Minimising alarm proliferation during system upgrades or replacements

Introduction

If your old control system is due for replacement, or perhaps it is being upgraded to the latest, greatest version; what can you do to ensure that post implementation, your operators are not suddenly overburdened with tens, hundreds or even thousands of new, unnecessary alarms?

This white paper will identify the main reasons so many upgrade and replacement projects cause so many problems after system handover.

Why do problems occur?

The simple answer is 'Management of Change' (MoC). However, this heading usually masks a combination of avoidable failings which lead to your poor operator floundering in a sea of unnecessary alarms following your system upgrade.

Typical reasons for the proliferation of unnecessary, nuisance alarms following a system upgrade or replacement are:

- Poor MoC process
- Inadequate documentation
- Poor project management
- Belief that your vendor / integrator will give you the system you want
- Lack of understanding or knowledge of the new system
- Poor configuration by poorly trained engineers and vendor defaults
- Time / Cost

Before considering why some systems degrade following upgrade or replacement, first take a moment to review two of the four 'core principles' underpinning the EEMUA 191 guidelines[1].

Under the heading *'Usability'*, the guidelines state that *'Alarm systems should be designed to meet user needs and operate within the user's capabilities'*.

Under the heading *'Investment in engineering'*, The guidelines state that *'Alarm systems should be engineered to suitably high standards. The design should follow a structured methodology in which every alarm is justified and properly engineered. The initial investment in design should be sufficient to avoid the operational problems and the safety, environmental and financial risks that often arise and which result in overall higher lifetime costs. Contract strategies should be chosen to ensure that alarm systems are engineered to good standards'*.

If you don't take control, the system delivered to you may not be the system you are expecting and if your upgrade / replacement project delivers a system with unmanageable numbers of unnecessary alarms; not only have you failed to deliver on the usability principle, but as you will have to spend time and money reducing alarm numbers through subsequent rationalisation and reconfiguration, one can speculate that the system had not been engineered to high standards thus failing to meet the principles of investment in engineering.

So how can you minimise the possibility of degrading your alarm system whilst it is upgraded or replaced?

Poor MoC

Is your MoC process fit for purpose? It may be eminently suitable for civil construction, but how well does it work when dealing with alarm system hardware or software upgrades or replacement?

Does your MoC process include stage gates or checks and balances which can be applied throughout the project? Whilst it may identify if a lift plan is required or hazards from working at height, does it also include for software acceptance testing? If not, why not?

Comments are often made during benchmark assessments that no-one uses MoC for alarm system changes as the process is either too onerous, too takes too long, or simply, isn't suitable for the changes required.

Before you start your upgrade or replacement, make absolutely sure you MoC process is relevant and appropriate.

Inadequate documentation

Of course, you will say 'we have an Alarm Philosophy'. But is it enough? Do you have an Alarm System Requirements Specification (ASRS)? If not, why not?

If you consult the international alarm management standards IEC 62682[2] and ISA 18.2[3], clause 7; you will see that an ASRS *"documents the alarm functionality expected of the control system"*. Whilst your Alarm Philosophy is based on your current system and its capabilities, the requirements defined in your ASRS are *"used to help evaluate systems, guide the detailed system design, and serve as the primary basis of alarm system function testing during implementation"*.

Furthermore, the standards state that an ASRS *"is typically generated early in the planning for a new control system"*.

So, an ASRS defines the functionalities you wish to have to help you manage alarms the way you want to.

In the recommendations clause, 7.2 in the standards, *"Planning for new control systems and major revisions to the alarm functionality of existing control systems should include an ASRS, …"* is stated.

If you don't have an ASRS, when you replace or upgrade your control system, you are likely be given the alarm functionalities the vendor has at the time, whether they meet your requirements or not.

Poor project management

No-one wants to be labelled a poor project manager so it's important to complete your project on time and under budget if possible. Therein lies the problem. Often, project managers push the vendor to complete and in doing so, miss vital checks that leave operations and maintenance departments to deal with multiple problems after handover.

This happened within the last three years in a major UK company. The project manager did not carry out acceptance testing prior to installation and handover, but the replacement system was installed and made live anyway as the project manager had committed to a schedule and was under time pressures from senior management.

What was the result? The installed system frequently crashed, sometimes twice a day, alarm information was often lost, floods of alarms were re-annunciated after server re-boots, the operators were unable to view alarm setpoints, …. The list goes on.

The system as installed was not fit for purpose, although the control system vendor worked hard to resolve the problems. The project had been 'completed' on time and closed, and all the issues became problems for the operations department and the operators.

Does this sound familiar? Project closed although the system does not meet requirements and the operations department carries the can AND the cost of rectification!

As a project manager, ensure you robustly follow all the stages of your MoC and with reference to the 'Investment in engineering' core EEMUA principle, "*Contract strategies should be chosen to ensure that alarm systems are engineered to good standards"*; ensure your project meets the requirements of your project specification. Put penalty clauses in your contracts which reference late delivery or failure to deliver key functionalities and invoke them if necessary.

Ensure your system is fully tested and don't install / handover the system until operations have assessed and confirmed that it meets their requirements.

Will you get the system you want?

Whether you are upgrading a system with the same supplier or migrating to a new system from a different supplier; what you want, is a system that is not worse than the one you currently have.

Obviously, your vendor / system integrator knows your system best, so they say; but do they really know exactly what you require of your system?

Unless you make them aware of the requirements set out in your Alarm Philosophy and ASRS, they may not deliver the system changes or improvements that you really want or need. However, even if they are aware of your requirements; are there any potential issues which may result in you ending up with a degraded system?

Lack of understanding or knowledge

Not being clear on how updated or new functionalities will impact the performance of your alarm system is a real issue which often causes problems during system upgrades.

It is possible that your current software may be upgraded to the latest version during a routine maintenance visit; but if it is, do you know how your system may be impacted, have you been informed? More importantly, does the engineer carrying out the upgrade understand everything about the upgrade?

Poorly trained engineers

You may think that by using the system supplier's engineers to configure or upgrade your system, your system will be appropriately configured. This is not necessarily the case. Often, system engineers work on a system without having been fully trained and really do not understand what every parameter is, what they do, and how they will impact your system.

In Q2 2019, the author worked with an engineer from a globally recognised control system vendor, who did not know what many of the parameters were on the system and had no idea if they were critical to operation or not.

When problems were encountered and the client needed answers, the engineer called a colleague in another country and shared the configuration screen by WhatsApp video, so that the remote engineer could give guidance as to which parameters should be enabled or modified. Incidentally, the remote engineer also struggled to answer many of the questions. A lot was done on a 'try it and see' basis.

In the end, the client delayed importing modified configuration until answers could be obtained as to how critical, identified changes to parameters may be.

Vendor defaults

Often, new features and functionalities are enabled by default whether you want them or not. This is particularly prevalent when moving from one system to a different one. Functionality which did not

exist on the original system appears on the new system and is enabled by default, potentially leaving your operator deluged with hundreds or thousands of alarms that he does not understand.

On one control system reviewed by the author, default settings were an issue; all alarm priorities had been set to High, Priority 1, by default. What would have been better, is that all potential alarms were disabled by default, and only enabled once individually justified and supported with an operator response.

Consider also, default values for the return to normal condition. One DCS vendor routinely set the return to normal condition as an alarm condition at the same priority as the alarm. Migrating from a system where this was not the case, resulted in a doubling of the operator's alarm load, without taking into account all the other 'new' alarm conditions that were enabled by default and that did not exist on the original system.

Beware unexplained parameters and default settings!

Time / Cost

You only get what you pay for; and often you may have imposed tight time schedules to meet a shutdown window which will minimise disruption to your plant, or perhaps your purchasing people have negotiated hard, and cut project costs to the bone.

Naturally, to meet your schedule and remain within budget, your vendor / system integrator will do only the tasks you have requested of them. Potentially, this can lead to the issues noted below.

System upgrades

As mentioned earlier, if you are upgrading your system to the latest version, you may find that there are new alarm features or settings which your current system does not have. These may be enabled by default when the upgrade is applied.

For a 'simple' upgrade, it is unlikely that anyone is going to take the time to go through the configuration of all your tags and check that only those alarms that you had previously exist, and that any new alarm settings are turned off unless you specified them to be turned on. After all, you've only paid for an upgrade, not a wholesale configuration check.

This very scenario happened to the author when installing upgraded software on a process plant some years ago. System engineers had provided the software for installation. The new version included an extra alarm field which the author had not been made aware of, and the system engineers had set to 'True'.

Result? For a system with only 1,000 tags, there were suddenly 1,000 extra, potential alarms. The author had to review the 1,000 parameters with the client and set appropriate values for each parameter. It took a little while!

System changeover

If you are migrating from one vendor's system to a different vendor's system, it is likely that much of the configuration on the new system will be done remotely via migration scripts.

Such scripts will transfer most, but not all, of the original system configuration to the new system. They will migrate all the important, common parameters such as tag, description, range, engineering units, deadband, etc., and insert them into the new system's configuration. This is where the migration can begin to unravel.

Parameters like tag and description should be no problem, they are only text fields, but what about deadband? Deadband can be expressed either in engineering units or as a percentage or range.

What if the migration script takes a deadband value of '3' from the original system and inserts '3' into the new system, will it matter? YES.

If the original system expressed deadband as a percentage of range, e.g. 2% on a range of 0-5 bar, this will create a deadband value of 0.1 bar. If the new system uses engineering units for deadband, the deadband will be 2 bar. Twenty times the intended deadband. Quite a difference, and a standing alarm waiting to happen.

This does happen and the author has seen configurations migrated from two different systems to a globally recognised DCS, and in both cases, hundreds of standing alarms were created as once alarmed, process variables did not clear due to deadband having been wrongly implemented as engineering units when a percentage was required.

Converting the deadband for each tag from a percentage to an engineering unit number or vice versa, is a time-consuming task. Has this been factored into your migration? Probably not.

Another migration related issue to watch out for, perpetrated by the very same DCS vendor's engineers, was transferring PID loop parameters straight from the original system to the new system. The original system used 'gain'; the new system used 'proportional band'. In the original system, the derivative term was set to zero to disable derivative action. In the new system, a derivative setting of zero did not disable derivative action but was used as part of the calculation. Due to the errors in not recalculating the PID parameters, the loops simply refused to act & control valves failed to move.

Even if the loops had worked, it is likely that nuisance alarms would have been generated due to the transferred loop parameters. Poorly tuned loops are recognised as one of the causes of nuisance alarms.

Conclusions

There should be no reason why your upgraded or new system should be worse than your current installation, although from time to time, this may happen.

The issues noted above can be avoided by making sure you have a properly written Alarm Philosophy and ASRS, and that your management of change process is robustly followed from project specification and initiation, through to completion and handover to operations.

Also, you must make sure you understand exactly what is going to change and how any change may impact your operators.

Unless you are specific with your requirements and robust in managing change, you may fall foul of the two core principles mentioned at the beginning of this paper and end up with a system which is unusable, and will cost a significant amount to put right, post installation.

[1] EEMUA 191 3rd Edition – Alarm Systems - A guide to design, management and procurement
[2] IEC 62682 Edition 1– Management of alarms systems for the process industries
[3] ISA 18.2-2016 – Management of alarms systems for the process industries

A brief biography of the author, Ian Brown of MAC Solutions, is given below:

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

Educated in Electrical and Electronic Engineering and with almost forty 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 twelve 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 also trained as 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