Are Burner management systems and SIL Determination an explosive mixture?

Gaynor Woodford-Phillips & Stephen Beedle, Principal Safety Consultants, ABB Consulting, Daresbury & Billingham

This paper aims to provide a pragmatic method of SIL Determination for existing Burner Management Systems with reference to a case study.

Safety Integrity Level (SIL) determination of a Burner Management System (BMS) is usually complicated by the fact that there will be multiple trip initiators which tend to act on the same isolation valves. If Layer of Protection Analysis (LOPA) is used as the method of SIL Determination, then applying strict rules of independence between layers can mean that for multiple initiators only one independent layer of protection can be claimed. This can often drive the SIL determination in the direction of applying fault tree analysis which is time consuming, and thus costly.

By careful definition of the safety functions assessed by the LOPA it is possible to claim some independence between layers. There will always be an element of non-independence due to the BMS logic which safety functions are routed through. For the purposes of the LOPA the failure rate of a modern SIL-rated BMS PLC is considered to be small compared to the failure rate of sensors or valves, thus the contribution of this element of non-independence is considered to be insignificant in terms of the overall LOPA assessment.

EN 746:2010 “Industrial thermoprocessing equipment Part 2: Safety requirements for combustion and fuel handling systems” gives requirements for the protective functions to be included in a BMS and for their integrity. If type approved equipment is not used, EN 746-2 sets SIL requirements for the protective functions. From these descriptions target SILs can be set for all of the combustion related protective functions in a BMS. However in setting these targets, EN 746-2 is being conservative as it applies to a wide range of applications and so cannot take account of end user risk reduction considerations such as installation location and personnel exposure time.

It is reasonable to apply other more application specific techniques such as LOPA when setting SIL targets particularly for older bespoke equipment that was not originally designed to comply with EN 746-2. For new builds the use of application specific techniques is recognised in EN 50156:2015 “Electrical equipment for furnaces and ancillary equipment – Part 1: Requirements for application design and installation” and in ISO 13577:2014 “Industrial furnace and associated processing equipment – Safety –Part 4: Protective Systems”. Conversely, it is unreasonable to use application specific techniques such as LOPA to conclude that protective functions required by EN 746-2 do not require SIL targets.

Keywords: LOPA, BMS, EN-746

Introduction

Companies with existing fired equipment may find themselves facing difficult challenges if they attempt to carry-out any form of risk assessment of the fired equipment. Typically this becomes an issue when companies attempt to manage their fired equipment safety functions using functional safety management systems and applying the safety lifecycle.

Typically fired equipment is supplied as a package item and the burner management systems will be designed to one of many prescriptive codes e.g. EN 746 “Industrial thermoprocessing equipment”, NFPA 85 “Boiler & Combustion Systems”, API 556 “Instrumentation and Control Systems for Fired Heaters and Steam Generators”, whereas the Functional Safety Standards IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems” and IEC 61511 “Functional safety - Safety instrumented systems for the process industry sector” are performance based and require a risk assessment based approach.

Figure 1 Simple risk assessment approach

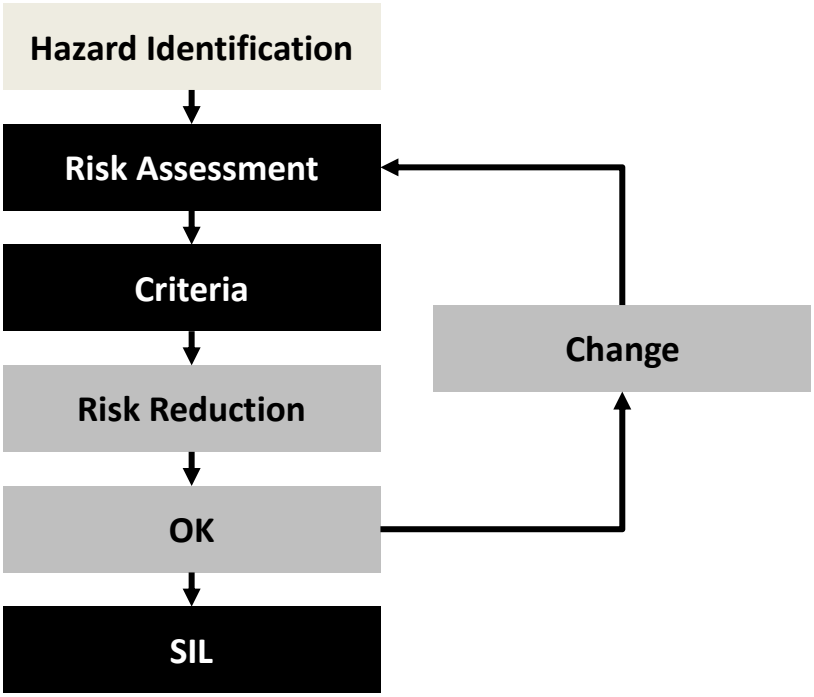


Figure 1 above shows a diagrammatic form of the steps required in a risk assessment that ultimately leads to specifying SIL requirements. The starting point is to understand the hazardous event, and the severity i.e. the number of potential injuries or fatalities. This then allows the output of the risk assessment to be compared with the relevant "tolerability" criteria, and depending on the criteria and the risk reduction provided by safety instrumented function(s) the Safety Integrity Level(s) (SIL) can be assigned for the safety function.

The prescriptive fired equipment codes typically describe the functional requirements of control and protective systems used for risk reduction, and include hazard identification and the preventative measures used to mitigate the hazard. However the prescriptive standards cannot consider the specifics of the location of the fired equipment and its proximity to vulnerable receptors. As a result they do not adequately address the risk assessment step because they cannot describe the ultimate hazardous event and do not compare the risk of the event with the operating company tolerable risk criteria. Hence there is an immediate mismatch between the prescriptive and performance based standards.

This paper describes some of the issues associated with hazard identification and subsequent risk assessment for the purposes of SIL determination for existing fired equipment and suggests a pragmatic approach to satisfy the functional safety standards without the need to resort to using fault tree analysis to define SIL requirements.

Hazard identification

The fired equipment under consideration may have been installed and operational for many years and finding any hazard identification documents generated during design is often a challenge, particularly for older sites. Fired equipment and certainly the burners and burner management systems are supplied as package items, sometimes "packages within packages" and therefore may have been supplied as a "black box".

Hazard Identification of "packages" at the design stage is often avoided. Although performing, for example a HAZOP (Hazard and Operability study)(IChemE 2000) is an excellent means of interrogating all aspects of the equipment design, any modifications requested in the study may invalidate the vendor warranty and will diminish the security bought from the knowledge that hundreds of identical units may be operating safely around the world. For a HAZOP of a vendor package to be effective it requires the attendance of a vendor representative and this could be a time consuming event, and if carried out retrospectively there may be little appetite by the vendor to be involved.

For these reasons in design a 'package boundary' is often drawn around the equipment and it is assumed the protective systems within the package provide an appropriate level of risk reduction, if supported by information from the equipment vendor such as:

- The fired unit design code
- Statement of codal compliance
- Burner Management System test report

- A list of protective systems
- Test method and test intervals for instrumented protective systems
- Documentation relating to relief streams
- Client list for the particular package

However this information may be difficult to obtain retrospectively if the vendor is no longer in business, or the equipment vintage means it was not designed to a recognised code or the code used is now superseded. It may be possible to use a fired equipment functional expert to conduct a gap analysis for the package versus the latest industry standards and codes. If significant gaps or concerns are identified then the 'package boundary' approach may not be appropriate, and expert advice is probably best sort on the suitability of the continued operation of the equipment and is beyond the scope of this paper. The 'package boundary' approach ideally needs to be combined with the application of a HAZOP of the interactions and process demands of the package with existing site services and facilities e.g. fuel, process streams, utilities.

Ultimately the output required from the Hazard Identification stage is a list of hazardous events associated with the fired equipment where claims are made for protective measures being provided by the burner management system, this can come from the codes or from another recognised hazard identification method. The hazardous events need to describe the consequences of the hazard specific to the location and operation of the fired equipment. The ideal output being a list of hazardous events, Safety instrumented functions, and any other safeguards, as shown in the example Table 1 below.

Table 1 Example output from hazard identification

Ref.	Hazardous event description	Safety instrumented functions	Other safeguards
a)	Low fuel gas pressure leads to flame failure allowing unburnt fuel and air to enter the hot combustion chamber leading to a significant explosion that could rupture parts of heater shell and/or damage pressure parts leading to a significant secondary fire. On-site fatality.	SIF01 Minimum fuel gas pressure (Main burners) SIF02 Minimum fuel gas pressure (Pilot burners) SIF11 Main burner flame detection SIF12 Pilot burner flame detection	Fuel gas low pressure alarm
b)	Main flame lift-off at high pressure allows unburnt fuel and air to enter the hot combustion chamber leading to significant explosion that could rupture parts of heater shell and damage pressure parts leading to a significant secondary fire. Sub-stoichiometric combustion allows unburnt or partially burnt fuel to enter the combustion chamber. If it encounters a secondary source of air – e.g. due to combustion chamber leaks and is still hot enough an explosion will occur. Such an explosion would less energetic than one caused by undetected flame failure but it could still break casings. On-site fatality.	SIF03 Maximum fuel gas pressure (Main burners) SIF04 Maximum fuel gas pressure (Pilot burners) SIF11 Main burner flame detection SIF12 Pilot burner flame detection	
c)	Reduced air:fuel ratio - Initially sub-stoichiometric combustion leading to increased CO generation. As the air flow falls further the main burner flames will be extinguished leading to an internal explosion. On-site fatality.	SIF05 Minimum air flow SIF11 Main burner flame detection	Low oxygen alarm
d)	High pressure in the combustion chamber. Burn injuries due to exposure of personnel in close proximity to viewing ports to hot flue gases or noxious exposure to asphyxiant-type gases. On-site injury	SIF07 High combustion chamber pressure	Low oxygen alarm
e)	Over-heating and damage to heater tubes causing a loss of process containment in all passes ultimately leading to process fires in the combustion chamber risking damage to additional passes, structural failure developing pool fire external to the heater. Onsite major injury.	SIF08 Heat Transfer fluid common return high temperature SIF06 Low process flow SIF09 High temperature on each of the passes SIF10 High temperature in convection section	Temperature control reduces firing
f)	Over-heating and damage to a single heater tube causing a loss of process containment ultimately leading to process fires in the combustion chamber risking damage to additional passes, structural failure developing pool fire external to the reboiler. Onsite major injury.	SIF08 Heat Transfer fluid common return high temperature SIF09 Heat Transfer fluid high temperature on each of the passes SIF10 high temperature in convection section	Temperature control reduces firing

Ref.	Hazardous event description	Safety instrumented functions	Other safeguards
g)	Single burner on-line: Flame loss from a single main burner admits unburnt fuel to the combustion chamber, subsequent delayed ignition causes a significant explosion that could rupture parts of heater shell and/or damage pressure parts leading to a significant secondary fire. Multiple burners on-line: Flame loss of a single burner is unlikely to result in accumulation of a significant flammable gas volume as immediate ignition from other burners would occur. The only exception relates to initiating causes where all on-line burners are extinguished at the same time, see hazardous event (a) and (b) above. Onsite fatality.	SIF11 Main burner flame detection SIF12 Pilot burner flame detection	Fuel flow rate limitation
h)	Accumulation of unburnt fuel in the combustion chamber leads to a significant explosion when the first pilot is lit that could rupture parts of heater shell and/or damage pressure parts leading to a significant secondary fire. Onsite fatality.	SIF13 System leak tightness check and/or valve proving system SIF14 Combustion chamber pre-purging	

As can be seen in Table 1 the ultimate consequences are described in terms of onsite fatality/major injury or injury, each of this consequences would be expected to have company specific tolerability criteria to allow comparison with the output of the risk assessment.

Risk Assessment

Use of LOPA

Often for speed and ease of use LOPA (Layer of Protection Analysis) is the preferred method of risk assessment used for the calculation of SIL (safety integrity level) requirements. The underlying principle with LOPA is that each layer or safeguard is independent from each other and the safety instrumented function being assessed (Figure 2).

Figure 2 Typical layers of protection in a LOPA which need to be independent

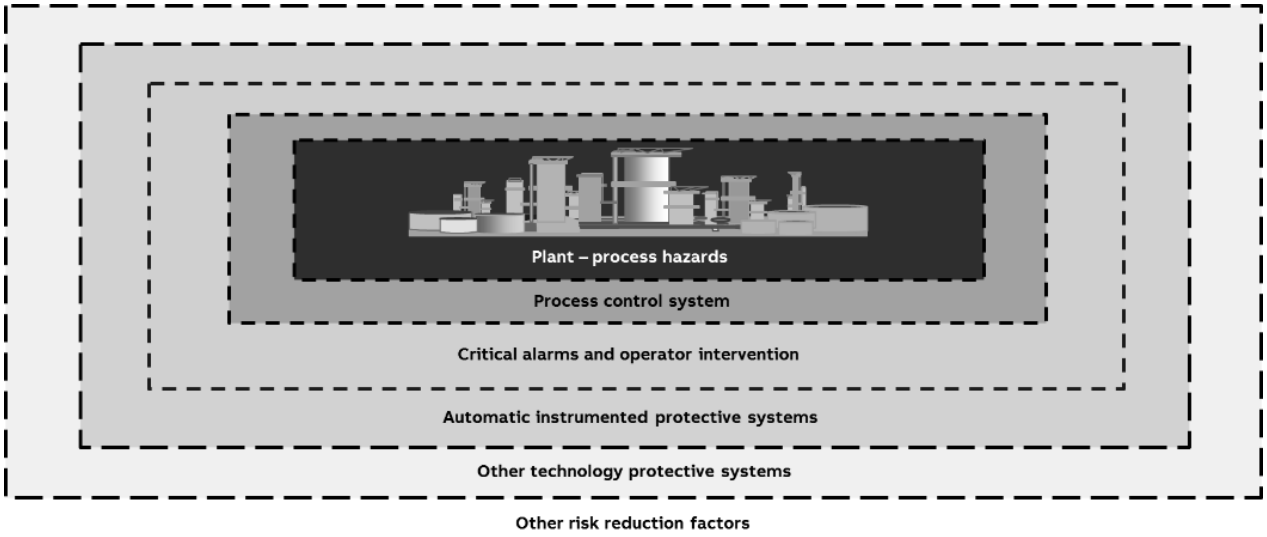
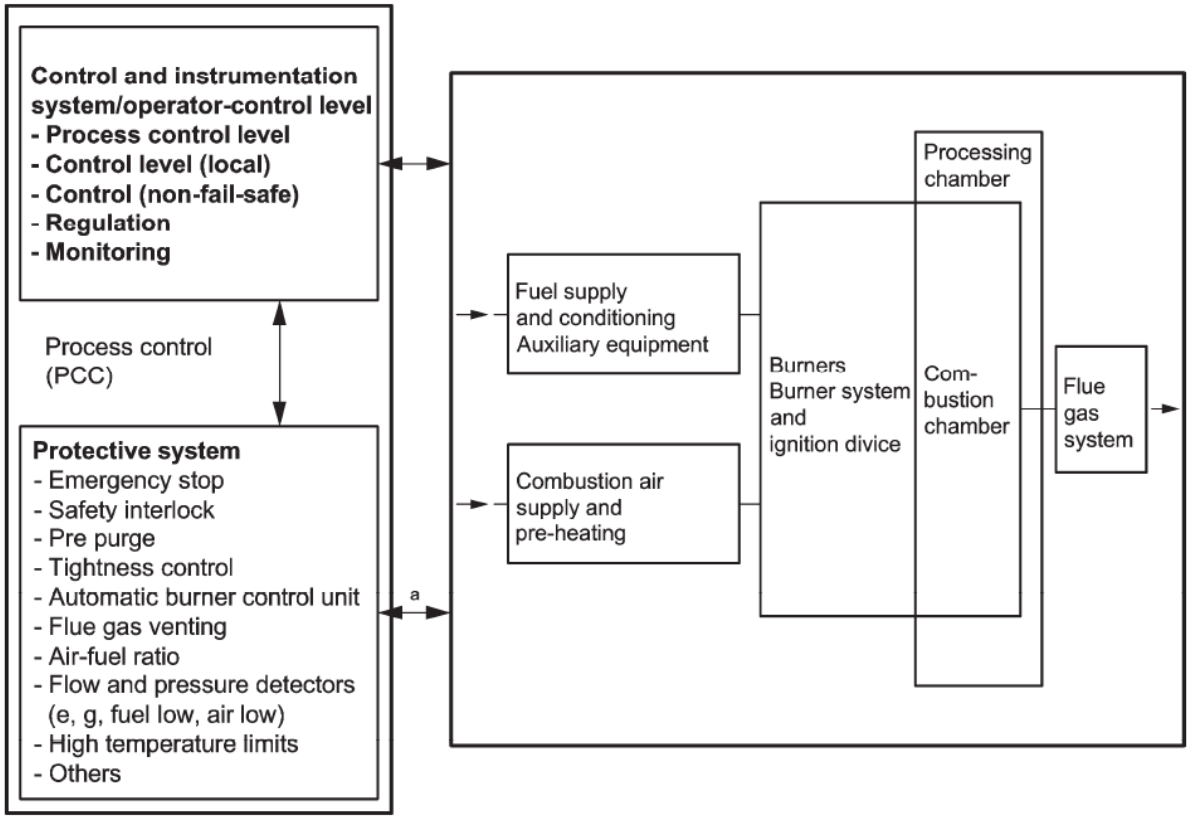


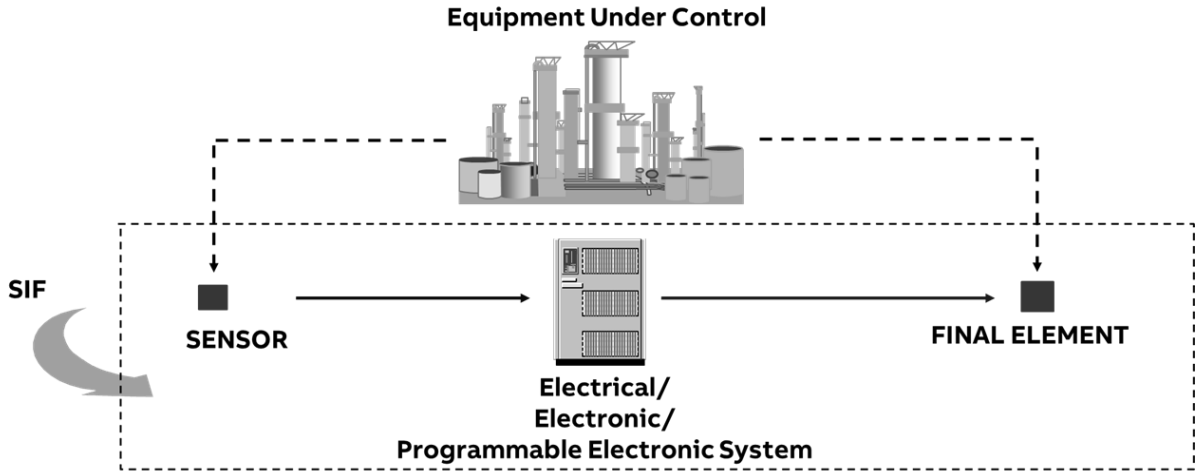
Figure 3 below is provided as an aid to understanding the relationship between the various elements of fired equipment control and protective system(s). By inspection of Figure 3 it can be seen that control and protection are provided by the same control system – the burner management system (BMS). It is also worth noting that for many of the consequences described in Table 1 above there are multiple safety instrumented functions protecting against the same hazard, which will be routed by the same BMS.

Figure 3 EN-746 Block diagram of control/protective measures and fired heater system



Safety instrumented functions are defined as from the sensor that detects the hazardous condition all the way through to the final element that acts to remove the hazard and including any logic or hardwiring (Figure 4).

Figure 4 Extent of Safety Instrumented Safety Function (SIF)



In general terms burner management systems have limited final elements on which they can act to remove the hazard i.e. isolation of the fuel supply. Therefore for each of the consequences described in Table 1, although apparently protected by multiple SIFs, it maybe that there is only one pair of fuel isolation valves to close.

This lack of independence between multiple SIFs and final elements and the common BMS, introduces a lack of independence which would usually mean that LOPA was rejected as a method of assessment. Modern burner management systems are designed to minimise random and systematic faults by including features such as self-checking and redundancy with the unit typically being placed in a safe state in the event of fault detection. Therefore the dangerous failure rates manufacturers' claim for modern SIL rated BMS PLCs is a very small in comparison with the failure rate of the sensors and valves the contribution of this element of non-independence is considered to be insignificant in terms of the overall LOPA assessment.

Independence of final elements

LOPA of BMS is complicated by the fact that multiple trip initiators tend to act on the same isolation valves. It is therefore important to define for each of the SIF initiators on the fired heater which final elements the initiators act on (see Table 2 below). In this example with 8 burners there are four possible combinations of final elements:

A. Closes 10 fuel safety shut-off valves. One in each of the 8 main burner systems and 2 on the common supply. Opens fuel header vent and locks out all main burners until fault reset.

B. Closes 10 fuel safety shut-off valves in pilot system. One in each of the 8 pilot burner systems and 2 on the common supply. And closes the same main burner system valves as A. Opens the fuel header vent (as A) and the pilot vent valve, and locks out the heater.

C. Closes the single main burner individual safety shut-off valve, single valve common with A and B. Locks out the main burner affected.

D. Closes the single pilot and main burner individual safety shut-off valves, single main burner common with A, B, C and single pilot burner valves common with B. Locks out the affected pilot and main burner.

Table 2 Example Table of BMS Safety Instrumented functions and final elements

SIF Ref.	SIF Description	Final elements
SIF01	Minimum fuel gas pressure (Main burners)	A
SIF02	Minimum fuel gas pressure (Pilot burners)	B
SIF03	Maximum fuel gas pressure (Main burners)	A
SIF04	Maximum fuel gas pressure (Pilot burners)	B
SIF05	Minimum air flow	B
SIF06	Low process flow	B
SIF07	High combustion chamber pressure	B
SIF08	Heat Transfer Fluid return high temperature	B
SIF09	Heat Transfer Fluid high temperature on each pass	A
SIF10	Convection section high temperature	B
SIF11	Main Burner flame failure	C
SIF12	Pilot burners flame failure	D
SIF13	Leak tightness check	B
SIF14	Combustion chamber pre-purging	B

Table 3 is used to illustrate the combinations of valves that operate where X is closed and O is open, and for final element combinations C and D, which are activated on flame failure, the valves operating for burner 1 are shown as way of illustration, the valves operating depend on the flame failure detection initiator which is one per main flame and one per pilot per burner, so could be 1 out of 1 up to 8 out of 8.

Table 3 Illustrative final elements valves (C and D are shown for burner 1 only, but could be up to 8 out of 8)

Burner (Main/Pilot)	Final element	Valve	A	B	C	D
M	Burner 1	XV01	X	X	X	X
M	Burner 2	XV02	X	X		
M	Burner 3	XV03	X	X		
M	Burner 4	XV04	X	X		
M	Burner 5	XV05	X	X		
M	Burner 6	XV06	X	X		
M	Burner 7	XV07	X	X		
M	Burner 8	XV08	X	X		
M	Common Header	XV20	X	X		
M	Common Header	XV21	X	X		
M	Common Header vent	XV22	O	O		
P	Burner 1	XV11		X		X
P	Burner 2	XV12		X		
P	Burner 3	XV13		X		
P	Burner 4	XV14		X		
P	Burner 5	XV15		X		
P	Burner 6	XV16		X		
P	Burner 7	XV17		X		
P	Burner 8	XV18		X		
P	Common Header	XV30		X		
P	Common Header	XV31		X		
P	Common Header vent	XV32		O		

From Table 2 and Table 3 it can be seen that 9 SIF initiators all act on the same final element valves "B". Applying the rules of independence strictly in a LOPA means that only one independent layer of protection can be claimed for 9 initiators because of the non-independence of the final elements. A further interesting comparison can be seen by combining the hazardous events and SIFs identified in Table 1 with the final elements in Table 2 into Table 4. This illustrates that again there is a lack of independence between the combinations of final elements.

Table 4 Hazardous events/SIFs and Final Element combinations

Ref.	Safety instrumented functions	Final elements
a)	SIF01 - Minimum fuel gas pressure (Main burners) SIF02 – Minimum fuel gas pressure (Pilot burners) SIF11 – Main burner flame detection SIF12 – Pilot burner flame detection	A B C D
b)	SIF03 - Maximum fuel gas pressure (Main burners) SIF04 - Maximum fuel gas pressure (Pilot burners) SIF11 – Main burner flame detection SIF12 – Pilot burner flame detection	A B C D
c)	SIF05 - Minimum air flow SIF11 – Main burner flame detection	B C
d)	SIF07 - High combustion chamber pressure	B
e)	SIF08 – Heat Transfer fluid common return high temperature SIF06 - Low process flow SIF09 - High temperature on each of the passes SIF10 - high temperature in convection section	B B A B
f)	SIF08 – Heat Transfer fluid common return high temperature SIF09 - Heat Transfer fluid high temperature on each of the passes SIF10 - high temperature in convection section	B A B
g)	SIF11 – Main burner flame detection SIF12 – Pilot burner flame detection	C D
h)	SIF13 - System leak tightness check SIF14 - Combustion chamber pre-purging	B B

Therefore a key feature of the BMS LOPA assessments is to identify 'independent layers' particularly in terms of the primary elements and the final elements, e.g. two layers of protection can be claimed if primary elements (such as minimum gas pressure and flame failure) closing different final elements. This means that some layers of protection have to be artificially split, for example for hazardous event (a) above:

- SIF01 Minimum fuel gas pressure closes XV20 and XV21 (1 out of 2) (main burner fuel supply common header)
- SIF11 Flame failure (e.g. burner 1) closes XV11 (1 out of 1)

Low fuel gas pressure also closes XV11 but this is not claimed as its SIF action, i.e. it is not claimed as a 1 out of 3. By this approach two independent layers can be claimed.

Example LOPA

The example LOPA below worksheet copied is intended to illustrate how the non- independence of layers has been accounted for:

Event Description	Unstable combustion causes pressure pulsation which is not a significant safety hazard. Ultimately low fuel gas pressure leads to flame failure allowing unburnt fuel and air to enter the hot combustion chamber leading to a significant explosion that could rupture parts of heater shell and/or damage pressure parts leading to a significant secondary fire. On-site fatality.
Event Type	Safety
Event Consequences	On-site fatality
Target Frequency Ft /yr	1.00E-05
Safety Function Loop Number	**SIF01 - Minimum fuel gas pressure (Main burners)**
Safety Function Trip Action	Closes all fuel safety shut-off valves in the main burner system XV20, XV21, XV01, X02, XV03, XV04, XV05, XV06, XV07, XV08) and opens vent (XV22). Locks out all main burners.
Achieved SIL comment	Primary element: 1oo1 Final element: 1oo2 Close XV20 (SIF action) Close XV21 (SIF action) The following are not claimed to be part of the SIF Close XV01, XV02, XV03, XV04, XV05, XV06, XV07, XV08 Open XV22

Initiating Causes			
Ref	**Description**	**Freq (/yr)**	**Justification**
A	Manual block valve closed in the fuel gas supply	0.01	Human error frequency for actions taken at least once per month ~0.1/year based on company guidance but there should be no routine requirement to adjust manual valves in the fuel gas system hence a lower frequency is applied. Hence an initiating cause frequency of 0.01/year is considered appropriate.
B	Fuel gas controller failure causing FV02 to close during normal multiple burner operation	0.1	BPCS instrument loop fail to danger
C	Plant upset causing a significant dip in fuel gas supply pressure during normal multiple burner operation.	0.025	Plant fuel gas supply (3.8 barg) and external (Grid) back-up supply (3.6 barg). Loss of plant fuel gas 1 per year and after several hours there would be a switchover to Grid gas. Operating experience is that there has been no co-incident failure of the Grid supply. No incidents in 40 years.
Independent Layers of Protection			
Ref	**Description**	**PFDavg**	**Justification**

1	Fuel gas low pressure alarm	1	No additional credit taken for operator response to alarms.
2	**SIF11** - Main burner flame detection (QI01\02\03\04\05\06\07\08). SIF action is Final element "C" to close a block valve to each burner. For example in the case of burner 1, detected by QI01: Close XV01.	0.05	Assume a SIL PFDavg for this function of 0.05 based on the LOPA for SIF11 and considers the worst case 8 burners would have to be isolated.
3	**SIF02** - Minimum fuel gas pressure pilot burners (PT11). SIF action is Final element "B".	1	SIF action is non-independent from other IPLs in terms of either primary element or final element.
4	**SIF12** - Pilot burner flame detection (QI11\12\13\14\15\16\17\18). SIF action on an 8 out of 8 is to isolate all main burner and pilot burner valves, therefore SIF action is Final Element "B"	1	SIF action is non-independent from other IPL in terms of either primary element or final element.
5	Pilot burner operational (thereby avoiding accumulation of flammable gas in the combustion chamber), requires only a single pilot to be operational.	0.03	The main burner and pilot burner are from a common gas supply but for causes B only the main burner is extinguished, thus the pilot would be operational and would immediately ignite gas from the main burner when fuel gas pressure returns to normal. However this would need failure of pilot flame detection. Apply a PFDavg of 0.03 equivalent to the expected reliability of the pilot flame failure SIF12 which for single pilot failure is Final element "D" and gives independence from the other IPLs if the closure of the pilot valve eg. XV11 is condered for burner 1. In this case the probability the pilot is operational is expected to be higher as there is no co-incident demand on this SIF.
6	Probability of delayed ignition.	0.5	When fuel gas is re-admitted to the combustion chamber (after the dip in fuel gas pressure) it may ignite immediately from hot surfaces including the burner tile thus preventing a build-up of flammable gas. Assume a minor risk reduction based on the burner design.
7	Probability person present and injured.	0.1	Normal plant occupancy 0.1 based on routine patrols.
8			

PFDavg Calculation

Initiating Cause	Frequency (/yr.)	Independent Layer of protection								Intermediate Event Frequency
		1	2	3	4	5	6	7	8	
A	0.01	1	0.05	1	1	1	0.5	0.1		0.000025
B	0.1	1	0.05	1	1	0.03	0.5	0.1		0.0000075
C	0.025	1	0.05	1	1	1	0.5	0.1		0.0000625
									Total Event Frequency, Fe /yr.	0.000095
									PFDavg for Safety Instrumented Function , Ft/Fe	1.05E-01
									Safety Integrity Level =	Unclassified

The LOPA analysis can be repeated across all the safety functions to determine a SIL requirement for each safety function in turn. This is summarised in Table 5.

Codal requirements

Fired equipment codes specify the hardware reliability requirements for safety functions using compliance with EN 746:2010 “Industrial thermoprocessing equipment Part 2: Safety requirements for combustion and fuel handling systems”. EN 746-2 gives requirements for the protective functions to be included in a BMS and for their integrity. If type approved equipment is not used, EN 746-2 sets SIL requirements for the protective functions. In paragraph 5.7.2 c), it requires that:

- Guarding functions (e.g. gas pressure, temperature) performed by components for which no relevant product standards are existing shall comply with at least SIL 2 / PLd.
- Functions which will lead to immediate hazard in case of failure (e.g. flame supervision, ratio control) performed by components for which no relevant product standards are existing shall comply with at least SIL3 / PLe.

From these descriptions target SILs can be set for all of the combustion related protective functions in a BMS. However in setting these targets, EN 746-2 is being conservative as it applies to a wide range of systems and so cannot take account of end user risk reduction considerations such as installation location and personnel exposure time. It is reasonable to apply other more application specific techniques such as LOPA when setting SIL targets particularly for older bespoke equipment that were not originally designed to comply with EN 746-2. For new builds the use of application specific techniques is recognised in EN 50156:2015 “Electrical equipment for furnaces and ancillary equipment – Part 1: Requirements for application design and installation” and in ISO 13577:2014 “Industrial furnace and associated processing equipment – Safety – Part 4: Protective

Systems". Conversely, it is unreasonable to use application specific techniques such as LOPA to conclude that protective functions required by EN 746-2 do not require SIL targets.

In this example the SIL targets determined by the LOPA study and derived from EN 746-2 have been compared to enable the targets to be set. The LOPA targets have been used where these are the lower value. However where the LOPA determined that no target is required but EN 746-2 requires the protective function, a target of SIL1 has been assigned so that it is documented and maintained as a SIF.

Table 5 Comparison of LOPA SIL with requirements of EN-746

SIF Ref.	SIF Description	Final elements	SIL from LOPA	SIL from EN-746-2	Target selection & basis
SIF01	Minimum fuel gas pressure (Main burners)	A	Un-classified	SIL2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF02	Minimum fuel gas pressure (Pilot burners)	B	None	SIL2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF03	Maximum fuel gas pressure (Main burners)	A	SIL1	SIL2	SIL 2 because over-firing has severe business consequences although the safety basis would be SIL1.
SIF04	Maximum fuel gas pressure (Pilot burners)	B	None	SIL2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF05	Minimum air flow	B	SIL1	SIL2	SIL 2 is common for minimum combustion air flow. SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF06	Low process flow	B	None	SIL2	SIL 2 because low process flow has severe business consequences although the safety basis would be SIL1.
SIF07	High combustion chamber pressure	B	None	SIL2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF08	Heat Transfer Fluid return high temperature	B	SIL1	SIL2	SIL 2 because high temperature could have severe business consequences although the safety basis would be SIL1.
SIF09	Heat Transfer Fluid high temperature on each pass	A	Un-classified	SIL2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF10	Convection section high temperature	B	None	SIl2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF11	Main Burner flame failure	C	SIL2	SIL3	LOPA is an assessment of the specific risk in this application.
SIF12	Pilot burners flame failure	D	SIL1	SIL3	LOPA is an assessment of the specific risk in this application.
SIF13	Leak tightness check	B	Un-classified	SIL2	SIL 1 so this EN 746-2 requirement is appropriately installed, tested and maintained
SIF14	Combustion chamber pre-purging	B	Un-classified	SIL2	SIL 2 is common for pre-purge but with a SIL 1 for SIF13, a SIL1 for this SIF overall gives an appropriate level of pre-ignition protection.

Conclusion

SIL determination for legacy burner management systems has many challenges, which start with the lack of adequate hazard identification. Applying layer of protection analysis requires careful consideration of the claims that can be made for independence between sensors and the final elements that activate, and therefore requires a careful statement of the claims that are made for the achieved SIL functionality. The underlying assumption is that given that modern SIL rated BMS PLCs have a very small failure rates in comparison with the failure rate of the sensors and valves, the contribution of this element of non-independence is considered to be insignificant in terms of the overall LOPA assessment, however this may not be true for vintage fired equipment.

Based on application specific hazard identification, as in the example used, the principal process safety hazards associated with the fired heater relate to an internal explosion due to the accumulation of a unburnt fuel in the combustion chamber that is then subject to delayed ignition. All Safety Instrumented Functions have been identified and subject to LOPA, and it can be seen that the most stringent safety target relates to the main burner flame failure detection SIF which is SIL2. The analysis has produced a conservative and pragmatic basis for using LOPA for SIL determination on BMS based safety functions, which allows for proof test periods to be defined on low demand systems. The required design and functionality of instrumented protection of fired equipment is defined explicitly in published codes, e.g. BS EN746-2 which defines relevant good practice, which means that the components installed in the design would need to be capable of meeting the code reliability requirements.

References

EN 746:2010 “Industrial thermoprocessing equipment Part 2: Safety requirements for combustion and fuel handling systems”

IChemE, 2000 “HAZOP Guide to Best Practice”

IEC61511 “Functional safety - Safety instrumented systems for the process industry sector”