

“Standards Compliance and User Requirements for Industrial and Utility Boiler Control Systems”

By: Dr. Issam Mukhtar & Geoff Rogers

Presented at IDC Boilers Conference, Perth November 2008

Abstract:

The AS61508 and AS61511 standards for Safety Instrumented Systems have been accepted by Australia as best practice engineering for general applications and as a basic requirement by the Energy Safety Authorities for “type B” appliance application approvals of gas fired plants.

Considerations of multi-fueled multiple-burner systems.

The paper outlines Premier Consulting Services experience in implementing the standards on Industrial and Utility Boilers, Process Heaters, Furnaces and Gas Turbine applications, with and without Heat Recovery Steam generators.

Issues and challenges in complying with AS3814/NFPA85 and AS61508 /61511 are also discussed highlighting some recommendations.

Issues to consider when selecting and maintaining control system hardware and software.

References to Australian Case studies on boilers, furnaces, gas turbines.

Introduction

Most companies in Australia have realised for some time that providing a safe working environment is not an optional management decision but it is a requirement to comply with safety standards due to insurance rate structure and some government regulations, and new industrial manslaughter provisions of various state OHS regulatory regimes, that can see criminal charges and jail terms for negligence.

For boilers and other combustion systems there has never been a lack of guidelines and standards. On the contrary, the confusion stems from the existence of multiple standards, guidelines and/or recommendations that could be applied.

For example consider a packaged boiler installed in a refinery, one has the following options with respect to design guidelines requirements.

- A. NFPA 85 Boiler and Combustion Control Systems Hazards code.
- B. API 556 Instrumentation and Controls for Fire Heaters and Steam Generators
- C. AS 3814 Industrial and Commercial Gas-Fired Appliances
- D. AS 61508 /AS 61511 Standard for Safety Instrumented Systems.

One may struggle to decide which direction to take. This paper clears the fog and addresses the differences between the different standards requirements.

Standards and Code

There are two different type of standards related to combustion systems

- A. Prescriptive type of standards such as NFPA 85 and AS 3814
- B. Performance based standards such AS61508 and AS61511

NFPA 85

The NFPA 85 document is primarily the document used for most industrial boilers and furnaces. As stated in the standard, the basic cause of a furnace explosion is the ignition of an accumulated combustible mixture within the confined space of the furnace or the associated boiler passes, ducts and fans that convey the products of combustion (or lack of combustion of a air fuel mixture) to the stack.

Numerous situations can arise in connection with the operation of a boiler furnace that that will produce explosive conditions; the most common experiences are as follows:

- Interruption of fuel or air supply or ignition energy to the burners.
- Fuel leakage into an idle furnace and the ignition of the accumulation.
- Repeated unsuccessful attempts to light off without appropriate purging.
- The accumulation of an explosive mixture of fuel and air as a result of a complete furnace flameout.
- Failure of flow controls leading to excess fuel for the amount of air.

To protect against these common Hazards, the NFPA 85 recommends certain interlocks based on their experience and previous accidents in boilers. It also provides guidance on the quantity and types of sensors / valves required for these interlocks along with the logic necessary for a safe trip.

These codes / standards do not adequately address different risk levels associated with the boiler. For instance, if your boiler was located next to a control room, which was staffed 24-hrs/day, the risk to personnel from explosion is significantly greater than if it was located in a remote unoccupied area of the facility.

Different (higher or lower) consequences would require different risk reductions and consequently would require different integrity levels for the protective interlocks.

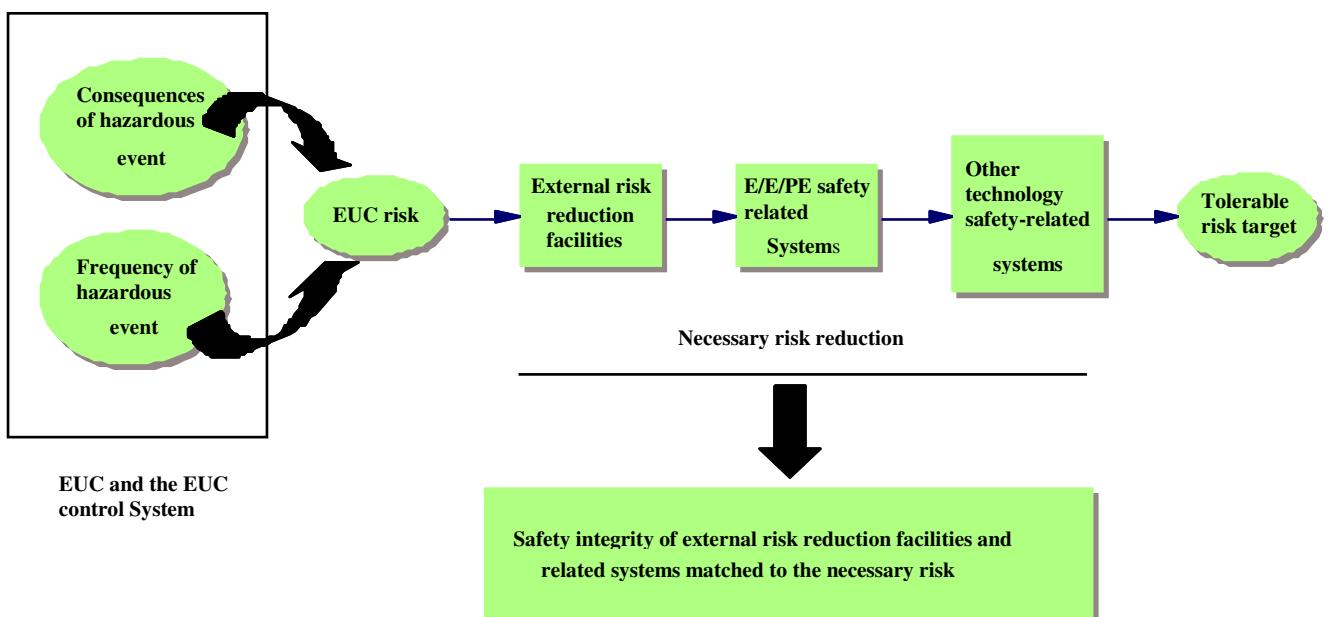
While the NFPA 85 tells you what interlock must be implemented it does not tell you how to implement it or at what integrity level it must be; particularly when it comes to the use of electronic based equipment and programmable electronic based logic solvers.

AS61508/AS61511

Performance based standards such AS61508 & AS61511 have been widely accepted as the basis for specification, design and operation of Safety Instrumented Systems (SIS). The standard sets out a risk-based approach for deciding the Safety Integrity Level (SIL) for systems performing safety functions which is in the case of the boiler is the BMS (Burner Management System) and other protective interlocks.

Whereas IEC 61508 is a generic standard common to several industries, the IEC 61511 is process industry sector specific standard.

These standards provide a set of criteria that must be met depending upon the amount of risk reduction required as determined by the end user. Thus, these standards are specifically written to address the risks associated within a given facility.



Both standards adopt the complete Safety Lifecycle. The Safety Lifecycle provides a framework of considerations for each stage of an SIS from conception to decommissioning. The intent is to force a logical and sequential procession for the project scope. Some of the basic components of the Safety Lifecycle include: Risk Analysis; Consequence Analysis, Layer of Protection Analysis; Safety Integrity Level (SIL) determination, Documentation of Safety Function Requirements; SIS Conceptual Design; SIL Verification; Detail Design and System Implementation.

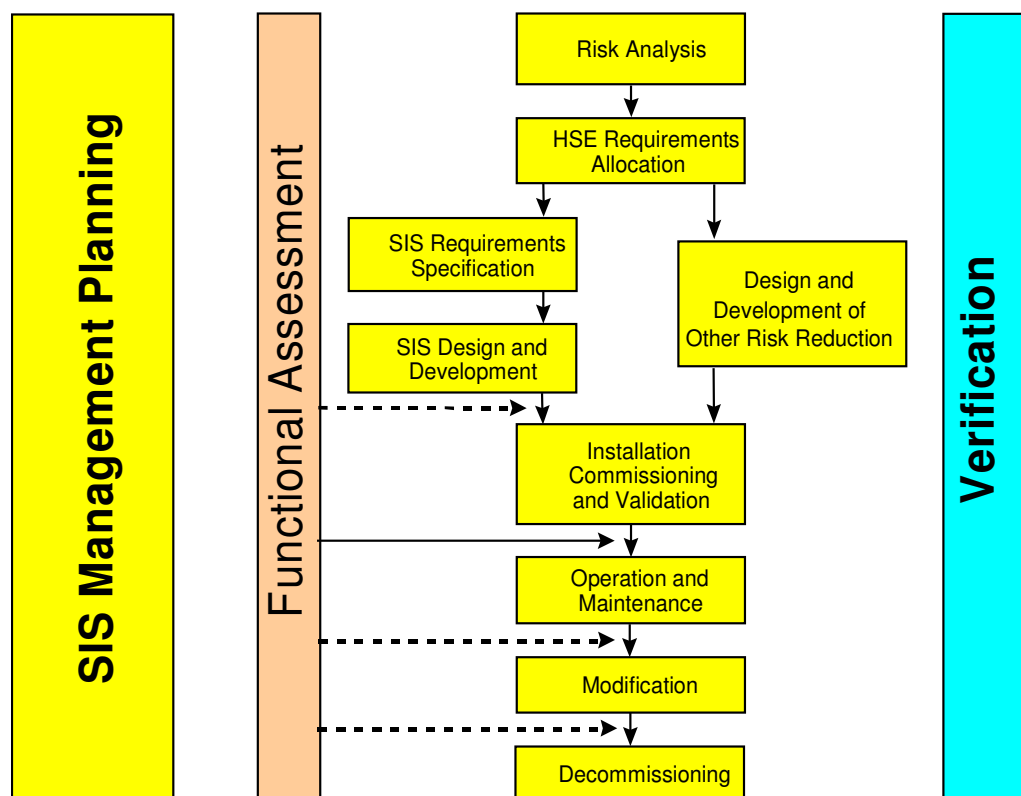
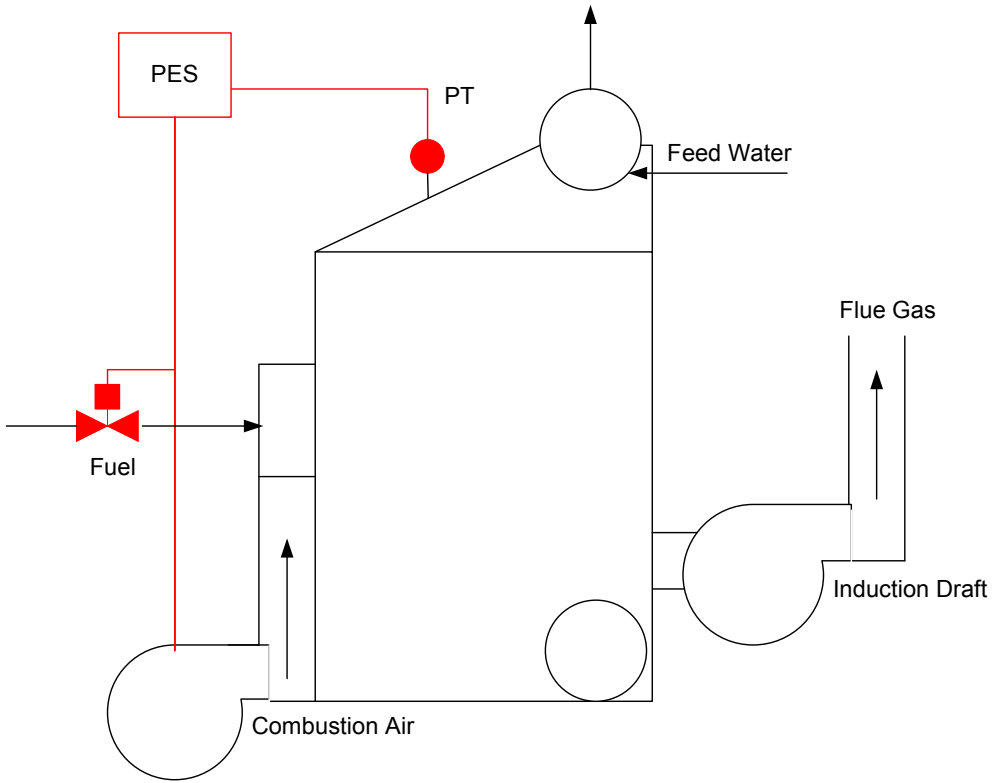


Fig (1) IEC61511 Safety Life Cycle



High Pressure in Boiler Furnaces

So, what is the Safety Integrity Level (SIL)?

A high/low pressure furnace interlock is a requirement by NFPA 85. Having decided to implement it, the following questions would arise:

- 1 How good must this interlock be?
2. What is the interpretation of “good”?
3. How to decide how good the interlock must be?
4. Who decides how good it must be?
5. And finally, how to design it to be that good?

How good must this interlock be?

This will depend on the consequences when the interlock fails on demand. It also depends on how often you get a high pressure, which to a large extent depend on the reliability of the fans and the combustion air flow control system.

What is the interpretation of “good”?

The interpretation of how good is given by the SIL which is the product of the consequence and demand frequency Fig (3) and it is expressed in numbers tied to Probability of Failure Dangerously ($PFD_{(Avg)}$) of the interlock including the sensor, logic solver and final element .

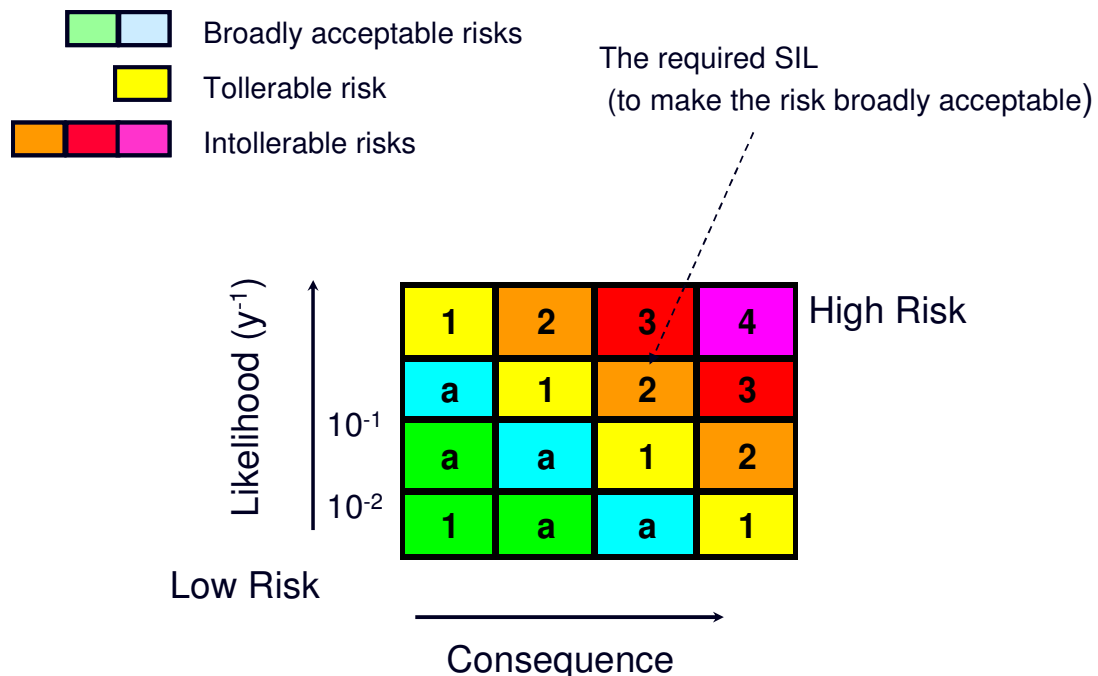


Fig 3 SIL is the product of Consequence and Frequency

Layer of Protection and Risk Reduction

How good the interlock must be could also be expressed in terms of the required risk reduction to meet the company's acceptable or tolerable risk. The risk associated with a failure on demand of the safety interlock is first expressed in different levels of tolerable risks. Having specified what level of risk is associated with failure of the particular interlock, the risk reduction required by the interlock to reduce the risk to the acceptable levels could then be extracted after considering all other risk reduction provided by other Layers of protection Fig (4).

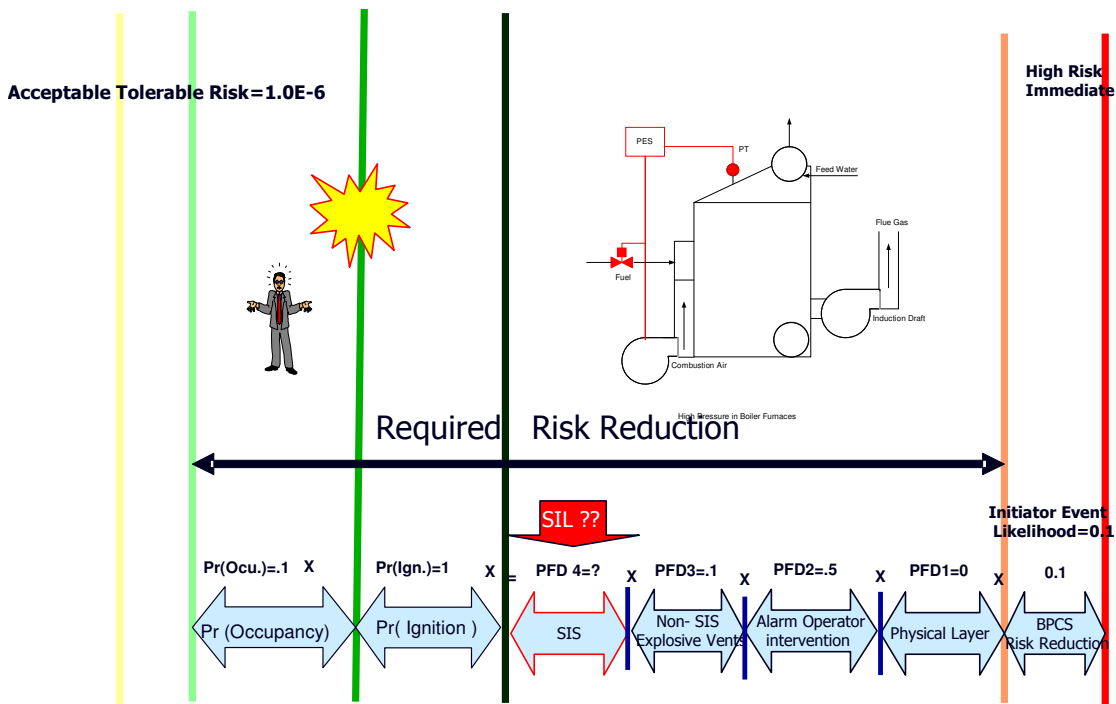


Fig 4 Risk Reduction by layer of Protection

3. How to decide how good the interlock must be?

Several methods that are acceptable for assigning SIL are available under IEC61511.

Risk matrix is one of them (Fig 3) where the SIL classification is based on defining the consequences and frequency of demand.

Layer of Protection analyses (LOPA) is another method that became very popular for SIL assignment. Apart from assigning the SIL, LOPA analyzes all the risk associated with each hazardous scenario.

4. Who decides how good it must be?

Normally it comprises a committee, in a facilitated workshop led by a Functional Safety Expert and attended by related experts in the boiler such as Designers, Process Engineers, Instrumentation & Control Engineers, Operators and EHS personnel.

5. how to design it to be that good?

There are two aspects in the design the safety interlocks:

- The first is related to meeting the interlock safety integrity requirement i.e. to meet the $PFD_{(Avg.)}$ number associated with SIL assigned for interlock as given in table (1). This would require calculating the $PFD_{(Avg.)}$ by modeling the interlock from the sensor, logic solver to the final element using fault tree analyses Fig (5).

-

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (Average Probability of failure to perform its design function on demand)	CONTINUES/HIGH DEMAND MODE OF OPERATION (probability of dangerous failure per hour)
4	$\geq 10 E-5$ to $10E-4$	$\geq 10 E-9$ to $10E-8$
3	$\geq 10 E-4$ to $10E-3$	$\geq 10 E-8$ to $10E-7$
2	$\geq 10 E-3$ to $10E-2$	$\geq 10 E-7$ to $10E-6$
1	$\geq 10 E-2$ to $10E-1$	$\geq 10 E-6$ to $10E-5$

Table 1 AS 61508 Safety Integrity Level

- The second design basic requirement is to prepare the Safety Requirement Specification (SRS) as defined in clause 10.3.1 in IEC61511. The safety Requirement Specification consists of 27 main points listed in table 2.

SRS No.	SRS REQUIREMENTS PER IEC61511 CLAUSE 10.3.1
1	Description of all safety instrumented functions necessary to achieve the functional safety
2	Requirement to identify and take account of common cause failures
3	Definition of safe state of the process for each safety instrumented function
4	A definition of any individually safe process states which, when occurring concurrently create a separate hazard (for example multiple relief to flare system)
5	Assumed sources of demand and demand rate on safety instrumented function
6	Requirement for proof testing interval
7	Response time requirements for the SIS to bring the process to a safe state
8	SIL and mode of operation (demand/continuous) for each safety instrumented function
9	Description of SIS process measurements and their trip points
10	Description of SIS process output actions and the criteria for successful operation
11	Functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissive
12	Requirement for manual shutdown
13	Requirement relating to energise or de-energise to trip
14	Requirement for resetting the SIS after a shutdown
15	Maximum allowable spurious trip rate
16	Failure modes and desired response of the SIS (for example alarms, automatic shutdown)
17	Any specific requirements related to the procedure for starting up and restarting the SIS
18	All interfaces between the SIS and other systems, including the BPCS and operators
19	A description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode
20	Application of software safety requirements as listed in 12.2.2 of AS IEC 61511
21	Requirements for overrides/inhibits/bypasses including how they are cleared
22	Specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected by the SIS. Any such action shall be determined taking into account all relevant human factors
23	Mean time to repair which is feasible for the SIS, taking into account travel time, location, spares holdings, service contracts, environmental constraints
24	Identification of dangerous combinations of output states of the SIS that need to be avoided
25	Extremes of environmental conditions that are likely to be encountered by the SIS
26	Identification of normal and abnormal modes of operation of plant as a whole and individual plant operation procedures
27	Requirements for any SIF to survive a major incident, for example time required for a valve to remain operational in event of a fire

The SRS is an important document for boiler safety. It is the document that the detailed design should be based on. A few of the issues in the SRS are considered in NFPA 85 in a different way such as interlock response time, requirement for manual shut down and others.

Other issues such as common cause, interlock spurious trips and proof testing period are not well addressed.

Common Cause failure

Accidents normally happen when the boiler loses all its layers of protection which are the control system, safety interlocks, alarms & operator intervention and others. It is very important to investigate possible common mode failure between the layers of protection and to ensure that there is a sufficient amount of independence between them.

Proof testing Period

Safety interlock instruments must be tested periodically to uncover dangerous failures. The testing period depends on the interlock's assigned SIL. The $PFD_{(Avg.)}$ calculations would recommend the testing period required to meet the SIL assigned. There is no recommendations in NFPA regarding this issue, but many are tested at intervals established somewhat arbitrarily, such as once per year.

Spurious Trips & Interlock response for different mode of failure

Hazards during start up considered greater and more likely than during normal operation cycle of a Boiler. Irrespective of the protection and supervision provided during start up, it would be advisable to reduce the number of tripping and start up events caused by the safety interlock safe failures. This could be achieved by providing redundancy and diagnostic for the safety interlock components. 2oo3 voting system would be advisable in this case for all safety interlocks including the sensor and logic solver (not necessary the final element, but certainly the solenoid valves that control the power fluid (usually air or oil)).to the main valve actuator.

The Selection of Logic Solver and Other Instrumentation

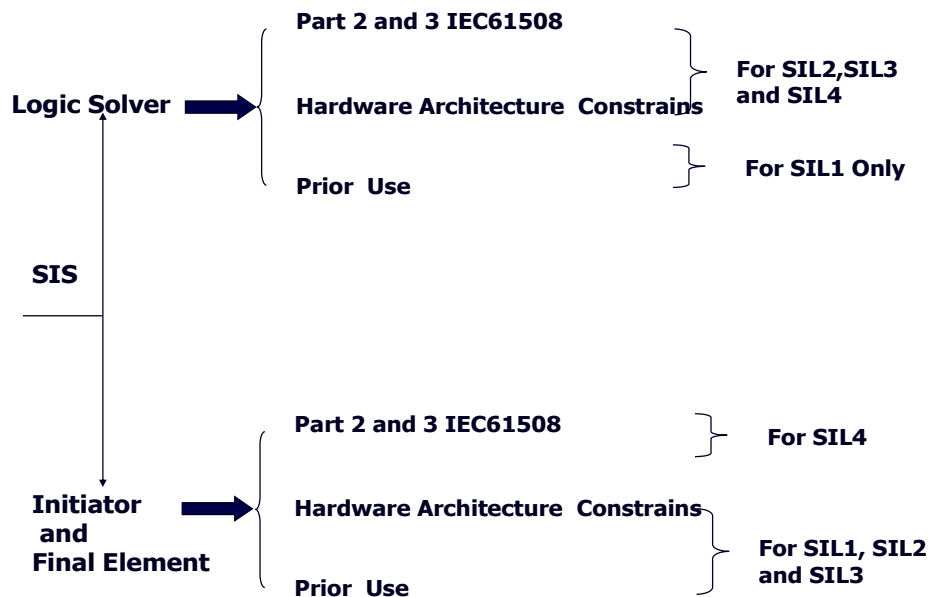
Clause A1.1. in the NFPA 86 quotes the following .

Technological advances in recent years and, in particular, the pervasiveness of microprocessor-based hardware, make it even more important that only highly qualified individuals be employed in applying the requirements of this code to operating systems. Each type of hardware has its own unique features and operational modes. It is vital that the designer of the safety system be completely familiar with the features and weaknesses of the specific hardware and possesses a thorough understanding of this code and its intent.

It is not possible for this code to encompass all specific hardware applications, nor should this code be considered a "cookbook" for the design of a safety system. Where applying any type of equipment to a safety system, the designer should consider carefully all of the possible failure modes and the effect that each might have on the integrity of the system and the safety of the unit and personnel. In particular, no single point of failure should result in an unsafe or uncontrollable condition or a masked

failure of a microprocessor-based system that could result in the operator unwittingly taking action that could lead to an unsafe condition.

There are very tentative guidelines in the NFPA 85 for the selection of the Logic Solvers for Boiler's BMS. By contrast The AS61508/61511 is particularly written for safety system hardware and software guidelines and therefore it is imperative to follow it when it comes to the section of the Logic Solver and other instrumentation. Fig (6) below outlines which of the two standards must be followed during the selection of the instrumentation and logic solver for safety interlocks.



Logic Solver Selection

As outlined in the NFPA 85 above that there are different configurations that could provide different integrity levels for the Logic Solver. These configurations may meet the safety requirement (SIL) but not necessarily the reliability (availability requirements) and therefore safety and availability of the Logic Solver should be considered during selection. One common mistake we come across when selecting the Logic Solver is the following:

I have a maximum of SIL 2 for most of safety interlocks then I need a SIL2 Logic Solver?

The assigned SIL 2 for safety interlock is not for the Logic solver, but entire loop including the sensor, logic solver and final element. By the time you add the $PFD_{(Avg.)}$ for the sensor and final element you would find the you may need a SIL 3 Logic Solver.

AS3814 Industrial and commercial gas-fired appliances

The objective of this Australian Standard is to provide the minimum requirements for the safe operation of gas-fired industrial appliances, such as gas fired boilers and other large appliances used for commercial applications.

Unlike other related standards the AS 3814 NOW refers to the AS61511 and AS 61511. Clause 2.26.3 (b) by quoting the following :

If a PES controller (logic solver and its associated I/O module) is used to perform Safety-related functions:

(i) It shall be a safety-related PES controller and possess a TÜV safety certificate to the appropriate safety integrity level (SIL) of AS 61508 or some equivalent certificate using only TÜV certified 'firmware' (or equivalent); or

(ii) Where a customer/contractor insists on using a non-safety-related PES controller to perform safety-related functions the safety-integrity of the PES controller shall be independently verified, to the required SIL, by an appropriate institution.

Then it quotes

(c) Contractors submit the following to the technical regulator:

(i) A relevant flow sheet written in plain English containing the description of events to occur within the PES. (Typically this would be done prior to writing the PES program).

(ii) The relevant parts (only) of the PES program.

(iii) The hard-wired electrical schematic diagram clearly indicating connection to the PES.

(iv) A copy of the TÜV safety certificate together with the TÜV documentation, on any restrictions applying to that PES controller.

(v) The qualitative SIL for the appliance application to be evaluated.

(vi) The quantitative SIL determination of the individual safety instrument system (SIS) loops to be evaluated to ensure the appropriate level of protection is provided by the PES based installation.

(vii) The quantitative SIL to be validated through either a simplified equation or a fault tree analysis as described in AS 61508, AS 61511 or equivalent.

It is very clear that the standard mandates the compliance with AS61508 & AS61511 when a decision is made to use Programmable Electronic System. However it is not clear if the standard wants you to comply with AS61511 /AS 61508 life cycle fully or partially. From the requirement of documentation that must be submitted to the regulator, it looks like partial compliance is mandated. This may not be a good idea as escaping some part of the standard cycle such as Safety Requirement Specification (SRS) may result in holes in the design of the safety interlocks that are not covered by other parts of AS 3814.

Conclusion and recommendations

1. Both prescriptive and performance standards are required in the boiler design to meet the safety requirement and government regulation. Since most boiler manufacturers have a near standard design based on Prescriptive Standards (NFPA 85, sections of AS3814) then it's advisable to implement performance standards (AS61511) first and check the designed system with the requirements of the NFPA-85. If it is a standard design that is based on NFPA 85 then there should be no problem.
2. It is recommended that AS 3814 requests the compliance with AS61508 /AS61511 fully and not partially.
3. Recommended supplier of instrumentation by Energy Safety regulators should provide failure rates or (FMEA reports) for their instrumentation to enable the more accurate calculation of $\mathbf{PFD}_{(Avg.)}$ for the safety interlocks. Use of generic data from published source such as OREDA is permissible under the standard, but tends to be conservative and may increase costs and testing requirements.

Dr. Issam Mukhtar : PREMIER CONSULTING SERVICES

Graduated from Manchester University in 1977 with PhD in Electrical Engineering. Dr Mukhtar has been involved industrial instrumentation & controls design since 1978. For last ten years he has been specifically focused on the installation and implementation of Safety Instrumented Systems in heavy industrial applications. In the Power, Chemical, Petroleum, Mineral processing and Steelmaking sectors in particular.

Dr Mukhtar is a certified TUV Functional Safety Expert working as a Principle Consultant for Premier Consulting Services in Europe, Middle East and throughout the Asia Pacific region.

Mr. Geoff Rogers Invensys TRICONEX – Technical and Industry Specialist

Engineering graduate (1977, Honours University of Melbourne) with experience in the application of Control and Safety Systems in the process industries.

Certified TÜV Functional Safety Engineer I. D. 35/04.

IICA Member/Victorian Committee-person. Former Vic Div Chairman and Federal President

Author of various technical papers on Control System and Functional Safety topics. Geoff has managed engineering teams designing and implementing process control, critical control of Turbomachinery and Burner Management for Boilers and safety systems for the Petrochemical, Chemical, Oil & Gas and Power industries. Additionally, he has 15 years of hands-on field experience in field operations, installations and start-ups.

Designed Fault Tolerant control systems, DCS systems from major suppliers, Currently specialized in application engineering and support of project teams implementing functional safety consulting, risk assessment, realization of Safety Requirements Specifications, especially from Logic Solver perspective.