72nd Annual
INSTRUMENTATION AND AUTOMATION SYMPOSIUM FOR THE PROCESS INDUSTRIES
JANUARY 24 – 26, 2017
MEMORIAL STUDENT CENTER • TEXAS A&M UNIVERSITY • COLLEGE STATION, TX

# Burner Management System Upgrade Challenges and Opportunities in Brownfield Installations

**Mike Scott, P.E., CFSE**
Executive VP, Global Process Safety Technology
aeSolutions

**Paul Gruhn, P.E., CFSE**
Global Functional Safety Consultant
aeSolutions

## Abstract

A two-prong templatized approach to multiple brownfield burner management system upgrades can result in significant cost savings. The first step requires coming up with an equivalent design for the safety instrumented burner management system following the ISA 84 safety lifecycle, as allowed in current NFPA standards. The second step utilizes a templatization approach for multiple units with common functionality that will allow an organization to further maximize savings. Actual experience doing this on repeat BMS projects indicate the level of overall savings can be as high as 75% on the safety lifecycle, 70% on the control system design and integration, and 35% on the operation and maintenance activities. The combined overall savings are roughly 60%.

## The problem

Equipment that uses burner management systems (BMS) in the process industries include boilers, process heaters, thermal oxidizers, incinerators, reformers, vaporizers, dryers, ovens, sulfur recovery units, kilns, calciners, furnaces, and more. Combustion control and burner management applications encompass single and multiple burners; multiple fuels; forced, natural, and balanced draft; parallel positioning (using either a mechanical jackshaft or positioned electronically); fully metered cross limited control with $O_2$ trim; and more.

Brownfield installations may date back 40 years or more. Most systems were originally designed according to prescriptive standards, almost a “cookbook” approach. However, most systems have required a variety of changes and upgrades over time. Applicable standards have changed considerably over that time period, the impact of which can result in a variety of problems and headaches.

As these fired devices begin to become obsolete many organizations are considering BMS upgrades. There are potential problems—as well as opportunities—when attempting to apply the ISA 84 [1] safety lifecycle to a BMS. Most fired device original equipment manufacturers (OEMs) are not well versed in the application of ISA 84 and are typically focused on providing a least credible based design. This issue is compounded by the fact that during a capital project the BMS process hazards analysis (PHA) and/or layer of protection analysis (LOPA) cannot be completed until a purchase order has been issued to the OEM, and the vendor has provided piping and instrumentation diagrams (P&IDs). Therefore, one does not know what safety integrity level (SIL) targets—if any—will be required for the BMS design until later in the project lifecycle. This has the potential to impact both the budget and schedule. If the project is being implemented by onsite facility engineers, and the fired equipment is a long lead item (e.g., 18

months), the packaged equipment might be procured and onsite before the onsite project team is fully engaged. So once SILs are selected, what happens if the OEM who provided a least credible design did not meet the SIL targets? Do you go back to the OEM for changes? Do you modify the field devices and controls in-house? Do you accept it as is, but upgrade it within the next five years? In such cases, the project will have the unfortunate "regret cost" conversation. Yet it doesn't need to be this way if certain things can be simplified.

In addition to the project timing issues described above, the actual BMS PHA / LOPA can expose additional problems and opportunities that will need to be addressed. When it comes to fired devices, some organizations use a checklist approach to execute the risk analysis. For example, "Does it have a burner management system?", and check the box "yes" or "no". If it does, people often assume that the design must be acceptable because it's based upon the governing code or standard (e.g., NPFA or API), and therefore does not warrant a deeper review. Yet an organization may have experienced problems (e.g., nuisance trips, difficulty lighting off, leaking valves, etc.) and/or near misses (e.g., small, uncontrolled combustion events—woofs and puffs) over time that would mandate a more exhaustive risk analysis approach.

Once the end user does decide to complete a more detailed risk analysis and perform a PHA and/or LOPA, are all the problems solved correct? Not necessarily. Different PHA/LOPA teams, led by different facilitators, using a generic and qualitative PHA/LOPA process will unfortunately arrive at a wide variety of risk ranking. Team A might say "severe injury" for one case, while team B might say "fatality" for the same scenario. Both teams may be correct in the grand scheme of the accuracy of such studies. Another factor that drives differences in risk ranking is the fact that PHA/LOPA teams tends to gravitate to the loudest voice in the room. If the team doesn't have BMS expertise and knowledge (e.g., it's a vendor package and not well understood), they might miss some safety functions (e.g., failed to identify proof of purge as a SIF), or have improperly defined safety functions (e.g., failed to take into account redundant and diverse technology in standard designs, such as a pressure switch and flame scanner). When upgrading multiple BMSs from a capital project perspective, this will result in different SIL targets being set for similar units.

These sort of problems are unfortunately rather wide-spread. Members of the ISA 84 committee have expressed similar problems. The end result is SIL targets being all over the map for similar unit operations, which is chaos in terms of capital projects. Management will have a wide variety of questions. Why are safety functions on this one heater SIL 0 and do not require an upgrade, while another has a bunch of SIL 1s, another has a bunch of SIL 2s, another has a bunch of SIL 3s, and another even has requirements for SIL 4?! They're all basically the *same* heater with similar occupancy factors! How can there be multiple order of magnitude differences between studies?

Perhaps new field devices may be required. Transmitters are generally preferred over discrete switches. Transmitters provide a live signal and a higher level of diagnostic coverage, meaning they generally have higher SIL capabilities than switches. However, if there is a single low pressure switch along with a flame scanner, and the flame scanner is self-checking, this diverse fault-tolerant set of technologies could also have high SIL capabilities. There is most likely a double block and bleed valve arrangement, and such a fault-tolerant arrangement would also have high SIL capabilities. There may be no significant issues on the field device side. It may in fact boil down to the logic solver; is it capable of meeting the SIL target?

A number of interesting things have happened to BMS standards in the last ten years. Back when the ISA 84 committee started working on the technical report for burner management systems [7], most of the prescriptive BMS standards in industry—such as NFPA and API—had not embraced or invoked the safety lifecycle. Starting in 2011, and now as of 2015, the NFPA BMS series of standards have *all* invoked it in some capacity. For a brownfield installation this represents a significant opportunity for potential cost savings.

## An approach to solve the problem

A two-pronged approach is needed in order to solve these problems for brownfield BMS upgrade projects where an organization may wish to apply the safety lifecycle. Step one is to conduct a PHA/LOPA and review the existing design versus the required SIL targets. Following the requirements of the safety lifecycle, the existing SIF architectures can then be reviewed for acceptability. If these existing acceptable SIF architectures deviate from the prescriptive "cookbook" requirements mandated by the latest governing code or standard (e.g., NFPA or API) one can now develop an "equivalent design" justification to support deviating from the prescriptive requirements. This does not mean that what is in NFPA and/or API is 'wrong', just simply that one can now follow the safety lifecycle to manage risk using alternate SIF designs. The governing codes and standards have documented that this methodology is acceptable. Step two is to use "templatization" to further reduce the costs of implementing the safety lifecycle on multiple similar unit operations. Both steps are described in more detail in sections below.

## Equivalent design

So what does "equivalent design" mean in NFPA 85, 86, and 87? It means that if an organization can get the authority having jurisdiction (AHJ) to approve what they are doing, then the proposed design will be acceptable. But who is the authority having jurisdiction? In the United States this could be the local fire marshal, or some form of state board or agency concerned with fired equipment who may come by and inspect boilers. The authority might be the organizations insurance carrier. If an organization is self-insured, there may be someone at the corporate level who would be the authority.

So the first step is to make sure the authority is "on board" with this equivalent design concept. The second step is to then conduct a hazard analysis on the fired device and follow a lifecycle approach to reduce risks. All three of the NFPA standards phrase these issues in slightly different ways, yet they essentially state to follow the ISA 84 standard in its entirety, and it will be considered equivalent. There is also a caveat to address all the requirements of the NFPA standards.

Here is one example. NFPA required an external master fuel trip relay in the past. Why was it mandated and part of the prescriptive requirements? It was there in case a general purpose programmable logic controller (PLC) output was stuck in the "on" state and the output could not be de-energized. For that case a secondary means of de-energization was required. Providing the master fuel trip relay meant you now would have a design in place that addresses the secondary means of de-energization. Today's safety PLCs provide an inherent secondary means of de-energization and offer performance greater than that provided by a relay. Many current BMSs have been designed and accepted with*out* requiring a master fuel trip relay. The standards also call for other specific requirements to address specific hazards, such as low gas pressure, high gas pressure, low air flow, flame out, etc.

The equivalent design concept is really a performance based design concept that is risk based. In essence, a) figure out what the risks are, b) propose an alternate BMS design that mitigates those risks, and c) get the authority having jurisdiction to approve and sign off on the deviations.

## An example

Let's consider the application of the 2015 edition of NFPA 85 on a multiple burner boiler / incinerator with multiple fuel streams. NFPA 85 governs the majority of it, although NFPA 86 may govern some of it for the incineration waste abatement issues. This application is not "one size fits all" per the standards. If one attempts to apply NFPA 85 - 2015, it mandates that the boiler shall have a double block and bleed valve arrangement for *each* individual fuel line to *each* burner. Considering that this application has multiple burners, each with multiple fuels lines, the cost of putting blinders on and prescriptively applying the requirements of the standard (i.e., double block and bleed valves for each line) would be very high. At the end of the day, is such a design *really* providing the level of risk reduction needed compared to the cost of implementing the change?

One could step back and conduct a consequence analysis (e.g., blast modeling) for each scenario that results in significant hazard. For example, consider leakage through the existing single block valves with the potential of fuel leakage into the combustion chamber. Look at failure of individual block valves failing to isolate. Is it possible to get a flammable mixture within the combustion chamber? How much fuel could build up within the firebox? What if it ignites? Determine blast radiuses. Then take all of this information into the risk analysis, process hazard analysis, and layer of protection analysis. With engineering documentation in place to drive consistency in the consequence, it would drive consistency in the resulting safety integrity levels that come out of the study. This would be one way to eliminate some of the chaos mentioned earlier. By following ISA TR84.00.07 as guidance on typical combustion related hazards and SIF architectures, a consistent risk analysis can be executed.

One could then complete a safety instrumented system BMS design. For instance, complete a SIL verification calculation for a multi-burner design with a single block valve on the header and individual burner valves. Does it meet the required target level of performance? If the answer is "no", then consider the addition of double block and bleed valves on the header (assuming that is the scenario that is driving the risk high). Perhaps it might be low combustion air, or some other scenario. Does the modified design meet the desired risk criteria, as opposed to installing double block and bleed valves across the board for *all* individual fuel lines?

Based on actual experience, the accepted design was accomplished using just *single* valves on the header and fuel lines. Considering that there were multiple boiler installations all using the same design, this represented a significant cost savings of not having to install *hundreds* of extra valves. One can now have an equivalent alternate design that is risk based. This ensures an organization is meeting their corporate risk criteria, as well as managing risks with a "right-sized" design. One can also look at this from a cost of ownership lifecycle perspective. One may be able to optimize and extend test intervals. All of this is to make sure an organization is spending money in the most cost effectively manner when designing a BMS.

As stated earlier, the NFPA series of standards all now invoke the SIS/BMS concept and allow these equivalent designs. This is a tremendous opportunity from a brownfield standpoint to sharpen ones pencil, take the blinders off, and not just prescriptively slap in what may be mandated by the governing

code or standard. An organization can now step back, follow a risk based approach, and minimize the costs associated with BMS upgrade projects, while cost effectively managing risk.

## Templatization

At this point reasonable safety integrity levels have been chosen for each function, and a cost effective equivalent alternate design has been selected. The NFPA standards state the safety lifecycle must be followed in its entirety. This means one must perform a process hazards analysis, SIL selection study, SIL verification calculations, develop a safety requirement specification, test plans, and more. Might there be a way to further save money and reduce the schedule on these projects? What if it were possible to "copy and paste" from the first project to the others?

Imagine there is an NFPA 85 boiler that is single burner and single fuel which is used at multiple sites, which is quite common for most companies. They will all be very similar. After engineering the first one, if it were possible to then copy and paste all the other instances, there would be a significant reduction in cost and schedule. This could be expanded to the instrumentation and controls design as well. The following would be some of the project deliverables.

- Approved vendor lists for instrumentation in line with SIL calculation assumptions
- PHA
- LOPA
- SIL verification calculations
- Safety requirements specification (SRS)
- Cause & effects diagrams
- Functional test plans
- Instrument datasheets
- Instrument index
- I/O (input/output) list
- Control panel design with bill of materials
- Control system architecture diagram
- Instrumentation and/or electrical installation details
- Control panel internal wiring diagrams
- Field wiring diagrams (loops/swing arms/schematics)
- Cable/conduit block diagrams
- Cable schedule
- Software requirements specification
- Logic solver configuration
- Logic solver simulation logic
- Local human machine interface (HMI) design and configuration
- Remote HMI design and configuration
- Historian configuration
- Factory acceptance test procedure and testing
- Site acceptance test procedure and testing
- Commissioning test procedure and testing

Again, what if it were possible to engineer all this once, and then copy and paste the rest of the similar projects?

The operations and maintenance phase is a significant portion of the lifecycle. This is where organizations identify bad actors. This is where one can remove risk from the business. Functional test plans are required for all field devices. Calibration and test plans must be loaded into a computerized maintenance management system. Test intervals must match the assumptions made in the hardware SIL verification calculations. Spare parts are needed in line with repair time assumptions. Operations and maintenance personnel need to be trained on the new systems. Personnel or software need to track the amount of time safety functions are in bypass, demand frequencies, initiating event frequencies, failure rates, late or incomplete testing, and more. Again, what if it were possible to engineer all this once, and then copy and paste the rest of the similar projects?

This documentation needs to be in place in order to follow the NFPA 85/86/87 and ISA 84 standards. The goal is to do this as cost effectively as possible, since this will not produce more product, nor will it improve product quality. Organizations need to reduce the man-hours as much as possible while still driving consistency and quality. So how could this be done?

The suggested approach is shown in Figure 1. It will require a database approach to the safety lifecycle that will handle all of the engineering deliverables. There will also need to be an intelligent drawing package. If these two things could be synchronized, there could then be templates for deliverables (e.g., SIL verification calculations, loop sheets, etc.). After all, by the time a few systems have been engineered, what's really changing? Tag numbers, trip points, calibrated ranges, etc. It's possible to take safety and software requirements and port them over to the safety PLC logic solver. Depending upon the vintage and sophistication of the logic solver, it's possible to auto configure certain things (e.g., calibrated ranges, I/O point assignments and descriptions, some of the logic definition). With the mantra of "work smarter, not harder" it's also possible to use a PC based emulation tool to auto-test the application logic much more thoroughly than compared to manual testing means. Such automated testing could be a precursor to factory acceptance testing.

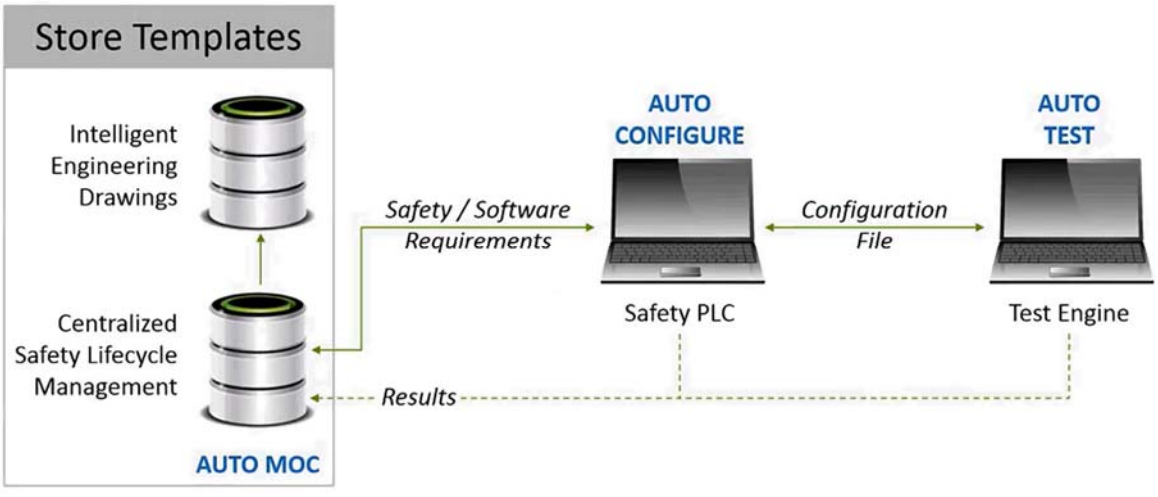


**Figure 1: Templatization Methodology**

There is also the potential for automated management of change (MoC). For example, imagine it's 3:00am and things aren't going well. Someone comes in and changes the purge timer from five minutes to five seconds to support troubleshooting. What if someone forgets to change the purge timer back to 5 minutes? Every time a change is made in the PLC, the file could be exported and the last valid test scripts in the PC based emulator test engine could be run against the new PLC configuration. In this case the test would fail as the SRS and test engine both contain a requirement for a 5 minute purge timer, while the actual PLC configuration has a 5 second purge timer. Such a check could be run once a week, or once a month. This would help ensure that proper MoC process is being followed; a) start with the SIS design requirements, b) it goes into the safety PLC configurator, c) it is adequately tested, and d) there is a validated test against the original requirements.

Using templates and doing all this can reduce the cost of engineering, as well as improve quality and consistency. It can even reduce the time for factory acceptance testing (FAT) by auto-testing the templates prior to FAT. This is especially useful in BMSs as many of the SIFs and logic are very similar from unit to unit. A side benefit is the loop-back for the automated MoC confirmation. Doing all this might potentially change the safety culture in an organization. Rather than making changes to systems at the 11$^{th}$ hour, this will ensure that a rigorous MoC process is in place for things that impact functional safety.

## Work smarter, not harder

Industry has evolved and can now take advantage of the benefits of automation to drive consistency, reduce costs and schedules—and more importantly—deliver a safety instrumented burner management system that looks at all the pieces; the engineering automation, safety instrumented system, factory acceptance testing, along with day-to-day operations and upkeep.

So how could an organization do this? Templates will be needed for a single burner boiler, an incinerator, a reboiler, etc. One could then go through the organization and figure out what combination of fired devices there are, come up with a design basis, and start designing the templates. One would test all the templates thoroughly to make sure that before a template was instantiated in 100 places, it was tested extensively and originated from the trusted library of templates maintained by the project via MoC. With this approach a small, dedicated team could execute this work, reduce the interfaces between resources on a project (e.g., engineering, construction, etc.), and keep costs in line. This would set the organization up for success.


**Figure 2: Financial benefit of templatization**

Doing all this can dramatically lower costs. The first project might cost $X, but by using the template approach on every project after that, one could drive costs down to a significantly lower level. This will also require having a continuous improvement mechanism in place to learn from the previous projects.

Copy is a four letter word for a reason. Each NFPA 85 boiler will not be exactly identical. One may have been installed in 1977, another in 1985, and there will be differences. They might be different from an operations and maintenance perspective. Yet there will probably be 70% consistency between the units. That means 70% of the things will be the same and an organization could take advantage of the copy and paste factor. Only 30% of the oddball different items require full engineering effort. This will also help shorten the schedule. A qualified functional safety professional would review and approve the templates. They could then be rolled out as a library to ensure that all items in the program were done with the highest quality in terms of functional safety.

## Cost savings up to 60%

Actual experience doing this on repeat BMS projects indicate the level of overall savings can be as high as 75% on the safety lifecycle, 70% on the control system design and integration, and 35% on the operation and maintenance activities. The combined overall savings are roughly 60%. It comes down to how many unique templates there are, and whether it's possible to treat this as a "program", rather than individual islands of projects that don't taking advantage of the templates and the copy factor. Considering the current price of oil (as of early 2016), this level of savings is significant.

### *An actual example*

One global oil, gas and chemical company conducted a field survey of more than 80 fired devices. They decided on an upgrade project to meet new corporate safety standards, ensure code compliance, and replace obsolete BMS-related controls. In early 2014 the company launched an 8-year program to design templates, complete detailed design, along with commissioning and construction plans that would take advantage of scheduled outages. The initiative involved collaboration between the company's capital projects group, its operations and maintenance staff, and a system integrator familiar with BMSs.

To achieve savings both in cost and schedule, the company mandated the use of templatization. Early results look very positive. The first several BMS upgrades will yield a savings of $70,000 each. As the program progresses, continuous improvement sessions are planned to brainstorm additional ways to reduce costs and shorten the schedule even further. Overall, the user is expected to save at least $6.5 million over the entire course of the program.

## Conclusion / Summary

First conduct a PHA/LOPA and come up with an equivalent design for the safety instrumented burner management system following the safety lifecycle approach. Get it approved by the authority having jurisdiction. This approach does not simply take at face value the prescriptive cookbook requirements in the NFPA standards. Instead it challenges them, right sizes them, and builds the most cost effective solution that meets the risk reduction requirements. Second, utilizing a programmatic templatization approach for multiple units with common functionality will allow an organization to maximize their savings.

## References


1. ISA 84 (IEC 61511 Mod) – 2004: “Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements”
2. NFPA 85: “Boiler and Combustion Systems Hazard Code” 2015
3. NFPA 86: “Standard for Ovens and Furnaces” 2015
4. NFPA 87: “Recommended Practice for Fluid Heaters” 2015
5. API RP 538: “Recommended Practice for Industrial Fired Boilers for General Refinery and Petrochemical Service” 2015
6. API RP 556: “Instrumentation, Control, and Protective Systems for Gas Fired Heaters, Second Edition” 2011
7. ISA TR 84.00.05: “Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)” 2009