MARY KAY O'CONNOR PROCESS SAFETY CENTER
INTERNATIONAL SYMPOSIUM
October 22-24 | College Station, Texas

Implementing Safety Instrumented Burner Management Systems: Challenges and Opportunities

Brittany Lampson, PhD
aeSolutions™
Greenville, SC
brittany.lampson@aesolns.com

Keywords

Safety Lifecycle, ANSI/ISA 84, IEC 61511, Safety Instrumented System, Burner Management System, Safety-Instrumented Burner Management System, BMS, SI-BMS

1. Abstract

Implementing a Safety Instrumented Burner Management (SI-BMS) can be challenging, costly, and time consuming. Simply identifying design shortfalls/gaps can be costly, and this does not include costs associated with the capital project to target the gap closure effort itself. Additionally, when one multiplies the costs by the total number of heaters at different sites, these total costs can escalate quickly. However, a "template" approach to implementing SI-BMS in a brownfield environment can offer a very cost effective solution for end users. Creating standard "templates" for all deliverables associated with a SI-BMS will allow each subsequent SI-BMS to be implemented at a fraction of the cost of the first. This is because a template approach minimizes rework associated with creating a new SI-BMS package. The ultimate goal is to standardize implementation of SI-BMS in order to reduce engineering effort, create standard products, and ultimately reduce cost of ownership.

2. Safety Instrumented Burner Management System (SI-BMS)

To clarify the issue at hand, let us first define the problem. A Burner Management System (BMS) is defined per NFPA 87 2015 edition as:

The field devices, logic system, and final control elements dedicated to combustion safety and operator assistance in the starting and stopping of fuel preparation and burning equipment and for preventing misoperation of and damage to fuel preparation and burning equipment.

To fully understand the definition of a Safety Instrumented System per IEC 61511 2004 edition one needs to review several different definitions together as whole:

Safety Function *- function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event.*

Safety Instrumented Function (SIF) *- safety function to be implemented by a safety instrumented system (SIS). Note: A SIF is designed to achieve a required safety integrity level (SIL) which is determined in relationship with the other protection layers participating to the reduction of the same risk.*

Safety Integrity Level (SIL) *- discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS. SIL 4 is related to the highest level of safety integrity; SIL 1 is related to the lowest.*

Safety Instrumented System (SIS) *- instrumented system used to implement one or more SIFs.*

Considering the aforementioned definitions, a Safety Instrumented Burner Management System (SI-BMS) can be defined as a Burner Management System, where the performance based risk reduction concepts of the Safety Lifecycle as contained in IEC 61511 have been applied to the fired device in addition to the prescriptive requirements mandated by the code/standard that governs the fired device. Traditionally, BMSs are designed and installed per prescriptive codes/standards such as:

- NFPA 85 - Boiler and Combustion Systems Hazard Code
- NFPA 86 - Standard for Ovens and Furnaces
- NFPA 87 - Recommended Practice for Fluid Heaters
- API 556 - Instrumentation, Control, and Protective Systems for Gas Fired Heaters

When one overlays the requirements of the Safety Lifecycle to a BMS design it requires one to:

- Identify the hazardous events resulting in unacceptable consequences
- Identify the safety functions that prevent hazardous events
- Establish the performance criteria (e.g., the risk reduction) for these safety functions
- Allocate safety functions to systems designed and managed to achieve the performance criteria
- Document the functional and integrity requirements in a design specification
- Verify that the design and management practices are sufficient to meet the performance requirements
- Document and implement operation and maintenance procedures to support performance requirements
- Manage changes to the process equipment and the safety systems to ensure safe operation

When conducting an SIS Grandfathering exercise (initially applying the Safety Lifecycle to existing systems) at a brownfield site, one will typically identify missing documentation along with a requirement for some new field devices and/or logic solvers. These findings result in the need for a capital project to upgrade the BMS to full compliance with IEC 61511 requirements.

3. Challenges Associated with Implementing an SI-BMS

There are multiple tasks associated with implementing an SI-BMS. Some of these tasks are mandated by IEC 61511, while the remainder are typical instrument and controls related deliverables and tasks required to properly design, install, and commission the upgraded SI-BMS. All of these tasks require time and money. If multiple fired devices need to be upgraded, these costs can escalate quickly. However, combining planning with a novel execution strategy, significant time and money can be saved.

Many different unit operations require a BMS, including reboilers, indirect heaters, steam boilers, process heaters, thermal oxidizers, and incinerators. There are many similarities between the operation, hazards, and code requirements of these various pieces of equipment. For instance, all of these fired devices typically have similar logic requirements around:

1) Pre-fire permissives
2) Proof of Purge
3) Light off
4) Normal Shutdowns
5) Post Purge

If a templatized programmatic approach is implemented, the above similarities can be leveraged to save on both engineering schedule and costs.

3.1 What are the tasks associated with a typical SI-BMS upgrade?

For simplicity sake, let us assume the SI-BMS upgrade effort has been scoped to include the following:

- Existing standalone general purpose PLCs will be replaced with new Safety PLCs
- Existing switches will be upgraded to transmitters
- New shutoff valves will be added only where required to meet SIL targets
- Local light off functionality will be provided via a flat panel
- General purpose area classification
- NEMA 4X Panel Design

To better understand the schedule and cost savings potentials, the tasks and deliverables required to complete the above simplistic scope of work will be described in more detail below.

Safety Lifecycle Tasks

The following is a summary of Safety Lifecycle related tasks that must be performed on each BMS to be upgraded. Refer to IEC 61511 for additional information for specific details.

- Process Hazards Analysis
- Layer of Protection Analysis with Safety Integrity Level (SIL) Selection
- Safety Requirements Specification with Functional Logic Definition
- Safety Integrity Level (SIL) Verification Calculations
- Functional Test Plans
- Functional Safety Assessments (Stage1, 2, and 3)

Instrumentation & Control System Design Tasks

The following is a summary of instrumentation and control system design related tasks that must be performed on each BMS to be upgraded.

- Instrument Approved Vendors List in line with SIL Calculation assumptions
- Instrument Datasheets
- Instrument Index
- I/O List
- Control Panel Design with Bill of Materials
- Control Panel Internal Wiring
- Field Wiring (Loops, Swing Arms, Schematics)
- Control System Architecture Diagram
- Instrumentation and/or Electrical Installation Details
- Cable and Conduit Block Diagram
- Cable Schedule
- Software Requirements Specification
- Logic Solver Configuration
- Logic Solver Simulation Logic
- Local Flat Panel Configuration

- Historian Configuration
- Remote BPCS HMI Configuration
- Factory Acceptance Test Procedure/Testing
- Site Acceptance Test Procedure/Testing
- Commissioning Test Procedures/Testing

Operations & Maintenance Tasks

The following is a summary of Operations and Maintenance related tasks that must be performed on each BMS to be upgraded.

- Functional Test Plans, Instrument Calibration, Valve Leak Testing loaded and scheduled into the site Computerized Maintenance Management System (CMMS) per Proof Test Coverage assumptions in SIL Calculations
- Spare Parts in Stores per Mean Time To Repair assumptions in SIL Calculations
- Operations and Maintenance Trained on new SI-BMS
- Program and personnel in place to track Time in Bypass, Demand Frequency, Cause Frequency, Dangerous Undetected Failures, and Late/Incomplete Testing of SIFs per IEC 61511 requirements

4. Templatization Opportunity

The “templatization” approach recognizes that if one can design a typical SI-BMS one time (i.e. a boiler) and then copy the design for each subsequent similar SI-BMS installation, (i.e. the next series of boilers) there is potential for significant time and cost savings. When using a “templatization” approach, information that will need to change from installation to installation is identified with placeholder tagging, wire labels, descriptors, and panel names. These placeholders can then be automatically updated with the actual BMS-specific tagging, wire labels, panel names, from system to system. This template encompasses as many tasks and deliverables as possible included in the following areas:

- Safety Lifecycle Tasks
- Instrumentation and Control System Design Tasks
- Operations and Maintenance Tasks

Note that differences will exist even within similar fired devices for a variety of reasons, for instance, there could be small differences between steam boiler installations. The goal is to use the templatization approach where ever possible to quickly complete the design for the majority of similar

functionality. The smaller quantity of new or unique functionality would then be designed using the normal traditional engineering approach.

4.1 Semi-Quantitative Risk Analysis

The most critical component to being able to leverage templates from one installation to the next is associated with the risk analysis. If independent teams with different facilitators are given the task of conducting a qualitative PHA/LOPA, one will end up with mis-defined SIFs, missing SIFs, and orders of magnitude of differences in SIL targets across the entire range of fired devices. This is due to the qualitative nature of the risk analysis process coupled with limited knowledge of the team associated with BMS hazards/operation because it is often associated with vendor packed equipment. These differences in analysis will result in large differences in instrumentation and controls scope which will result in chaos that cannot be readily consumed by the associated SI-BMS upgrade capital project. To keep to the budget, it is imperative that a consistent semi-quantitative based risk analysis be conducted to drive consistency in the SIF definitions and SIL targets. Consistency can be achieved as follows:

1. Select BMS unit operation (i.e. boiler)
2. Review all code/standard mandated protection layers (i.e. NFPA 85 mandated alarms and interlocks)
3. BMS unit operation Subject Matter Expert (i.e. boiler BMS guru) develops a PHA/LOPA template that includes all code/standard mandated protection layers and typical causes
4. Perform consequence modeling on typical hazards (i.e. uncontrolled combustion event for various chamber volumes) to provide team specific guidance on consequence selection (i.e. severe injury vs fatality)
5. PHA/LOPA team would start with the PHA/LOPA template, confirm cause frequencies for noted causes, add installation specific causes, confirm consequence and occupancy for the installation, and confirm all protection layers

The above approach will reduce team time, but, more importantly, it will ensure consistent risk analysis results are achieved. Consistency is achieve because this above approach is semi-quantitative as opposed to the traditional qualitative approach, which is subject to team member opinions and limitation of BMS unit operation knowledge.

4.2 Database Driven Approach

The key to the templatization is utilization of a database centric approach towards completion of project mandated deliverables / tasks. Three major databases are required to be synchronized and carefully managed through the project:

- Safety Lifecycle Management Database to execute Safety Lifecycle Tasks and Operations and Maintenance Tasks

- Intelligent Engineering Drawing Database to execute Instrumentation and Control System Design Tasks
- Safety PLC configuration Database to support configuration and testing of the Safety PLC application logic

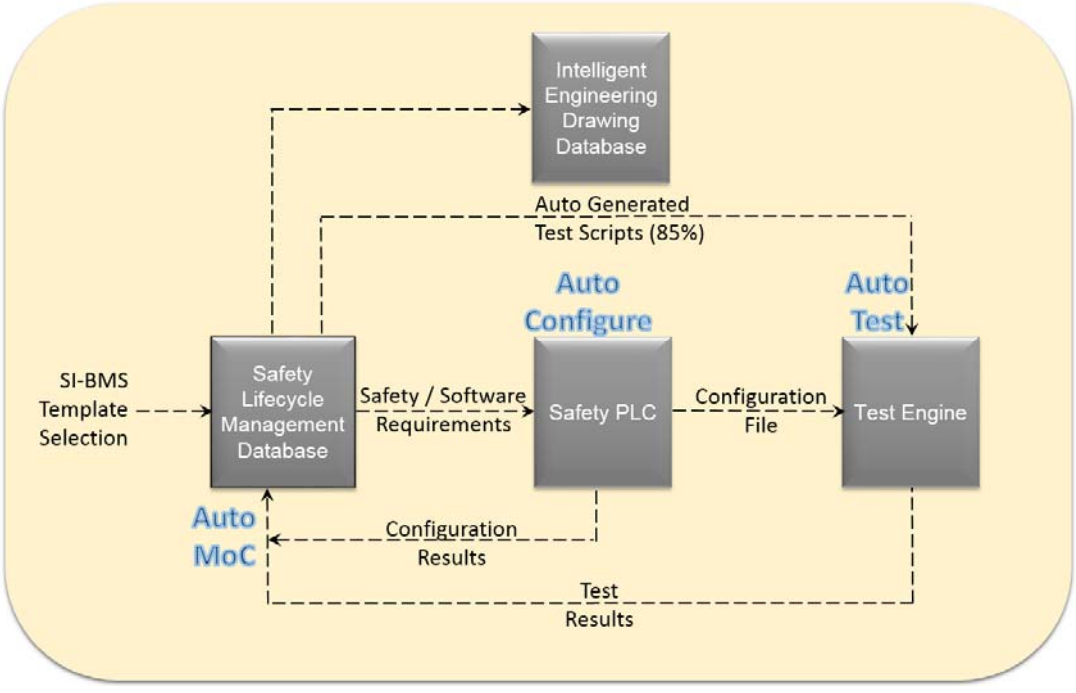
The Safety Lifecycle Management Database is the master data record and should have a vigorous internal Management of Change (MoC) schema in place to efficiently manage overall project data.

Figure 1 below provides a high level overview of how the templatized work process is executed. The stepwise execution is described as follows:

1. Perform a site survey to identify the total number of BMS templates required (i.e. boiler, reboiler, vaporizer, etc.) and note any code/standard violations.
2. Create SI-BMS templates and standards for the typical unit operations noted in site survey
3. Start new project – select which SI-BMS Standard template applies for this unit operation (i.e. boiler).
4. Load SI-BMS standard template (i.e. boiler) into the Safety Lifecycle Management Database and replace alias tags with real world tag numbers and information. Assume for now 80% of unit operation functionality (i.e. boiler) Safety Lifecycle Safety Lifecycle Tasks are addressed by the standard template.
5. Complete Safety Lifecycle Safety Lifecycle Tasks on installation specific unique features. Assume 20% new or unique functionality that is not covered in the SI-BMS template, will be added to project design basis.
6. Safety Lifecycle Management Database will export tagging details, I/O tags, calibrated ranges, trip points, time delays, etc. to the intelligent engineering drawing package used for updating Instrumentation and Control System Design Tasks. Assume for now 80% of unit operation functionality (i.e. boiler) Instrumentation and Control System Design Tasks are addressed by the standard template.
7. Complete Instrumentation and Control System Design Tasks on installation specific unique features. Assume 20% new or unique functionality that is not covered in the SI-BMS template, will be added to project design basis.
8. Safety Lifecycle Management Database will export Safety Requirements and Software Requirements to the Safety PLC configuration work station. This would include the following: I/O tags, calibrated ranges, trip points, time delays, function block/logic template instances, soft tags, logic definition (pre-fire, purge, pilot light off, main light off, normal shutdown, post purge, etc.), tags that must be passed to historian, diagnostics, etc.

9. Safety PLC configuration work station will then automatically configure I/O point assignments and application software logic. It is expected that 80% of the logic will be capable of being automatically generated. This is simply referred to as ability to ***Auto Configure*** the system.
10. Complex configuration is assumed to be 20% or less and will be configured through normal engineering practices.
11. Safety PLC configuration when finalized will generate a configuration file, which will be sent to the Test Engine, which is a PC based controller software simulation package.
12. Safety Lifecycle Management Database will generate a test script to be executed in the Test Engine to conduct exhaustive automated tests on the application logic. This is simply referred to as ability to ***Auto Test*** the system.
13. Later, once the SI-BMS has been commissioned and installed in the field, the Safety Lifecycle Management Database will compare current configuration against the safety and software requirements and test scripts. If discrepancies are detected, it is in theory identifying a failure in the MoC work process, where application software changes would start with the requirements and testing requirements being updated in Safety Lifecycle Management Database as opposed to going directly to the safety PLC to make logic changes. This is simply referred to as ability to ***Auto MoC*** of the system.

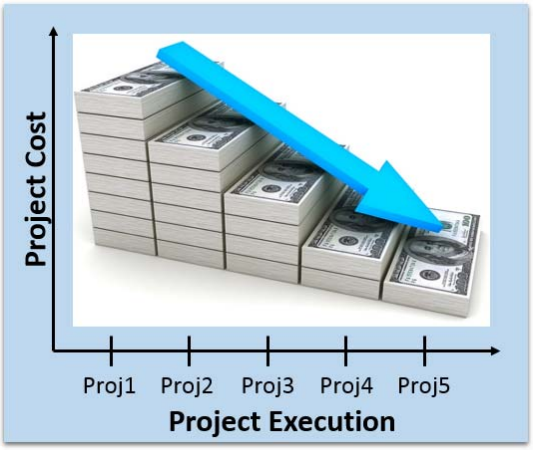
Figure 1 – SI-BMS Templatization Dataflow Diagram



5. Cost and Schedule Savings Opportunity

By implementing the templatization approach noted above, significant savings can be achieved throughout all aspects of the project as can be seen in Figure 2 below.

Figure 2 – SI-BMS Program Savings



After each template instantiation (i.e. project 1, project 2, project 3, etc.), a continuous improvement lessons learned session should be conducted to identify areas where future savings can be achieved. These lessons learned are then incorporated in the program templatization methodology to maximize future savings as reflected in Table 1 below.

Table 1 – Potential Savings

Task	Potential Savings
Safety Lifecycle	Up to 75%
Instrumentation and Control System Design	Up to 70%
Operations and Maintenance	Up to 35%
Total Tasks	Up to 60%

By reducing engineering effort, one also realizes a significant schedule savings. This time savings can be leveraged to allow multiple SI-BMS upgrades to occur concurrently within a calendar year. One will be able to remove risk from the business faster than a traditional project execution approach that designs each BMS as a standalone project.

Another savings included above is implementing a procurement strategy of bulk purchase agreements on instrumentation and controls, where the OEMs offer deeper discounts to support the program. This

has been very successful around control system hardware and software and it also freezes the project automation scope on a known set of firmware and software versions to justify reliance automated application logic testing to reduce FAT durations. Note construction savings could also be leveraged by implementing a tiger team approach to reduce construction efforts. The tiger team approach would use small dedicated groups of construction staff to leverage learnings and increase construction efficiencies. This approach has been excluded from the white paper as not every brownfield site may have enough BMS installations to garner significant savings. However, this should be definitely be addressed as part of the overall SI-BMS upgrade program considering typical construction costs and the possibility of additional savings.

6. Conclusion

With readily available database tools and technology, implementation of a Safety Instrumented Burner Management (SI-BMS) upgrade program across multiple brownfield sites can be executed using a templatization approach that could yield significant cost and schedule savings of up to 60% for the end user. This can be achieved via three easy steps:

1. **Plan** the SI-BMS Upgrade Program to be template centric
2. **Execute** templatization with small high performing teams
3. **Save** on cost and schedule while delivering a high quality consistent project

For more information on how you can benefit from templatization contact aeSolutions at www.aesolns.com.

7. References

1. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1: Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. The Instrumentation, Systems, and Automation Society. Research Triangle Park, NC.
2. ANSI/ISA-TR84.00.05-2009. *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)*. ISA. Research Triangle Park, NC.
3. NFPA 85 - *Boiler and Combustion Systems Hazard Code* - 2015; NFPA, Quincy, MA
4. NFPA 86 - *Standard for Ovens and Furnaces* - 2015; NFPA, Quincy, MA
5. NFPA 87 - *Recommended Practice for Fluid Heaters*- 2015; NFPA 1, Quincy, MA
6. API 556 - *Instrumentation, Control, and Protective Systems for Gas Fired Heaters* – 2011; API Washington, DC
7. Scott, Michael D. 2002. *Burner Management System Safety Integrity Level Selection.* The Instrumentation, Systems, and Automation Society. Research Triangle Park, NC.