personnel believe they can 'do what they want to make their life easier', or change things without following procedure 'because they can', or simply because 'this is the way it has always be done' and they don't want to change.

Of course, dealing with issues like this falls under the 'Management' category, and as difficult as it may be, cultural issues must be addressed to ensure the success of any system of alarm governance and to mitigate the use of Alarm Enforcement.

Technical aspects

In order to perform Alarm Enforcement, there must be a MADb where all the attributes of the (different) alarm systems are stored and kept updated in a versioning system. Basically, there are 'old' versions, there is the 'current' version operational in the control system and there is the 'new' or 'next' version which contains all validated changes to the alarm attributes. Within the newest version, there might be a distinction between validated and non-validated alarm system parameters.

For flexibility, Alarm Enforcement may contain an option to restore the current alarm system parameters or the newest.

When enforcing the newest, the current becomes the previous version and the newest the current. Care should be taken when enforcing the newest values, as operations personnel may not have been made aware of changes to parameters which may affect the way the plant is operated.

There are several ways to achieve enforcement. One is to overwrite the alarm settings, for example through an OPC DA interface, another is to restore through a back-up file. Care should be taken in restoring from a backup file, as in some systems this may cause the PCS to re-initialise itself thus shutting down the plant. In continuous processes, a sequenced restore through OPC DA is preferable. In industries where there is no 24-hour production, for example batch processes, enforcement may be achieved by restoring a back-up without suffering process interruption.

Practical aspects

It is considered to be good practice to monitor any changes to the alarm system parameters. In modern process control systems, this can very often be achieved automatically by monitoring the OPC DA server, whilst the process for legacy systems is likely to require manual intervention.

In general, however, it is not considered good practice to allow operators to change alarm system parameters. Changes to the alarm system should undergo a strict review and testing process to ensure unforeseen risks are avoided. Of course, in some systems (such as safety PLCs, Emergency Shutdown Systems (ESD's) etc.), it is impossible to change alarm parameters without the appropriate programming device.

When a plant owner allows users or operators to modify alarm system parameters, a User Interface into the PCS must be provided. Where there is such an interface, activity logging should be available and enabled to track all modifications. Log files should be regularly reviewed to identify any changes made, and where necessary, permanent modifications may be prepared, reviewed and approved appropriately via the MADb tool.

Modifications identified through such activity logs can be traced back to a single operator or a repeating shift to identify the reason for the modifications. In some cases, operators may use modified alarm settings as early warnings, while their colleagues may find such modifications a hindrance. Where alarm settings are regularly being changed to give early warnings, the introduction of operator-configurable alerts should be considered. Any unauthorised changes to alarm parameters should always be reported to the person responsible for the alarm system, and this person should take immediate action; for example, by enforcing the current settings from the MADb or formalising the identified changes through the MoC process.

Arguments in favour or enforcement

Reset operator changes

Where operators have been allowed to make changes during their shift, a reset at the end or start of the next shift of the alarm system parameters with the agreed settings, is a must. Operators usually do not take the time to go through all the changes the previous operator made and restore these one by one. It is better to start the shift from a well-defined and agreed set of parameters.

- Operators are not the appropriate people to make changes as they may not consider the full consequence and risk assess the changes they are making. Operators should not be allowed to make changes.

Impose settings for a recipe

In the batch industry, each recipe could come with its own purpose-defined alarm settings. Enforcing is a good practice to set the alarm parameters to the right values for each recipe.

- To achieve this; enforcement will either have to be running continuously to be able to detect all product changes or be manually initiated at the beginning of every batch. In a properly designed system, alarm parameters should be automatically loaded as part of the batch setup and be modified appropriately in each phase.

Operations based enforcement

In some industries, the process is only active during one or two day-shifts. After the last shift, a cleaning process could take place, for which a separate set of alarm system attributes could be loaded. After cleaning, the process may be put into a hibernation type of mode, for which a third set of alarm system parameters could be required. At the start of the production, the normal operating settings could be enforced.

- Enforcement will either have to be running continuously or be manually initiated at each stage of the cleaning process. In a properly designed system, logic or state based alarming should be implemented within the control system where possible, to provide the right alarm at the right time.

Overhaul enforcement

After a shutdown of the process or a holiday break, many parameters in the system may have changed; new devices and instruments might be installed, control loops might be configured

differently, equipment can be replaced, back-up or additional equipment installed, etc.

For all of these systems, new alarm parameters could have been designed, reviewed and been approved in the MADb as the newest version of the alarm parameters. The enforcement mechanism can assist in a swift and adequate way to update all the alarm system parameter settings.

- The project and maintenance processes should include a commissioning step which ensures all parameters are updated where new or different equipment is installed, or maintenance of existing equipment has been carried out.

Arguments against enforcement

Quality of the enforcement process

The enforcement process needs to be thoroughly tested, tightly controlled and be of exceptional quality to avoid situations where either, not all alarm system parameters are updated or, parameters are updated with incorrect values. What happens to enforcement when the application loses communication with our control system? Verifying the process will be a huge task that we don't have time to do.

- This is more likely to be a valid argument where enforcement is carried out by third party applications than if the mechanism is an integral part of the control system design.

Interruption of production

If the enforcement process requires temporary stoppage of the control logic, for example where backup files must be reloaded which may be the case for many legacy systems, it is not advisable to apply or allow enforcement.

- In a well-managed system, the number of variances should be small and when identified, these could easily be addressed manually, therefore there should be no requirement for system downtime.

Validation of the process

In some industries, for example the pharmaceutical industry, all processes are validated; after which no changes should be made until the process has been re-validated. In such industries, alarm enforcement should not be applied.

- Enforcement can be manually initiated and applied once identified changes have been reviewed and approved, and these checks can be included as part of the validation process.

Cyber security

Those that have a MADb and also employ Enforcement need to carefully consider that fraudulent individuals inside or outside the organisation now only need to access the MADb to affect your Control System. Knowledge of databases, their structures & configuration is more widely spread than knowledge of the configuration or programming of your PCS. Attackers are very clever at exposing weaknesses in such systems and as a MADb with Enforcement has to reside on a network with real-time, trusted access to the PCS; if it is poorly implemented, you could be opening a very wide door for attack. You may just have built the perfect Trojan horse!

A MADb without Enforcement can reside on a network 'air gapped' from the PCS, however, the use of USB sticks or portable drives to bridge the 'air gap' to restore alarm parameters as part of the enforcement process is also risky and must be managed very carefully.

- If network and system security is addressed correctly, the threat from external or internal tampering can be significantly reduced.

Good practices

Ban operator-allowable changes to the alarm system

When making changes to the system to overcome perceived issues, operators are very unlikely to

consider the full implications of their change or put mitigations in place, and will often fail to document or communicate their changes.

- If they make changes because of nuisance alarms, consider the use of 'alarm shelving'.
- If they chose to make changes to give 'early warnings', consider the use of operator 'Alerts'.

Proper alarm system changes

Establish a process, eventually with digital signatures, to approve any change to alarm system parameters. Use enforcement only to write approved changes to the alarm system. All alarm system changes should be in accordance with the current alarm philosophy.

Test all changes, train the operator

There is an emphasis on testing and training in the alarm management standards. Not only should all approved changes be tested after each enforcement, but the operators should also be trained on the new alarm system parameters when these are updated.

As all operators should be acquainted with the alarm philosophy, they should be assured that all changes are carried out in accordance with the current alarm philosophy.

System audits

Auditing is a requirement of the standards, and indeed one of the recommended alarm performance metrics is a measure of 'unauthorised alarm attribute changes'. An Alarm Enforcement tool could therefore be used in a read only capacity to supplement our auditing processes.

One of the benefits of an Alarm Enforcement tool is, if you disregard the update/restore functionality; the ability to compare the PCS alarm attributes to those of the MADb at any time, to identify if any unauthorised changes have been made to the system. It is much easier and quicker to have a tool to compare attribute values between the PCS and MADb, than to manually call up and review each of the thousands of attributes within our system.

Control at all times

Do not allow enforcement to run in the background and make changes automatically without any form of notification and acceptance. Ensure a positive confirmation is required before any parameter update.

Take cyber security into account

When establishing a Master Alarm Database, ensure it is on the right side of the firewall. Consider also, controls to minimise or prevent the use of memory sticks or CD's/DVD's within the control system.

Conclusions

Q: Should we really 'need' Alarm Enforcement in a well-designed, managed and maintained alarm system?

A: No. Alarm Enforcement is no substitute to a robust system of governance and MoC which is rigorously adhered to.

- However; how many sites have resolved all their alarm management issues and can demonstrate a robust system of governance which stands up to the closest scrutiny?
- If you can't, then you may need to consider the use of Alarm Enforcement to temporarily resolve some shortcomings. However, Alarm Enforcement should be thought of as just a 'sticking plaster' to use until all your maladies (design, management, maintenance and cultural) are truly healed.
- Once you are in control, the process of Alarm Enforcement becomes redundant and it is effectively a process that is used 'because you can', not 'because you need to'. The comparison engine functionality, however, can become an important tool for application in the auditing process.

Q: Is Alarm Enforcement a good thing?

A: Yes and No. Alarm Enforcement can be considered to be a RAGAGEP (Recognised And Generally Accepted Good Engineering Practice), but only if it is implemented correctly and for the right reasons.

- Yes - It is a good thing when used for example to:
    - Update PCS alarm parameters quickly, easily and securely to the new, approved values stored in the MADb as part of a robust MoC process, following rationalisation or modification projects .
    - Update PCS alarm parameters to the authorised values if a PCS has been re-initialised following maintenance or repair to the system. (The PCS may not have been backed up regularly and may contain old settings which can be updated by Alarm Enforcement).
    - Ensure that alarm parameter settings are restored to the authorised values in the event of unauthorised changes being detected, due to internal tampering or external malicious attack, as long there is absolute confidence that the MADb itself is secure.
- No - It is not a good thing if it is implemented simply to compensate for poor governance or bad practices:
    - If Alarm Enforcement is to be used as a tool to (regularly) 'clean up' your alarm system as the MoC process is poor or non-existent, or unauthorised changes are tolerated; then this is an indicator that you are not in control of your system.
    - If you are not in control of your system and you use Alarm Enforcement to hide problems or as an excuse to avoid implementing a robust system of 'alarm management', then you are not in control of your plant.
    - If you are not in control of your plant, you are actively condoning the possibility of harm to people, the environment, or damage to your reputation, assets and financial loss.

Q: Should I embrace Alarm Enforcement?

A: Yes. But welcome Alarm Enforcement as you would a new pet. Don't be 'persuaded' to implement it, ensure you get it for the right reasons; and make sure you control it, don't let it control you!

Although Alarm Enforcement is neither a requirement of the standards, nor an essential tool; and as earlier stated, in a well-designed, managed and maintained system it should not be 'needed'; its use will augment the processes, procedures and auditing capabilities you develop for the management of alarms and alarm systems on your site.

This article has been co-authored by Lieven Dubois of Manage4U and Ian Brown of MAC Solutions. Brief biographies of the authors are given below:

Lieven Dubois
Manage4U
Principal Consultant

Lieven Dubois (°1957) studied electronic engineering and software engineering in Belgium, following which, he gained experience in the process automation industries and subsequently with real-time expert systems. Lieven is co-author of several papers about the application of real-time Artificial Intelligence technology, in particular, in the area of Alarm Management. He is a multilingual presenter (fluent in Dutch, French, English and proficient in German and Italian) on Alarm Management and Situational Awareness at seminars, workshops and conferences, and he presented at the triennial IFAC HMS conferences in Valenciennes 2010 and Las Vegas, 2013.

Lieven contributed to the ISA 18.2 TR4 in 2009 and is now a voting member of ISA 18.2 and elected co-chair of WG8. He 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 member of the ISA 101 committee for Human Machine Interfaces and participated in the final meetings of the standard development. In addition, he is a qualified ISA IC39c course instructor.

Contact Details:
Mob: +31 653 892060 or +32 493 199355
Email: Lieven@alarmmanagement4u.com
Web: http://www.alarmmanagement4u.com

Ian M Brown
MAC Solutions (UK) Ltd
Alarm Rationalisation and Services Manager

Educated in Electrical and Electronic Engineering and with over thirty-five years of experience in the process industries, Ian has accumulated knowledge across a range of sectors, including industrial, chemical, speciality chemical, pharmaceutical, petrochemical, power generation, nuclear and oil & gas; and has held a variety of technical (hardware & software configuration), maintenance management and consultancy roles.

Having successfully led a number of alarm rationalisation projects for clients over the past ten years, which resulted in significant reductions in annunciated alarm rates and improvements to their management of alarms; Ian's expertise covers IEC 62682, ISA 18.2 and EEMUA 191. In addition to being a member of the ISA, he is also a TÜV certified Functional Safety Engineer (6424/13).

Contact Details:
Tel: +44 (0)1246 733120
Mob: +44 (0)7808 039250
Email: ian.b@mac-solutions.co.uk
Web: http://www.processvue.com