Codes and Standards Update: Safety Instrumented Burner Management Systems

(Note: This paper was presented at the 2016 Texas A&M University Instrumentation Symposium for the Process Industries.)

Ged Farnaby
Director Business Development & Marketing
aeSolutions

Michael Scott, P.E., CFSE
Exec VP - Global Process Safety Technology
aeSolutions

Keywords

Abstract
Invoking the concept of a Safety Instrumented – Burner Management System in all three of the NFPA 85, 86 and 87 series of codes / standards is a significant milestone for industry. In 2002 when the ISA S84 committee first began developing the Technical Report, TR84.00.05 Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS), none of these codes / standards recognized the concept of a Safety Instrumented System. This issue directly contributed to schedule delays in the development process, which ultimately resulted in pushing the final publication of the Technical Report out to December of 2009.

However, recently all three of the NFPA codes / standards that govern fired device Burner Management Systems (BMSs) have been updated to invoke the concept of Safety Instrumented Systems (SIS). These include the following:

2. NFPA 86 - Standards for Ovens and Furnaces 2015 Edition

This paper will highlight changes to the above codes / standards as they apply to the concepts of Safety Instrumented Systems. This will include a discussion on equivalency clauses and / or linking paragraphs to ISA S84.00.01 - 2004 (IEC 61511 Mod) possibly allowing deviation from prescriptive requirements. Also of significant note is the modification of logic solver requirements with inclusion of a direct reference mandating the use of Safety PLCs with minimum SIL capabilities in certain instances. In addition, changes related to sensors and valve requirements will be highlighted. This
paper will also highlight areas where the concepts of Safety Instrumented Systems in the author’s opinion have been potentially misapplied within the NPFA series.

Background

NFPA 85, Boiler and Combustion Systems Hazards Code, applies to the following:

“(1) Single burner boilers, multiple burner boilers, stokers, and atmospheric fluidized bed boilers with a fuel input rating of 3.7 MWt (12.5 million Btu/hr) or greater
(2) Pulverized fuel systems at any heat input rate
(3) Fired or unfired steam generators used to recover heat from combustion turbines [heat recovery steam generators (HRSGs)] and other combustion turbine exhaust systems at any heat input rate”

NFPA 86, Standard for Ovens and Furnaces, applies to the following:

“...shall apply to Class A, Class B, Class C, and Class D ovens, dryers, and furnaces; thermal oxidizers; and any other heated enclosure used for processing of materials and related equipment.”

NFPA 87, Recommended Practice for Fluid Heaters, applies to the following:

“...covers Type F, Type G, and Type H fluid heaters and related equipment. Within the scope of this recommended practice, a fluid heater is considered to be any thermal fluid heater or process fluid heater with the following features:
(1) Fluid is flowing under pressure.
(2) Fluid is indirectly heated.
(3) Release of energy from combustion of a liquid or gaseous fuel or an electrical source occurs within the unit.”

As one can see from the above, NFPA 85, 86 and 87 cover a wide variety of fired devices used in the process industry today. In North America, use of these standards is very prevalent. As such, it is imperative that they provide sound and consistent guidance when invoking SIS concepts to a BMS unit operation.

Performance versus Prescriptive

Per NFPA, “Performance-based codes and standards specifically state their safety goals, and reference approved methods that can be used to demonstrate compliance with their requirements. The document may be phrased as a method for quantifying equivalencies to an existing prescriptive-based code or standard, or it may identify one or more prescriptive codes or standards as approved solutions. Either way, the document allows the use of any solution that demonstrates compliance.”

The last sentence is extremely important in that a truly performance based code / standard does not mandate a specific design solution (i.e. install a pressure switch at this location and close 1oo2 valves
in the fuel gas piping) instead it allows the user to evaluate options for mitigating risk and choosing the “best” solution per their requirements.

ANSI / ISA S84.00.01 / IEC61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector invokes a performance based approach to managing risks to personnel and / or the environment through adoption of the safety lifecycle. Simplistically, the safety lifecycle embodies a three-step methodology of overall risk management, which can be summarized as follows:

1. **Execute** safety lifecycle documentation
2. **Monitor** leading/lagging process safety indicators
3. **Sustain** safe unit operations through corrective actions

Thus, using Burner Management Systems as an example, ANSI / ISA S84.00.01 / IEC61511 does not provide specific guidance on BMS related hazards and / or the “best” way(s) to design a BMS to safely and efficiently design, install and maintain instrumentation / controls to prevent uncontrolled combustion events that could be hazardous to personnel and / or the environment. It “**allows the use of any solution that demonstrates compliance**” to the standard.

NFPA 85, 86 and 87 on the other hand are generally prescriptive in nature in that they provide specific requirements on BMS designs. This includes requirements related to specific BMS related hazards:

- Sensor types and installation locations
- Main burner block valve and vent valve locations
- Pilot burner block valve and vent valve locations / sizing
- Testing frequency
- Logic solver requirements
- Etc.

Many of these requirements noted above have been added over the years in response to actual BMS hazardous incidents. NFPA 85 for instance can trace its roots back to NBFA 60, *Regulations of the National Board of Fire Underwriters for the Installation of Pulverized Fuel Systems as Recommended by the National Fire Protection Association*, which was initially published in 1924. As hazardous incidents related BMS incidents occurred in industry, design recommendations based upon these events were added to the NFPA body of work.

One should note however that NFPA 85 for instance states “It is not possible for this code to encompass all specific hardware applications, nor should this code be considered a “cookbook” for the design of a safety system. In applying any type of equipment to a safety system, the designer should consider carefully all the possible failure modes and the effect that each might have on the integrity of the system and the safety of the unit and personnel.”

As of the 2015 editions of NFPA 85, 86 and 87 all three now include direct references to ANSI / ISA S84.00.01 / IEC61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector. However, in many instances the references related to SISs have been done so in a prescriptive manner, which is directly in conflict with the originating performance based requirements of the
safety lifecycle. In some instances, it is the author’s opinion that these misapplied SIS concepts could be potentially unsafe and/or increase cost of ownership.

Equivalency Statements

The 2015 editions of NFPA 85, 86, and 87 now all contain language that allows one to apply the performance based design concepts of ANSI/ISA S84.00.01 / IEC61511. Specifics for each standard are noted below:

NFPA 85

NFPA 85, *Boiler and Combustion Systems Hazards Code*, invokes the safety lifecycle through the equivalency clause in Section 1.5 which states:

“**Equivalency.** Nothing in this code is intended to prevent the use of systems, methods, or devices of equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety over those prescribed by this code.”

Section 4.11 defines prescriptive requirements for the Burner Management System Logic.

NFPA 85 Annex A provides additional explanatory material.

“Annex A is not a part of the requirements of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.”

“A4.11 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 ANSI/ISA 84.00.01, Application of Safety Instrumented Systems for the Process Industry, or IEC 61511, Functional Safety—Safety Instrumented Systems for the Process Industry Sector.

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 4.11.8.1 through 4.11.8.6 of this code include 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

**NFPA 86 / NFPA 87**

NFPA 86, *Standard for Ovens and Furnaces*, and NFPA 87, *Recommended Practice for Fluid Heaters* both invoke the safety lifecycle through the equivalency clause associated with section 8.3, which defines prescriptive requirements for the Burner Management System Logic.

NFPA 86 / 87 Annex A provides additional explanatory material.

“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 the Process Industries, and IEC 61511, Functional Safety: Safety Instruments Systems for the Process Industry Sector, 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.”

Therefore, it would be acceptable under NFPA 85, 86 and / or NFPA 87 for an end user to propose an alternate BMS design with different sensors / voting arrangements, different valves / voting arrangements, different logic solver designs, etc. and as long as one can demonstrate conformance to ANSI/ISA 84.00.01/ IEC 61511 with approval by the appropriate Authority Having Jurisdiction (AHJ). This flexibility is both good and bad. It is great for an end user with brownfield legacy BMS designs that wishes to justify the existing design is acceptable as designed, installed and maintained. However, for new equipment, it provides added flexibility that a fired device Original Equipment Manufacturer (OEM) might struggle with in attempting to properly address SIS requirements. The reason being the fundamental concept behind ANSI/ISA 84.00.01/ IEC 61511’s tolerable risk criteria. There is not a uniform globally accepted set of risk criteria. Thus, each end user company selects their own risk criteria and applies it to their safety system designs. This could result in principle to one BMS needing a large quantity of SIL 1 SIFs, while the same exact BMS installed at a different end user location could require a large quantity of SIL 2 SIFs. This makes it difficult for an OEM to supply a BMS design that is least credible from a cost standpoint and also meets all possible SIL requirements ranging from SIL 1 to SIL 3. The OEM is most likely going to provide their standard least credible cost design that does not utilize a safety PLC and as such will have limited ability to meet a given SIL target.
Logic Solver Requirements

In the past, one of the major differences between NFPA BMS standards and ANSI/ISA 84.00.01/IEC 61511 would be the minimum requirements for logic solvers. NFPA BMS standards focused on listed devices, whereas ANSI/ISA 84.00.01/IEC 61511 users typically mainly focus on the use of certified safety PLCs. This is usually driven by ANSI/ISA 84.00.01/IEC 61511 logic solver requirements when SIL 2 SIF targets have been specified. This disconnect between minimum acceptable logic solvers often results in the need to upgrade an OEM BMS design to incorporate use of a safety PLC in lieu of a general purpose PLC design with external watchdog timers and external master fuel trip relays.

This has been somewhat rectified in the 2015 editions of NFPA 85, 86 and 87, where all recognize the concept of a safety PLC. However, in the author’s opinion this is also an example of where the performance concepts of SIL have potentially been prescriptively misapplied.

NFPA 85

NFPA 85, *Boiler and Combustion Systems Hazards Code*, invokes the following requirements on PLC’s for single burner boiler applications. The concept of Safety PLCs is not invoked with regards to multiple burner boiler applications within NFPA 85.

“5.4.6.1 In addition to the requirements in Section 4.11, the boiler control system for single burner boilers shall be permitted to be combined with the burner management system under one of the following conditions:

(1) If the fuel-air ratio is controlled externally from the boiler control system; or

(2) If the combined boiler control and burner management system is specifically listed or labeled for the application;

Or

(3) A single safety-rated programmable logic system shall be permitted to be used to implement both burner management system safety and process logic where both of the following conditions are met:

(a) The processor and input/output (I/O) modules are approved or certified by a notified body according to IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, to be at least SIL 3 capable;

And

(b) The burner management system logic is isolated from other logic and boiler controls, and the related data of the burner management system program, including I/O data, are protected from being unintentionally affected by data of other user programs.”

NFPA 85 Annex A provides additional explanatory material.

“A.5.4.6.1(3) The term SIL 3 capable defines the qualities of a logic system as to its diagnostic functions and separation of safety logic from nonsafety logic. It does not imply a requirement for a
SIL 3 safety instrumented system implemented in accordance with IEC 61511, Functional Safety Safety Instrumented Systems for the Process Industry Sector.

SIL 3 capable was purposely specified as the minimum safety level for a single programmable logic system (excluding field devices) used for both the burner management system and operating controls based on the existing safety levels presently required in this code, which can be considered SIL 2, SIL 1, and/or SIL 0. The notified body or third-party certification is critical in the SIL 3 capable requirement because self-certification is permitted in the safety-rated programmable logic system marketplace for SIL 1 or SIL 2 capability, and with self-certification there is no assurance that critical safety functions, such as the secure separation of the safety and process logic, are provided. Isolation between the burner management system and the other logic can be accomplished by using separate processors or by selecting a single processor that ensures isolation through the use of an isolated programming area protected by locks or passwords.”

NFPA 85 – Logic Solver Requirements Areas of Concern

Thus, NFPA 85 is invoking use of a 3rd party certified SIL 3 Safety PLC if one desires to combine combustion controls and BMS logic within a single Safety PLC. It states that a SIL 3 certified safety PLC is required to ensure the BMS logic and combustion control logic is appropriately segregated within the control system proper. However, there are several areas of concern that need to be addressed with this type of design. From a risk analysis standpoint NFPA is now endorsing combining BPCS and SIS logic within a single Safety PLC without including a significant and mandatory disclaimer contained in ANSI / ISA S84.00.01 / IEC61511 as noted below:

“11.2.2 Where the SIS is to implement both safety and non-safety instrumented function(s) then all the hardware and software that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL.

NOTE 1 Wherever practicable, the safety instrumented functions should be separated from the non-safety instrumented functions.

NOTE 2 Adequate independence means that neither the failure of any non-safety functions nor the programming access to the non-safety software functions is capable of causing a dangerous failure of the safety instrumented functions.

11.2.4 If it is intended not to qualify the basic process control system to this standard (ANSI / ISA S84.00.01 / IEC61511), then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

NOTE 1 Operating information may be exchanged but should not compromise the functional safety of the SIS.

NOTE 2 Devices of the SIS may also be used for functions of the basic process control system if it can be shown that a failure of the basic process control system does not compromise the safety instrumented functions of the safety instrumented system.
11.2.10 A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand for the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared component because if the shared component fails, a demand will be created immediately to which the SIS may not be capable of responding. For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.”

ANSI / ISA S84.00.01 / IEC61511 provides additional requirements regarding common cause issues.

“9.5.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative.

9.5.2 The assessment shall consider the following:

- independency between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS (for example, can plugging of relief valves cause the same problems as plugging of sensors in a SIS?).”

With failure of the Combustion Control System (CCS) potentially an initiating cause for loss of flame and the BMS needing to properly respond to the potential hazard associated with the loss of flame scenario, combining BPCS and BMS logic within the same logic solver should be only attempted with careful review of common cause errors and/or systematic errors as noted in the requirements of ANSI / ISA S84.00.01 / IEC61511 above. Some Safety PLCs in the market today may be third party certified to address such a combined CCS / SIS design but, potentially not all. Thus, an unsophisticated end user or OEM may purchase a SIL 3 safety PLC, not follow the safety manual in its entirety, and unknowingly be left with design with significant common cause failure concerns.

In addition, the CCS would need to be included under strict Management of Change per the requirements contained in ANSI / ISA S84.00.01 / IEC61511 11.2.2, where CCS is now treated like a SIS. Thus, it is the author’s opinion that NFPA 85 is understating a significant risk and increased cost of ownership by prescriptively invoking the concept of SIL 3 for the logic solver and endorsing combining CCS and SIS in one logic solver without mandating one fully apply the safety lifecycle to the installation.
The safety lifecycle mandates one design to a SIL target, as well as, a nuisance trip rate target. Thus, it ensures the BMS will meet minimum safety requirements while maximizing availability. One could in theory design a SIL 3 BMS that trips once a week. By failing to invoke compliance with the safety lifecycle, unsophisticated end users or OEM’s might in fact be unknowingly installing BMS’s with higher nuisance trip rates coupled with the rigorous MoC requirements, could increase cost of ownership, as well as, increase end user risk (i.e. needing to light off more).

Also, mandating prescriptively the required SIL for the BMS logic solver, is not in line with the performance based design requirements contained in ANSI / ISA S84.00.01 / IEC61511. ANSI / ISA S84.00.01 / IEC61511 would have one conduct a risk analysis and design a logic solver that is capable of meeting the highest required SIL for all SIF’s associated with the given BMS.

**NFPA 86**

NFPA 86, *Standard for Ovens and Furnaces*, invokes the following requirements on PLC’s:

“8.4.2 Where PLCs are not listed for combustion safety service or as combustion safeguard, the PLC and its associated input and output (I/O) used to perform safety functions shall be as follows:

(1) Third-party certified to IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, safety integrity level (SIL) 2 or greater

(2) Applied to achieve at least an SIL 2 capability per the manufacturer’s safety manual

8.4.4 Safety PLCs.

(A) Where used for combustion safety service, safety PLCs shall have the following characteristics:

(1) The processor and the I/O shall be listed for control reliable service with an SIL rating of at least 2.

(2) Access to safety functions shall be separate from access to nonsafety functions.

(3) Access to PLC logic dedicated to safety functions shall be restricted to prevent unauthorized changes.

(4) All safety function sensors and final elements shall be independent of operating sensors and final elements.

(B) Safety PLCs shall not implement the following:

(1) Manual emergency switches

(2) Continuous vapor concentration high-limit controllers”

NFPA 86 Annex A provides additional explanatory material.

“A.8.4.2 “…The requirements for SIL capability in 8.4.2 pertain only to the PLC and its I/O and not to the implementation of the burner management system. The purpose of the SIL capability requirement is to provide control reliability.”

NFPA 86 defines “listed” as noted below.
“3.2.5 Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, 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.”

NFPA 86 does not provide a definition of “control reliable”.

**NFPA 86 – Logic Solver Requirements Areas of Concern**

Mandating prescriptively the required SIL for the BMS logic solver, is not in line with the performance based design requirements contained in ANSI / ISA S84.00.01 / IEC61511. ANSI / ISA S84.00.01 / IEC61511 would have one conduct a risk analysis and design a logic solver that is capable of meeting the highest required SIL for all SIF’s associated with the BMS.

To further complicate the matter NFPA 86 states the safety PLC “shall be listed for control reliable service with an SIL rating of at least 2.” This is confusing at best. The term control reliable is not defined within NFPA 86. Further the term “control reliable” is associated with machine safeguarding. Machine safety and process safety have many potential significant differences:

- continuous / high demand mode vs low demand mode
- energize to trip vs de-energize to trip

For instance a simple relay designed for high cycle service (energizes / de-energizes millions of times over its life) certified to SIL 3 per the machine safety standard IEC 62061 will not be appropriate for a low demand mode (de-energizes once every 10 years) application. One would need to specify a SIL 3 relay certified to IEC 61508 for process industry usage. Thus, by invoking machine safe guarding concepts while also invoking safety instrumented system concepts. With most BMS applications in the process industry being low demand mode, this will be confusing to the unsophisticated end user or OEM.

Compounding above is the fact that NFPA 86 notes that following the entire safety lifecycle is not required. The safety lifecycle mandates one design to a SIL target, as well as, a nuisance trip rate target. Thus, it ensures the BMS will meet minimum safety requirements while maximizing availability. One could in theory design a SIL 2 BMS that trips once a week. By falling to invoke compliance with the safety lifecycle, unsophisticated end or OEM’s users might in fact be unknowingly installing BMS’s with higher nuisance trip rates, which would increase cost of ownership as well as, increase end user risk (i.e. needing to light off more).

In addition, with existence of SIL 2 general purpose safety configured PLCs in the marketplace, as well as, IEC61508 fully certified platforms it is critical an end user fully understand the implications / design requirements of these logic solvers. In a global economy with demand for a least credible design, it is assumed many end users / OEMs would not invoke the entire safety lifecycle. Thus, it is the author’s opinion that NFPA 86 is understating a potential risk by prescriptively invoking the
concept of SIL 2 for the logic solver without mandating one fully apply the safety lifecycle to the installation.

**NFPA 87**

NFPA 87, *Recommended Practice for Fluid Heaters*, invokes the following requirements on PLC’s:

“8.4.2 For PLCs that are not listed for combustion safeguards, the PLC and its associated I/O used to perform safety functions should be certified to IEC 61508 for use in safety applications with a safety integrity level of 3 or greater.”

**NFPA 87 – Logic Solver Requirements Areas of Concern**

Mandating prescriptively the required SIL for the BMS logic solver, is not in line with the performance based design requirements contained in ANSI / ISA S84.00.01 / IEC61511. ANSI / ISA S84.00.01 / IEC61511 would have one conduct a risk analysis and design a logic solver that is capable of meeting the highest required SIL for all SIF’s associated with the BMS.

At this time, the authors are only aware of one safety PLC that has been specifically listed for combustion safeguard service. Therefore, most end users of OEMs attempting meet NFPA 87 BMS requirements will be doing so by attempting to meet the remainder of the BMS logic solver requirements contained in NFPA 87.

As with NFPA 86, NFPA 87 does not provide guidance on whether one should follow the entire safety lifecycle or not. The safety lifecycle mandates one design to a SIL target as well as a nuisance trip rate target. Thus, it ensures the BMS will meet minimum safety requirements while maximizing availability. One could in theory design a SIL 3 BMS that trips once a week. By falling to invoke compliance with the safety lifecycle, unsophisticated end users or OEMs might in fact be unknowingly installing BMS’s with higher nuisance trip rates, which would increase cost of ownership as well as, increase end user risk (i.e. needing to light off more).

**Sensor Requirements**

As of the 2015 editions of NFPA 85, 86 and 87 all three now allow the use of transmitters as well as switches as initiating devices / sensors to the BMS. As a good engineering practice, installation of a transmitter wired to a control system with a Human Machine Interface (HMI) that is reviewed by operations on a routine basis provides a certain degree of diagnostics. If a pressure sensor tap becomes plugged, it is hoped that operations will eventually take notice that the analog signal displayed on the HMI has not moved recently and as such will initiate a maintenance request. Thus, by displaying an analog value to the operator on a routinely monitored HMI, it is possible to detect potentially dangerous undetected failures (i.e. plugged taps) prior to an initiating event and / or prior to functionally testing the device. A transmitter can also provide a wide variety of diagnostics:

- less than 4mA alarm or trip,
greater than 20 mA alarm or trip,  
• stuck signal alarm or trip, etc.

For this reason, analog transmitters are favored over blind initiators (i.e. switches). If the instrument tap has become plugged associated with a switch installation, this will only be detected during functional testing or during the incident investigation of an associated event, whether a near miss or actual loss of primary containment.

Specific sensor requirements for each code / standard are noted below:

**NFPA 85**

NFPA 85, *Boiler and Combustion Systems Hazards Code*, invokes the following requirements on transmitters:

“4.11.4 The burner management system interlock and alarm functions shall be initiated by one or more of the following:

1. One switch or transmitter dedicated to the burner management system
2. Voting logic derived from two or more switches or transmitters

4.11.4.1 When multiple transmitters are used in the burner management system, such signals shall be permitted to be shared with other control systems for control purposes.

4.11.4.2 When signals from multiple switches or transmitters are provided to initiate interlock or alarm functions, those signals shall be monitored in comparison to each other by divergence or other fault diagnostic alarms.

4.11.4.3 When signals from multiple switches or transmitters are provided to initiate interlock or alarm functions, the provided signals shall be generated by individual sensing devices connected to separate process taps.”

**NFPA 85 – Sensor Requirements Areas of Concern**

NFPA 85 fails to provide guidance on issues regarding sharing sensors between the BMS and CCS.  
ANSI / ISA S84.00.01 / IEC61511 notes:

“11.2.10 A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand for the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared component because if the shared component fails, a demand will be created immediately to which the SIS may...
not be capable of responding. For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered."

As stated earlier, ANSI / ISA S84.00.01 / IEC61511 provides additional requirements regarding common cause issues.

“9.5.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative.

9.5.2 The assessment shall consider the following:

- independency between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS (for example, can plugging of relief valves cause the same problems as plugging of sensors in a SIS?).”

BMS and CCS transmitters can be shared but they must be carefully designed. NFPA 85 does not include verbiage warning end users of the potentially dangerous issues as noted above from shared sensors. By not mandating full compliance to ANSI / ISA S84.00.01 / IEC61511 and not providing prescriptive guidance / warnings regarding shared sensors, an unsophisticated end user or OEM could make poor decisions that unknowingly place their BMS installation at increased risk.

**NFPA 86 / NFPA 87**

NFPA 86, *Standard for Ovens and Furnaces*, and NFPA 87, *Recommended Practice for Fluid Heaters* both invoke the following requirements on transmitters:

“8.2.11 Where transmitters are used in place of switches for safety functions, the following shall apply:

(1) The transmitter shall be safety integrity level (SIL) 2 capable.

(2) Transmitter failure shall be detected and initiate a safety shutdown.

(3) The transmitter shall be dedicated to safety service unless listed for simultaneous process and safety service.”

**NFPA 86 / 87 – Sensor Requirements Areas of Concern**

Mandating prescriptively the required SIL for the transmitter is not in line with the performance based design requirements contained in ANSI / ISA S84.00.01 / IEC61511. As stated earlier, ANSI / ISA S84.00.01 / IEC61511 would have one conduct a risk analysis and design a SIF that is capable of
meeting the required SIL. For instance, a typical BMS risk analysis might result in SIL 2 requirement for a BMS SIF as a whole. When the hazard can be detected by the pressure transmitter or flame scanner, ANSI / ISA S84.00.01 / IEC61511 would not mandate that a SIL 2 capable transmitter be installed. This statement implies that an OEM or end user must purchase a SIL 2 rated transmitter in lieu of a standard transmitter. ANSI / ISA S84.00.01 / IEC61511 allows the use of certified transmitters or devices selected upon prior use. In a brownfield facility with many BMS installations, it may not be desirable or even cost effective to change out all standard transmitters for certified transmitters. Per the requirements of ANSI / ISA S84.00.01 / IEC61511, this is left to the discretion of the end user. NFPA 86 / 87 should take a similar position and not be mandating use of SIL 2 capable transmitters.

In addition, by not mandating one comply fully with the requirements of ANSI / ISA S84.00.01 / IEC61511, an end user may not be aware of specific design requirements contained within the safety manual provided by the OEM of the SIL 2 certified transmitter. If these design requirements are not implemented in the BMS design, the SIL 2 rated transmitter may not even be capable of meeting SIL 1.

In the author’s opinion, this is another example of where the performance concepts of SIL have potentially been prescriptively misapplied within NFPA 86 / 87.

Conclusion

Invoking the concept of a Safety Instrumented – Burner Management System in all three of the NFPA 85, 86 and 87 series of codes / standards is a significant milestone for industry.

These include the following:

2. NFPA 86 - Standards for Ovens and Furnaces 2015 Edition

The above documents include references allowing alternate equivalent BMS designs to the prescriptive requirements contained within NFPA, when one follows the safety lifecycle as contained in ANSI / ISA S84.00.01 / IEC61511 with Authority Having Jurisdiction (AHJ) approval. This is powerful in that it allows a sophisticated and competent end user to produce alternate BMS designs to mitigate their risk while minimizing lifecycle costs.

NFPA 85, 86 and 87 series of codes / standards also invoke prescriptive SIL requirements associated with logic solvers and transmitters. In the authors opinion these SIL requirements have been misapplied by NFPA and could result in increased risk to an end user and / or increased cost of ownership to an end user. As such it is recommended that NFPA 85, 86 and 87 be corrected in future releases to eliminate these issues that could result in unnecessary increases in cost of ownership and more importantly potential increased operational risk to the end user.
Disclaimer

Although it is believed that the information in this paper is factual, no warranty or representation, expressed or implied, is made with respect to any or all of the content thereof, and no legal responsibility is assumed therefore. The examples shown are simply for illustration, and, as such, do not necessarily represent any company's guidelines. The reader should use data, methodology, formulas, and guidelines that are appropriate for their own particular situation.

References


Abbreviations and Definitions

AHJ   Authority Having Jurisdiction
ANSI  American National Standards Institute
BMS   Burner Management System
BPCS  Basic Process Control System
CCS   Combustion Control System
HMI   Human Machine Interface
IEC   International Electrotechnical Commission
ISA   International Society of Automation
NFPA  National Fire Protection Association
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented System</td>
</tr>
</tbody>
</table>