Safety Integrity Level of Shut-Off Valve in a Burner Management System

Mohammed BSISS[1], Fatima Ezzahra NADIR[2], and Benaissa AMAMI[1]

[1] Department of Computer Science, Systems and Telecommunications (LIST), Faculty of Sciences and Technology Tangier, Morocco
[2] Research Team: Optimization of Industrial Systems (EROS), Engineering Sciences and Energy Management Laboratory (LASIME), Higher School of Technology, Ibn Zohr University, Agadir, Morocco
mbsiss@uae.ac.ma, f.nadir@uiz.ac.ma, b_benaissa@hotmail.com

Abstract. The safety control and command system, such as the burner management system, requires that the system must be reliable, available and safe. The reliability is based on choosing equipment, with a high level of safety and which is suitable for the safety system. The availability and security are provided, among others, by redundancy. It is presented by M-Canal out of N-Canal (MooN) architecture, the (N-M) indicates how many dangerous faults are possible, without the performance of the systems being impeded. An essential quantitative analysis based on the evaluation of the PFD_{avg} is part to give high trust in the BMS. This paper will discuss how a quantitative method can be used to select the appropriate SIL according to shutdown system for Burner Management System (BMS). This system is a part of a safety solution that manages a combustion system; it allows the safe start-up operation, and the shutdown of multiple burner furnace section of a boiler, and main flame detection.

Keywords: Burner Management System (BMS), risk analysis with RBD, PFD_{avg}, Safety Integrity Level (SIL), Shut-off Valve.

1 Introduction

The BMS is used in different industries like Oil and Gas, Power Generation, Chemical or further equipment that uses a flame. It allows an Auto Relight, temperature Control, Remote Monitoring, Control, and Emergency Shutdown. The BMS can detect the flame absence in the combustion application and it can reignite the burner flame (Auto relight). The BMS will manage temperature setpoint, it can detect dangerous failure in process and can bring the system in a safe state if dangerous failure occurs, such as low or high fuel pressure, and loss of flame. A typical dangerous failures controlled by the BMS are listed in Table1 [2].

Table 1. A typical dangerous failures controlled by BMS.

SIF	Dangerous failures
SIF-001	An uncontrolled access of fuel and air can lead to an explosion.

SIF-002	An uncontrolled access of fuel and air by loss of ignition can cause an explosion.
SIF-003	An uncontrolled access of fuel and air by fuel interruption may result explosion.
SIF-004	Improper maintenance in subsystems which can cause the flame to be extinguished in the presence of unburned fuels can lead to a possible explosion.

In order to evaluate the SIS associated to the BMS, we propose a comparison between the calculation of PFD_{avg} using Reliability Bloc Diagram, this calculation is based on IEC61508 standard with simplified equations, and the evaluation giving by exSILentia.

2 Presentation of the BMS with 1oo2 architecture

The BMS with 1oo2 architecture presented in Figure 1, with a description of a simplistic Piping and Instrumentation Diagram for the Burner Management System, which should be evaluated. The shutdown valve subsystem can be considered as, 1oo2 arrangement of two shut off valves SSOV01X1 and SSOV01X2. The safety function is performed by stopping the flow of gas, if the pressure in boiler is too high and prevent or mitigate the hazardous event.

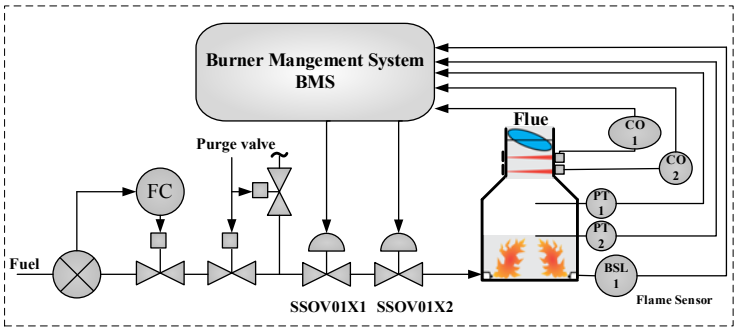

Fig. 1. The simplified Burner Management System.

The safety devices provided by harmonized EN 746-2 standard required for subsystem Fuel-Gas, flame and process, are [3]:

- Isolation manual valve, filter, fuel-gas measurement
- Double block and bleed valves
- Temperature measurement at the process outlet
- Flow measurement at the process inlet, Self-checking flame detector

The safety function is performed by the 1oo2 series configuration of shut off valve in the main fuel, to ensure that the both valves close in case of dangerous failures be occurs. The 1oo2 arrangement architecture uses two channels, which is adopted for the sensor, the IS barrier, and the PLC control circuit in parallel, driving two valves connected in series. The shut off valve can fail dangerously for detected λ_{DD} or undetected failures λ_{DU}. Figure 2 presents the 1oo2 architecture adopted for the pressure sensors, the IS barrier, the logic solvers and the final elements.

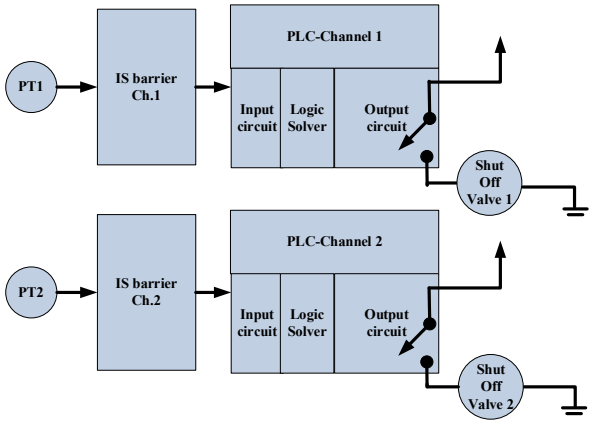

Fig. 2. The 1oo2 system architecture in BMS application.

3 BMS Reliability

The PFDavg value of the BMS system expresses the safety performance of safety instrumented function (SIS). It's frequently used to reduce process hazards in many risk applications. For each potentially dangerous process, the BMS system is designed, to detect the dangerous situation and automatically takes action to prevent or mitigate the hazardous event defined in Table 1. The IEC 61511 standard requires an allocation process to define the required SIF and evaluate the associated Safety Integrated Level for each SIF. In case of the low demand operating system such as the BMS, the PFD_{avg} values are defined, in IEC 61508, for each of the four Safety Integrity Level (SIL).

The calculation of the PFDavg is based on the simplified equations defined in [5]. The low demand mode for shut off valve subsystem is considered, because of its low frequency of demands. This probability must be calculated based on different parameters:

- The failure rates λ of each subsystem in the BMS, the diagnostic coverage DC.
- Redundancy of devices (MooN architecture).
- Proof Test Interval T_i, Proof Test Effectiveness (efficiency).
- Mean Time to repair & Mission Time.

- Operational and Maintenance capability.

In order to simplify the PFDavg calculation of each component of the BMS, we only take the undetected dangerous failure λ_{DU}, and the proof test interval T_i. giving in Table 3 The PFD_{avg} for the system is the sum of the PFD_{avg} of each component:

$$PFD_{avg(Loop)}=PFD_{avg(Sensor)}+PFD_{avg(Logic)}+PFD_{avg(Actuator)} \quad (1)$$

4 Simplified equations for PFD_{avg} calculation

The calculation of the PFD_{avg} depends on the architecture adopted to each subsystem. We use the simplified equations defined in [5], to calculate the $PFD_{avg.}$ The following equations do not take account of common cause failure β and diagnostic coverage DC.

Table 2. Simplified equation for PFD_{avg} calculation

	Architecture of the SIS			
	1 out of 1	***1 out of 2***	***2 out of 2***	***2 out of 3***
PFD_{avg}	$\frac{T_i\lambda_{DU}}{2}$	$\frac{(T_i\lambda_{DU})^2}{3}$	$\lambda_{DU}T_i$	$(\lambda_{DU}T_i)^2$

5 Reliability Block Diagram of BMS

The IEC 61508 standard requires a qualitatively risk analysis method of each part of equipment, or subsystem of these, used for risk reduction purposed of safety-related systems. Among these methods, we chose the Reliability Block Diagram, which defines the logical interactions of dangerous failures of functional blocks. Each component of the SHUT OFF VALVE system, is a functional block connected by a series configuration for SHUT OFF VALVE and a parallel configuration for sensors and PLC. The figure 3 presents the RBD adopted to the shut off valve subsystem, with a 1 out of 2 architecture. This means that the safety function can still be executed by one channel in case the other channel fails. The chosen architecture therefore tolerates a single dangerous failure.

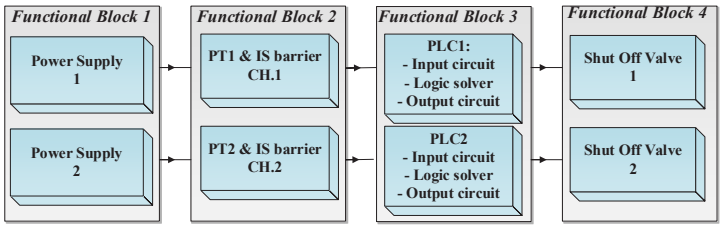

Fig. 3. Reliability Bloc Diagram associated to BMS Shut Off Valve with 1oo2 structure.

The unreliability data for the shut off valve subsystem components is given in table 3, for one year T-proof test interval [5], and for 1oo1 architecture.

5.1 Sensors

The sensor chain is composed of IS barrier and pressure transmitters (PT1, PT2), which are located in the combustion room on the fuel gas skid. Each sensor is connected independently to redundant analogue input cards of PLC. In the SIS, the 1oo2 configuration is applied for the channel comprising IS barrier, transmitter, and analogue input. The figure 4 represents the RBD according to the sensor subsystem.

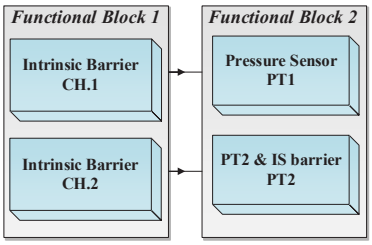

Fig. 4. Reliability Bloc Diagram associated to the sensor.

The sensor chain has the following failure rate:

$$\lambda_{DU} = \lambda_{DU\,PT} + \lambda_{DU\,IB}$$
$$= 8\times10^{-4} + 19\times10^{-4} \approx 2,7\times10^{-3}$$
$$PFD_{avg}(1oo2) = \frac{1}{3}(2,7\times10^{-3})^2$$
$$= 2,43\times10^{-6}\ per\ year$$

5.2 Logic Solver

The logic solver has a voting architecture of 1oo2, to improve safety. The logical part is built around the PLC with remote inputs/outputs, CPU cards, and communication module. The Logic solver subsystem's RDB, can be represented into three blocks in figure 5.

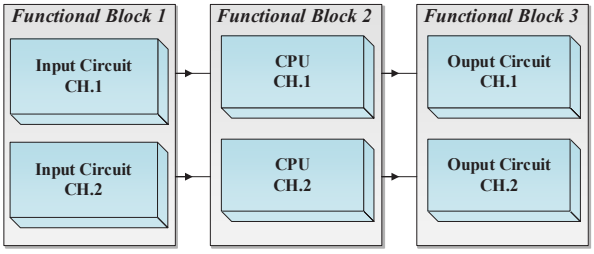

Fig. 5. Reliability Bloc Diagram associated to the logic solver.

$$PFD_{avg} = \lambda_{DU} = 10^{-5}\ per\ year$$

5.3 Actuator

The pre-actuator and actuator part, presented by de shut off valve, can be represented in the RBD as a 1oo1 structure, because the Valve is not SIL rated [5].

The actuator chain has the following failure rate:

$$\lambda_{DU} = \lambda_{DU\,valve} = 0{,}02183 \; per\ year$$
$$PFD_{avg} = 0{,}010915 \; per\ year$$

6 Safety Integrity Level

To accord a Safety Integrity Level (SIL) to a Safety Instrumented Function, we need to take account about [5]:

- Systematic Capability; architecture constraints, requirement of the need for minimum redundancy; and a PFD_{avg} calculation

Typical documents (not including software) to consider are:

- Design requirements specification; architecture description, detail design (schematics, drawings, BoMs, design descriptions, design reviews), techniques & measures plan, Verification & Validation (V&V) plan / results, Safety plan, manufacturing documentation and monitoring field failure performance

For SIF design verification, we will use the exSILentia tool [6]. The figure 6 presents the risk graph in exSILentia, a Target of **SIL3,** for the SIF will result.

The following parameters are giving at exSILentia, from the simplified equations.

- Mission Time = 5 years, work Time 24 yours, MTTR = 24 hours
- Proof Test Interval is equal to one year for the pressure transmitter, and five years for the valve and the logic solver
- A diagnostic coverage DC=100%, for sensor and logic solver, and for the actuator shut off valve, DC= 50%

This result gives a PFD_{avg} of 9, 86E-01 per year, with No SIL. The subsystem PFD_{avg} contribution for the sensor is 8,46E-01, for the Logic Solver is 2,63E-06 and for the Shut of Valve is 9,06E-01.

It can be deduced that the chosen element for SIF satisfied only availability but not the security of the system. Another sensor and actuator with certified SIL will be chosen.

- Endress+Hause Cebar S PMP71 digital pressure transmitter with welded metal sensor up to SIL2 according to IEC 61508
- Perpperl+Fuchs KCD2-SCD-(Ex) 1 smart current Driver and valve positioned up to SIL2 according to IEC 61508

- Mission Time = 5 years, Work Time 24 yours, MTTR = 24 hours
- Proof Test Interval for sensor and final element PTI= 1; Proof Test Interval for logic solver PTI= 5 years
- A diagnostic coverage for sensor and logic solver DC= 100%.

This result gives a PFD_{avg} of 1,63E-04 per year, which corresponds to a SIL3. The selection of safe sensor and actuator certified SIL, has improved the system safety integrity level. The subsystem PFD_{avg} contribution for the sensor is 1,15E-05 per year, for the Logic Solver is 2,63E-06 per year, and for the Shut of Valve is 1,49E-04 per year.

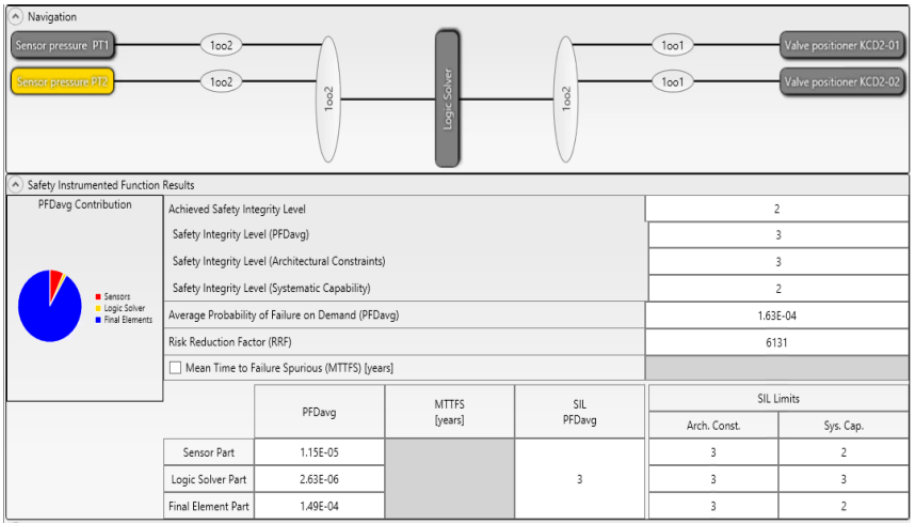

Fig. 6. The exSILentia results for Burner Management Systems.

Table 3. SIL values of each subsystem of the BMS.

Component	MTBF (yr)	λ_{DU} /yr	PFD_{avg} 1oo1	% of total PFD_{avg}	RRF= 1/ PFD_{avg}	*SFF*	*SIL Level*
Pressure Transmitter (PT)	102	0,00080	0,0004	3,40%	2500	91,8%	SIL2
Barrier D1014D	314	0,0019	0,000095	0,81%	10526	94%	SIL3
PLC	685	0,00001	0,000005	0,04%	200000	99,3%	SIL3
Valve	12	0,02183	0,010915	92,87%	92	73,8%	SIL1
Power Supply	167	0,0007	0,000350	2,97%	2857	88,3%	SIL3
Total (SIF)	**10**	**0,02353**	**0,011765**	**100%**	**85**	-	**SIL1**

Conclusion

The following sample calculation is carried out for a Burner Management System. The PFDavg value of the BMS shut off valve, is based on the Reliability Block Diagram (RBD). This modularization allows us to quantify the system PFDavg, by the sum of the sensor PFDavg, of the logical solver PFDavg and of the actuator PFDavg. The purpose of this quantification is to classify the system security level with a SIL.

The numerical result of PFD_{avg} is 0,1092E-1 per year, with a proof interval of one year, correspond to a No SIL, using values of table 3. However, with these elements of the functional chain, we can't realize the safety function of the BMS shut off valve. Therefore, we need sensors and actuators SIL certified. The exSILentia tool allows us to choose these components, with a very large choice of components, and from different SIL certified society. Using exSILentia tool suggests, this SIF could now achieve SIL3, with a one-year proof test, for the sensor and the actuator. This can reach only using certified SIL2 sensor and actuator. The proposed the BMS shut off valve design consists of the following component: a single SIL2 certified level transmitter, a SIL 3 certified logic solver, and a single remote actuated valve.

References

1. IEC, "61508-6: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems", e2.0d, pp.30-35, 2010.
2. M. Scott, I. Van Beurden, D.Cochran " What's the Safety integrity Level of My Existing Burner Management System?", AE Solution Articel, 11.2015.
3. J. Sanchez, "SIL Application in Burner Management System- A case Study: Thermal Burner", Safety Control & Instrumentation Systems Conference 2009-IDC Technologie. 2009.
4. A Summary of the IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, version 2.0, january2, 2006
5. A. Basilio, F. Novelli, G.Landrini, M.Baldrighi " SIL Manuel Safety Instrumented Systems",3rd edition ,G.M. Internaltional S.r.l.
6. ExSIlentia. (2017). https://my.exsilentia.com/Citrix/StoreWeb/: exida.
7. F. E. Nadir, I. Hadj Baraka and B. Amami, "PFH Calculation of a PID Controller 2oo3 system Implemented in FPGA Using Reliability Block Diagram", International Journal of Research in Business and Technology (IJRBT), vol. 10, no. 08, pp. 46-52, December, 2017.
8. S. Alizadeh, S. Sriramula, "Unavailability assessment of redundant safety instrumented systems subject to process demand", Reliability Engineering and System Safety, pp. 18–33, 2018.
9. F. E. Nadir, I. Hadj Baraka, M. Bsiss, and B. Amami, "Influence of Failure Modes and Effects Analysis on the Average Probability of Failure on Demand for a Safety Instrumented System", IEEE 4th Edition of the International Colloquium on Information Science and Technology, October 4-7, 2016, Tangier, Morocco.
10. F. E. Nadir , M. Jbilou, M. Bsiss, and B. Amami, "Safety fuzzy logic controller with 2oo3 architecture implemented in FPGA", IEEE 5th International Conference on Systems and Control (ICSC 2016), Cadi Ayyad University, pp.186-191, 25-27 May, 2016, Marrakesh, Morocco.