# Application of Functional Safety to a Burner Management System – How to Avoid Common Pitfalls

Mike Scott, PE, CFSE, CEO / ISA S84 Co-Chair, aeShield, LLC, Anchorage, AK 99502

Abstract and Keywords

Burner Management System, BMS, Boilers, Burners, Safety Integrity Level, SIL, Safety Instrumented System, SIS, ANSI/ISA 84, TR84.00.05, IEC 61508, IEC 61511, Safety Lifecycle

In the process industry fired devices are one of the most common unit operations. Typical examples include boilers, fired heaters, reformers, claus units, vaporizers, calciners, furnaces, hot oil heaters, reboilers, glycol heater treaters, bath heaters, etc. and many more.

These unit operations have common hazards associated with potential uncontrolled combustion events (e.g., explosions) that have been well documented in industry. So much so that in many areas globally, prescriptive standards have been developed to improve the safety performance of these fired equipment unit operations.

However, in the author's experience often when one attempts to overlay performance-based IEC 61511 requirements on top of the existing local prescriptive regulatory requirements, things often go awry. These include:

- Excessively high Safety Integrity Level (SIL) targets that drive possible need for changing standard Burner Management System designs
- Excessively low SIL targets that potentially raise the question as to why we have Burner Management System at all
- Incorrect Safety Instrumented Function definitions that drive possible need for changing standard Burner Management System designs

This can be further complicated if the Burner Management System (BMS) is being procured as part of an OEM vendor package on a capital project. With vendor details arriving later in the project execution, these late changes to the OEM design can have significant budget / schedule impacts.

This presentation will outline a methodology to allow one to cost effectively and efficiently apply the performance-based concepts contained in IEC 61511 to a fired device in either a brownfield or greenfield application. This methodology will address:

- Standardization in Layer of Protection approaches to fired devices
- Standardization in Burner Management System IEC 61511 compliance requirements
- Transforming design emphasis from a document centric to a digital data centric approach
- Leveraging IEC 61511 performance-based requirements and availability of digital data to generate leading indicators on fired device safety performance

IEC 61511 if applied appropriately to a fired device, should result in increased awareness of potential hazards and direct meaningful insight into the safety performance of that unit operation of the life of its operation. It should not be causing one to completely re-design one of the most common unit operations in the process industries.

## Typical Risk Analysis Woes

In the process industry fired devices are one of the most common unit operations. With a large installation base, industry also has experience with a large number of uncontrolled combustion events associated with fired devices. As such various countries / industries have developed detailed prescriptive standards governing the BMS design and operation of fired devices.

However, when attempting to conduct a Process Hazards Analysis (PHA) and subsequent Layer of Protection Analysis (LOPA) on a BMS, resultant Safety Instrumented Function (SIF) definitions / targets are often incorrect resulting the perception that application of IEC 61511 to fired devices is costly. The author counters that IEC 61511 can be efficiently applied to a BMS if the risk analysis is conducted effectively.

The BMS related PHA / LOPA becomes complicated due several primary issues:

- Fired equipment has various modes of operation namely – pre-firing, light off, normal operation and post purge. The PHA / LOPA facilitator is typically not a fired device expert and is solely reliant on the PHA / LOPA team to provide input on how to document hazards with regards to the various modes of operation. This results in very wide variances in PHA / LOPA content / scenarios if one compares different teams / facilitators for like pieces of fired equipment.

  Common example: Proof of Purge LOPA with local light off and potential for single fatality

**Figure 1 – Proof of Purge SIF with INCORRECT RRF Target**

| Consequence | TMEL | Initiating Event or Cause | Initiating Event Frequency | Conditional Modifiers | | BPCS | Operator Response to Alarms, etc. | Mitigated Event Frequency w/o SIF | Proof of Purge SIF Target RRF to meet TMEL |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Ignition Probability | Occupancy | | | | |
| Failure to purge firebox due insufficient air flow / volume turnover.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | 1.00E-04 | Combustion air fan failure | 0.1 | 1.0 | 1.0 | 1.0 | 1.0 | 1.00E-01 | 1000 |

The above incorrect risk analysis / LOPA results in very high and unrealistic RRF target of 1000 or SIL 3 for the proof of purge SIF with local light off. Industry prescriptive proof of purge requirements typically mandate instrumentation capable of meeting low SIL 1 performance. This risk analysis would have an end user spending capital to re-design the proof of purge SIF.

- One needs to understand combustion control strategies / burner design / BMS design to properly identify and document BMS related hazards. This level of expertise is often not present during the risk analysis and this will result in very wide variances in PHA / LOPA content / scenarios if one compares different teams / facilitators for like pieces of fired equipment. This can be further complicated if the Burner Management System is being procured as part of an OEM vendor package on a capital project. With vendor details arriving later in the project execution, these late changes to the OEM design can have significant budget / schedule impacts.

  Common example: Incorrect crediting of a Continuous Pilot indicated a SIF is not required.

**Figure 2 – INCORRECT Continuous Pilot IPL Credit**

| Consequence | TMEL | Initiating Event or Cause | Initiating Event Frequency | Conditional Modifiers | | Continuous Pilot | Operator Response to Alarms, etc. | Mitigated Event Frequency w/o SIF | Low Combustion Air Flow SIF Target RRF to meet TMEL |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Ignition Probability | Occupancy | | | | |
| Loss of main flame.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | 1.00E-04 | Combustion air fan failure | 0.1 | 1.0 | 0.1 | 0.01 | 1.0 | 1.00E-04 | 1 |

The above incorrect risk analysis / LOPA results in very low and unrealistic RRF target indicating a Low Combustion Air Flow SIF is not required. Combustion engineers associated with current in progress efforts to update API 556 3rd edition and ISO 5133 are attempting to correct the misapplication of continuous pilots in risk analysis / LOPA. Refer to ISA TR84.00.05 for additional guidance. It should be noted in order for a continuous pilot to be considered a valid IPL in LOPA it needs to be a separate fuel source from the main and capable of re-lighting the main burner under all firing conditions. Thus, if the main flame goes out at 100% firing rate, is the pilot capable of safely re-lighting the main burner? If this cannot be answered by the burner vendor, then combustion trials are required to prove this capability. The combustion engineers indicated in many instances an independent pilot is not in place and should not be used as an IPL.

- A BMS typically implements several or more SIFs to address unacceptable hazardous events associated with the fired equipment unit operation. Identification of an individual SIF within a BMS may seem simple, but many errors are common, such as:
  - Not including all process measurements that can detect the hazardous condition
  - Including actions that are not required to achieve or maintain a safe state
  - Including measurements that do not detect the hazardous condition

  Common example: SIFs are aligned with Cause & Effect interlocks instead of the actual hazard scenario. This typically applies to Low Gas Pressure, High Gas Pressure, Loss of Flame, and Low Combustion Air Flow SIFs.

| Consequence | TMEL | Initiating Event or Cause | Initiating Event Frequency | Conditional Modifiers | | BPCS | Operator Response to Alarms, etc. | Mitigated Event Frequency w/o SIF | Low Combustion Air Flow SIF Target RRF to meet TMEL |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Ignition Probability | Occupancy | | | | |
| Low combustion air flow causes unstable flame operation and loss of flame with subsequent introduction of unburned fuel gas.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | 1.00E-04 | Combustion air fan failure | 0.1 | 1.0 | 0.1 | 1.0 | 1.0 | 1.00E-02 | 100 |

**Figure 3 – Low Combustion Air Flow SIF with INCORRECT SIF Definition**

The above risk analysis / LOPA yields "typical" RRF targets, however the SIF definition must be specified correctly, or an end user might end up spending capital to re-design the low combustion flow SIF or testing way too frequently.

| | | | Description | Main Burner Block Valve | Main Burner Block Valve | Main Burner Vent Valve | Pilot Block Valve | Pilot Block Valve | Pilot Vent Valve | Igniter |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Action | Close | Close | Open | Close | Close | Open | Off |
| | | | Equip | UV-306 | UV-308 | UV-307 | UV-203 | UV-205 | UV-204 | BN-307 |
| Tag | Description | Voting | Num | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| PSLL-103 | Low low Combustion Air Flow | 1oo1 | 1 | X | X | X | X | X | X | X |
| BSLL-311 | Loss of Flame | 1oo1 | 2 | X | X | X | X | X | X | X |

**Figure 4 – Simplified BMS C&E Diagram**

If the SIF is defined as PSLL-103 voted 1oo1 de-energizes 7 outputs, one will find that meeting a target RRF of 100 is impossible. This SIF definition is incorrect. Correct SIF definition is imperative. Figure 5 shows some possible incorrect and correct SIF definitions for Low Low combustion Air Flow SIF. The correct SIF definition is based upon the following unit operation details:

- Pilot is only used to light main burner during a typical 10 to 15 second trial for ingition period. Once main burner is proven, pilot double block and bleed valves are de-energized. So one needs to determine if the pilot block valves need to be included in the SIF defintion. In this example the pilot block valves can be excluded. This is not always the case. It is an additional action in this example.
- Hazard is uncombusted fuel built up in the combustion chamber following a low low combustion air flow event that resulted in loss of flame. Prescriptive BMS designs typically mandate redundant and diverse sensors to detect this hazard. If a single sensor is inlcuded in the SIF definition, one will not meet RRF target of 100 and HFT requirements for SIL 2 and again be forced to re-design.
- Bleed valves do not prevent uncombusted material from entering the combustion chamber. For this reason, bleed valves are not included in the SIF definition. It's purpose is to prevent leaking block valves from voiding the purge by preventing uncombusted hydrocarbons leaking through the double block valves and into combustion chamber continuously while offline. It is an additional action.
- The ingiter is already off following completion of pilot trial for ignition and does not prevent the hazard of uncombusted fuel entering the combustion chamber. It is an additional action.

**Figure 5 – Low Low Combustion Air Flow SIF Definitions**

| Option | Sensor | Voting | Logic Solver | Final Element | Voting | Voting | Voting | SIF Definition Status |
|---|---|---|---|---|---|---|---|---|
| | | | | UV-306 | | | | |
| | | | | UV-308 | 1oo2 | | | |
| | | | | UV-307 | 1oo1 | 2oo2 | | |
| | | | | UV-203 | | | | |
| | | | | UV-205 | 1oo2 | | | |
| | | | | UV-204 | 1oo1 | 2oo2 | | |
| 1 | PSLL-103 | 1oo1 | BMS | BN-307 | 1oo1 | 1oo1 | 3oo3 | Incorrect |
| | PSLL-103 | | | UV-306 | | | | |
| 2 | BSLL-311 | 1oo2 | BMS | UV-308 | 1oo2 | -- | -- | **Correct** |

- The risk analysis is further complicated when multiple initiating causes can result in a hazardous event, but not all initiating causes are detected by the same process measurement. In this case, multiple SIF may be defined, each of which provide risk reduction against a set or subset of the initiating events that can cause the hazard. When selecting the risk reduction and the associated SIL for these SIF, the aggregation effect of the multiple SIFs protecting against the same hazardous event should be considered. In many cases, the lack of independence between the SIFs necessitates the consolidation of the functions as a single function with diverse process measurements.

  Common example: What causes result in low gas pressure / loss of flame and can only be detected by loss of flame?

**Figure 6 – Loss of Flame SIF due to Low Pressure**

| Consequence | TMEL | Initiating Event or Cause | Initiating Event Frequency | Conditional Modifiers | | Mechinical Stop | Operator Response to Alarms, etc. | Mitigated Event Frequency w/o SIF | Low Combusiton Air Flow SIF Target RRF to meet TMEL |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Ignition Probabiity | Occupany | | | | |
| Loss of main flame.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | 1.00E-04 | Fuel gas control valve failure | 0.1 | 1.0 | 0.1 | 0.1 | 1.0 | 1.00E-03 | 10 |

When conducting the risk analysis associated with low pressure or loss of flame events, one must carefully review the location of the low low gas pressure measurement. Often the low low gas pressure measurement is upstream of the fuel gas firing valve. Therefore, if the fuel gas firing valve fails towards its closed condition, the upstream low low pressure sensor cannot detect the resultant low low pressure at the burner. This initiating cause can only be detected by the flame scanner itself assuming adequately sighted. Also included in the above risk analysis is the presence of a mechanical stop on the fuel gas firing valve to prevent valve from traveling below low pressure burner limits. With this IPL included in the risk analysis / LOPA, an RRF target of 10 is mandated and existing prescriptive flame scanner designs are acceptable. If the risk analysis results in a very high flame scanner RRF target, which mandates additional scanners, one should question wither the risk analysis has been executed correctly before re-designing field devices.

## Examples of Fired Device Knowledge Requirements

To ensure consistent results from ones BMS related PHA / LOPA here is a list of some of the issues the team needs to be able to address:

1. Stable Burning Limits for the burner
2. Burner turndown
3. Hazards radius if an uncontrolled combustion event (e.g., weak deflagration) were to occur
4. Occupancy associated with the hazard radius
5. Tolerable Risk Criteria
6. Limitations on use of Continuous Pilot as IPL
7. Avoiding Cross Lighting of Burners
8. Combustion Control Strategy
9. Combustion Related Process Safety Time
10. Use of Low NOX burners
11. Fuel properties
12. Bogging
13. Etc.

ISA has produced a Technical Report TR84.00.05 - *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)* that provides details on the above items associated with fired device unit operation subtleties in hopes of increasing fired heater risk analysis knowledge and awareness. Readers are encouraged to review this reference if additional insight / knowledge on fired device hazards is desired.

## Method for Success

To prevent inconsistent risk analysis results associated with fired devices, the author recommends end users create internal guidance notes / templates on the fired device operations that are present in the organization. This guidance note would include guidance on consequence selection, determination of hazard radius, occupancy, ignition probability, cause consequence pairings and associated protection layers / SIF definitions, enabling conditions, etc.

Instead of facilitating a PHA / LOPA starting with a blank sheet and letting the team inconsistently dictate the outcome, the facilitator would instead leverage the information contained within the end user's guidance note to guide the team to a consistent risk analysis basis. Where the team wants to deviate from the corporate guidelines, this would be documented and agreed to by end user fired device expert(s) who are responsible for the guidance note. In this manner a user can:

- Ensure like fired equipment from different plant sites is risk ranked consistently
- Drive consistency in SIF definition from site to site for like fired equipment
- Eliminate potential unnecessary spend to modify BMS related SIFs to meet over inflated RRF targets
- Eliminate potential increased risk associated with missing SIFs or SIF RRF targets that are too low
- If any risk gaps are uncovered, end user can confidently make decisions on spend / gap closure knowing risk analysis has been approved by corporate SME and is consistent from site to site

If the associated IEC 61511 mandated deliverables are also documented in the guidance note / template further significant engineering savings and consistency in Safety Critical Equipment (SCE) / Mechanical Integrity requirements can be obtained. This would include:

- Instrumented SCE / Protection Layer List for the fired device
- SIL Verification Calculations
- SRS
- C&Es
- Proof Test Plans
- Mandates for fired device performance monitoring requirements:
    - SIF / IPL Demand tracking
    - SIF / IPL Bypass tracking
    - SIF / IPL proof testing completion / failure classification tracking
    - SIF / IPL Risk Gap Tracking
    - Fired device ESTOP actuation

Tracking fired heater LOPA and SIS design assumptions versus actual performance is the ultimate goal of IEC 61511 and leveraging templatization of SIS deliverables will enable an end user to achieve this benefit much faster and more efficiently. Instead of focusing on completion of compliance documentation (e.g., SIS notebooks), the end user can focus on digital transformation and the underlying data that governs fired device risk / safety performance. The above KPIs will become critical leading indicators that an ends user will use to proactively manage fired device risks.

Consistent proof test plans and failure classification guidance will enable an end user to more efficiently collect enterprise level failure rate data to support actual real-world prior use failure rate data calculations. If initial failure rate data assumptions were conservative, this exercise could result in end users being able to begin extending proof test intervals through engineering analysis of their real-world performance. Depending on the unit operation, this could yield significant financial benefits for an end user.

Refer to Figure 7, for a depiction of a simplistic Piping and Instrumentation Diagram for the Burner Management System to be evaluated. Note for simplicity purposes, not all Basic Process Control System (BPCS) instrumentation, manual valves, etc have been included. Also process unit operation related interlocks such as low low drum level for boilers or low low pass flow for fluid heaters have been excluded for simplicity. Table 1 and 2 provide some sample information one might include in a corporate fired device guidance note.

**Table 1 – Typical BMS Hazards and Associated Safety Instrumented Functions**

| SIF # | Hazard Description | Causes | Sensors | Final Elements | Additional Actions |
|---|---|---|---|---|---|
| SIF-001 | Low combustion air flow causes unstable flame operation and loss of flame with subsequent introduction of unburned fuel gas.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | • Combustion Air Fan failure<br>• Combustion air inlet screen plugging | PSLL-103 or BSLL-311 | Close UV-306 or UV-308 | • Open main vent valve (UV-307)<br>• Maintain combustion air flow at current firing rate flow rate<br>• Maintain pilot block valves (UV-203 and UV-205) closed<br>• Maintain pilot vent valve (UV-204) open<br>• Maintain igniter (BN-307) off |
| SIF-002 | High fuel gas pressure causes unstable flame operation and loss of flame with subsequent introduction of unburned fuel gas.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | • Fuel gas regulator (PCV-503) failure towards open position | PSHH-309 or BSLL-311 | Close UV-306 or UV-308 | • Open main vent valve (UV-307)<br>• Maintain combustion air flow at current firing rate flow rate<br>• Maintain pilot block valves (UV-203 and UV-205) closed<br>• Maintain pilot vent valve (UV-204) open<br>• Maintain igniter (BN-307) off |
| SIF-003 | Low fuel gas pressure causes unstable flame operation and loss of flame with subsequent introduction of unburned fuel gas.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of | • Loss of fuel gas supply<br>• Inadvertent closure / re-opening of manual valve<br>• Plugged strainer<br>• Fuel gas regulator (PCV-503) failure towards closed position | PSLL-305 or BSLL-311 | Close UV-306 or UV-308 | • Open main vent valve (UV-307)<br>• Maintain combustion air flow at current firing rate flow rate<br>• Maintain pilot block valves (UV-203 and UV-205) closed<br>• Maintain pilot vent valve (UV-204) open<br>• Maintain igniter (BN-307) off |

| SIF # | Hazard Description | Causes | Sensors | Final Elements | Additional Actions |
|---|---|---|---|---|---|
| | ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | | | | |
| SIF-004 | Failure to purge firebox due insufficient air flow / volume turnover.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | • Combustion air fan failure<br>• Combustion inlet screen blockage<br>• Combustion air damper not at purge position | PSLL-103 and ZSH-102 for purge duration | Prevent light off sequence from proceeding | |
| SIF-005 | Loss of main flame.<br><br>Combustibles in the firing chamber may result in development of a flammable or explosive mixture, which may then be exposed to a source of ignition, causing undesired combustion, and potentially an explosion (deflagration), which may result in mechanical damage to the boiler and may also result in personnel impacts to persons near the equipment. | • Plugged burner nozzle<br>• Fuel gas contamination with non-flammable material (e.g., Nitrogen left in piping system from hot work) results in unstable mixture that cannot support combustion<br>• Improper fuel / air ratio<br>• Fuel gas control valve failure<br>• Inadvertent closure / re-opening of burner isolation valve at burner | BSLL-311 | Close UV-306 or UV-308 | • Open main vent valve (UV-307)<br>• Maintain combustion air flow at current firing rate flow rate<br>• Maintain pilot block valves (UV-203 and UV-205) closed<br>• Maintain pilot vent valve (UV-204) open<br>• Maintain igniter (BN-307) off |

As can be seen by Table 1, the prescriptive standards have mandated the use of redundant and diverse of sensors for most SIFs, as well as, redundancy in final control elements.

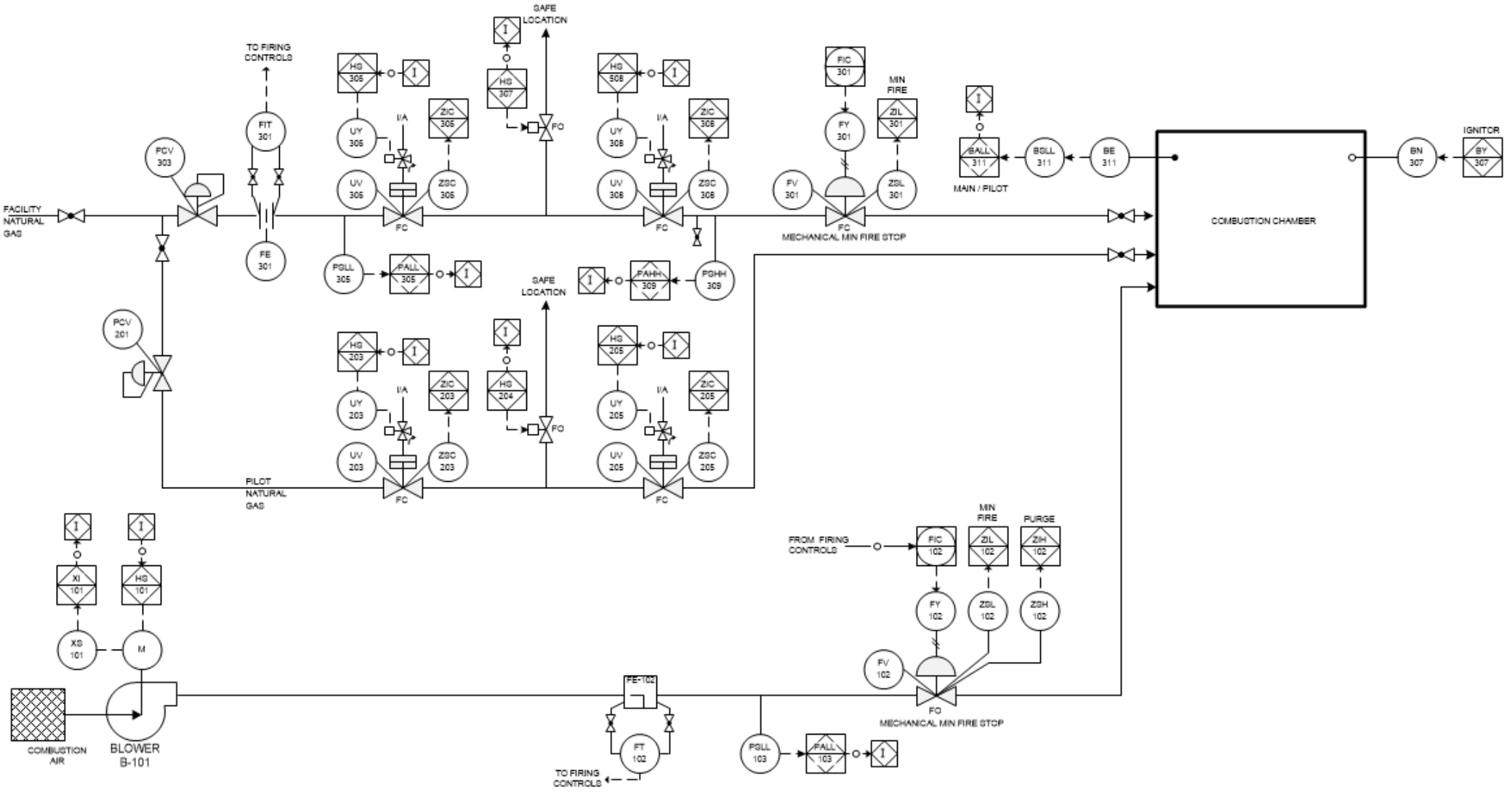
**Table 2 – Typical BMS Safety Integrity Level Calculations**

| SIF # | SIF Description | Target SIL PFDavg – Note 1 | Test Interval | SIL Arch Constraints | Achieved SIL – Note 1 |
|---|---|---|---|---|---|
| SIF-001 | Low low combustion air flow or loss of flame isolates main burner fuel gas to combustion chamber. | 2 | 12 Months | 2 | 2 |
| SIF-002 | High high fuel gas pressure or loss of flame isolates main burner fuel gas to combustion chamber. | 2 | 12 Months | 2 | 2 |
| SIF-003 | Low low fuel gas pressure or loss of flame isolates main burner fuel gas to combustion chamber. | 2 | 12 Months | 2 | 2 |
| SIF-004 | Confirm combustion damper is at purge position and combustion air discharge pressure is above required minimum pressure for entire purge timer duration. If either condition is not met inhibit subsequent start-up steps. | 1 | 12 Months | 1 | 1 |
| SIF-005 | Loss of flame isolates main burner fuel gas to combustion chamber. | 1 | 12 Months | 1 | 1 |

Note 1 - SIL targets are provided as examples only for possible comparison to end user risk analysis results. Actual SIL Targets are a function of an end users tolerable risk criteria, corporate procedures governing allowing LOPA credits, enabling conditions, frequency modifiers, etc. and whether or not the end user uses summing of causes within the LOPA. As each end user needs to establish SIL Targets in alignment with their corporate requirements.

Note 2 – Achieved SIL results are provided as examples only for possible comparison to end user SIL Verification calculations. SIL Verification calculations are a function of failure rate data, common cause, proof test coverage, mission time, field device type, etc. As each end user needs to establish achieved SIL results in alignment with their corporate requirements.

**Figure 7 – Typical BMS Gas Train**



## Conclusion

In the process industry for unit operations with known and well documented hazards like fired devices, the traditional blank sheet approach towards PHA / LOPA yields wide and varying results in consequence selection, protection layers applicability, protection layer definitions and SIL targets. This approach could result in increased risk and cost of ownership for end users when attempting to manage fired equipment based upon the PHA / LOPA results. A better approach the author contends is for an end user to develop a BMS Unit Operation PHA / LOPA guidance note / template for each major type of fired device in their organization (e.g., Boiler, Thermal Oxidizer, etc.). This document includes guidance on consequence selection, protection layers applicability, protection layer definitions, typical SIL targets, enabling conditions, frequency modifiers, etc. The Facilitator can continue to use a "blank sheet" approach in the study but now leading the team to document scenarios in line with the governing BMS guidance note / template. With this work process in place in theory all Fired Devices should be analysed in the PHA / LOPA in accordance with the unit operation specific guidance note / template The guidance note should include details on one should document deviations to the guidance note requirements and the appropriate means for getting this these deviations approved. If a similar guidance note / templatization approach is implemented with regards to Functional Safety deliverables – SIL Verification Calculations, SRS, C&Es, Test Plans, etc., BMS designs will be implemented and documented consistently across the organization. This will position end users for potentially significant cost savings on process safety / functional safety deliverables, as well as, ensuring the business is properly managing fired device risks which have been developed with a fired device SME and consistently rolled out to the organization.

Templatization will position end users to be able to leverage the true goal of IEC 61511, which is monitoring LOPA / SIS design assumptions and comparing them to actual performance. In this manner KPIs / leading indicators on overall corporation fired device performance can be monitored and allow the end user to consistently and proactively manage fired device risks throughout their business.

## 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


1. ANSI/ISA TR84.00.05, *Application of Safety Instrumented Systems for the Process Industries*, The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2009.
2. IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Safety-related Systems*, Part 1-7, Geneva: International Electrotechnical Commission, 2010.
3. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, Parts 1-3, Geneva: International Electrotechnical Commission, 2017.
4. NFPA 85, *Boiler and Combustion Systems Hazards Code*, Quincy, MA, National Fire Protection Association, 2019