White Paper

Project:

Integrated Safety for a Single BMS

Evaluation Based on Siemens Simatic PCS7 System

Version 1, Revision 2, August 4, 2016

Jim Jenkins, William Goble

Management Summary

Any industry that has a requirement for a heated medium, whether it is used for process, utilities or emissions, utilizes equipment that has combustion controls and combustion safequards.

There has been an evolution in these controls from a traditional control that separates the DCS from either a relay-based system, PLC or Safety PLC for combustion safeguarding, to combined control for systems with less complexity as in a single burner BMS.

Functional safety standards like IEC 61511 do permit combined control and combustion safeguarding in one system. Other standards like the 2015 edition of NFPA 85 now explicitly allow combining combustion control and combustion safety in the same logic solver for certain applications. However several design issues must be considered and properly addressed in order to maintain or improve safety performance.

A properly designed combination combustion control and combustion safeguarding system can enhance the Safety Lifecycle by reducing engineering, operations and maintenance errors and improve combustion safety.

Table of Contents

1 Simple Rules

There are a number of simple rules suggested for use in safety instrumented system (SIS) design. These simple rules were created for less experienced persons to avoid detailed analysis so that design work does not require much SIS engineering expertise. One of these rules is that no common equipment should be used for control of a process variable and automatic safety protection of that process parameter. This rule was created because:

A. There are situations where the failure of control system causes a potential hazard. An SIS must provide protection against this hazard. However, if the piece of equipment that failed in the control system is also needed for protection in the SIS then protection is lost.

B. For those using LOPA analysis to establish the needed SIL level, protection credit is often given for alarm functions or shutdown functions implemented in the control system. LOPA credit requires separate equipment where failures do not disable independent layers of protection.

C. For programmable controllers, the management of change rules are often quite different for control and safety. Control functions are not as critical and many sites allow not only control parameter changes but control strategy changes without much formal administrative control and approval. Safety requires far more administrative control with justification and approval required before any changes are made. One easy way to help enforce this is to never have control and safety together within one programmable controller. Some in the safety community even have a rule that dictates different manufacturers and perhaps different technology be used so that entirely different configuration languages and procedures are additional means of enforcing the management of change procedures.

As described above, the simple rules have merit. And there are those in the safety community that insist these rules are part of the “ten commandments” of safety design which must never be violated under any circumstances.

2 Optimal Safety

However, there are situations when the design resulting from these simple rules is overly complex for a small application resulting in increased operational and maintenance work load as well as high cost. It is also recognized that different configuration languages and different maintenance procedures create confusion that gives rise to maintenance errors which can reduce safety. Given the importance of operations and maintenance on the lifecycle safety of an automation system (T1, T2), safety may be optimized by a simpler design that uses some common devices. And installed cost may be reduced significantly.

3 Single Burner BMS Systems

A boiler or furnace with a single burner has several control and safety functions. The two traditional systems involved are called the combustion control system and the combustion safety system. The safety system is commonly called a Burner Management System (BMS). The BMS has gone by a number of different names including Burner Safety System, Combustion Safeguards, Furnace Safeguard System, and many other variations.

3.1 Traditional Architecture

A traditional architecture for the burner system is shown in Figure 1.

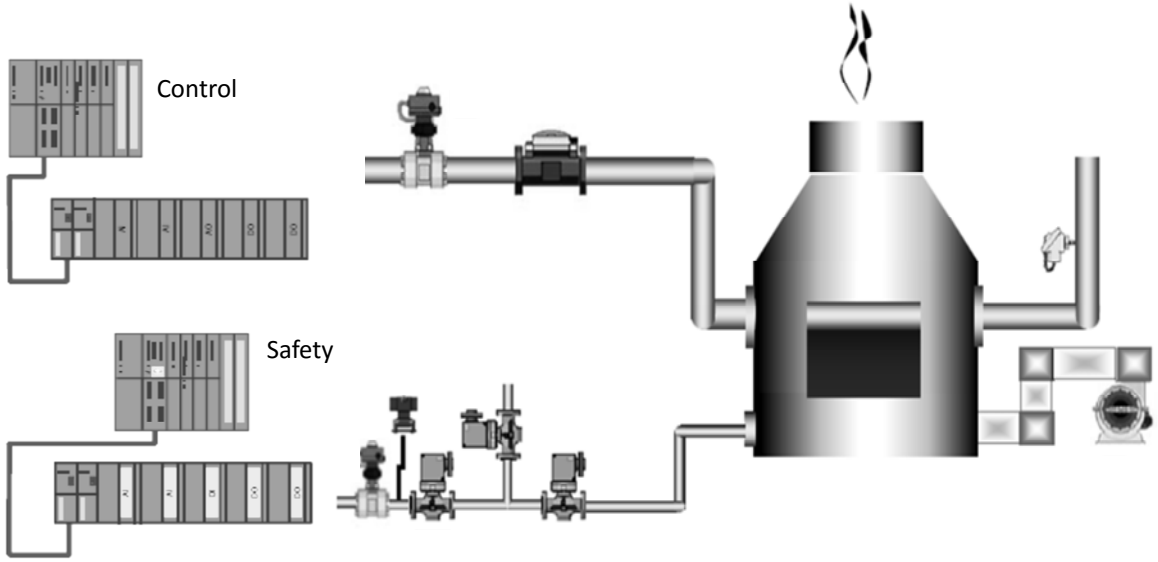

Figure 1: Traditional Architecture

Following the simple rule of using completely separate equipment for control and safety, the traditional architecture has two full sets of separate sensors, programmable controllers, and valves for each system. In such designs, controller capacity is often much greater than the needs of the process resulting in the obvious question – why do we need two controllers?

Another question often discussed is where to put each specific function – Does this function go into the control system or the safety system? Purge and sequencing functions have been put into the control system especially when the safety system has limited functionality and only accommodates typical trip functions. However, other designs put the purge and sequencing into the safety system as those functions are important to safety. Table 1 shows a list of typical control and safety functions for a burner.

Table 1: Burner Functions

Function Name	Function Type
Firing Rate	Control
Fuel/Air Flow	Control
Furnace Draft	Control
Drum Level	Control
Feed Water Control	Control
Master Fuel Trip	Safety
Pre-fire Interlocks	Safety
Burner Trips	Safety
Purge	Safety
Sequencing	Safety

There has also been an argument that separation of control and safety equipment improves cybersecurity by making it harder for a hacker to disable both control and safety. This may or may not be true depending on how vulnerable the controllers may be to cyber-attack. Two independent devices that are vulnerable to attack are not better than one device which has been certified to be cyber hardened per IEC 62443-4-1 (N4).

3.2 Combined Architecture

The recognition that optimal safety over the lifecycle of the system may be achieved with less complexity is expressed in the latest edition of NFPA 85:2015 (N1). This recent update to the standard has a number of changes including a reference to IEC 61508 SIL 3 certified PLCs and combined control and safety implementations. A combined architecture is shown in Figure 2.

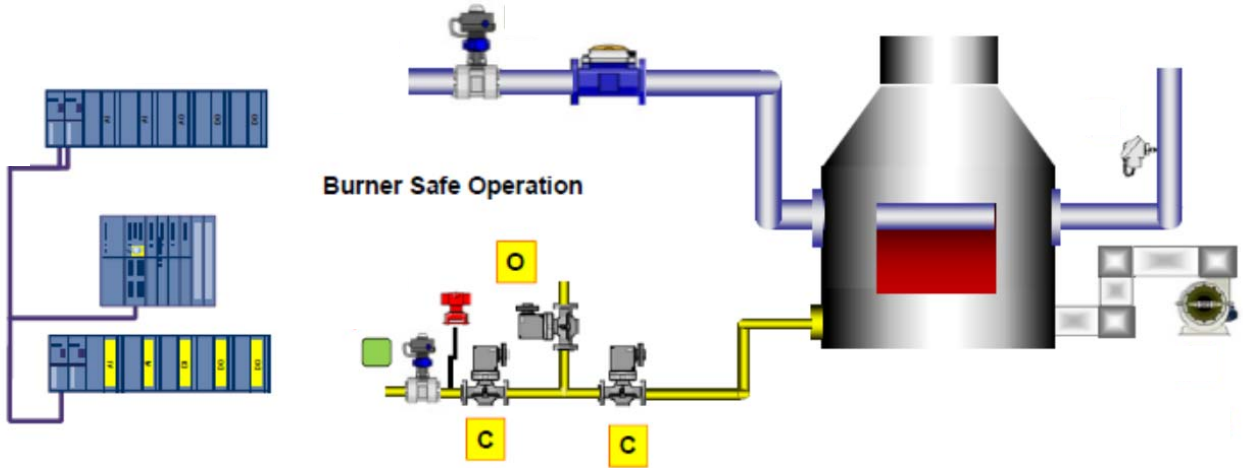

Figure 2: Combined Architecture

While a combined architecture system can provide optimal safety and cost, this design does require knowledgeable engineering and design verification. The verification effort must show that the requirements of NFPA 85 and IEC 61511 have been met.

4 Combined Architecture Verification

The combination of control and safety into one controller can be done but verifying that all design rules have been met is needed. There are specific rules expressed in NFPA 85:2015. Additional rules appear in IEC 61511:2003 (N2) as well. These rules must be met.

4.1 NFPA 85:2015 Verification

Clause 5.4.6 of NFPA85:2015 addresses the combined architecture with three alternative approaches, one of which must be met. Alternative Item 3 states “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 (an Accredited Certification 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 uses the term “notified body” although that term applies to electrical and flame safety not functional safety per IEC 61508.

4.2 IEC 61511 Verification

IEC 61511 requires that an analysis be done to show that no single failure of the common equipment can cause a process hazard and disable the safety function. This is normally done by documenting the safety functions and identifying possible failure modes in the common components and the mitigation provided in the design. Table 2 shows an example analysis.

Table 2: Safety Function Hazard Analysis Example

BMS Safety Functions		
Safety Function	**Initiating Event**	**Independence Issue**
Emergency Shutdown (Master Fuel Trip)		
Low Combustion Airflow	(1) FD Fan Failure (mechanical, electrical) (2) **Air Flow Control Failure (BPCS)**	Yes, may require one measurement for BPCS and a separate measurement for BMS And SIL 3 Safety PLC with interference-free control functionality
Loss of all ID fans	FD Fan Failure (mechanical, electrical)	
Loss of all FD fans	ID Fan Failure (mechanical, electrical)	
Loss of all flame	If there is no flame, initiate a Master Fuel Trip	
High Furnace Pressure	(**1)Furnace Draft Control (BPCS)** (2) Damper Failure (mechanical) (3) Plugging in the flue gas path (operational)	Yes, may require one measurement for BPCS and a separate measurement for BMS And SIL 3 Safety PLC with interference-free control functionality
All fuel inputs shut off	If all fuels are proven closed, initiate a Master Fuel Trip	
Low Instrument Air Press	(1) Compressor failure (mechanical, operational) (2) Valve closed in error (Operator error)	
Loss of Power	Loss of BMS power supply	
Furnace negative pressure	Excessive ID Fan capacity	
Low Fuel Pressure (may not be MFT)	(1) **Fuel Pressure Control Failure (BPCS**) (2) Regulator Failure (mechanical)	Yes, may require one measurement for BPCS and a separate measurement for BMS unless regulator is used (common practice)
High Fuel Gas Pressure (may not be MFT)	(1) **Fuel Pressure Control Failure (BPCS)** (2) Regulator Failure (mechanical)	Yes, may require one measurement for BPCS and a separate measurement for BMS unless regulator is used (common practice)
Drum Level	1) **Level Control Failure (BPCS)** (2) BFW Pump Failure (mechanical)	Yes, may require one measurement for BPCS and a separate measurement for

		BMS And SIL 3 Safety PLC with interference-free control functionality
High Steam Pressure	(1) **Steam Header Pressure Control Failure (BPCS)** (2) Mis-operation of the boiler (operational)	Yes, may require one measurement for BPCS and a separate measurement for BMS And SIL 3 Safety PLC with interference-free control functionality

It is clear that separate sensors should be used to greatly simplify analysis. This may imply that separate controller I/O modules are used. If the logic solver offers a combination of control and safety I/O there can be an advantage in using those. However most SIL 3 certified PLC systems have certified I/O modules and this will allow single cards (refer to the controller safety manual) to be used. The common controller must be a SIL 3 certified device. These products are assessed to make sure that all functionality is certified to meet IEC 61508 requirements or un-certified functions cannot interfere with the safety functionality.

There is also a requirement that programming and parameter changes in the common controller meet all management of change requirements for safety functions. In the advanced safety certified controllers this requirement is met by a number of alternative means with some controllers providing isolated and independent configuration platforms for control and safety.

The SIL selection process must also be checked to verify that no independent layer of protection credit was taken within the control system in which a BPCS failure is an initiating event for the hazard.

4.3 Cybersecurity Verification

The design of the architecture must consider cybersecurity risk and mitigation. This is often done with appropriate firewall devices and separation of various networks typically done per IEC 62443-2-4 (N5) if any network is used at all.

4.4 Verification Checklist

Requirement	Source	Result (Example)
processor and input/output (I/O) modules are approved or certified by (an Accredited Certification Body)* according to IEC 61508, Systematic Capability of SC3.	NFPA-85: 2015	SIL 3 Systematic Capability controller was used (T3).
burner management system logic is	NFPA-85: 2015	Controller has protection of

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."		safety memory and independent safety execution (T3).
no single failure of the common equipment can cause a process hazard and disable the safety function	IEC 61511	SIL 3 controller has redundant safety channels (Internal processing mechanisms equivalent to HFT=1).
no credit is taken for controller in LOPA	IEC 61511	No credit was taken for controller in the LOPA analysis.
programming and parameter changes in the common controller meet all management of change requirements for safety functions	IEC 61511	SIL 3 controller provides independent memory space with separate configuration passwords (T3).
architecture must consider cybersecurity risk and mitigation	IEC 62443-2-4, IEC 62443-4-1	SIL 3 controller has cybersecurity manual which details design and installation requirements. They were followed on the project (T3).

5 Process and Roles

5.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, cybersecurity and availability with over 400 man-years of cumulative experience in these fields. Founded by several of the world's top reliability and safety experts from assessment organizations, end-users, and manufacturers, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on field failure data of over 250 billion unit operating hours.

5.2 Reference documents

5.2.1 Industry Standards

Item	Identification	Description
N1	NFPA 85:2015	Boiler and Combustion Systems Hazards Code, National Fire Protection Association, Quincy, Massachusetts, 2015
N2	IEC 61511: ed2, 2016	Functional Safety: Safety Instrumented Systems for the process industry sector, International Electrotechnical Commission, Geneva, Switzerland
N3	IEC 61508: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, Geneva, Switzerland
N4	IEC 62443-4-1: CCDV, 2016	Industrial communication networks - Security for industrial and control systems - Part: 4-1: Product development requirements, International Electrotechnical Commission, Geneva, Switzerland
N5	IEC 62443-2-4: ed1, June 2015	Industrial communication networks - Security for industrial and control systems - Part: 2-4: Security program requirements for IACS service providers, International Electrotechnical Commission, Geneva, Switzerland

5.2.2 Technical References

Item	Identification	Description
T1	White Paper, April 11, 2016	Assessing Safety Culture via the Site Safety Index™, J.V. Bukowski, D. Chastain-Knight, 12th Global Congress on Process Safety, AIChE, GCPS 2016, http://www.exida.com/articles/assessing-safety-culture-via-the-site-safety-index.pdf
T2	White Paper, April 11, 2016	Quantifying the Impacts of Human Factors on Functional Safety, J.V. Bukowski, L. Stewart, 12th Global Congress on Process Safety, AIChE, GCPS 2016, http://www.exida.com/articles/quantifying-the-impacts-of-human-factors-on-functional-safety.pdf
T3	White Paper, June 2014	Three Steps in SIF Design Verification, exida, Sellersville, PA, USA, www.exida.com
T4	Certification Report, December 2015	Simatic S7 F/FH Safety Manual

6 Terms and Definitions

BMS	Burner Management System
BPCS	Basic Process Control System
DCS	Distributed Control System
FD	Forced Draft
HFT	Hardware Fault Tolerance
ID	Induced Draft
IEC	International Electrotechnical Commission
I/O	Input / Output
LOPA	Layer Of Protection Analysis
NFPA	National Fire Protection Association
PLC	Programmable Logic Controller
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System

7 Status of the document

7.1 Liability

exida provides services and analyses based on methods advocated in international and national standards. *exida* accepts no liability whatsoever for the correct and safe functioning of a plant or installation developed based on this analysis or for the correctness of the standards on which the general methods are based.

7.2 Releases

Version: 1
Revision: 2
Version History: V1, R2: Edits based on V1, R1 review, August 4, 2016
V1, R1: Released document, July 26, 2016
V0, R1: First Internal Draft, May 31, 2016
Author: Jim Jenkins, William Goble
Reviews: V0, R1: Jim Jenkins, Siemens
V1, R1: William Goble, Siemens
V1, R2: William Goble
Release Status: Released
Future Enhancements: At request of client