Why AC800M High Integrity is used in Burner Management System Applications?

Prepared by:
Luis Duran
Product Marketing Manager Safety Systems
ABB Process Automation/Control Technologies
TÜV Functional Safety Engineer 902/07

Table of Content

Introduction

This document is intended to explain the certification of ABB's 800xA Safety AC800M High Integrity in relation to Burner Management System applications. 800xA High Integrity is extensively used worldwide in Integrated Control and Safety System (ICSS) including Emergency Shutdown Systems, Safety Instrumented Systems, Fire and Gas Systems and Burner Management Systems. The introduction of Independent High Integrity allows the use of AC800M High Integrity in similar applications but without the use of System 800xA Operations as the HMI.

Burner Management Systems Defined

Burner Management Systems (BMS) are a subset of industrial automation and control systems that are employed in the process industries to provide interlocks and permissives to prevent misoperation of equipment and to safely handle faults caused by equipment failure. These events potentially result in uncontrolled fires, explosions, or implosions and in the unintended release of the materials being heated.

Fired equipment is found throughout the process industries in many applications, including various types of heaters and boilers, the hazards associated with burner operation are managed by an instrumented system commonly referred to as the burner management system (BMS).

Reference: ISA-TR-84.00.05-2009

A Burner Management System is defined 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.

Reference: NFPA 85 2011 Section 3.2.26

The definition above is consistent with that of a Safety Instrumented System (SIS) according to ANSI/ISA-84.00.01-2004 (ISA84).

Standards Applicable to Burner Management Systems

There are several engineering best practices and many standards that cover the design of BMS. The most common are probably NFPA 85 Boiler and Combustion Systems Hazards Code and NFPA 86 Standard for Ovens and Furnaces, but there are others such as FM7605 Approval Standards for PLC based Burner Management System, BLRBAC – *Black Liquor Recovery Boiler Advisory Committee*, and API 556.

BMS applications are found in different industries including Power Generation, Pulp and Paper, Chemical and Petrochemical, Refining and Upstream Oil & Gas production. However all these industries, excluding Nuclear Power Generation are grouped as the process industries and covered under ANSI/ISA-84.00.01-2004.

The ANSI/ISA-84.00.01-2004 standard applies to safety instrumented systems (SISs), which are instrumented systems implemented to prevent an event that results in major consequences and unacceptable lasting effects, usually involving significant harm to humans, substantial damage to the environment, and/or loss of community trust with possible loss of franchise to operate.

Use of performance-based design is not currently the norm for BMS within the process industries. BMS have traditionally been designed and implemented according to other good engineering practices, such

as NFPA 85. These prescriptive practices do not require evaluation of the risk reduction capability of the BMS. However recent editions of NFPA standards reference ANSI/ISA-84.00.01-2004 as a performance base standard that can be followed to determine the hazard and the appropriate risk mitigation strategy.

Reference: ISA-TR-84.00.05-2009

Benefits of Applying ANSI/ISA-84.00.01-2004

The ISA 84 standard (or the international equivalent - IEC 61511) is performance-based rather than prescriptive as the user must determine the risk associated to the process, the risk reduction strategy and the risk reduction performance of each Layer of Protection. Other Layers of Protection include the Basic Control System (BPCS), Alarms and Safety Instrumented Systems (SIS).

In this case safety consequences can result from the misoperation of fired equipment during start-up, normal operation, maintenance, and shutdown. A BMS is implemented to prevent misoperation and to safely handle faults caused by equipment failure.

Misoperation can be caused by equipment failure or improper firing and can potentially result in uncontrolled fires, explosions, or implosions and in the unintended release of the materials being heated. Consequently, the hazard and risk analysis for the fired equipment often focuses on events that lead to hydrocarbon fuels being introduced into the equipment under abnormal operating conditions.

The ANSI/ISA-84.00.01-2004 Safety Lifecycle addresses SISs used to prevent unacceptable hazardous events, generally involving harm to people and/or damage to the environment. The lifecycle is supported by a management system that focuses on reducing the potential for SIS failure through effective SIS design and management. BMS can be considered as a Layer of Protection as defined in Functional Safety Standards.

Reference: ISA-TR-84.00.05-2009

NFPA 85

The scope of NFPA 85 extends beyond the control unit (Logic Solver) and covers application, installation, performance, inspection, testing and maintenance of the systems.

Typically compliance to NFPA 85 is enforced by an “Authority Having Jurisdiction” (AHJ) which will typically require a product to be listed or previously evaluated or tested by a National Recognized Testing Laboratory (NRTL).

Reference: NFPA 85-2011

Certification to NFPA 85 and FM7605

Since the scope of NFPA 85 extends beyond the control unit; the control unit, in this case AC800M High Integrity, is tested and certified to those sections of the standards applicable to the product.

The system is tested and certified to comply with the requirements defined in NFPA 85. Additional details can be found in Appendix A.

Reference: NFPA 85-2011

Product Requirements associated with Burner Management System applications

NFPA 85 requirements related to the logic system are included in Attachment A

Reference: NFPA 85-2011, section 4.11

TÜV Certification to NFPA 85 and FM7605

ABB choose TÜV SUD as the independent third party assessor to demonstrate compliance to multiple Functional Safety Standards and Application specific standards. TÜV SUD is an accredited safety assessor with years of demonstrated experience in Functional Safety and a National Recognized Testing Laboratory (NRTL) in the US. TÜV Certification and associated report (Doc No. Z10-08-10-29902-005) confirm compliance to NFPA 85 and FM7605 among other standards.

All configuration guidelines to apply the system are documented in the ABB 800xA High Integrity Safety AC800M Safety Manual (Doc No. 3BNP004865-510).

Reference: System 800xA Safety AC 800M High Integrity Safety Manual Doc No. 3BNP004865-510

ABB Experience

ABB have over a 300 AC800M High Integrity installations worldwide performing as a Burner Management System.

Conclusion

A Burner Management System can be considered a Safety Instrumented System and its design and implementation should follow NFPA guidelines and requirements and consider ANSI/ISA-84.00.01-2004 standard.

The use of a SIL capable and certified controller can provide performance improvements and cost savings during the implementation over the use of general purpose controllers.

AC800M High Integrity is a SIL capable and certified controller that satisfies the requirements of NFPA 85 and IEC 61508 ANSI/ISA-84.00.01-2004/61511 Functional Safety Standards as indicated in the TÜV certificate.

Although TÜV is a National Recognized Testing Lab, AC800M High Integrity is not yet “listed” by an "Authority Having Jurisdiction" (AHJ) in the US.

Appendix A

The logic system is tested and certified to comply with the requirements of NFPA 85 as indicated on the following table. There might be other elements in the NFPA 85 code that the system complies to based on Application Design.

Section No.	Description
3.3.26*	**Burner Management System.** 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.
4.11*	**Burner Management System Logic.**
4.11.1*	As a minimum, the requirements of 4.11.2 through4.11.10 shall be included in the design to ensure that a logic system for burner management meets the intent of those requirements.
4.11.2	The logic system for burner management shall be designed specifically so that a single failure in that system does not prevent an appropriate shutdown.
4.11.3	The burner management system interlock and alarm functions shall be initiated by one or more of the following: (1) One or more switches or transmitters that are dedicated to the burner management system (2) One or both signals from two transmitters exceeding a preset value (3) The median signal from three transmitters exceeding a preset value
4.11.3.1	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.
4.11.3.2	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 tags.
4.11.4*	Alarms shall be generated to indicate equipment malfunction, hazardous conditions, and misoperation.
4.11.5	The burner management system designer shall evaluate the failure modes of components, and as a minimum the following failures shall be evaluated and addressed: (1) Interruptions, excursions, dips, recoveries, transients, and partial losses of power (2) Memory corruption and losses (3) Information transfer corruption and losses (4) Inputs and outputs (fail-on, fail-off)

	(5) Signals that are unreadable or not being read (6) Failure to address errors (7) Processor faults (8) Relay coil failure (9) Relay contact failure (fail-on, fail-off) (10) Timer failure
4.11.6*	The design of the logic system for burner management shall include and accommodate the following requirements: (1) Diagnostics shall be included in the design to monitor processor logic function. (2) Logic system failure shall not preclude proper operator intervention. (3) Logic shall be protected from unauthorized changes. (4) Logic shall not be changed while the associated equipment is in operation. (5) System response time (through-put) shall be short to prevent negative effects on the application. (6) Protection from the effects of noise shall prevent false operation. (7) No single component failure within the logic system shall prevent a mandatory master fuel trip. (8) The operator shall be provided with a dedicated manual switch(es) that shall actuate the master fuel trip relay independently and directly. (9) At least one manual switch referenced in 4.11.6(8) shall be identified and located remotely where it can be reached in case of emergency. (10)*The logic system shall be monitored for failure. (11) Failure of the logic system shall require a fuel trip for all equipment supervised by the failed logic system. (12) Logic shall be maintained either in nonvolatile storage or in other memory that retains information on the loss of system power.
4.11.7*	**Requirement for Independence.**
4.11.7.1	Except as noted in 4.11.8.2, the burner management system shall be provided with independent logic, independent logic solving hardware, independent input/output systems, and independent power supplies and shall be a device functionally and physically separate from other logic systems.
4.11.7.2	For single burner boilers, the boiler control system 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 (2) If the combined boiler control and burner management system is specifically listed or labeled for the application
4.11.7.3	The burner management safety functions shall include but shall not be limited to purge interlocks and timing, mandatory safety shutdowns, trial timing for ignition, and

	flame monitoring.
4.11.7.4	The logic system shall be limited to one boiler or HRSG.
4.11.7.5	The same hardware type used for burner management systems shall be permitted to be used for other logic systems.
4.11.7.6	Network communications between the burner management system and other systems shall be permitted. The network communicating with other systems shall not be the same network that the burner management system uses to communicate with its input/output hardware.
4.11.7.7*	Signals and the manually operated devices specified in 4.11.6(8) that initiate mandatory master fuel trips shall be hardwired.
4.11.8	**Momentary Closing of Fuel Valves**
4.11.8.1	Logic sequences or devices intended to cause a safety shutdown, once initiated, shall cause a burner or master fuel trip, as applicable, and shall require operator action prior to resuming operation of the affected burner(s).
4.11.8.2	No logic sequence or device shall be permitted that allows momentary closing and subsequent inadvertent reopening of the main or ignition fuel valves.
4.11.9	**Circuit Devices.** No momentary contact or automatic resetting device, control, or switch that can cause chattering or cycling of the safety shutoff valves shall be installed in the wiring between the load side (terminal) of the primary or programming control and the main or ignition fuel valves.
4.11.10	**Documentation.** Documentation shall be provided to the owner and the operator indicating that all safety devices and logic meet the requirements of the application.

References

Document No.	Title
ISA-TR84.00.05-2009	Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)
NFPA 85-2011	Boiler and Combustion Systems Hazards Code
Z10-08-10-29902-005	TÜV Certification and Report
3BNP004865-510	System 800xA Safety AC 800M High Integrity Safety Manual