

Lifecycle Cost Analysis of Alternatives for Complying with Required Safety Integrity Level (SIL) at a Petrochemical Plant

Luiz Fernando Seixas de Oliveira

PhD in Nuclear Engineering
Certified Safety Engineer – DNV Vice-President, Manager of DNV Energy Solutions South America
Rio de Janeiro, Brazil
E-mail: Luiz.Oliveira@dnv.com

Luciana Moreira Chame

M.Sc. in Production Engineering, Chemical Engineer, Certified Safety Engineer, CFSE TÜV Rhineland (TÜVFSEng 766/07)
DNV Senior-Consultant, DNV Energy Solutions South America
Rio de Janeiro, Brazil
E-mail: Luciana.Chame@dnv.com

ABSTRACT

International Standards IEC 61508/61511 indicates various methods for determining the required Safety Integrity Level (SIL) for Safety Instrumented Systems (SIS). After determining the required SIL, one problem that still remains is the practical implementation of this requirement as there are always several ways of doing that. Complying with the highest SIL levels requires a detailed evaluation of the alternatives, which range from the use of more reliable components to the use of redundant configurations or different test policies, including the possibility of performing partial-stroke tests. This paper presents a methodology for a comparative analysis of possible alternatives for complying with a required SIL-3 for a high integrity safety system in a large petrochemical plant. The methodology is based on the comparison of the lifecycle cost of each proposed alternative. The results of this practical application show that the intelligent deployment of frequent partial tests of actuators, combined the realization of complete tests of the whole SIS at a much lower frequency, is capable of guaranteeing compliance with SIL 3 and at the same time has a much lower lifecycle cost than using configurations with higher redundancy without partial stroke testing. This is particularly true in cases where complete process shutdowns have very high costs such as in large petrochemical plants.

1. INTRODUCTION

As a result of the occurrence of new industrial accidents, protective measures are increasingly implemented to reduce their future occurrences. This movement has

followed an ascending trajectory in the last decades, strongly emphasizing the importance of guaranteeing the reliability of protection systems of industrial production plants. The introduction of Safety Instrumented Systems significantly facilitated the large-scale application of increasingly complex and sophisticated safety interlock systems. However, this raised a series of issues regarding the levels of reliability required and actually reached by such novel systems. In part as a response to such issues, the IEC 61508 (Ref. 1) and IEC 61511 (Ref. 2) standards were published, proposing performance-based criteria for SIS development and implementation, respectively, for industrial plants in general and in petrochemical plants in particular. Adopting a safety lifecycle approach (from specification & design until final decommissioning), a central piece of the new standards is the concept that a required Safety Integrity Level (SIL) must be established for each Safety Instrumented Function (SIF) based on the level of risk that the function is protecting against.

After determining the required SIL for an SIF, one problem that still remains is the practical implementation of this requirement as there are always several ways of doing that. Complying with the highest SIL levels requires a detailed evaluation of the alternatives, which range from the use of more reliable components to the use of redundant configurations or different test policies, including the possibility of performing partial-stroke tests. Although complying with the same required SIL, each configuration is bound to present a different lifecycle cost value, characterized by an entire set of cost values ranging from acquisition costs, operational and maintenance costs mainly dictated by the required proof-testing frequency and spurious failure costs.

This paper presents a lifecycle cost method for a comparative analysis applied to the practical case of specifying an SIS for protection against high pressure episodes in a large petrochemical plant unit. Such an SIS is typically referred as a High Integrity Pressure Protection System (HIPPS). The results of this comparative analysis showed that the intelligent deployment of frequent partial tests of actuators, combined with the realization of complete tests of the whole SIS with longer intervals (of up to every 5 years), is capable of guaranteeing compliance with required SIL 3 while having lower lifecycle costs than using SIS configurations with higher hardware redundancy without partial stroke testing. This is particularly true in cases where complete process shutdowns have very high costs such as in large petrochemical plants. The results of various sensitivity analyses with the most influential parameters show that the results are robust as the conclusions do not change much within a reasonable range of variation of the referred parameters.

2. OVERVIEW OF THE CONFIGURATION SELECTION METHOD

The overall idea of the Configuration Selection Method presented in this paper is that the operating company must select the SIS hardware configuration that meets the Required SIL value “AND” has the lower lifecycle cost. A general overview of the steps of the comparative selection method is illustrated in Figure 1.

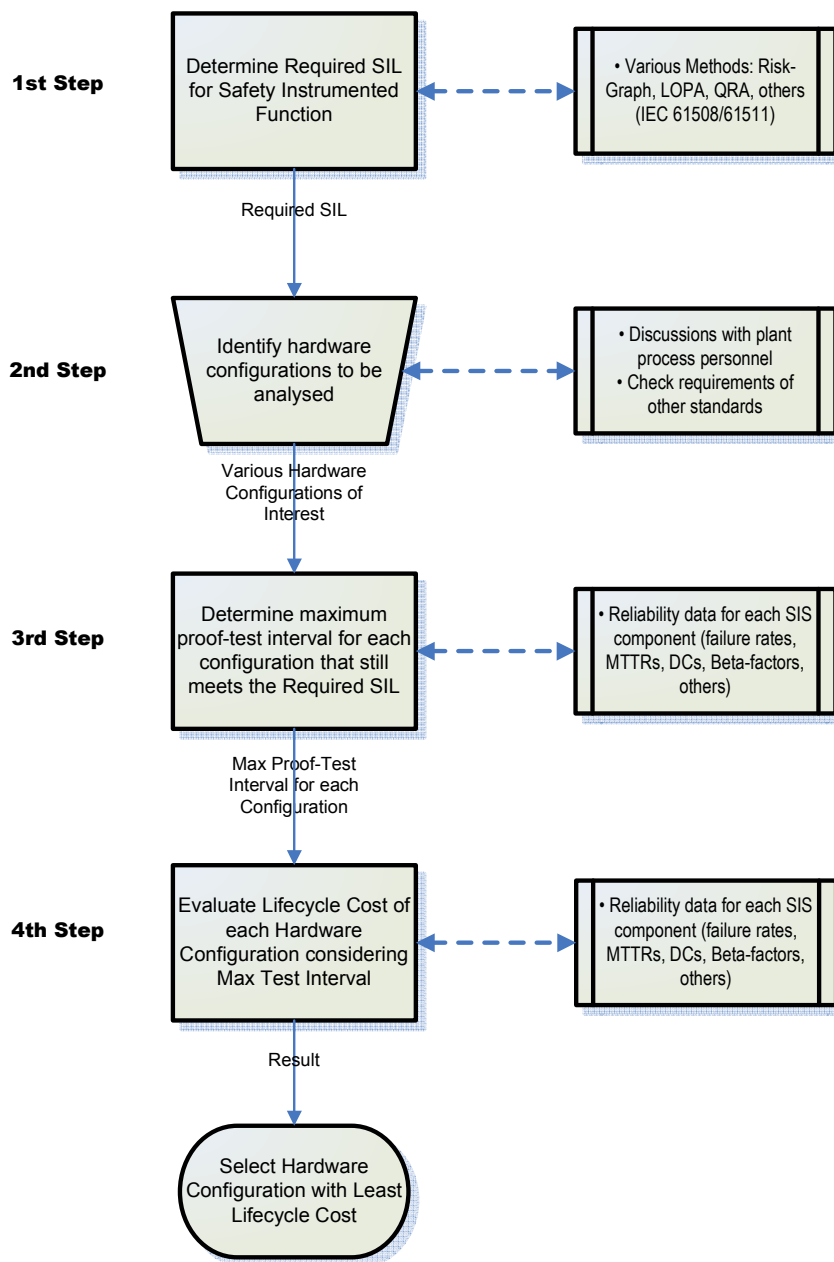


Figure 1 - Overview of the Main Steps of the Configuration Selection Method

The four main steps of the Configuration Selection Method are explained below:

- 1st Step: Determine the Required SIL for the Safety Instrumented Function (SIF) to be implemented.
 It is a direct requirement from IEC 61508/61511 (Refs. 1 and 2) that a Required SIL must be determined for each SIF that is implemented via a Safety Instrumented System (SIS). The standards indicate several methods that can be used for the Required SIL determination, among which the

most commonly used, are the Risk-Graph Method, LOPA and quantitative risk analysis (QRA). This step is not further discussed in this paper as the main interest here is to solve the problem of finding a best configuration that complies with a given Required SIL value.

2nd Step: Identify the hardware configurations that are to be analyzed. There certainly are several hardware configurations (or architectures) that can be used to comply with the Required SIL for a given SIS. Those can vary in the type of technology or the level of redundancy of each part of the SIS (initiators, logic unit and actuators). Therefore this second step consists of identifying a suitable number of hardware configurations to be analyzed. It depends on the results of discussions with the plant process personnel for identification of process requirements as well as special requirements from other standards. The result of this step is a set of hardware configurations specifying the level of redundancy and the type of component for each part of the SIS.

3rd Step: Determine the maximum proof-test interval for each hardware configuration such that it still meets the Required SIL value.

As shown in Figure 2, the PFD of each hardware architecture is an increasing function of the proof-test interval and each SIL value is defined as a one order of magnitude range for the PFD. This step consists of determining the value of the proof-test interval that is just at the upper border of the Required SIL value. This is exactly the maximum proof-test interval that would still guarantee that the SIS is still compliant with the Required SIL value. As an alternative procedure, one could choose any PFD value inside the Required SIL range, such as the mid-point, for instance. For the method proposed in this work, it is important that the chosen PFD value be the same for all configurations, meaning that they all provide the same level of plant protection. Otherwise the procedure should be modified to include another term in the LCC evaluation, corresponding to the different cost implied by the critical failures of each SIS configuration.

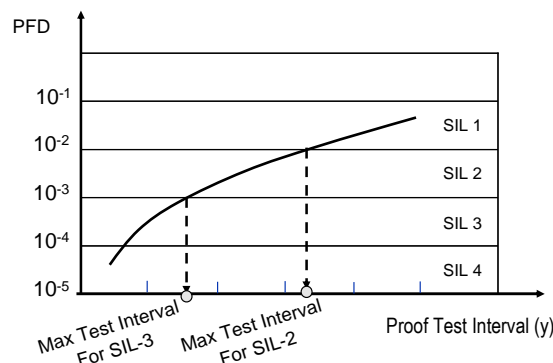


Figure 2 - Illustration of Maximum Test Interval for a Required SIL

4th Step: Evaluate the lifecycle cost (LCC) for each hardware configuration considering their respective maximum proof-test interval. The LCC for each hardware configuration is formed by the sum of all costs incurred by the plant throughout its lifecycle as a result of the implementation of each configuration. They involve the following main contributions: acquisition costs, operational costs, maintenance costs and spurious failure costs. Detailed explanations are given in Section 4.

3. CASE STUDY: FLARE HEADER OVERPRESSURE PROTECTION

When designing the expansion of a large petrochemical plant, to which a new process unit would be added, it was verified that the flare header would not have the capacity to withstand the depressurization release from both new and pre-existent units, in case of a shutdown of all the units in the facility. In this case, the traditional solution would involve expanding the current flare header or building a separate new header to meet demands from the new unit. Both solutions involve high costs and would cause serious operational disturbances during their construction period.

Aligned with the new possibilities opened by current project standards such as API-RP 521 (Ref. 3) and ASME-BPCV-VIII (Ref. 4), project designers sought to solve the problem through the use of a HIPPS System in the new unit (similar solutions have been examined in Ref. 5). In the present case, the HIPPS function would be to block the energy source (vapor) to the main column reboiler of the new unit (only) upon the sudden joint shutoff of all units of the installation but would not interfere in the depressurization of the existing units.

A schematic diagram representing the entire petrochemical facility is shown in Figure 3, showing the flare header that takes discharge from both the existing and the new units. A simplified arrangement of the blocking system analyzed in this paper is shown in more detail in Figure 4.

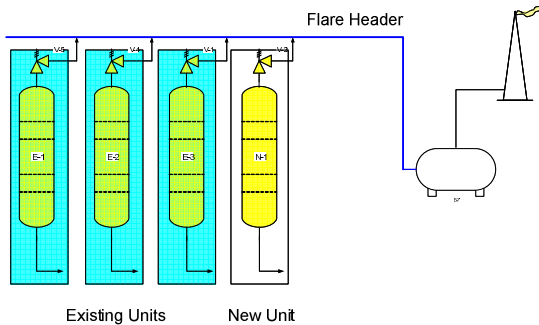


Figure 3 – Existing Units and the New One

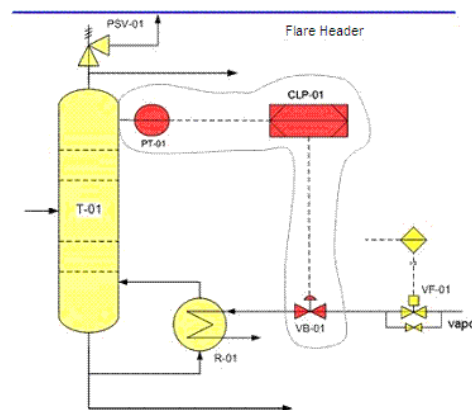


Figure 4 – New Unit Reboiler Blocking System (RBS)

The Reboiler Blocking System, hereinafter RBS, is a Safety Instrumented System (SIS) and, as such, is formed by three basic parts: an initiator, a logic unit and an actuator. In the simplest alternative, the initiator would be a single pressure transmitter, the logic unit would be a (simplex) PLC and the actuator would be a single block valve (with its associated valve solenoid). This is the configuration shown in Figure 4. A series of other configurations is possible, and several of them are analyzed in the next section.

4. APPLICATION OF CONFIGURATION SELECTION METHOD TO THE NEW UNIT REBOILER BLOCKING SYSTEM

4.1. Determination of the Required SIL

Based on a detailed quantitative risk analysis of all overpressure scenarios for the existing unit that would also require depressurization of the existing units, the plant owners have decided that the Reboiler Blocking System (RBS) should be a SIL-3 Required system. The assumptions and method used for reaching this decision is not of interest of this work and will not be further discussed here.

4.2. Possible Configurations Considered for Meeting SIL Requirement

As indicated in Figure 1, the analysts must now decide which configurations they want to analyze knowing that they all must meet a Required SIL-3. Each alternative configuration analyzed in this paper is composed, at least, by an initiator, a logic executor, and an actuator. In this work, ten alternative configurations for the reboiler blocking system are analyzed. These alternatives involve different configurations (the most usual in the process industry) comprising the following components: pressure transmitters (initiators), programmable logic controllers (PLCs) and block valves (actuators).

Two types of block valves are considered in the alternative configurations: the first is a conventional block valve with its associated solenoid valve. This type of valve is called here a "Type 1 Block Valve". The second type is a novel and more sophisticated block valve with a mechanism that allows for partial testing of the valve function (called "Type 2 Block Valve"). Several types of block valves with partial stroke testing (PST) capability are currently being marketed by different manufacturers. Their detailed description is not of relevance in this work (please see Refs. 6-10). Therefore, examining the ten configurations listed in Table 1, one can see that in terms of component redundancy, there are only five different configurations but because two different types of block valves are being considered, the overall number of analyzed configurations comes out to ten (five with simple block valves – Type 1 - and five with PST block valves – Type 2).

Again, the most basic alternative configuration proposed for the RBS consists of a single pressure transmitter, simplex logic unit (PLC) and a single block valve (with its associated solenoid valve). This configuration is shown in Figure 3 and represented in Figure 5 as a block diagram. Many other configurations are possible and the ones selected for analysis in this paper are listed in Table 1.



Figure 5 - Alternative SIF A-1

Table 1 – Alternative Configurations Analyzed in this Work

Alternative	Initiator	Logic	Actuator
SIF A-1	Pressure Transmitter (1oo1)	PLC (1oo1)	Type 1 Block Valve* (1oo1)
SIF B-1	Pressure Transmitter (1oo1)	hot standby PLC (1oo2)	Type 1 Block Valve* (1oo1)
SIF C-1	Pressure Transmitter (1oo1)	hot standby PLC (1oo2)	Type 1 Block Valve* (1oo2)
SIF D-1	Pressure Transmitter (1oo2)	hot standby PLC (1oo2)	Type 1 Block Valve* (1oo2)
SIF E-1	Pressure Transmitter (2oo3)	hot standby PLC (1oo2)	Type 1 Block Valve* (1oo2)
SIF A-2	Pressure Transmitter (1oo1)	PLC (1oo1)	Type 2 Block Valve** (1oo1)
SIF B-2	Pressure Transmitter (1oo1)	hot standby PLC (1oo2)	Type 2 Block Valve** (1oo1)
SIF C-2	Pressure Transmitter (1oo1)	hot standby PLC (1oo2)	Type 2 Block Valve** (1oo2)
SIF D-2	Pressure Transmitter (1oo2)	hot standby PLC (1oo2)	Type 2 Block Valve** (1oo2)
SIF E-2	Pressure Transmitter (2oo3)	hot standby PLC (1oo2)	Type 2 Block Valve** (1oo2)

* Type 1 = Block Valve with solenoid

** Type 2 = Block Valve with positioner, which allows running partial tests without production downtime

4.3. Determination of the Maximum Proof-Test Interval for Each Configuration

The maximum proof test interval for each configuration was obtained using the various simplified PFD equations given in Part 6 of IEC 61508 (Ref. 1). Because the system must comply with SIL-3, the maximum proof test interval was obtained by equating the PFD to 10^{-3} which is the maximum value of the SIL-3 range, as shown in Figure 2.

Typical failure data for each component were obtained from Ref. 11 which includes the dangerous failure rate, λ_D ; the safe failure rate, λ_S ; the diagnostic coverage factor, DC; and the beta factor for undetected dangerous failures. The data used in the present analysis are shown in Table 2.

Typical Mean Time to Restoration values were obtained from Brazilian process industry experience (see Ref. 12) and are listed in Table 3: the Mean Time to Restoration (MTTR) for a dangerous failure detected at test, and the MTTR for a safe or spurious failure. In this paper, the MTTR is actually the average time until function restoration of

the failed component; channel or system after the failure is discovered. Table 3 also contains a column showing the actual acquisition cost in dollars for the purchase of each failed SIF component to be used in the subsequent LCC analysis.

Table 2 - Analysis Data – Source: SINTEF (Ref. 11)

Equipment	λ_D (/h)	λ_S (/h)	DC	β
Pressure Transmitter	0,80E-06	0,50E-06	0,60	0,03
Simplex PLC	1,00E-06	1,00E-06	0,90	0,02
Type 1 Valve	4,00E-06	4,60E-06	0,30	0,02
Type 2 Valve	2,70E-06	2,70E-06	0,25	0,02

Table 3 - Analysis Data – Source: Process Industry

Equipment	MTTR (h)	sp. MTTR (h)	Cost (US\$)
Pressure Transmitter	8	6	1,000
Simplex PLC	4	4	25,000*
Type 1 Block Valve (w solenoid)	24	5	15,000
Type 2 Valve (w PST)	24	5	20,000

*The estimated cost of a hot standby PLC is US\$ 40,000

In the evaluation of the PFD and the resulting maximum proof test interval for each configuration the following additional assumptions were adopted:

- For alternatives that use a Type 2 block valve (with PST capability), a partial test detection coefficient of **0.8** was considered for λ_D , meaning that 80% of the dangerous undetected failures are detected during partial tests of the component (in this case the block valves);
- The adopted frequency of partial testing for type 2 valve(s) is 15 days (**360 hours**).
- Values for β_D were taken as equal to 0.5β , that is, beta-factors for detected failure modes were taken as 50% of those of the corresponding undetected failure modes given in Table 2.

4.4. Lifecycle Cost Analysis of Alternative Configurations

The Lifecycle Cost Calculation (LCC) is a management tool that aims at minimizing costs and maximize yield for various types of systems. Determining the LCC is a method that allows comparing alternative solutions in terms of their total lifecycle cost rather than just comparing a part of their costs, such as their acquisition costs.

The LCC of any system is equivalent to its total cost during its whole life; however, the cost factors that must be considered in a lifecycle cost analysis may vary from one system to the other. In this work, the LCC is calculated according to equation 1:

$$\text{Lifecycle Cost} = \text{CAPEX} + \text{OPEX} + \text{RISKEX} \quad (1)$$

where **CAPEX** stands for Capital Expenditures, **OPEX** for Operating Expenditures and **RISKEX for** Risk Expenditures. In this analysis, CAPEX involves basically the acquisition of the equipment for each configuration, and OPEX represents the cost necessary to keep the system operating, which includes:

1. the expenses (human + material) incurred for the realization of tests and repairs of SIS components;
2. the production loss due to plant shutdown for periodic testing of SIS components (this value considers the minimum number of tests which must be carried out to keep the system operating and in compliance with SIL-3 Required (maximum proof test interval for each configuration)).

By its turn, RISKEX considers only the cost of losses pertaining 'spurious plant shutdown' due to spurious failures of SIS components. RISKEX could also consider the plant accident costs derived from SIS failures but were not considered here since all configurations must necessarily meet SIL 3 and therefore the plant accident rate is the same for all configurations (the PFD value for all configurations were taken at the maximum value of the Required SIL range as indicated before).

The second OPEX contribution listed above can be calculated by multiplying three factors: 1) the minimum number of tests for each configuration, 2) the number of hours necessary to restore production after a shutdown for test, and 3) the value of the production loss per hour of plant shutdown.

5. RESULTS

5.1 PFD Results and Maximum Proof Test Intervals

The PFD values for each configuration are shown in Table 4 for proof test intervals varying from 1 month to 5 years. They were calculated using the simplified equations given in Appendix B of Part 6 of IEC 61508 (Ref. 1), which were built into a special software (Ref. 13) developed by DNV – Det Norske Veritas for performing integrity/reliability analysis of functional safety systems.

In Table 4 is also shown the corresponding SIL attained by each configuration for each proof test interval. It can be seen that the simplest of all configurations (1001 + 1001 + 1001) cannot attain SIL-3 unless the test interval is made shorter than one month. Actually as shown below in Table 5, the maximum test interval for such a configuration is 555 hours. This would imply a total of 15.7 plant shutdowns per year for SIS testing, resulting on a tremendous operational cost.

Analyzing the results, one verifies that alternatives SIF D-2 and SIF E-2 offer the best results in terms of PFD and that they are very close to one another. The same reasoning is valid for alternatives SIF A-1 and SIF B-1, which present the poorest results in terms of PFD, and which are also quite close to one another.

Table 4 – Testing Intervals for each considered Alternative

Alternative		Test Interval						
		1 month	3 months	6 months	1 year	2 years	3 years	5 years
SIF A-1	PFD	1,27E-03	3,58E-03	7,16E-03	1,42E-02	2,83E-02	4,24E-02	7,06E-02
	SIL	SIL 2	SIL 2	SIL 2	SIL 1	SIL 1	SIL 1	SIL 1
SIF B-1	PFD	1,23E-03	3,47E-03	6,94E-03	1,38E-02	2,75E-02	4,11E-02	6,85E-02
	SIL	SIL 2	SIL 2	SIL 2	SIL 1	SIL 1	SIL 1	SIL 1
SIF C-1	PFD	1,46E-04	4,29E-04	8,86E-04	1,86E-03	4,10E-03	6,73E-03	1,32E-02
	SIL	SIL 3	SIL 3	SIL 3	SIL 2	SIL 2	SIL 2	SIL 1
SIF D-1	PFD	2,78E-05	8,77E-05	2,01E-04	4,98E-04	1,39E-03	2,67E-03	6,41E-03
	SIL	SIL 4	SIL 4	SIL 3	SIL 3	SIL 2	SIL 2	SIL 2
SIF E-1	PFD	2,78E-05	8,80E-05	2,02E-04	5,03E-04	1,41E-03	2,72E-03	6,54E-03
	SIL	SIL 4	SIL 4	SIL 3	SIL 3	SIL 2	SIL 2	SIL 2
SIF A-2	PFD	6,64E-04	1,26E-03	2,17E-03	3,98E-03	7,59E-03	1,12E-02	1,84E-02
	SIL	SIL 3	SIL 2	SIL 2	SIL 2	SIL 2	SIL 1	SIL 1
SIF B-2	PFD	6,25E-04	1,15E-03	1,96E-03	3,55E-03	6,73E-03	9,92E-03	1,63E-02
	SIL	SIL 3	SIL 2	SIL 2	SIL 2	SIL 2	SIL 2	SIL 1
SIF C-2	PFD	1,33E-04	3,71E-04	7,38E-04	1,47E-03	2,93E-03	4,39E-03	7,36E-03
	SIL	SIL 3	SIL 3	SIL 3	SIL 2	SIL 2	SIL 2	SIL 2
SIF D-2	PFD	1,46E-05	2,94E-05	5,30E-05	1,02E-04	2,11E-04	3,33E-04	6,18E-04
	SIL	SIL 4	SIL 4	SIL 4	SIL 3	SIL 3	SIL 3	SIL 3
SIF E-2	PFD	1,46E-05	2,98E-05	5,43E-05	1,07E-04	2,31E-04	3,78E-04	7,44E-04
	SIL	SIL 4	SIL 4	SIL 4	SIL 3	SIL 3	SIL 3	SIL 3

The maximum SIF testing interval that guarantees compliance to SIL 3 requirements, for each of the ten alternatives analyzed, is presented in Table 5. Shown on Table 6 are also the minimum number of plant shutdowns per year for each configuration.

It may be verified, by the results presented in Table 5, that the SIF D-2 and SIF E-2 alternatives are the ones that allow the largest total testing intervals observing SIL 3 requirement - approximately 7 and 6 years, respectively. Since those values are larger than the intervals between scheduled plant turnarounds, which according to company policy is done every 5 years, the maximum test period for those configurations were set at 5 years. The consequences of this assumption are analyzed later in this work. Table 6 presents this alteration, proposed for alternatives SIF D-2 and SIF E-2, renamed SIF D-2* and SIF E-2* from now on.

Table 5 - Testing Intervals for SIL 3 Requirement Compliance

Alternative	Max Interval between tests (hours)	Max Interval between tests (years)	Max amount stops/year
SIF A-1	555	0.063	15.783
SIF B-1	575	0.066	15.235
SIF C-1	4914	0.561	1.783
SIF D-1	14158	1.616	0.619
SIF E-1	14036	1.602	0.624
SIF A-2	1535	0.175	5.707
SIF B-2	1753	0.200	4.998
SIF C-2	5957	0.680	1.471
SIF D-2	63345	7.231	0.138
SIF E-2	54004	6.165	0.162

Table 6 – Maximum Proof Test Intervals Considering the Scheduled Plant Turnarounds

Alternative	Maximum Interval between tests (hours)	Maximum Interval between tests (years)	Minimum number of plant stops/year
SIF D-2*	43800	5,000	0,200
SIF E-2*	43800	5,000	0,200

5.2 Results of the Lifecycle Cost (LCC) Analysis

The CAPEX values of each configuration are shown in Figure 6 below, having been calculated with the data presented in Table 3. Likewise, OPEX and RISKE X values for each alternative are presented in Figures 7 and 8 below.

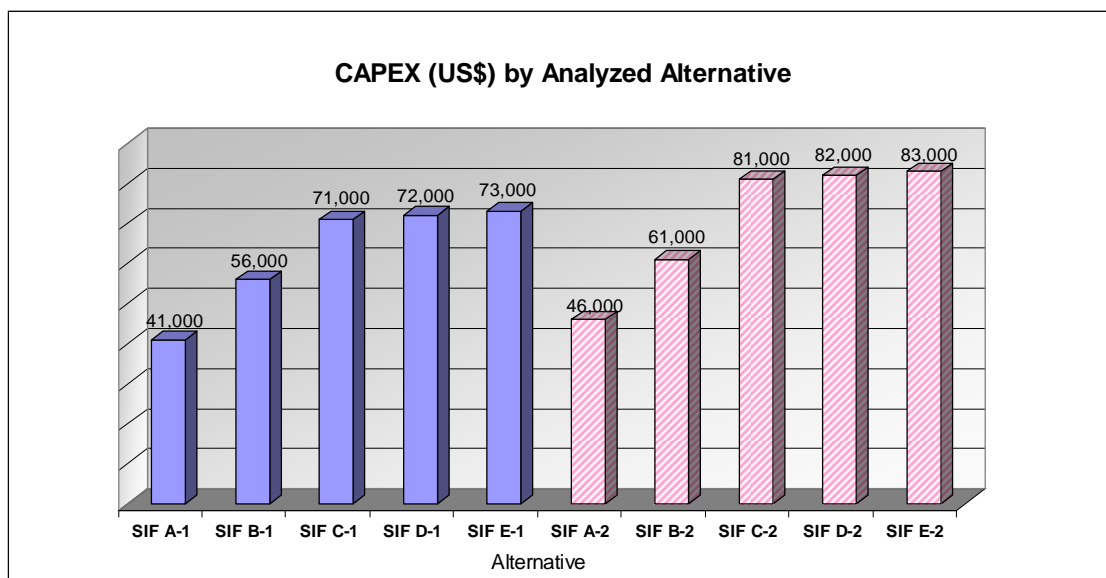


Figure 6 - CAPEX (in US\$) by Analyzed Alternative

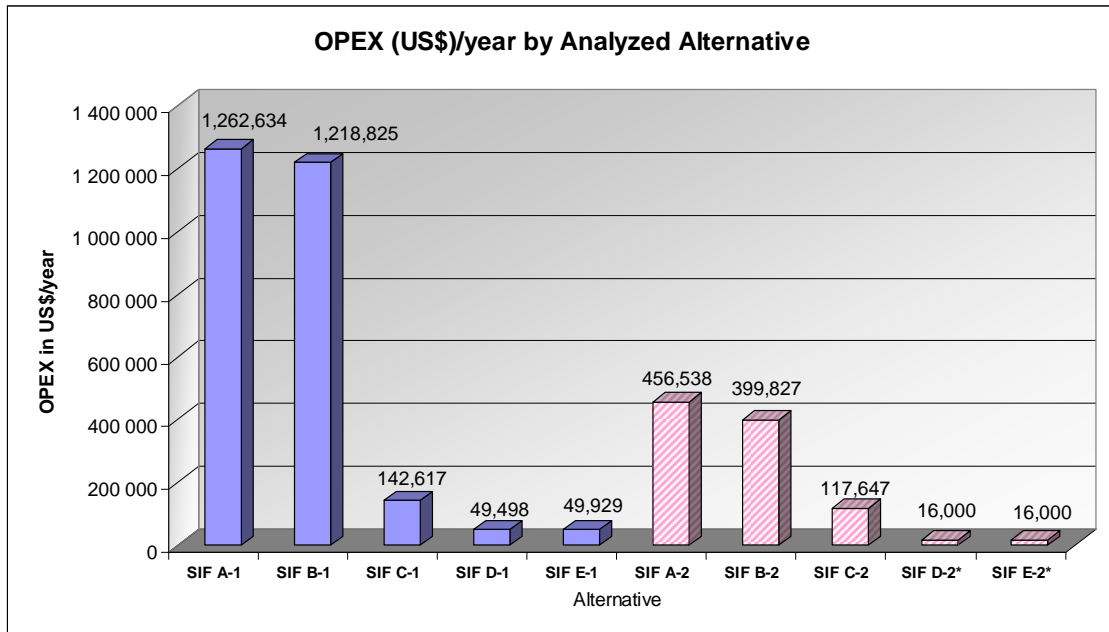


Figure 7 - OPEX (in US\$) by Analyzed Alternative

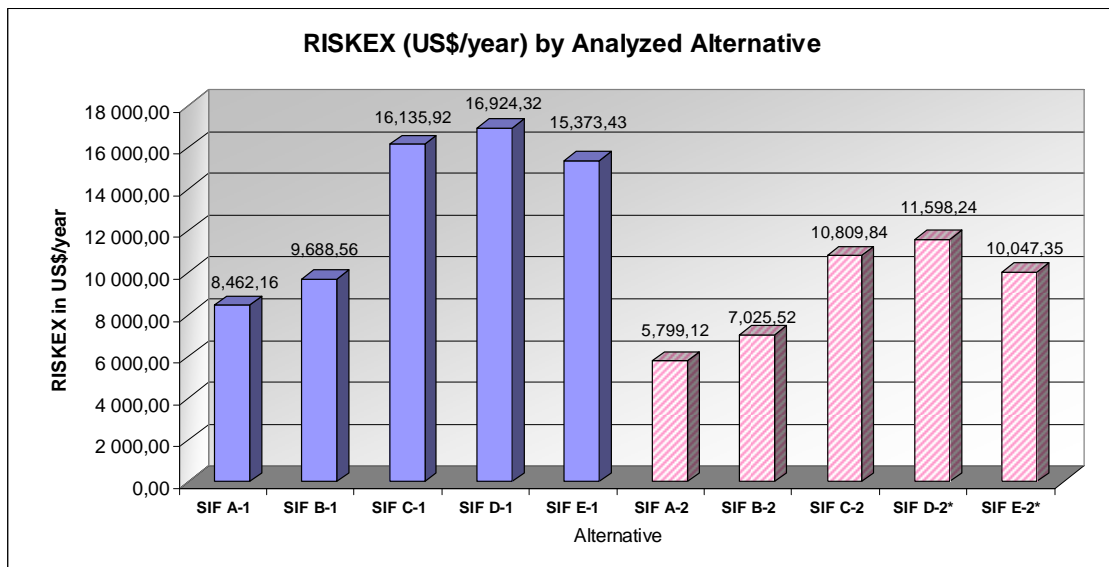


Figure 8 - RISKEX (in US\$) for Analyzed Alternative

It may be verified from the results presented in Figure 6 that, as expected, the greater the system redundancy, the greater the CAPEX value will be for that configuration, as this is a direct reflection of the number of components in the configuration and its increased complexity. Thus, it follows naturally those configurations SIF E-1 and SIF E-2 are the ones that present the highest equipment acquisition costs and consequently the highest CAPEX.

As to the OPEX, from the results in Figure 7 one notices that the annual operational costs for alternatives SIF A-1 to SIF E-1 are, respectively, quite above the values for the annual operational costs of alternatives SIF A-2 to SIF E-2, respectively. This result is justified by the fact that configurations involving type 1 block valves require a higher number of plant shutdowns for testing than those with Type 2 block valves (with PST). Therefore, the configurations that present the least OPEX are SIF D-2 and E-2. The alternative that presents the highest operational cost is the one that requires the largest amount of annual tests, in other words, with the highest probability of failure on demand, in this case, SIF A-1, which is the one with the simplest configuration in terms of redundancy.

As shown in Figure 8, RISKEK values bear a direct relation to the complexity of the configurations. This trend is only reversed for the last configurations (SIF E-1 and SIF E-2* with respect to SIF D-1 and SIF D-2*) because the introduction of 2oo3-type redundancy result in less spurious failures by the initiator subsystem as compared to those resulting from the 1oo2-type redundancy in the D-1 and D-2* configurations.

Since CAPEX is typically expressed as Net Present Value whilst OPEX and RISKEK are annualized values, to obtain a correct LCC value, the three parcels must be expressed on the same time basis, in this case, as Net Present Values. The conversion from annualized to NPV estimates consider the period of useful life, and an interest rate that reflects the cost of capital in the market. Typical values for the present Brazilian economy were used as indicated below.

The usual NPV Equation 2 was used, where "A" represents the annual value, "i" the interest rate (at 12% per year) and "n" the facility's useful life period, assumed to be 30 years (a typical value in the process industry):

$$P = A \frac{(1+i)^n - 1}{i(1+i)^n} \quad (2)$$

where:

- P = Net Present Value (dollars);
- A = annualized value (dollars / year);
- i = annual interest rate; and
- n = period of time, in years (usually the facility's expected useful life).

The three contributions and the resulting LCC value, expressed as NPV are numerically shown in Table 7 and graphically presented in Figure 9 (only the LCC value).

Table 7 - Lifecycle Cost for each Analyzed Configuration Expressed as NPV

Alternative	CAPEX (US\$)	OPEX (US\$)	RISKEK (US\$)	Lifecycle Cost (US\$)
SIF A-1	41.000	10.170.753	68.164	10.279.917
SIF B-1	56.000	9.817.860	78.043	9.951.903
SIF C-1	71.000	1.148.804	129.978	1.349.782
SIF D-1	72.000	398.712	136.329	607.041

Alternative	CAPEX (US\$)	OPEX (US\$)	RISKEX (US\$)	Lifecycle Cost (US\$)
SIF E-1	73.000	402.184	123.836	599.020
SIF A-2	46.000	3.677.500	46.713	3.770.213
SIF B-2	61.000	3.220.676	56.592	3.338.268
SIF C-2	81.000	947.667	87.075	1.115.742
SIF D-2*	82.000	89.116	93.426	304.309
SIF E-2*	83.000	104.531	80.933	292.816

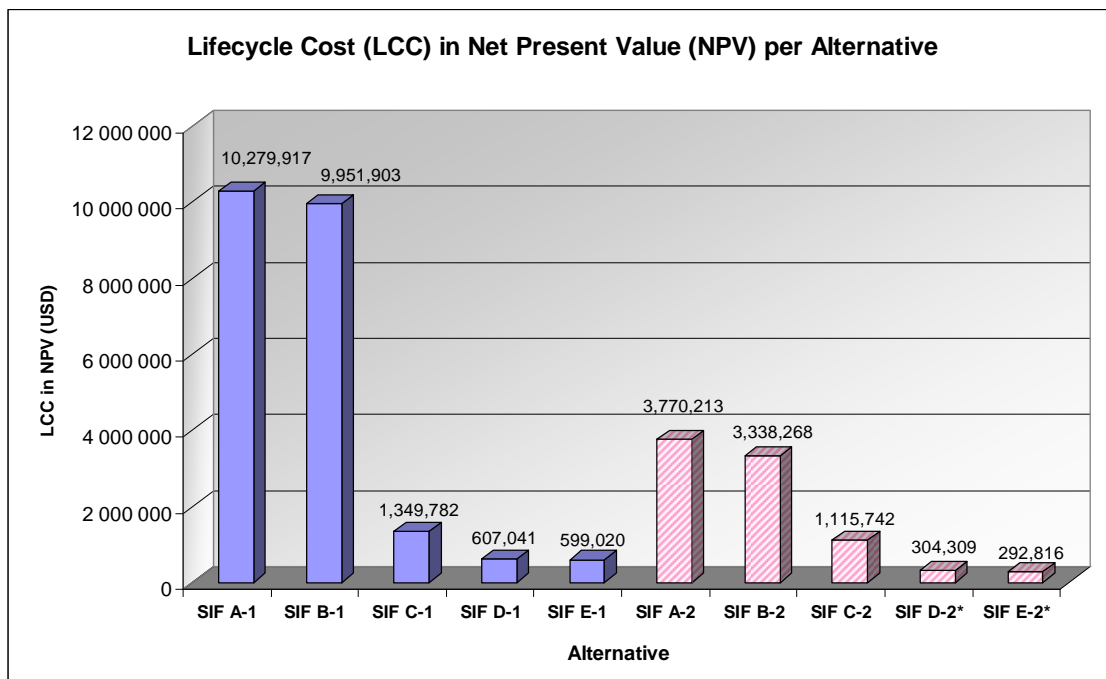


Figure 9 - Lifecycle Cost (in Net Present Value) per Alternative

From the results shown in Table 7 and visualized in Figure 9, it is possible to verify that the configuration that complies with SIL-3 and at the same time presents the lowest lifecycle cost is SIF E-2*. Despite having the highest CAPEX, its very low OPEX more than compensate for the higher acquisition cost when the overall LCC is compared with the other configurations. Its low OPEX value is a direct result of the combination of three factors: 1) its higher level of dependency which by itself allows for a lengthier interval between tests, thus reducing the number of costly plant shutdowns, 2) the partial-stroke testing capability of its actuators elements, by itself also a strong contributor to the reduction of plant shutdowns for SIS testing, and 3) the 2oo3-type redundancy for the actuators RISKEX value to be lower than that of the D-2* configuration.

The second lowest LCC value is that of the SIF D-2* configuration, whose only difference to the SIF E-2* is the 1oo2-type redundancy of the initiators. con to it comes configuration SIF D-2*.

In general, it can be said that even if one could meet SIL-3 with a low redundancy configuration, by testing more often, that would not be the best solution by a large

margin. The low CAPEX of this type of solution would be more than offset by its extremely high OPEX. Of course, this depends very much on the lost production cost per plant shutdown which is typically very high for most petrochemical plant applications.

The results in Figure 9 also shows that the introduction of emergency blocking valves with partial-stroke testing capability may have a dramatic impact in the LCC values of the SIS. By significantly reducing the number of needed annual plant shutdowns for testing, they may bring about a very important reduction in the OPEX value. The consequence here again are that their much lower operational costs may more than offset their higher acquisition costs. They are definitively an option to consider when specifying SIS that depend on emergency blocking.

It must be pointed out that the LCCs of alternatives SIF D-2* and SIF E-2* were calculated with 5-year test intervals due to the limitation imposed by the facility turnaround policy (every 5 years). The LCC values for these alternatives would be even lower if they had been calculated taking their maximum test interval periods required for SIL 3 compliance, approximately 6 and 7 years, respectively. That would only further corroborate the results of this work.

5.3 Results of Sensitivity Analysis

To examine the robustness of the conclusions presented in the preceding section with respect to variations in the values of key parameters, sensitivity analysis were performed for the following parameters:

1. the partial-test detection coefficient, assumed to be equal to 0.80 in the LCC calculations;
2. the acquisition cost of the block valve with PST capability (Type-2 valves), estimated to be US\$20,000 each in the LCC calculations, and
3. the interval between partial tests of the Type-2 block valves, considered to be of 15 days (360 hours).

Results of the sensitivity analysis for the partial-test detection coefficient showed that even for a value of 0.69, the configuration SIF E-2 would still comply with SIL-3 for a total-test period of five years (used in the LCC calculations). Therefore up to this value there would not be any change in the final results of the LCC calculation and therefore all conclusions would remain absolutely the same. For values below 0.69, the maximum proof-test interval would be less than 5 years and that would start imposing higher OPEX contributions with the consequent increase of the LCC costs of that configuration. Results showed that even for values as low as 0.5, the SIF E-2 configuration would still be the solution with the least LCC value.

Results of the sensitivity analysis for the acquisition cost of the block valve with PST capability are shown in Figure 10, where it can be seen that only if the referred cost were US\$180,000 (instead of the US\$20,000 used in the LCC calculations), the overall LCC value of the SIF E-2* configuration would reach the same value as the LCC of the SIF E-1 configuration.

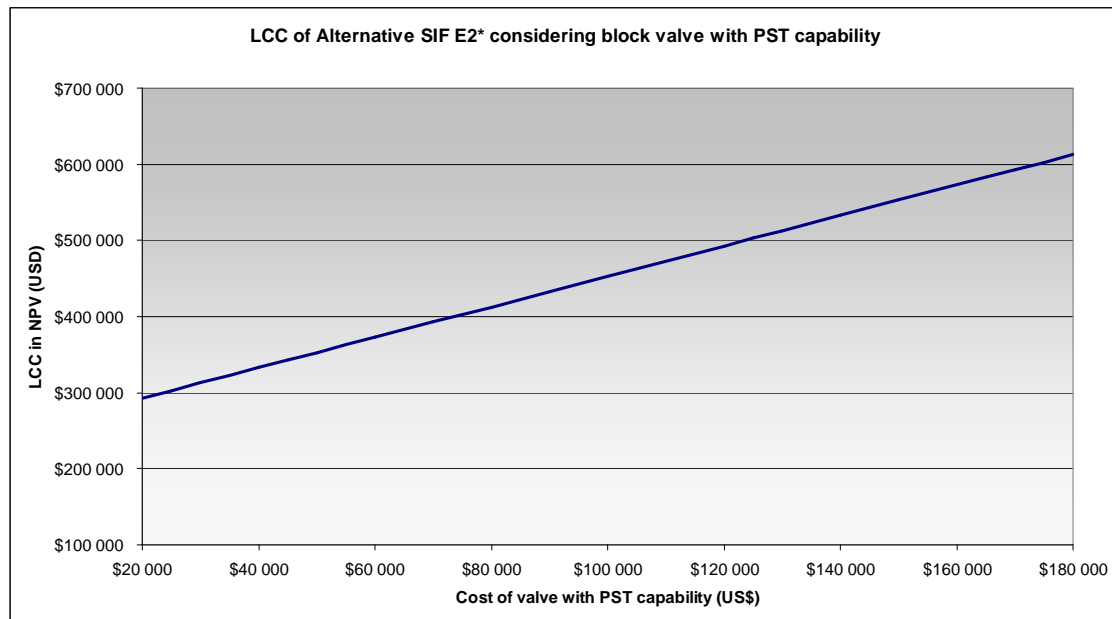


Figure 10 - LCC of Alternative SIF E2* considering block valve with PST capability

With respect to the interval between partial tests, results from the sensitivity analysis showed even if those partial tests were performed every 9 months (instead of every 15 days as assumed in the LCC calculations), configuration SIF E-2* would still comply with SIL-3 for a complete-test interval of five years. This means that the calculated results would remain absolutely the same within this very large range of variation of this parameter.

6. FINAL COMMENTS

This paper presented the application of a method for selection among various hardware configurations (or architectures) of Safety Instrumented Systems (SIS) that comply with a Required SIL value for a desired safety function. The selection logic is based on the least Lifecycle Cost ($LCC = CAPEX + OPEX + RISKE X$) of the configurations.

The Configuration Selection Method presented here goes beyond the analytical methods presented in IEC 61508/61511 for determination of Required SIL and its analytical/numerical verification. It nicely complements them when the analyst is faced with a variety of choices of hardware configurations that can meet the Required SIL value by adopting different proof test intervals. The proposed method considers that the easiest and most economical way of starting to solve the problem is by taking the maximum possible proof-test interval for each configuration that still allows it to comply with the Required SIL value. Variations of this assumption can be adopted but were not explored in this paper.

The results obtained for the practical case studied in this paper demonstrate that there may be large potential for reduction and optimization of lifecycle costs of the facility safety system. The lifecycle costs of the most efficient alternative are about 97% lower than those of the simplest configuration (the least redundant and with least CAPEX cost).

It was also demonstrated by the results of this work that the highest contribution to the lifecycle cost of the alternatives pertain the OPEX, due to the high costs of plant shutdowns required for SIS testing to guarantee compliance with the Required SIL. This result supports the conclusion that, in cases similar to the one studied here (high required SIL and high shutdown costs), investments in the acquisition of equipment that allows a lower amount of shutdowns for safety system testing is very advantageous. This was particularly well demonstrated for the use of block valves that offer partial-stroke test capability.

It is worth mentioning that considerations related to the architectural constraints imposed by the IEC Standards (Refs. 1 and 2) may have an impact on the results of this work. This may be even more important if some of the components are Type B as defined by the Standards (as may be the case of the PST valves), for those are subject to more restrictive constraints. The influence of such constraints on the configuration selection results were not investigated in this paper.

7. REFERENCES

1. IEC (International Electrotechnical Commission), *Functional Safety of Electrical/Electronic-/Programmable Electronic Safety-Related Systems*, IEC 61508, 1st edition, 1998.
2. IEC (International Electrotechnical Commission), *Functional Safety – Safety Instrumented Systems for the Process Industry Sector*, IEC 61511, 1st edition, 2003.
3. ANSI/API-521, *Guide for Pressure Relieving and Depressuring Systems*, API - American Petroleum Institute, USA, 1997.
4. ASME, *Code Case 2211 of ASME - Section VIII*, ASME - American Society of Mechanical Engineers, USA, 1996.
5. SUMMERS, A., *Flare Load Mitigation with High Integrity Protection Systems*, presented at ISA Expo-2003.
6. COCKMAN, R., ESD Valve Testing, ICS Triplex Trusted Application Note, June 2003.
7. RYIAZ, A., and GOBBLE, W., *Smart Positioners to Predict Health of ESD Valves*, presented at the 59th Annual Instrumentation Symposium for the Process Industries, Texas A&M Univ. College Station, Texas, Jan. 20-22, 2004.
8. RAMACHANDRAN, G., Valve Ranking and Partial Stroke Testing, presented at ISA AUTOMATION WEST, 2004.
9. KNEGTERING, B., *Safety-PLC's Striking Role for Partial Valve Stroke Testing*, Presented at ISA 2004 Houston Technical Conference.
10. BINGHAM, K., Partial Stroke Testing of Emergency Shutdown Valves, Process West, Summer 2005.
11. SINTEF, *Reliability Data for Safety Instrumented Systems – PDS data handbook*, 2006 edition.
12. CHAME, L.M., *Reliability of Safety Instrumented Systems: Cost-Benefit Analysis of Alternatives for Compliance with Required SIL in Industrial Installations*, MS Dissertation, Universidade Federal do Rio de Janeiro, 2007 (in Portuguese).
13. CHAME, L.M., & OLIVEIRA, L.F.S., *ORBIT SIL User's Guide and Technical Manual*, Revision 1, Det Norske Veritas, Rio de Janeiro, 2007.