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

Bio: Mike Scott

- B.S. Mechanical Engineering - University of Maryland
- Masters of Engineering - University of South Carolina
- Licensed Professional Engineer - AK, GA, SC, and IL
- Certified Functional Safety Expert (CFSE)
- IEC 61511 committee member
- ISA Fellow
  - Co-Chairman of ISA S84 committee on Electrical/Electronic/Programmable Electronic Systems (E/E/PES) for Use in Process Safety Applications
  - Co-Chairman ISA S84 BMS sub-committee member on Burner Management Systems
  - Past Chairman of the ISA S84 Working Group on Performance Based Fire & Gas Systems
- Granted 7-US Patents on Safety Lifecycle
- Embedded Process Safety / Functional Safety role for 18 sites

CEO
Cell +1 (907) 301-3111
mike.scott@aeshield.com

Problem Statement

- Burner Management Systems (BMS) are a very common unit operation in the Process Industry
- However, when LOPA is applied to a BMS it often results in:
  - Incorrect Safety Instrumented Function definition
  - Orders of magnitude differences in Safety Integrity Level (SIL) targets for like unit operations
- This results in:
  - Increased risk to end user
  - Increased cost of ownership to end user
  - Confusion to Operations and Maintenance on BMS Safety Critical Equipment

Common BMS Issues to Avoid

- Inconsistent consequence selection
- Incorrect SIF definitions
- Incorrect Cause / Consequence Pairings
- Too high of SIL targets – e.g., SIL 3
- High Demand Mode selection
- Instrumentation Furnished with Packaged Equipment
- BMS / BPCS combined in a single logic solver as part of an OEM burner upgrade

Goal: Avoid your name and the words *critical path* being used in the same sentence!

Fired Device Risk Analysis Goals

- Consistency in Risk Ranking like Fired Equipment across the organization
- 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 SIL 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

Develop Fired Device Guidance Notes

- Develop Guidance Notes on typical Fired Equipment in your organization
- Guidance Note to include:
  - Consequence Selection
  - Independent Protection Layer Guidance
  - Typical SIF definitions
  - Typical expected SIL targets
  - Typical SIS deliverables
  - Etc.

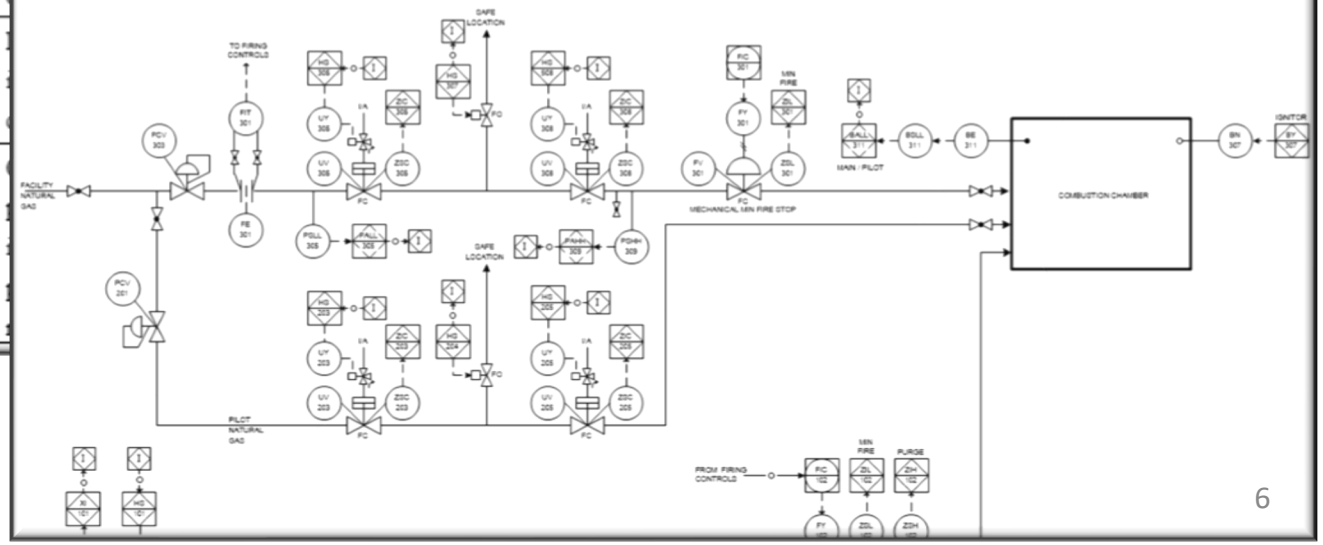
Table 1 – Typical BMS Hazards and Associated Safety Instrumented Functions

SIF #	Hazard Description	Causes	Sensors	Final Elements	Additional Actions
SIF-001	Low combustion air flow causes unstable flame operation and loss of flame	• Combustion Air Fan failure • Combustion air	PSLL-103 or BSLL-311	Close UV-306 or UV-308	• Open main vent valve (UV-307) • Maintain combustion air

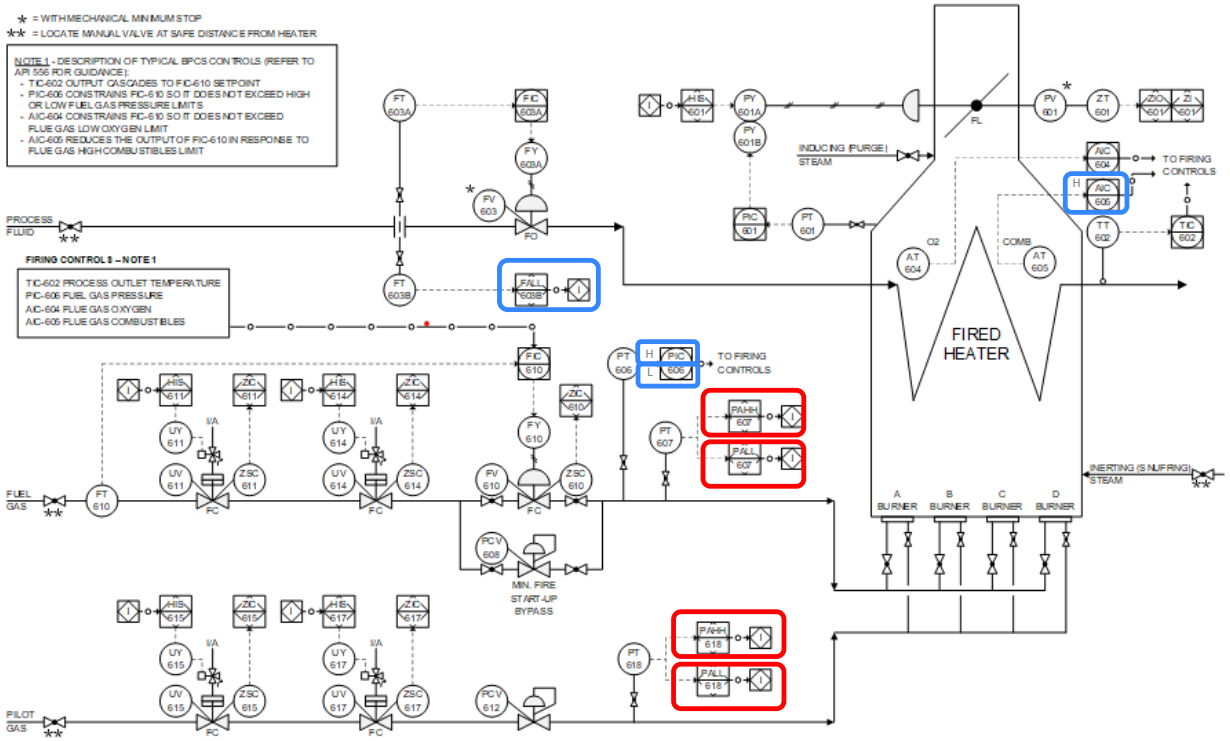
Table 2 – Typical BMS Safety Integrity Level Calculations

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	2	12 Months	2	2
SIF-002					
SIF-003					
SIF-004					

Figure 7 – Typical BMS Gas Train



Document Centric Approach Multi-Burner Heater

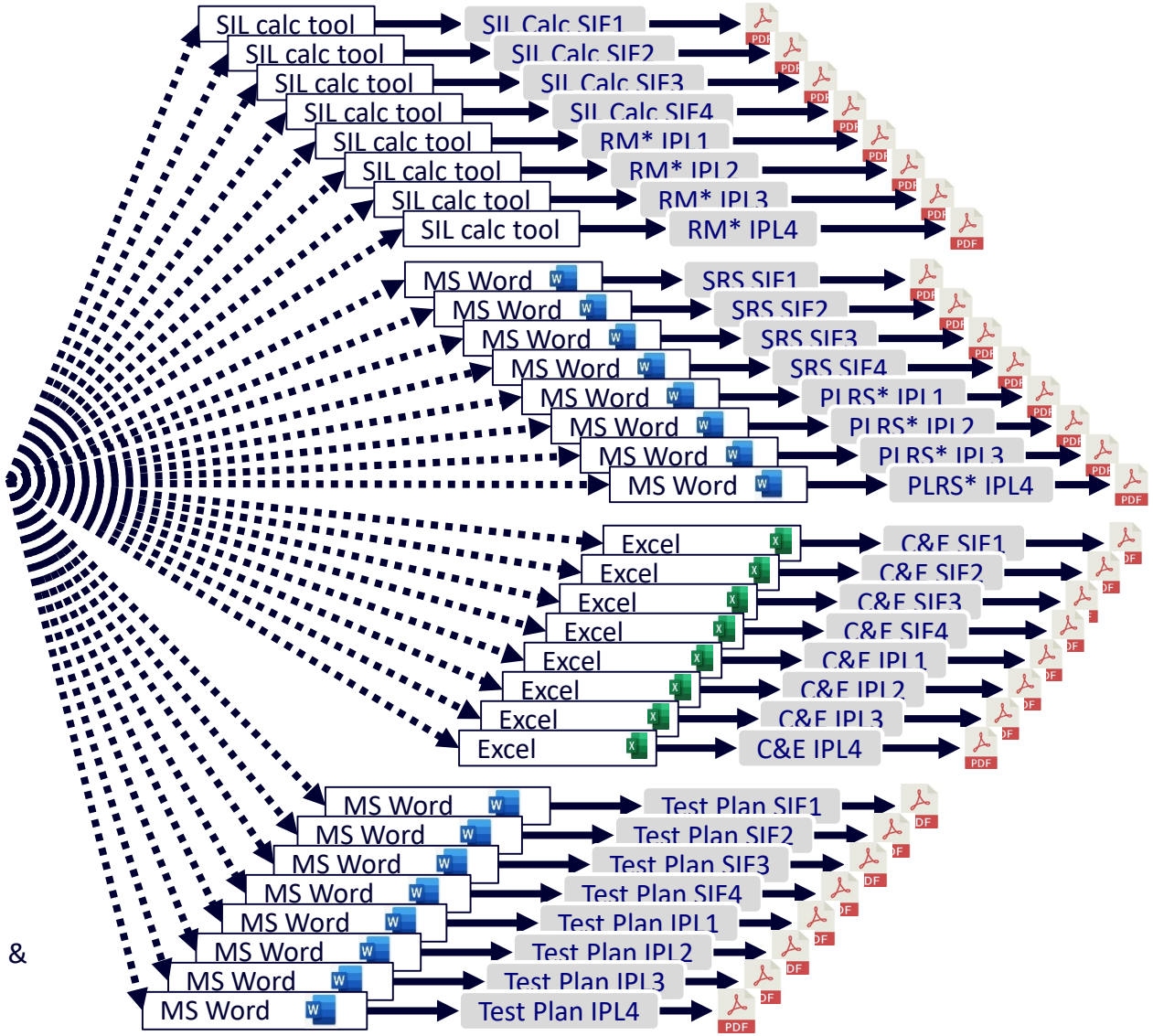


SIF

IPL

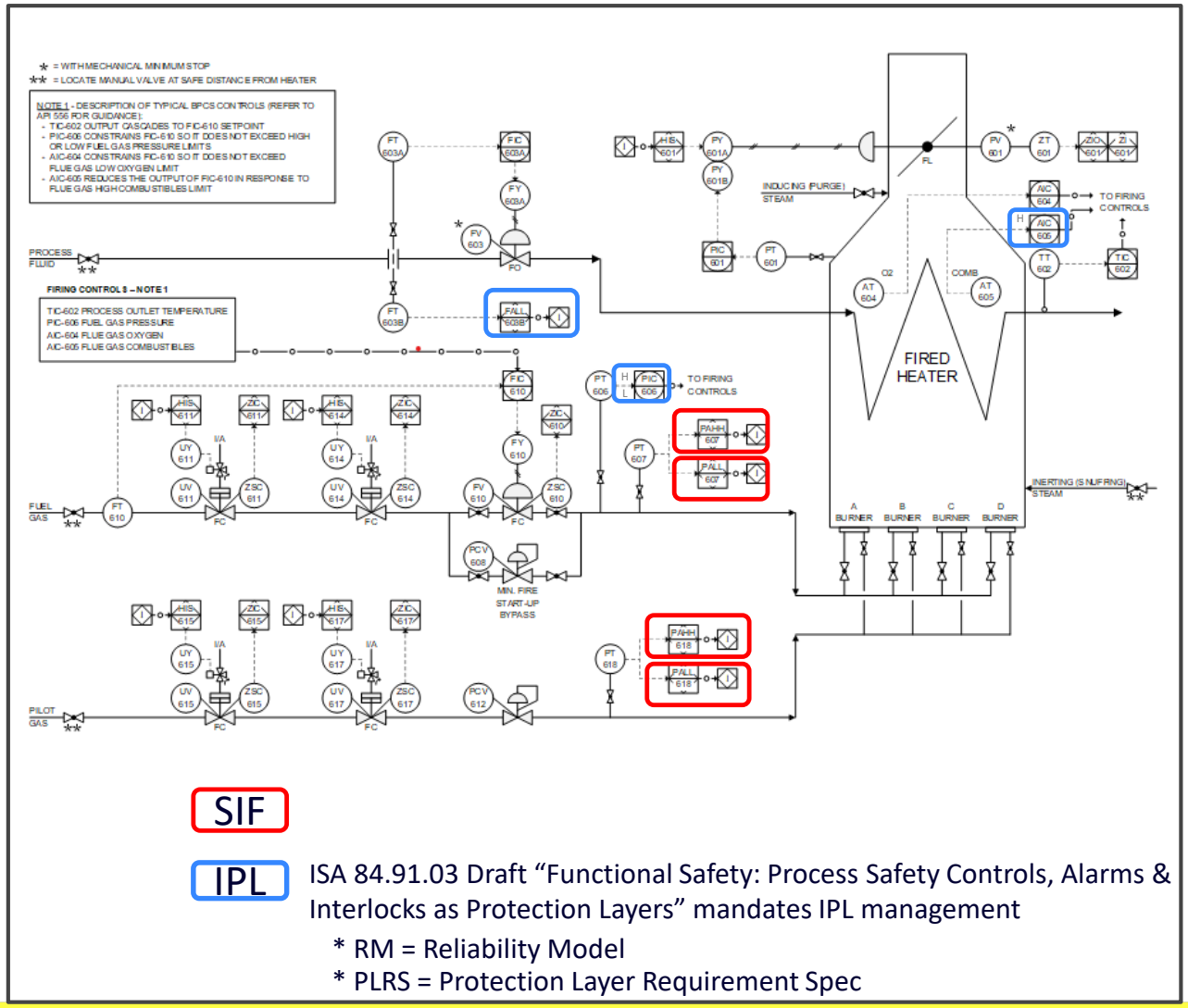
ISA 84.91.03 Draft "Functional Safety: Process Safety Controls, Alarms & Interlocks as Protection Layers" mandates IPL management

* RM = Reliability Model
* PLRS = Protection Layer Requirement Spec



Manually Enter Data For Each SIF/IPL To Comply with IEC 61511

Templatization Approach Multi-Burner Heater



SIF

IPL ISA 84.91.03 Draft "Functional Safety: Process Safety Controls, Alarms & Interlocks as Protection Layers" mandates IPL management

* RM = Reliability Model
* PLRS = Protection Layer Requirement Spec

Bulk Insert **All Tags & Voting** from I/O List

Bulk Update SIL Calcs and Docs for **All SIFs & IPLs**

- 8 SIL Calcs/RMs
- 8 SRS/PLRS
- 8 C&E
- 8 Test Plans

Reduced Time to Complete IEC 61511 Docs from >40 hours to <1 Hour

End Goal of IEC 61511

PHA/LOPA

Reliability Calculations

Safety Requirements

Safety Cause & Effects

Capital Project Execution

Functional Test Plans

Heart & Soul of Standard

Monitor & Sustain

Single Connected Data Model to Drive Fired Heater KPIs

Questions?

Mike Scott, PE, CFSE
CEO
mike.scott@aeshield.com