Burner Safety Systems: A Case Study
Bob Kotoski, Honeywell
David Farthing, Federal Services LLC, Member NFPA
Total Solution Offering

ONE SUPPLIER FOR BURNER MANAGEMENT SYSTEM SOLUTIONS

COMBUSTION AND BMS

RM7800

SMART TRANSMITTERS

C7061 FLAME SCANNER

MAXON SAFETY VALVES

GAS DETECTORS
HC900 PAC – Now TUV SIL2 Approved

HC900 is a Programmable Automation Controller (PAC)...

It can be used for a wide variety of applications ranging from Process PLCs to DCSs and safety applications.

...for Process AND Safety

Boilers, Furnaces, BMS, ESD, Spill Prevention, etc…
Presented by David Farthing, member NFPA

*Federal Services LLC, Oklahoma City, OK*

This presentation is not an official NFPA or Exida document and represents the presenters interpretation of the recommended practices outlined in the NFPA-87-2011 publication and Exida GAP assessment.

The NFPA Member logo is used with permission
Background

• West Texas Gas Processor operating in the Hemphill Shale required a new Burner Safety Management system for their Gas Regen Heater.

• Original Specification required API-556 with option for SIL-2 Capability.

• Alternate spec allowed NFPA-87 compliance.
  – WHATS THE DIFFERENCE?
General Comments

- Section 8 RP specifically applies to systems with 12.5 MM/Btu/Hr. input and greater.
  - Systems smaller than 12.5 MM/Btu/Hr. are still governed by ASME/CSD-1. (8.2.1 General)
  - Many producers and processors still follow the recommendations of NFPA for all of their ‘Inside the Fence’ applications for the protection of personnel and assets.
History of NFPA Burner Safety in Oil & Gas Applications

• “The need for NFPA to develop a document on O&G fluid heaters became apparent over a number of years as NFPA received requests for interpretation as to whether fluid heaters were covered by any existing NFPA codes or standards.” (Origin and Development of NFPA 87, page 87-1)

• Recognizing the unique hazards associated with O&G processing fired fluid heaters, in June 2010 NFPA published the first edition of NFPA-87 “Recommended Practices for Fluid Heaters”.
The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of NFPA Documents. Nor does NFPA list, certify, test, or inspect products, designs, or installations for compliance with their documents. Any certification or other statement of compliance with the requirements of a specific NFPA recommended practice shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement \(^{[n1]}\).
A SIL Certifier fills the gap left by NFPA for listing and certification of individual products and may provide reviews of the overall integrity of a compiled system for the intended functionality.

– ‘Products’ not ‘Systems’ are SIL Certified for the purpose.
– ‘Systems’ are SIL Capable of meeting the intent.

A SIL Certifier, like Exida and other listing organizations, has specific documentation requirements for the purpose of substantiating a product or total system’s safety functionality.
NFPA-87 Documentation

• A NFPA compliant system typically provides for
  – Electrical Schematic of the application
  – P&ID of the process identifying the SIF functions separately from the general process functions
  – Logic functionality documents
    • HC900 Self Documenting feature is a big help with this requirement
  – Sequence of Operations
  – List of spare instruments
  – Manufacturer’s O&M documents
  – Instrument Minimum Functionality with Listing Agency Certificate number
  – Loop drawings of each SIF
SIL-2 GAP

• Documentation
  – A SIL Capable system has fifty other document requirements that serve to quantify the systems capability to meet the intended purpose and the specified Safety Integrity Level.

• Review
  – A SIL Certifier will use this documentation to perform a static review of the ‘Total System’ capability to reach a specific SIL level based on the application.
The Safety Instrumented Functions of the Combustion Process

- Safety Controls - SIF
  - Should be Listed or Approved
  - Functionally Specific for the purpose
  - Should (not shall) be separate and independent devices listed for the intended purpose.
SIL-2 GAP

A SIL-2 SYSTEM ADDS A LAYER OF PROTECTION TO THE NFPA INTERLOCK SHUTDOWN CIRCUIT

• Safety Controls - SIF
  – “Shall be” Listed and SIL-2 Certified by a ‘Authorized SIL Authority’, (i.e. Exida or TUV)
  – Individual stand-alone device for each SIF
    • Required if Logic Solver is not SIL-2 Certified
    • May be required based on specific application
SIL-2 GAP

Minimum Safety Instrumented Functions

Safety Controls Latching Shutdown

• High Burner Fuel Pressure
  – Measured at the burner
• Low Fuel Gas Pressure
  – Measured at the Fuel Train entrance
• High Media Temperature
  – Redundancy of Temperature Element typically required
• High Stack Temperature
  – Redundancy of Temperature Element typically required
• Low Media Level or Flow (Process Dependent)
• Excess Media Flow (Process Dependent)
  – Redundancy of transmitters may be required
SIF - Hardwired Switches

- Power for the SIF circuit is provided through the E-Stop
- Devices are either “Listed” or “Approved” for the intended service
- Switches are wired in series and terminate at the Safety Interlock
  - i.e. Tr7 of a Honeywell RM7800 Safeguard Relay
Each switch is a stand-alone device monitoring a specific SIF

- Each SIF may be parallel wired to the Logic Controller for annunciation and alarming
SIF - Switches and Transmitters

• Combining Hardwired Switches and Transmitters in Logic Processors

• Hardwired switches are powered through the E-Stop and enter the Logic Processor at the COMMON terminal of the first Transmitter activated RELAY output

• Each additional SIF is series wired through consecutive relay outputs so that no single relay out can cause the system to fail in an unsafe condition
Hardwired Switches w/Transmitters - NFPA-87

T1 SIF-5  
T2 SIF-6  
T3 SIF-7

R1  
R2  
R3

LOGIC PROCESSOR

SIF-1  SIF-2  SIF-3  SIF-4

E-Stop

SAFETY INTERLOCK

Tr7
• Unless the Logic Processor is a SIL-2 Certified device then for the system to be SIL-2 Capable each of the Transmitted PV would require a SIL-2 Analog Safety Relay in series with the Safety Circuit
  • Redundancy of transmitters may be required
SIL-2 GAP

TO HC900 NON-SIL CERTIFIED LOGIC SOLVER

T1 SIF-5  T2 SIF-6  T3 SIF-7

SR1  SR2  SR3

TRANSMITTED FIELD LOGIC

E-Stop
SIF-1  SIF-2  SIF-3  SIF-4

SAFETY INTERLOCK

Tr7
Minimum Safety Instrumented Functions

- Safety Controls Integrity
  - All Safety Functional Instruments ‘shall’ as a minimum have the ability for...
  - Health Checking of the signal
  - Fail in a Safe Mode
  - Cause a Safety Shutdown on signal failure
  - Be SIL Certified for the intended purpose
Listed or Approved Device?

Safety devices should be...

• **Listed** device for service and environment.
  – Listed devices are those devices that have been tested and certified (listed) as safe for use in a specific application and/or environment by a Listing Agency.

• **Approved** device where listed devices are not available.
  – An approved device is a device that has been evaluated or reviewed by the owner or an outside authority and ‘approved for service’ in a specific application, but does not necessarily carry an approval ‘stamp’ or ‘listing’.
What’s a “LISTED” Device?

What’s an “APPROVED” Device?

APPROVED FOR SERVICE BY ASSET MANAGEMENT

Exida SIL-3 Capable
Section 8 - Combustion Safeguards

Best Practice would specify a Combustion Safeguard provide as a minimum:

- **Safe-Start Checks**
- Igniter Ignition period *(Timed)*
- Pilot Trial-for-Ignition period *(Timed)*
- Main Flame Trial-for-Ignition period *(Timed)*
- Flame Failure Response *(Timed)*
- Interlock circuitry for the fuel safety shutoff valve(s)
SIL-2 GAP - Combustion Safeguards

SIL-2 would ‘require’ a Combustion Safeguard provide as a minimum…

• Safe-Start Checks
• Igniter Ignition period (Timed)
• Pilot Trial-for-Ignition period (Timed)
• Main Flame Trial-for-Ignition period (Timed)
• Flame Failure Response (Timed)
• Interlock circuitry for the fuel safety shutoff valve(s)
• Carry a SIL Certificate for the purpose
• Be a separate ‘Stand-Alone’ device
Combustion Safeguards are **Listed** devices

- Listed as either a ‘Primary’ or a ‘Programming’ Burner Controller
- Primary Controllers provide the minimum functionality listed in the previous slide
- Programming Controllers add the following functionality…
  - Preignition circuitry
  - Fixed tamper-proof Purge Timer
  - Purge Proving circuitry
  - Low Fire Position Start circuitry
COMBUSTION SAFEGUARD
i.e. Burner Controller
Pre-Ignition Interlocks
Safe-Start Check
Purge Timing
Purge Proofing
Ignition Trials
Interlocks
Flame Management
Safety Shutdown

SEQUENCER
INDICATOR
LIGHTS

LOCAL INTERLOCK RESET BUTTON

RUN/TEST SWITCH
REMOTE INTERLOCK RESET CON.

FIXED PURGER TIMER

DISPLAY
Sequence and Diagnostics

FLAME AMPLIFIER
8.4 Programmable Logic Controller (Solver) Systems

- 8.4.1 PLC-based systems listed for combustion safety service.

- 8.4.1.1 PLC-based systems, except those listed for combustion safety service should be used in accordance with 8.4.2 – 8.4.4
What 8.4.2.5 means is that a robust PLC should be used. One with the following minimum features…

- 250,000 Hours MTBF
- Non-Volatile Memory
- Secured Software
- The ability to differentiate between a good input/output or a defective one
- Internal self-diagnostics for Health Checking of the processor, I/O cards, and logic execution
8.4.3.4 Output checking should be provided for PLC outputs controlling fuel safety shutoff valves

- Use of External Watchdog Valve Control Relays...
  - External Watchdogs are used to certify the sane execution of the PLC logic and in turn control the primary power source to the safety shutoff valve(s) via either a Valve Control Relay or a Master Control Relay.

- Power for the safety shutoff valve(s) should (shall) be supplied through a hardwired emergency stop that is fed from the Combustion Safeguard, 8.4.2.9
Heating System Safety Equipment and Application
- Hardwired Devices

8.4.2.8 External Hardwired Devices

- Manual Emergency Shutdown switch
- Combustion Safeguards
- Safe-Start Checks
  - Typically an integral part of the Combustion Safeguard
- Trial-for-Ignition periods
  - Always a part of a “Listed” Combustion Safeguard
- Ignition Transformers
- Excess Temperature Controllers
  - May be in the Logic Solver if the Logic Solver has this capability. Application and Customer specific.
- Valve-Proving Systems
Internal View of a Complete BSMS System

- **HC900 Burner Management PLC**
- **RM7800 Combustion Safeguards FM & SIL-3 Listed for service**
- **SIL-2 Safety Rated Master and Valve Control Relays with External Watchdog Relay**
- **Discrete & Analog Inputs Field Inputs with SIL-2 Transmitters**
- **Global ESD**
SIL-2 GAP

- HARDWARE MUST MEET IEC8501

- SOFTWARE MUST MEET IEC8504
  - Each SIL-2 Certified device in the system is required to meet the requirements of IEC 8501 to the hardware integrity and IEC 8504 to the software integrity.
• Questions?

• CONTACT INFORMATION
  – DAVID FARTHING
  – Federal Services LLC
  – David.Farthing@federalservicesllc.com
  – 800.289.3331 or 405.760.2831