Options for Developing a Compliant PLC-based BMS

aeSolutions
info@aesolns.com
aeSolutions, Greenville, South Carolina, USA

Abstract

Facilities are focusing on improving the reliability of their burner management systems (BMS) through simplified troubleshooting and greater hardware diagnostics. A primary means for accomplishing this is through the use of a programmable logic controller (PLC) based BMS. A PLC-based BMS offers substantial hardware diagnostics as well as first-out trapping (if programmed in the application software) for easy troubleshooting following a BMS trip. Current industry codes including NFPA 86, NFPA 87, and API 556 permit three distinct methods for employing a code compliant PLC-based BMS: 1) Consider the BMS to be a Safety Instrumented System (SIS) with its design, configuration, and ongoing management and testing adherent to the complete safety lifecycle as mandated by ANSI/ISA 84.00.01-2004 (S84), 2) Use a PLC specifically listed for combustion safeguard service, or 3) Hardwire the burner safety interlocks “around” the PLC logic solver such that a BMS trip will occur independent of the PLC. NFPA 85 for boiler applications also permits the use of a PLC based BMS under its equivalency clause by considering a PLC based BMS implemented in accordance with the S84 safety lifecycle as being equivalent to the minimum requirements of the standard.

This paper will consider each of these approaches individually. The design and implementation complexities, advantages, and disadvantages of each approach will be illustrated. Additional features of a PLC based BMS solution such as on line testing will be explored.
General NFPA 85, 86, 87/API 556/CSA B149.3-10 Code and Recommended Requirements for PLC Burner Management System (BMS) Interlocks and Sequencing.

Facilities are focusing on improving the reliability of their burner management systems (BMS) through simplified troubleshooting, greater hardware diagnostics, and compliance with the latest applicable Code/Recommended practices for their fired equipment. A primary means for accomplishing this is through the use of a programmable logic controller (PLC) based BMS.

A PLC-based BMS can offer substantial hardware diagnostics as well as first-out trapping, event record logging and startup permissive statuses for easy troubleshooting during equipment startup or following a BMS trip. A PLC-based BMS also offers robust operator interface capabilities and communications options with DCS and SCADA systems.

Current industry codes for fired equipment include NFPA 85 (boilers and HRSGs), NFPA 86 (ovens, furnaces, thermal oxidizers), NFPA 87 (fluid heaters), API 556 (petro-chemical), and CSA B149.3-10 (Canadian general application of the NFPA Codes), which in general permit the following three distinct methods for employing a code compliant BMS using PLCs:

1) Hardwire the burner safety interlocks “around” the PLC logic solver such that a required BMS trip will occur independent of the PLC.

2) Use a PLC specifically listed for combustion safeguard service.*

3) Consider the BMS to be a Safety Instrumented System (SIS) with its hazard and layer of protection analysis, safety requirements, design, configuration, factory and site acceptance testing, ongoing management, and periodic testing adherent to the complete safety lifecycle as mandated by ANSI/ISA 84.00.01-2004 (ISA 84).

* NFPA 85 (boilers and HRSGs), while not using the term listed, requires that the designer of the BMS to evaluate and address the failure modes of the components and also requires that the design include and accommodate for hardware and software diagnostic monitoring, protect against logic system failures, and protect against unauthorized changes, among others.

**Hardwired Interlocks with General Purpose PLC**

Industry codes list specific hazards burner management systems must address and traditional approach used prior to PLC systems to address the hazards is by hardwiring all of the required interlocks to control the fuel and ignition sources. Required system timers would likewise be required to be physical devices and hardwired and tamper-proof. This option would limit troubleshooting, startup permissives, hardware diagnostic capabilities, system monitoring, first out indications, and operator communications. Maintenance and documentation updates on hardwired systems has in the past proven to be time consuming and troublesome.
A PLC can still be utilized for safety interlocks but the PLC interlocking would only be redundant to the safety rated hardwired interlocks. The main purpose of a PLC in this case would be for communication of interlocks and statuses to a facility's DCS/SCADA.

An example of a required interlock would be for combustion air. NFPA 85 5.4.4.3.2 states, “Fans supplying air to the boiler room for combustion shall be interlocked with the burner so that airflow is proven during equipment operation.” A flow switch could be used to determine if the minimum air flow is present and hardwired to a master fuel trip relay to interlock the system if sufficient flow is not present. The master fuel trip relay would directly close fuel shutoff valves and de-energize ignition sources.

**Compliance Using a Listed Non-Programmable Solid State Controller or Listed PLC**

The Codes and Recommendations listed above provide that non-programmable solid-state controllers and programmable logic controllers (PLCs) can be used for burner management in lieu of hardwiring of interlocks and timers provided the equipment has been listed by an approved organization.

The NFPA’s official definition of listed is as follows:

> “Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.”

BMS vendors may offer listed non-programmable solid state controllers or listed PLC systems if they have gone through the approval process required by certain regulatory bodies such as FM or TÜV. Generally, a listed BMS would have specific limitations on usage based on what the package system was designed and intended for and a maximum SIL rating that the system/controller has been tested for, such as for an NFPA 85 single gas burner drum boiler for SIL 2 capability.

Currently there are several listed non-programmable solid-state type BMS controllers available, but there are very few PLC systems that have to date been listed specifically for BMS service.

Non-programmable solid-state type listed BMS controllers have been successfully applied to various applications (single fuel/dual fuel, boilers, ovens, etc.) but are still generally limited to smaller single burner applications. For more complex applications many of the BMS interlocks will need to be hardwired in series external to the controller in order to utilize the non-programmable type devices. This will increase the troubleshooting time and first-out alarming, among others.
Compliance Through SIS Approach to BMS

Code References Requiring or Recommending ISA 84 Application

NFPA, API, or CSA codes all contain specific requirements for non-listed PLCs to be used as a BMS logic solver. Within those codes are references to performance-based requirements listed below:

- NFPA 86 (2011) and NFPA 87 (2011) both state in Appendix for Section 8.3:
  
  A.8.3 Furnace controls that meet the performance-based requirements of standards such as ANSI/ISA 84.00.01, “Application of Safety Instrumented Systems for Process Industries”, can be considered equivalent. The determination of equivalency will involve complete conformance to the safety life cycle including risk analysis, safety integrity level selection, and safety integrity level verification, which should be submitted to the authority having jurisdiction.

- NFPA 86 (2001) states:
  
  8.4.5 …safety programmable logic controllers shall have the following characteristics:
  
  1. The processor and the input and output (I/O) shall be listed for control reliable service with a SIL rating of at least 2.

- NFPA 85 states in Appendix A for section 4.11 Burner Management System Logic:
  
  A.4.11 Utilizing the equivalency provision in Section 1.5, an alternative design to meet the requirements of the code can be accomplished where all the following are provided:
  
  1. Approval of the authority having jurisdiction.
  2. A documented hazard analysis that addresses all the requirements of this code.
  3. A documented life-cycle system safety analysis that addresses all requirements of this code and incorporates the appropriate application-based safety integrity level (SIL) for safety instrumented systems (SIS). One methodology for achieving a life-cycle system safety analysis is to use a process that includes SIL determination and a SIS design and implementation consistent with the ISA 84 standard series.

The designer or designers have the responsibility to ensure that all the hazards identified in this code are adequately addressed in the alternative design.

It should be noted that the intent of the independence requirements in 4.11.7.1 through 4.11.7.7 of this code includes the following:

1. Separating the burner management system from other systems to reduce the risk of human errors

2. Providing layers of protection and security to reduce risk by having dedicated protection functions in the burner management system

3. Reducing risks through elimination of common mode failures
4. Providing protective features that independently limit process parameters that complement other control systems.

- API 556 (2011) states under 3.4 Protective Systems:

3.4 Protective actions include the following:

- Basic Process Control System (BPCS) Action – control overrides independent of the initiating cause.
- Operator Action – operator response to alarms, including emergency response.
- SIS Action – startup permissives and interlocks, close safety shutoff valves, open dampers.

The diversity in the design of fired heaters requires that each heater be independently evaluated to ensure that each hazard scenario is effectively mitigated. A SIF assigned a safety integrity level (SIL) of 1, 2, 3, or 4 shall comply with the requirements of ANSI/ISA 84.00.01-2004 (IEC-61511 MOD). Although this standard is accepted good engineering practice as is recommended for the protection of personnel and the environment, the work process may be applied to asset protection.

- CSA Standard B149.3-10 (2010) states under section 9.7 Programmable Controllers:

When microprocessors are used as a primary safeguard device they shall conform to CSA C22.2 No. 0.8, and the requirements of Clause 9.7.2 shall apply... The authority having jurisdiction may require that the burner management systems (BMS) be designed in accordance with internationally recognized safety standards such as the IEC 61511 series of Standards, NFPA 85 (2007), or NFPA 86 (2007).

Author's note: CSA C22.2 No. 0.8 (2012) (“Safety functions incorporating electronic technology”) defines the requirements for protection against faults to ensure functional safety for electronic equipment in a manner somewhat similar to IEC 61508. Comparisons between the two standards are too lengthy for this discussion.

It is apparent from the above selected Code and Recommended Practices citations that application of ISA 84 is now either required or used for equivalency to deploy PLC based BMS systems.

ISA 84 Safety Lifecycle Description and Implementation Methods for PLC-Based BMS

The ANSI/ISA 84.00.01 standard contains 19 clauses concerning the safety lifecycle which can be generally categorized into three phases: Risk Analysis, Realization, and Operation.

- Risk Analysis – Includes the identification and understanding of the hazards present, the challenge to apply inherent safety, and the definition/optimization of independent engineered and administrative safeguards to meet an organization’s tolerable risk criteria.
- Realization – Includes safeguard validation, detailed engineering, procurement, automation, installation and commissioning, pre-startup safety review, and functional safety assessments. This phase also includes integration of critical IPLs into operating procedures, training, maintenance programs, and process safety information.
Operation – Includes operation, maintenance, bypass management, and management of change of safety instrumented functions (SIFs) and non-SIF IPLs. It also includes the collection of reliability data, auditing, reporting on performance metrics, and active risk management.

If the ANSI/ISA 84.00.01 standard is applied, the BMS may be treated as a Safety Instrumented System (SIS). Organizations subject to US Occupational Safety and Health Association’s (OSHA’s) process safety standard, 29 CFR 1910.119, US Environmental Protection Agency’s (EPA’s) risk management standard, 40 CFR 68, or other global process safety standard, implemented hazard analysis and risk assessment programs in the mid-1990s. What has taken place in the last 10 years is an emphasis on risk-based process safety management as a means of prioritizing investments with limited resources and capital. This has driven companies to establish clear risk tolerance criteria as the bases for making sound, consistent, defensible business decisions. The risk tolerance criterion is typically in the form of a risk matrix with severity and frequency scales.

Clause 8 of ANSI/ISA 84.00.01 links the design basis of safety instrumented systems to an organization’s risk tolerance criteria. The design basis of a safety instrumented function is quantified as a probability of failure on demand and achieves a reduction of the frequency or likelihood that an initiating event will propagate forward to a loss of containment or consequence of concern. PHA methodology is used to identify the hazards present for a process, the initiating events considering failure of administrative and engineered systems, the potential consequences without safeguards, and a qualitative assessment of the mitigated event likelihood or frequency with safeguards. Organizations are then using the semi-quantitative layer of protection analysis (LOPA) methodology, or more rigorous forms of numerical analysis, to quantify the risk reduction credit of non-SIS independent protection layers (IPL). The mitigated event likelihood is compared to the tolerable mitigated event likelihood, with the difference documented as the basis for design of the related safety instrumented function, or SIS IPL.

Clause 9 defines the calculation methods, architectural constraints, and hardware fault tolerance that are to be taken into account when defining the SIF. This front end loading (FEL) engineering work requires competencies in mathematical methods, dynamic process control, instrumentation and control architecture, and control processors (logic solvers or programmable logic controllers) and communication highways. The SIS FEL phase of engineering also requires input from a strong process engineer capable of defining the process safety time of an event from cause to consequence and working with the SIS engineer to optimize the SIF with an understanding of the process dynamics and response to a trip.

Clause 10 requires the functional safety requirements to be documented in the form of a specification as the basis for detailed design and engineering.

Clause 11, 12, 13, 14, and 15 identify the requirements for the detailed engineering, factory acceptance testing, installation, commissioning, and validation of an SIS system before turnover to operations.

Clause 16, 17, and 18 identify the requirements for the continued operations and maintenance of a SIS System. These requirements include management of change, procedure development, operator and maintenance training, as well as the testing, demand tracking, and auditing of each safety instrumented function.
Clause 19 identifies the document control measures intended to be in place relevant to executing the lifecycle activities.

Burner management systems as a result of ISA 84 layer of protection analysis (LOPA) generally include at least one SIL 2 rated safety instrumented function. Most programmable logic solvers are not capable of meeting SIL 2. A general purpose safety configured PLC is defined as an industrial grade Programmable Electronic (PE) logic solver, which has been specifically configured for safety applications. A general purpose safety configured PLC would need to be evaluated per IEC 61511 criteria regarding “proven-in-use” when a documented assessment has shown there is appropriate evidence, based upon the previous use of the component(s), that the component(s) is/are suitable for use in a Safety Instrumented System. This includes fulfilling the following criteria:

1) The device has been used or tested in configurations representative of the intended operational profiles.

2) For SIL 1 or 2 applications, a General Purpose Safety Configured PLC may be used provided that all of the following additional provisions are met:
   a) Understanding of unsafe failure modes,
   b) Use of techniques for safety configuration that address identified failure modes,
   c) The embedded software has a good history of use for safety applications, and
   d) Protection against unauthorized or unintended modifications.

3) A formal assessment shall be carried out for any PE logic solver used in a SIL 2 application and shall show:
   a) It is both able to perform the required functions and the previous use has shown there is a low enough probability it will fail in a way which could lead to a hazardous event when used as part of a safety instrumented system, due to either random hardware or systematic faults in hardware or software.
   b) Measures are implemented to detect faults during program execution and initiate appropriate reaction; these measures shall comprise the following:
      i) Program sequence monitoring,
      ii) Protection of code against modifications or failure detection by online monitoring,
      iii) Failure assertion or diverse programming,
      iv) Range check of variables or plausibility check of values, and
      v) Modular approach.
   c) Appropriate coding standards have been used for the embedded and utility software.
   d) It has been tested in typical configurations, with test cases representative of the intended operational profiles.
   e) Trusted verified software modules and components have been used.
   f) The system has undergone dynamic analysis and testing.
   g) The system does not use artificial intelligence or dynamic reconfiguration.
h) Documented fault insertion testing has been performed.

4) For all SIL 2 applications, a safety manual including constraints for operation, maintenance and fault detection shall be available covering typical configurations for the PE logic solver and the intended operational profiles.

5) The PE logic solver must be capable of meeting the minimum hardware fault tolerance based upon Table 1:

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFF &lt; 60%</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Special requirements apply - See IEC 61508</td>
</tr>
</tbody>
</table>

Deploying a general purpose safety configured PLC for BMS service that is evaluated per IEC 61511 criteria regarding “proven-in-use” is time consuming, costly, and requires extensive paperwork for an end user and his design engineer who are untrained with the requirements of ISA 84 for “proven-in-use”. Failure, operational, and application data for a general purpose PLC system may not be available or not to be trusted, thereby making a “proven-in-use” justification very difficult.

Selection of a safety PLC system and its components that has been certified by a recognized listing agency to a certain maximum required LOPA SIL level is a much better approach. LOPA target SIL levels for selected SIFs can be readily ascertained, justification for logic solver SIL capability will need not to be justified, failure data will be readily available to backup SIL verification calculations, and a safety manual will be available to define a road map as to how the PLC system is to be configured and programmed to comply with the certified SIL capability rating of the safety PLC as well as providing security to prevent unwarranted data/program changes, and providing the flexibility for design and safety development enhancements that may develop during the life cycle of the SIS.

**End User Compliance Responsibility**

The Authority Having Jurisdiction (AHJ) of the end user who is responsible to determine which if any Code or Recommended Practice is to apply for deployment of any new or replacement BMS system at his facility. The AHJ is also responsible to review and approve any and all variances to the selected Code or Recommended Practice.

The AHJ is also responsible for reviewing and approving compliance with the latest published Codes as to how the BMS is to be deployed – hardwired, listed PLC, or through an SIS approach.
Even when the BMS deployment is through using an ISA 84 based SIS approach, it is still the end user who is responsible for compliance and not an OEM BMS vendor or system integrator. If the end user opts to deploy an PLC-based ISA 84 Safety Instrumented BMS (SI-BMS), not only does the BMS system as a whole need to comply with the applicable Code or Recommended Practice selected by the AHJ, but so does it have to follow the applicable requirements of ANSI/ISA 84.00.01.

Summary

Replacement BMS or new BMS deployments are permitted to be installed by the various Codes and Recommended Practices in three major categories:

- Hardwired with a general purpose PLC performing none of the primary interlocking and sequencing
- Using a listed non-programmable solid state controller or a listed PLC system
- Using ISA 84 requirements to justify the required safety level of the PLC

The trend, however, in recent years has been toward an increased focus on safety by end users. Especially with regard to fired equipment and the burner management systems that control them. To that end SIL 2 and SIL 3 capable safety PLC systems have been developed and listed. These systems not only provide the inherent programmability of PLC for flexibility, rapid deployment, robust communication to DCS, CCS, and SCADA systems, and easier troubleshooting and maintenance, but also add the known and justifiable reliability, safe failure modes, security, and protection against unwarranted change inherent with this SIL capable class of safety PLCs.

When deploying any PLC system, safety rated or general purpose, the end user must be aware that not only does PLC-based BMS must meet the interlocking and sequencing requirements of the latest applicable Code or Recommended Practice for their industry and equipment, but that the end user must also meet the requirements to apply the ISA 84 life cycle hazard review and safety requirements.

Disclaimer

The following paper is provided for educational purposes. While the authors have made reasonable efforts in the preparation of this document, aeSolutions makes no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of this document.