

SAFETY INSTRUMENTED BURNER MANAGEMENT SYSTEMS - REQUIREMENTS FOR THE PAPER INDUSTRY

Bud Adler
Director, Business Development
AE Solutions
Lake Mary, FL 32746

Mike Scott, PE, CFSE
V P, Process Safety
AE Solutions
Greenville, SC 29616

KEYWORDS

Burner Management System, BMS, Safety Instrumented System, SIS, Safety Instrumented Burner Management System, SI-BMS, FM Approved, ANSI/ISA 84, IEC 61508, IEC 61511, Black Liquor Recovery Boilers, Dryers, Boilers, Kilns, Thermal Oxidizers, Safety Lifecycle Analysis

ABSTRACT

Companies around the globe are awakening to the fact that providing a safe working environment is no longer a judgment call by management but is strictly defined in safety standards. And, there is growing urgency to comply with these standards due to insurance rate structures and OSHA authority. The consequence of an incident occurring in a plant that has not complied with the standards has met with steep fines from OSHA and/or the EPA followed by legal repercussions that involve liability settlements and potential incarceration. The moral obligation to manage the threat to human life and the environment raises the obligation to an even higher level.

What most of the companies do not yet realize is that all safety critical processes must be analyzed and their potential risk determined. It has come as a surprise to many that Burner Management Systems (BMS) associated with fired devices in the pulp and paper industry such as, dryers, kilns, thermal oxidizers, power boilers and black liquor recovery boilers are all defined as Safety Instrumented Systems (SIS) if they contain sensors, a logic solver and a final control element according to ANSI/ISA 84.01. Additionally, FM Approval Standard 7605 requires that PLC based BMS must comply with IEC 61508.

This paper will explore the requirements for conformance to ANSI/ISA 84, IEC 61508, IEC 61511, NFPA 85, NFPA 86 and BLRBAC guidelines.

By actively embracing the concept that a BMS and some other lower profile operating equipment may in fact be a SIS, companies can ensure that these systems are designed, maintained, inspected and tested per both the applicable prescriptive standards (BLRBAC, NFPA, etc.) as well as the latest SIS performance-based standards (ANSI/ISA, and IEC). Do you know if you are installing and / or operating fully compliant Safety Instrumented Burner Management Systems?

INTRODUCTION

This paper will explore the requirements for conformance to ANSI/ISA 84, IEC 61508, IEC 61511, NFPA 85 and NFPA 86. The methodology and benefits of Lifecycle Analysis will be described.

By actively embracing the concept that a BMS may in fact be a SIS, companies can ensure that these systems are designed, maintained, inspected and tested per both the applicable prescriptive standards (API, NFPA, etc.) as well as the latest SIS performance-based standards (ANSI/ISA, and IEC).

Application of performance-based standards for Safety Instrumented Systems (SIS) has gained widespread acceptance in the process industry. These standards are now being applied to the design of Burner Management Systems on a continually increasing scope. A BMS can be designed that meets all requirements of the prescriptive standards such as NFPA 85 or 86 and yet will NOT satisfy the requirements of a Safety Instrumented System. It is imperative that end users gain the necessary knowledge to properly implement BMS related projects. Simultaneously six (6) different codes, standards and / or recommended practices have been, or are currently being developed, that mandate a BMS is a SIS until proven otherwise. This mandate will impact almost every industrial BMS project!

Many companies naively believe that existing burner management systems are grandfathered in accordance with whatever standards or practices were in place when the system was originally installed. ANSI/ISA 84 is very clear on the actual facts pertaining to grandfathering. This paper will highlight the requirements of invoking the grandfather clause.

STANDARDS AND CODES

Prescriptive standards such as NFPA 85 or 86 have done well at identifying “what” interlocks should be implemented based upon lessons learned from previous incidents and near misses. However, in today’s microprocessor-based world, it is more important to know “how” to properly implement the prescriptive based interlocks.

When the logic solver was comprised of relays with simple and well-defined failure modes, it was very easy to understand what level of risk reduction the BMS provided. However, someone with the best intentions could replace a relay based BMS with a new microprocessor-based logic solver and the end result could be a system that is actually less safe! This issue contributed to the development of the performance-based Safety Instrumented System standards that are being utilized today throughout the process industry.

These performance-based standards address the “how to” of properly implementing the prescriptive-based interlocks.

These standards are:

- ANSI / ISA 84.00.01-2004 – Application of Safety Instrumented Systems for the Process Industries
- IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511 - Functional safety: Safety Instrumented Systems for the process industry sector

There are now six different code or standards documents from multiple industries and organizations that have been, and /or are being developed that invoke SIS requirements for a BMS. It is significant that primarily end users have developed all six of these documents. These efforts reflect the serious concern for safety of these users; not a vendor or consultant trying to influence market direction. These are:

- *The Black Liquor Recovery Boiler Advisory Committee (BLRBAC)* has developed several guideline documents regarding design and operation of Recovery Boilers in the Pulp and Paper Industry. These documents invoke SIS requirements on the Recovery Boiler BMS.
- *FM 7605* – Factory Mutual requires that any PLC listed for use in combustion safeguard service meet the SIS requirements contained in IEC 61508. At this writing we are aware of only one vendor who has a product submitted to FM for approval with respect to Safety Instrumented Burner Management Systems.
- *TR84* – The ISA S84 committee has formed a BMS sub-committee to develop a document that clarifies how SIS concepts apply to a BMS. Examples being included in the document for each code or standard are:
 - *NFPA 85* – Single burner boiler
 - *NFPA 86* – Thermal oxidizer
 - *API 14C* – Process heater with multiple burners
 - *API 556* – Glycol Reboilers

The goal of the SP84 committee is for industrial users to properly follow the safety lifecycle to define the risk associated with every BMS to determine if it is a SIS.

- NFPA 86 Committee is planning to update this standard to reflect their agreement that an industrial BMS is a SIS and that a safety PLC should be used. A linking paragraph will be added that refers to ANSI/ISA 84.00.01-2004 as acceptable methodology.
- EN 50156-1 is a German standard covering electrical equipment for furnaces that is scheduled for revision in 2004. This document invokes SIS requirements for a BMS.
- API 556 document governs design of BMS's in the petroleum industry. It is being revised to invoke SIS requirements on BMS's.

SIS REQUIREMENTS

Safety Lifecycle

The Safety Lifecycle provides a framework of considerations for each stage of a SIS from conception to decommissioning. The intent is to force a logical and sequential procession for the project scope. Some of the basic components of the Safety Lifecycle include: Risk Analysis; Consequence Analysis, Layer of Protection Analysis; Safety Integrity Level (SIL) determination, Documentation of Safety Function Requirements; SIS Conceptual Design; SIL verification; Detail Design and System Implementation.

Risk Identification and Quantification

ANSI/ISA 84.00.01-2004 (IEC 61511) is a performance-based SIS standard released by ISA in October 2004. It is identical to the IEC 61511 standard endorsed by over 144 member countries around the globe except for the addition of a grandfather clause. The standard requires that a risk analysis be made as one component of the mandated safety lifecycle. Risk ranking represents the act of evaluating consequence (what could happen if any component of the BMS fails to function) and likelihood (an estimate of how often the failure could occur) of an event. In some facilities this may be called a "Hazop Analysis" or a "Process Hazards Analysis". The concept is the same: a team of knowledgeable people considers all possible scenarios of operation and conducts a "what if" analysis to identify and document all risks. By quantifying the risks associated with each hazard, a ranking can then be made.

SIL Determination

Following the risk identification and ranking is the selection of a Safety Integrity Level or SIL. SIL is a measure of required risk reduction. ANSI/ISA 84 recognizes SIL 1, 2, and 3 in the process industry.

It is an end user's responsibility to define the risk associated with his operation. This inherent process risk is then compared to the corporate *tolerable risk criteria*. If the inherent risk is *less than* that target for tolerable risk, no action is required. The results of the analysis should be documented and attention directed elsewhere... a SIS is not required. If the inherent risk is *greater than* what the company can tolerate, a Safety Instrumented System (SIS) can be utilized as a means to bring the risk back within tolerable limits.

The quantification of the identified risks to establish the required SIL for each Safety function determines "how good" the BMS needs to be. The standards apply Safety Integrity Levels (SIL) to risk reduction. A required reduction of 10 to 100 times is a SIL 1 requirement while a required reduction of 100 to 1,000 times is a SIL 2. Although very rare, a SIL 3 requires reducing risk by 1,000 to 10,000 times. Refer to FIG 1

SIL Safety Integrity Level (ANSI/ISA 84)	Safety Availability	PFD Probability of Failure on Demand (1-Availability)	Risk Reduction Factor (1 / PFD)
3	99.9 – 99.99%	0.001 – 0.0001 (E⁻³ · E⁻⁴)	1,000 - 10,000
2	99 – 99.9%	0.01 – 0.001 (E⁻² · E⁻³)	100 – 1,000
1	90 – 99%	0.1 – 0.01 (E⁻¹ · E⁻²)	10 – 100
0	Basic Process Control System (BPCS)		

FIG 1

Based upon how much risk is inherent in the operation of the fired equipment in a plant, the performance-based SIS standards provide methods to determine:

- How “good” the hardware components need to be?
- How much redundancy is required?
- How often testing of the system is required?
- What level of reliability is required of the individual components

Grandfather Clause

The grandfather clause of the ANSI/ISA standard provides for the continued use of existing safety systems if it can be shown through a rigorous risk analysis that the system meets the required level of risk reduction commensurate with the corporate risk tolerance level. If it does, then the mandated process of documentation of ongoing testing, management of change etc. must be implemented. If the original design does not meet these requirements or if modifications are made, the system will require following the safety lifecycle as described in the standard.

SIL Verification

SIL verification calculations must be performed on the BMS (sensors, logic solver, and final elements) to ensure that the required SIL has been achieved by each safety function of the BMS. It has been determined that most industrial process related BMS’s typically include several SIL 1 functions and at least one SIL 2 Safety Instrumented Function. Thus, a logic solver capable of meeting at least SIL 2 is typically required for these BMS applications.

Functional Testing

SIL capability of a SIS is heavily dependent on the functional test interval assumed. Functional testing is mandatory. OSHA has; in fact, fined a facility for failure to test its SIS. (An example of functional testing is the procedure of removing pressure from the low fuel pressure switch and verifying the desired actions occur.)

System Integration Qualifications

IEC 61508 mandates that those involved with design and implementation of SIS demonstrate competence in applying the SIS standards. Certified Functional Safety Expert (CFSE) designation represents a Professional Engineering type certification / examination to evaluate the competence of SIS personnel. Certification requires completion of a rigorous examination and demonstration of at least 8 years of experience in safety related endeavors. Use of CFSE’s on SIS projects provides an end user with assurance that the individual has at least a minimum acceptable level of competence in SIS related matters.

LOGIC SOLVER SELECTION

There are widely diverse opinions in industry concerning what is considered a suitable choice for a logic solver. The choices range from hard-wired relays up through safety-certified PLCs. Depending upon what agency, committee, or insurance company provides “sign-off” on applicability for service, the codes or standards followed are similarly diverse. While many companies follow NFPA, others follow corporate standards, national or international safety standards or no standard at all.

NFPA allows the use of relay-based systems or approved / listed PLC-based systems. However, there have not been any listed PLC systems available in recent years. At this writing there is one system nearing the end of its approval cycle and another vendor that is considering beginning the cycle.

ANSI/ISA 84.00.01-2004 (IEC 61511) allows the use of general purpose PLC’s in SIL 1 and SIL 2 applications. However, general purpose PLCs do have certain limitations. These limitations have been recognized by the SIS community and are reflected within the requirements of the standards. However, once a BMS includes a SIL 2 function, the requirements for using a general purpose PLC are extremely time consuming and costly. Theoretically, a General Purpose PLC could be used by reference to the “proven-in-use requirements” of the standard. However, this procedure is almost impossible without extensive vendor support to supply all of the required documentation of failure analysis and reliability. Most vendors are unlikely or unable to support such requests.

A Safety PLC represents industry’s attempt to develop a failsafe microprocessor based system by invoking the requirements of IEC 61508 in its hardware and software design. By designing the system for both safety and availability, risk can be reduced while simultaneously minimizing nuisance trips. As such, a certified Safety PLC becomes the clear choice from a cost and schedule basis for most industrial BMS applications.

While there are many vendors of Safety Certified PLCs that are well suited for use in SIS, there are only a handful that have demonstrated experience in BMS applications. The scope of the project will help to narrow the choice. The system requirements of an industrial power plant are far different than a process heater in a chemical plant. One size does not fit all from both an economic and from a functional point of view. *A user should exercise caution when making architectural decisions about a logic solver.* It is dangerous to under design and unnecessarily high lifecycle costs are a consequence of over-design.

Typically users and suppliers applying a BMS to a low risk / low consequence fired device may well meet all reasonable expectations for safety using a relay-based system and be in complete compliance with applicable codes and standards (NFPA 85 or 86). FM listed flame safeguard systems such as those offered by Siemens, Honeywell and Fireye, when used with approved sensors and shutoff valves, are appropriate.

As a fired device grows in complexity and/or size the risk typically increases as well. For example, a system with multiple burners and dual fuels has far more safety issues than a skid mounted oil heater. This is where the discrepancies began. The choice of when to use a relay-based system, an industrial PLC or a safety certified PLC is quite blurred in the eyes of most users. Very few are aware of the requirement in FM 7605 that a PLC based BMS must follow IEC 61508. And, if they are, they do not understand the implications of following the safety lifecycle.

Pulp & Paper Industry Insights

Since this industry has been operating in a depressed mode for so many years, there have been few expansion or upgrade projects where safety decisions had to be made. An opinion stated by one engineer is that older systems, that predate both NFPA and ISA standards and codes, operate under grandfather clauses. This may be just fine if the original systems were properly designed but could be a recipe for disaster if they were not and aging equipment begins to fail. This conclusion is in direct conflict with the mandates of the grandfather clause of the standard.

One mill that is updating a process heater is wholeheartedly endorsing the following of applicable safety standards codes and is only considering BMS’s that can bring them into compliance with NFPA, FM and ANSI/ISA 84.

Another facility reported that compliance with NFPA was considered adequate although they said that upgrades must go through a corporate risk management group that has an understanding of the requirement for compliance

with safety standards. It is apparently left to the knowledge base of the committee members to determine risk and decide if it is acceptable.

Another insight is that the Black Liquor Recovery Boiler Advisory Committee (BLRBAC) has endorsed the use of the safety lifecycle for burner management. This information does not seem to have gotten to many of those making decisions about safety implementation in their mills. When it does filter down, there will be many facilities that may require changes to their designs to bring them into compliance.

Burner Manufacturer Insights

All vendors that the authors have dealt with seem to have a concern about meeting NFPA codes but none had a clear understanding of when conformance with the safety standards may be required. Some did not know at all of how to provide a proposal when the client required “a SIL 2 system” or “system must be designed in accordance with IEC 61508”. Others have identified safety qualified consultants and/or safety integration firms that become contractors to the OEM. One vendor recommends that the client work with a safety qualified system integrator in the early stages of the project to gain an insight into the actual risk reduction required by his installation so that a proper BMS may be designed/proposed. As was pointed out above, installing a SIL 2 system when a SIL 1 would have been adequate is a clear waste of money and choosing the vice-versa alternative is a recipe for potential disaster.

There is a legal settlement that approaches \$100 million that was levied against a BMS supplier that was attributed to faulty design and faulty testing methods in their system. The resultant explosion destroyed an 11-story boiler in a utility power station.

Field Device Insights

There is an assortment of devices including flame scanners, pressure switches, flow switches, purge timers, control relays, temperature switches, pressure and flow transmitters and fuel shutoff valves that have distinguished themselves from the pack by securing 3rd party certification for suitability of service in accordance with various codes and/or standards.

Most commonly, UL or FM certification for suitability for use to meet NFPA codes is the most common. The more knowledgeable suppliers have an understanding that, to meet the safety standards, other certifications are required. For transmitters, a Failure Modes Effects and Diagnostic Analysis (FMEDA) report provides the basic data to perform SIL verification... a required step in the Safety Lifecycle. An FMEDA is a statistical analysis of the hardware of the device and does not include any consideration for the manufacturing process, management of change policies and procedures, software design and implementation or installation and operation considerations. A more complete certification of a device that covers all of these issues and others is performed by agencies such as TUV and FM.

In summary, what approvals are required depends on the industry, the application and the desire / requirement for conformance with various codes and standards. Prescriptive codes like NFPA may only require listed devices to be used while the performance-based safety standards (ANSI/ISA 84 & IEC 61511) require following the Safety Lifecycle which includes consideration of such factors as “fail dangerous data”, “Safe Failure Fraction” (SFF), “Mean Time To Fail – Spurious”(MTTFS), etc. to verify that a system design will meet the SIL required based on the results of the risk analysis performed.

CONCLUSION

Some plants use systems that are designed to be field-certifiable by FM or the Authority Having Jurisdiction (AHJ). The degree of safety provided is directly related to the knowledge and motivation of the AHJ. This can range from a very knowledgeable corporate risk analysis team down to a local fire chief with no knowledge of safety standards. If the Safety Lifecycle has not been properly followed, the resultant system may well be SIL 0 when it should have been designed to meet SIL 2. Even worse than non-compliance is the naïve belief of upper management that compliance – and the resultant degree of safety – has been accomplished... when it has not.

Explosions and fires associated with boiler, furnace and heater accidents have gotten front-page press coverage that has increased awareness of the potential dangers. The explosion in the power plant in Kansas not only destroyed an 11-story boiler, but also generated a legal settlement against both the utility and the BMS supplier. A boiler explosion in Algeria killed 25, injured about 75 and caused over \$800 million in damage. There have also been fires in chemical and refining facilities traced to fired heaters that have caused considerable damage and will certainly have related liability issues.

FM and other insurance underwriters are getting increasingly aware that there are more appropriate standards and are now charging premiums or not issuing policies for facilities that are not in conformance.

The mandate that “A BMS is a SIS until proven otherwise” is a concept that is here to stay whether users accept it or not. Pressures from OSHA, liability issues and increased insurance rates for non-compliance will foster increasing attention to these requirements. It is time for users to aggressively embrace the performance-based standards and learn how to cost effectively implement them on their projects.

To the uninitiated user, getting a grasp on proper project implementation can be an overwhelming task. It begins with gaining an understanding of exactly what is meant by the codes and standards when they “*invoke SIS requirements on a BMS*”.

There are some vendors who have recognized the turbulence in the BMS industry and have seized upon this opportunity to develop specific Safety-Instrumented Burner Management Systems. Some of these vendors also offer a complete compliment of Safety Lifecycle project related services to help meet the BMS needs of users in all industries.

There is a wide variation in the capabilities of safety systems service providers. Some offer only consulting services while others can offer every level of service from consultation to complete turnkey system packages.

A SIS is only as strong as its weakest link. Improper choices of equipment, poor design, faulty hardware or software configuration, improper installation, flawed testing procedures and inadequate operator training each can contribute to excessive cost, inadequate safety or excessive nuisance failures. To design a proper system, requires knowledge of basic field devices, logic solvers and final control devices and the ability to properly integrate them into a safe and reliable system. If communication is desired between the BMS and the combustion control system (CCS), a proper interface is necessary. A select few vendors can supply a totally integrated solution using both safety-certified PLCs for BMS and standard fault-tolerant PLCs for combustion control and DCS functionality all from the same product family. Cost savings for spare parts, maintenance and sharing common HMIs are just some of the advantages. For these reasons it is extremely important for users to select a design team that has demonstrated competency in Burner Management Systems, Safety Instrumented Systems and basic process control.