Seventh International Conference on Control, Automation,
Robotics And Vision (ICARCV'02), Dec 2002, Singapore

# Introduction to the Risk based design of Safety Instrumented Systems for the process industry

**Jan A.M. Wiegerinck**
Senior Consultant Instrumentation and Plant Automation
Shell Global Solutions, The Hague, Netherlands
E-mail: jan.a.m.wiegerinck@opc.shell.com

## 1 Abstract

This paper introduces issues related to the design of safety-instrumented systems (SIS) using a risk-based approach. The paper does not aspire to give an exhaustive guidance to actually designing such systems. The design and realisation of safety systems is a highly specialised skill, this paper only aims to introduce the various concepts and terminologies to the reader.

Ever since the IEC 61508 was being drafted, the risk based design as opposed to deterministic designs, is becoming more and more accepted. Since the publication of ISA/ANSI SP84.01 and later IEC 61508, authorities started to require compliance or at least regard compliance as the best practice to compliance with authority regulations with regards to the design and maintenance of safety systems that use instruments to perform the functions. E.g. OSHA [1] regards ISA/ANSI SP84.01 as the benchmark for compliance to their 29 CFR 1910.119. Authorities in Europe regard compliance to IEC 61508/61511 as benchmark for compliance to the Seveso 2 directive.

Risk based design of safety instrumented systems (SIS) aims to establish the risk reduction that the SIS is to provide to arrive at an acceptable or at least tolerable remaining risk. If the risk without the SIS is already acceptable, no SIS would be required. If the initial risk without SIS is high, the risk reduction factor needs to be high and hence the integrity requirements for the SIS are high.

This paper outlines how initial risks are established, how integrity requirements for SIS are defined and how those requirements are achieved both in the SIS design and in the life-cycle management.

## 2 Introduction

The initial risk (without risk reduction measures) associated with operating a process unit or a piece of equipment, may be reduced by applying a range of risk reduction measures, including SISs. As shown in Figure 1, the summed contribution of reductions from all risk reduction measures must bring the remaining or residual risk to a level below the acceptable or tolerable level (defined by corporate risk tolerability criteria).
As shown, reduction is usually achieved using a number of means, including mechanical devices (relief valves, bursting discs, etc.) and instrumented devices (SIS). In most designs, both types of protection systems are applied, with the mechanical system being usually the last line of defence wherever possible.
An SIS is required if the summed contributions of all non-SIS risk reduction measures does not reduce risks below the acceptable or tolerable level. If the risk, without the SIS, is already acceptable, the SIS is not required.
The allocation of risk reduction to layers of protection (including SISs) is done via proper design practice verified by a Technical Desk HSE Review, HAZOP or PHA study.

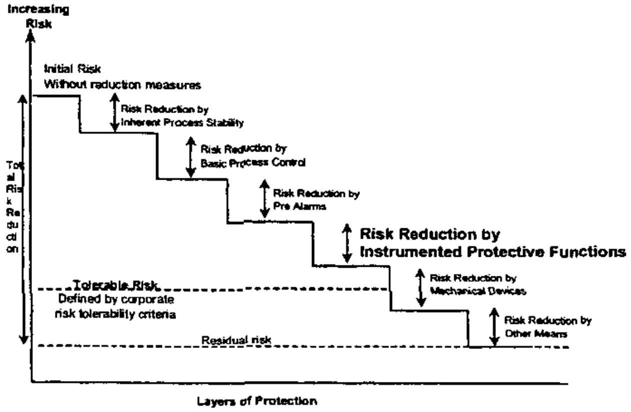


Figure 1, Risk Reduction by Layers of Protection

Shell is currently busy to further improve their existing 'IPF' method (Instrumented Protective Functions Classification) to provides a methodology that includes a Layers of Protection Analysis (LOPA), consequence questionnaires, means to establish if a SIS is 'As Low As Reasonably Practical' (ALARP) and means to

[1] Occupational Health & Safety Authority (USA)

design and verify the designed SIS to see if the integrity requirements are met. This new SIL assessment and SIS design method and tool has been dubbed 'SIFpro™'.

## 3 Objectives of a safety instrumented system

The IEC 61511 defines a safety function (for the process industry) as: "function to be implemented by a SIS, other technology safety-related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event"
However depending on the severity of the hazardous event and the probability of occurrence, one will install a safety function with a high integrity (very low chance of failure) for highly hazardous events and with a low integrity for less hazardous events. This concept of designing a safety system depending on the severity and probability of the hazards (= risk) is referred to as a 'risk based design'.

The above concept is visualised in Figure 2, severity, probability and risk

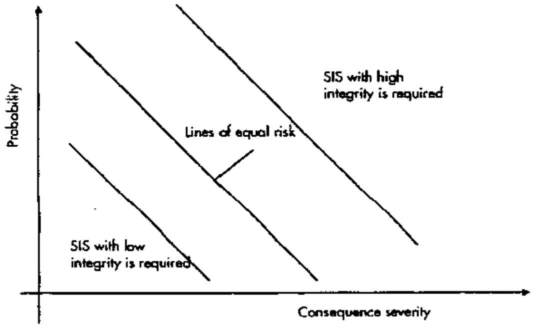


Figure 2, severity, probability and risk

Because any safety function has a certain (low) probability of failure on demand, the safety function actually only reduces the probability of the consequences actually occurring. I.e. the safety function only reduces the risk (probability * consequences) and never completely eliminates the risk. It would be sufficient to reduce the risk to an acceptable level, where the society and corporate standards formulate what risks would still be acceptable.

Therefore the objectives of a SIS may be defined as "to reduce the frequency at which a hazard may occur to an acceptable or at least a tolerable level". E.g. A furnace without an automatic fuel cut-off in the event of a flame-out, may explode every 10 years leading to the possible loss of one live. If it is assumed that only in less than 10% of the time the operator is in the vicinity of the furnance, the initial risk may be put at one casualty every 100 years. If the company has set the target at less than 1 casualty every 10,000 years, the risk associated with operating the furnace has to be reduced further. The risk reducing alternative of choice in this case would be to install a flame eye that automatically closes fuel supply. This SIS would need to reduce the risk by a factor 100.

Some safety functions do not reduce the probability of the consequences. Instead the consequences are reduced. E.g. a fire detection system cannot prevent the fire to occur. So the frequency at which the fire occurs is not reduced. Instead the consequences of the initial detected fire are mitigated by e.g. activating the automatic sprinkler system.

The concept of risk reduction by (preventing or mitigating) safety functions is visualised in Figure 3.

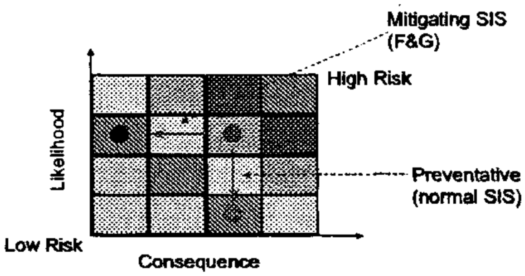


Figure 3, Risk reduction by safety functions

### 3.1 ALARP concept

In assessing the initial risk one should determine if (from IEC 61511 part 3 Annex B [1] ):
a) the risk is so great that it is refused altogether; or
b) the risk is, or has been made, so small as to be insignificant; or
c) the risk falls between the two states specified in a) and b) above and has been reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction.

With respect to c), the ALARP principle recommends that risks be reduced "so far as is reasonably practicable," or to a level which is "as low as reasonably practicable" (these last 5 words form the acronym 'ALARP'). If a risk falls between the two extremes (i.e., the unacceptable region and broadly acceptable region) and the ALARP principle has been applied, then the resulting risk is the tolerable risk for that specific application. According to this approach, a risk is considered to fall into one of 3 regions classified as

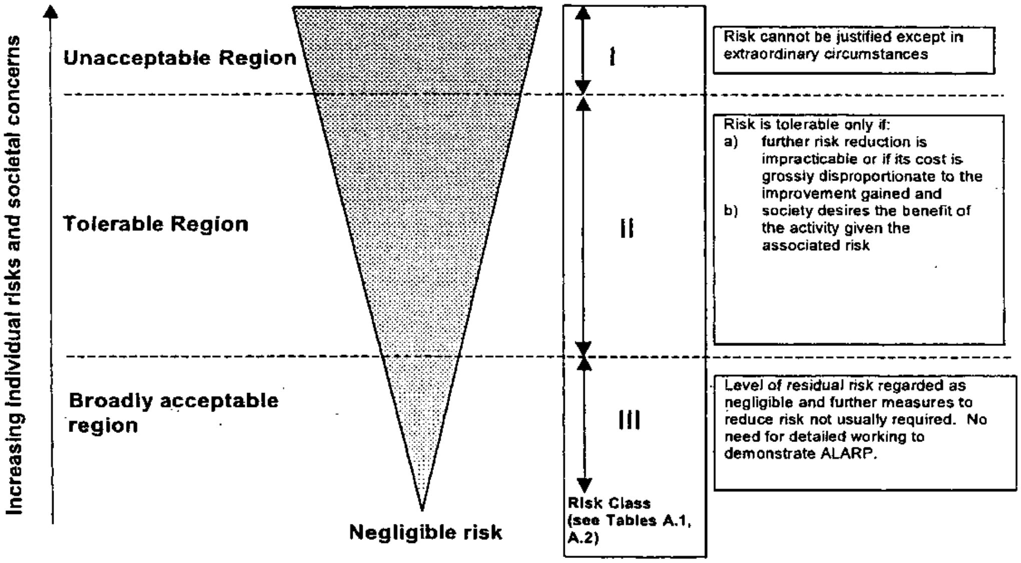

Increasing individual risks and societal concerns
Unacceptable Region
Tolerable Region
Broadly acceptable region
Negligible risk
I
II
III
Risk Class (see Tables A.1, A.2)
Risk cannot be justified except in extraordinary circumstances
Risk is tolerable only if:
a) further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained and
b) society desires the benefit of the activity given the associated risk
Level of residual risk regarded as negligible and further measures to reduce risk not usually required. No need for detailed working to demonstrate ALARP.

Figure 4, Tolerable risk & ALARP

“unacceptable”, “tolerable” or “broadly acceptable” (see Figure 4).

Above a certain level, a risk is regarded as unacceptable. Such a risk cannot be justified in any ordinary circumstances. If such a risk exists it must be reduced so that it falls in either the “tolerable” or “broadly acceptable” regions, or the associated hazard must be eliminated.
Below that level, a risk is considered to be “tolerable” provided that it has been reduced to the point where the benefit gained from further risk reduction is outweighed by the cost of achieving that risk reduction, and provided that generally accepted standards have been applied towards the control of the risk. The higher the risk, the more would be expected to be spent to reduce it. A risk that has been reduced in this way is considered to have been reduced to a level that is as “low as is reasonably practicable” (ALARP)

Below the tolerable region, the levels of risk are regarded as so insignificant that further improvements are not required. This is the broadly acceptable region where the risks are small in comparison with the every day risks we all experience. While in the broadly acceptable region, there is no need for a detailed working to demonstrate ALARP; however, it is necessary to remain vigilant to ensure that the risk remains at this level.

When determining if a safety system is ALARP the following aspects are normally taken into account:

- The initial investment cost and depreciation of additional measures or systems
- The additional yearly maintenance, managerial and inspection costs.
- The new risks introduced by the additional measures. E.g. additional safety functions will lead to additional spurious trips causing production and product losses and the additional safety risk associated with a re-start.
- The additional risk reduction achieved by the additional measures

## 4 Layers of protection

The application of multiple protection layers to safeguard a process is often used In the process industries. It is illustrated in Figure 5.

In this figure, each protection layer consists of physical properties, equipment and/or administrative controls that function in concert with other protection layers to control and/or mitigate process risk.

When determining the initial risk without the SIS, all available protection layers are taken into account. If the initial risk is already broadly acceptable, no SIS would be required.

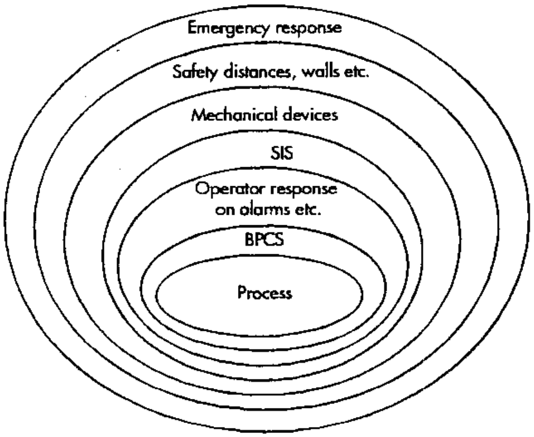

Emergency response
Safety distances, walls etc.
Mechanical devices
SIS
Operator response on alarms etc.
BPCS
Process

Figure 5, Protection layers, the "onion" model

If the initial risk were in the tolerable region (see Figure 4), one would normally install a safety function unless it can be demonstrated that any SIS would not be justified by the additional risk reduction gained. If this is the case one needs to demonstrate that the initial risk is ALARP. If the initial risk is in the intolerable region additional risk reduction measures are required. Often the installation of a SIS is the risk-reducing alternative (RRA) of choice.

## 5 Analysis of the layers of protection (LOPA)

To establish the need for and the amount of additional (in addition to the layers already available or designed) risk reduction required, a widely accepted technique is the 'layer of protection analysis' (LOPA).

LOPA is an acknowledged and proven methodology of ensuring that "Safety Instrument Functions" (SIF) are classified properly – their requisite performance is sufficient to assure that corporate risk criteria is successfully met when called upon to do so. The LOPA method applied by Shell is compliant with International draft Standard IEC 61511. The methodology is finding increased use by both the US and international refining and petrochemicals communities. This implementation of the methodology also has the additional benefit of being compatible with any customer's risk criteria.

Shell Global Solutions is currently developing a software tool (SIFpro™) that employs a form of LOPA to carry out a simplified risk assessment that is standardized to a set of rules. LOPA typically uses order of magnitude categories for cause frequency, consequence severity, and the likelihood of failure of independent protection layers (IPLs) or safeguarding barriers to determine an approximation of risk of a hazardous scenario. LOPA is an analysis tool that typically builds on the information uncovered during a qualitative hazard evaluation, such as hazard and operability studies (HAZOPs).

Like many other hazard analysis methods, one primary purpose of LOPA is to determine if there are sufficient layers of defence against an accident scenario. Depending on the process complexity and potential severity of an accident, a scenario may require one or many layers of defence. For a given scenario, only one layer must work successfully for the consequence to be prevented. However, since we know that no layer is perfect, we must layer sufficient defences so that we are convinced the risk of the accident is tolerable.

LOPA provides a consistent basis for judging if there are sufficient IPLs to control the risk of an accident for a scenario. If the estimate risk of a scenario is not tolerable, the customer may wish to add IPLs. LOPA does not suggest which IPLs to add, but it helps judge between alternatives for risk mitigation. LOPA is not a fully quantitative risk assessment approach, but is rather a simplified method for assessing the value of protection layers for a well-defined accident scenario.

The primary output of LOPA is the establishment of a Safety Integrity Level (SIL) for each SIF that is commensurate with the risk of a hazardous scenario

A brief description of LOPA follows:

A HAZOP or HEMP team defines a hazardous scenario. The scenario is basically the sequence of events between an initiator of the scenario (an equipment failure for example) that may ultimately lead to a significant consequence if all safeguarding barriers fail or are defeated. Pictorially, the LOPA analysis is given in the following picture.

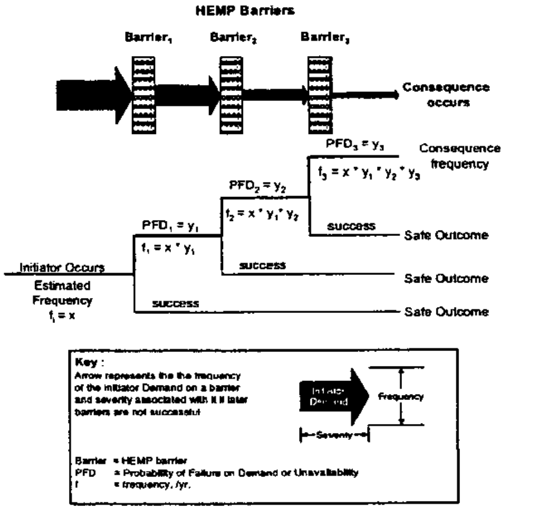


Figure 6, layers of protection analysis

Each barrier has a certain 'probability of failure on demand' (PFD). If there is a demand on a barrier it will normally be successful in preventing the consequences. Only in case of failure on demand, the consequences will occur. The frequency at which the consequences occur in case of failure of the barrier is equal to the PFD of the barrier * the frequency of demand on the barrier.

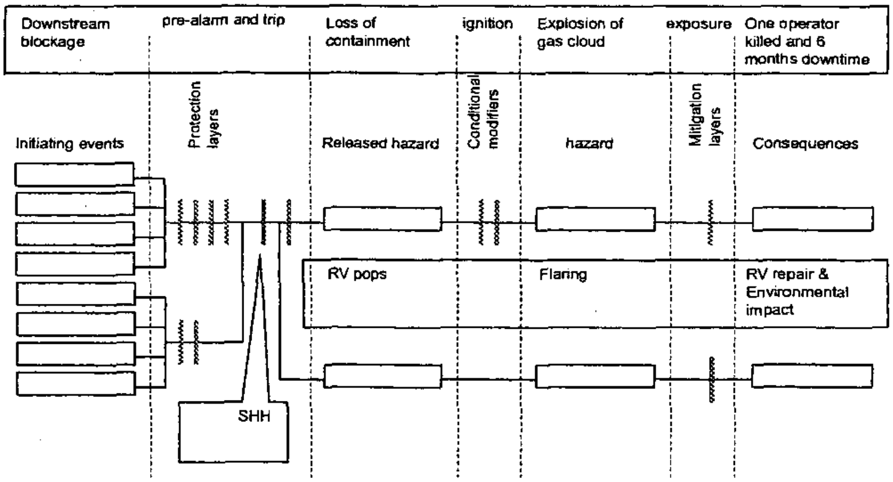


Figure 7, Example LOPA analysis as applied in SIFpro™

If the barriers are completely independent one may calculate the frequency at which the consequences occur, by multiplying the PFD's of the barriers in the path from the initiating event to the occurrence of the consequences.

When Barrier3 is a SIS and the residual risk (the product of the demand rate on the barrier and the severity of the consequence of barrier failure) is intolerable to the customer, the PFD of Barrier3 can be improved by increasing the integrity requirements of the SIS.

## 6 Determining the Safety Integrity Level (SIL) of the safety function

In accordance with IEC 61508 and IEC 61511 the integrity requirements for safety functions are expressed as the Safety Integrity level as follows:-

Table 1, Safety Integrity Levels, PFD and risk reduction

| Safety Integrity Level | Probability of Failure on Demand (PFD) | Risk Reduction factor (RR) |
|---|---|---|
| SIL - | PFD > 0.1 | < 10 |
| SIL 1 | 0.01< PFD < 0.1 | 100 > RR > 10 |
| SIL 2 | 0.001< PFD < 0.01 | 1000 > RR > 100 |
| SIL 3 | 0.0001< PFD < 0.001 | 10000 > RR > 1000 |
| SIL 4 | PFD < 0.0001 | RR > 10000 |

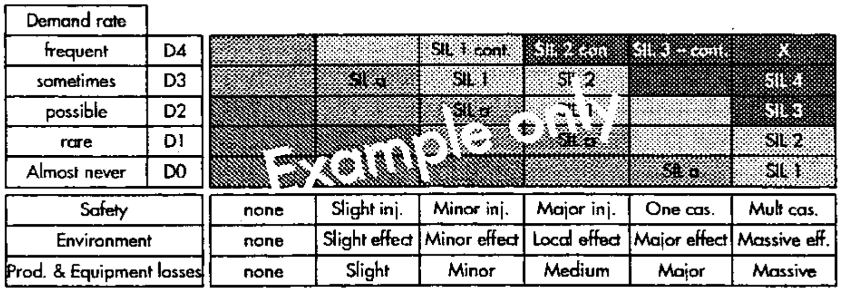
There are various methods available and described in IEC 61511 part 3:-

- Semi qualitative method
- Safety Layer matrix method
- Semi qualitative method – calibrated risk graph
- qualitative method –risk graph

Shell currently uses the semi qualitative method using a calibrated risk matrix. Shell is developing a more advanced method (SIFpro™) where LOPA is used to determine the initial probability (frequency) of occurrence of the consequences of the hazard and a calibrated risk matrix to determine the SIL required to achieve a broadly acceptable remaining risk.

Often a process design already includes the sensors and final elements that should bring the process to a safe state in any foreseen situation. This SIS design is often copied from a previous project.
In that case the SIL assessment would be done in the following steps

1. Select a sensor and define the hazard detected by the sensor
2. Determine if other sensors also detect the same hazard
3. Determine the initiating events and the layers of protection. This leads to the 'demand rate' on the safety function. See Figure 7 for an example LOPA analysis in SIFpro™.
   The demand rate used in step 5 is the frequency at which the consequence occur if the PSHG function were not present.
4. Determine the consequence of failure on demand of the function, i.e. determine the severity of the consequences.
5. Use the risk matrix to determine the SIL required to achieve an acceptable remaining risk.
   See Figure 8 for an example of the risk matrix as used by Shell for SIL assessments.
6. In case the SIL can not practically be achieved or only at great expenditure, determine which –



| Demand rate | | | | | | | |
|---|---|---|---|---|---|---|---|
| frequent | D4 | | | SIL 1 cont | SIL 2 con | SIL 3 – cont. | X |
| sometimes | D3 | | SIL a | SIL 1 | SIL 2 | | SIL 4 |
| possible | D2 | | | SIL a | SIL 1 | | SIL 3 |
| rare | D1 | | | | SIL a | | SIL 2 |
| Almost never | D0 | | | | | SIL a | SIL 1 |
| Safety | | none | Slight inj. | Minor inj. | Major inj. | One cas. | Mult cas. |
| Environment | | none | Slight effect | Minor effect | Local effect | Major effect | Massive eff. |
| Prod. & Equipment losses | | none | Slight | Minor | Medium | Major | Massive |

Figure 8, Semi qualitative Risk Assessment Matrix as used by Shell

lower- SIL is ALARP by analysing all alternative designs that at least would reduce the risk to a tolerable level.

As can be seen in Figure 8, Shell uses.3 consequence categories to establish the consequence severity:

- Personal safety
- Environment
- Production and equipment losses (i.e. dollars)

## 7 Process Safety Time

The process safety time is the period of time in which the process can be operated without protection and with a Demand present without entering a dangerous condition. The Process Safety Time determines the dynamic response requirements of the safety function.

During SIL assessment, the process safety time for each safety function should be determined. As shown in Figure 9, the process safety time is a function of the process dynamics and is defined as the period of time that the process can be operated without protection and with a demand present without entering a dangerous condition. The process safety time will determine the trip setting and the combined dynamic performance and accuracy requirements for the components in the SIS,

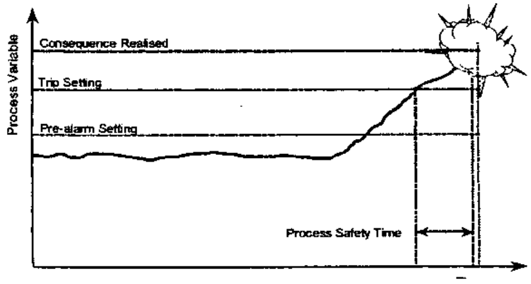


Figure 9, Process Safety Time

e.g., process measurement delay, time between input state change and output state change in the SIS and valve stroke time.

E.g. a process pressure trip is set at 150 kPa. The consequences of overpressure will not be fully realised until the pressure rises to 170 kPa. Given the dynamics of the process and the causes of the overpressure, this will take at least 2 minutes. The process safety time is 2 minutes.

Note that in some cases the consequences may also be realised when the variable does not continue to rise above the trip setting but remains too high for a long period (e.g. accelerated coke formation in furnace tubes above the outlet temperature trip setting).

## 8 Designing the safety function

### 8.1 Function definition

According IEC 61511 safety function is "intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event". Such defintion is not particular helpful if the functions is to be realised with actual instruments. Therefore Shell has defined a functions as "comprising of one or more Sensors, a Logic Solver and one or more Final Elements whose purpose is to prevent or mitigate hazardous situations".

This implies that function is defined by the sensor subsystems (e.g. 'High Pressure in Separator'), the Logic Solver (e.g. 'ESD system') and the final elements (E.g. 'Close inlet and outlet').

In this definition, the sensor subsystems (a subsystem could comprise of multiple sensors e.g. in a 2oo3 configuration) are all the subsystems required to detect the hazard. The final element subsystems are all the subsystems required to avert or sufficiently mitigate the hazard.

Therefore it is crucial to carefully define the hazard the safety function is intended to avert.

In case multiple sensors subsystems are required to detect the hazard, one should define the 'success criterion'. This is a statement that defines when the hazard is successfully detected. E.g. if a run-away reaction in a reactor is detected by the combination of pressure and temperature sensors and the hazard will only be detected in case both subsystems work, the success criterion would be 2oo2.

Likewise, in case multiple final element subsystems are required to successfully avert the hazard, one needs to define the success criterion. E.g. If all 4 inlet valves to a vessel need to be closed to avoid overfilling, the success criterion would be 4oo4.

## 8.2 Designing the defined function

Once the sensor, logic solver and final element subsystems are defined together with the success criterion, the function needs to be designed such that it fulfils the following criteria

- The function performance criteria are met.
- The subsystem minimum fault tolerance criteria are met
- The overall function PFD is better than the required PFD based on the SIL

### 8.2.1 Performance criteria

The performance of a safety function is related to following aspects:

- Speed
  The overall response time of the hardware should be better than the process safety time. The overall response time is normally the sum of the response time of the sensors, the logic solver and the final element (e.g. valve stroking time). Any 'spare' in the speed of the function could be used to delay the action to prevent spurious trips as caused by transients.
- Accuracy
  The sensors should be sufficiently accurate to detect a developing hazard. E.g. If a process normally operates at 20 Barg and a trip should be activated at 21 Barg and no later than 21.5 Barg, the accuracy of the sensor should be ● 0.5 Barg.
- TSO
  If a valve needs to be closed to avert the hazard, one should verify if the valve may leak or should be tight shut-off in order to avert the hazard or prevent to create another hazard. TSO requirements have a large impact of test requirements and test coverage factor. If TSO is required to perform the safety mission, a prooftest would need to verify if the valve indeed is TSO. If not, the valve would not be able to perform its safety mission and should be assumed to have failed the test.

A safety function would fulfil the performance requirements if all the above requirements are met.

### 8.2.2 Minimum fault tolerance

IEC 61508 and IEC 61511 require subsystems to comply with minimum fault tolerance requirements irrespective of achieving the PFD. For field instruments and non-programmable electronic logic solvers IEC 61511 requires the following minimum fault tolerance:

Table 2, Fault tolerance requirements for sensor and final element subsystems and non PE logic solvers

| Safety Integrity Level | Fault tolerance |
|---|---|
| SIL 1 | 0 |
| SIL 2 | 1 |
| SIL 3 | 2 |
| SIL 4 | In accordance with IEC 61508 part 2 tables 2 and 3 |

A fault tolerance of 1 means that the subsystem is still capable of performing its safety mission in the presence of 1 dangerous fault. E.g. a 1oo2 architecture has a fault tolerance of 1 because if one of the channels failed dangerously (i.e. will not detect the hazard), the other channel will still bring the process to a safe state.

The requirements of Table 2 are only valid for instruments where the dominant failure mode is to the safe state or dangerous failures are detected, otherwise the fault tolerance shall be increased by one.

The requirements of Table 2 may be reduced by one if the instruments used in the subsystem are 'prior used'. If sufficient experience exist that demonstrate that the instruments are suitable for the application, the instrument may be regarded as 'prior use'. Typically major companies have lists of preferred make and types of instruments that reflect the positive experience.

### 8.2.3 Overall PFD

Finally the overall probability of failure on demand of the safety function is to be established. The achieved PFD is to be better (lower) than the required PFD in accordance with the SIL (see Table 1). The following parameters should be taken into account when establishing the PFD of sensor, logic solver and final element subsystems:-

- Sensor subsystem success criterion. See 8.1.
- Final Element subsystem success criterion.
- Subsystem success criterion (e.g. a subsystem consists of a 2oo3 transmitter, or a valve is equipped with 1oo2 solenoid valves)
- Manual proof Test intervals
- Manual proof test coverage factor (the % of dangerous failure the test may possibly detect)
- Diagnostic Test intervals

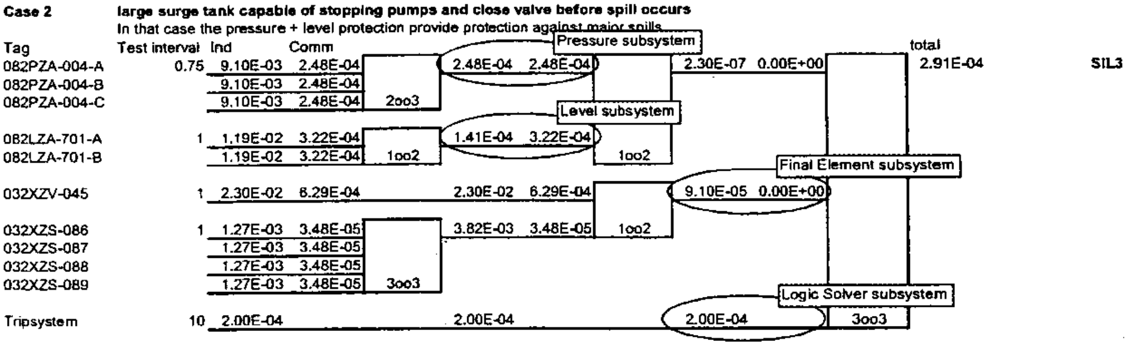


Figure 10 Example PFD calculation

- Diagnostic test coverage factor (the % of dangerous failure the diagnostic test may possibly detect)
- Dangerous and safe failure rates (it is normally assumed that the failures occur randomly)
- The common fault factor (β) for dangerous failures. (the % of dangerous failures that will affect multiple channels in a redundant subsystem)
- The common fault factor (β) for safe failures.
- The repair time in case component may be repaired on-line. The repair time is the time the component will be unable to perform its safety function as caused by repairs following a detected dangerous or safe failure.
- Mission time of the component (e.g. 10 years)

An example calculations is shown in **Error! Reference source not found.**0

## 9 Life Cycle management of the safety function

During the development, design, realisation and operation of a safety system many things may go wrong. Assumptions may not be realised, miscommunication, poor integration of subsystems, software bugs, poor competence of user and maintenance personnel etc, may all lead to the safety system not achieving its safety mission.

Therefore the lifecycle of a safety system needs careful planning and management. This aims to ensure that each phase of a lifecycle has delivered its unambiguously documented deliverables.

Figure 11 shows the lifecycle model as proposed by IEC 61511. This model is used to define requirements for each phase. The section numbers refer to sections in the Shell standard that describe detailed requirements as applicable in the Shell context.

Because many projects are executed in 3 phases, the conceptual phase, the project specification phase and the project execution phase, the lifecycle model needs to be expanded to support this practice. The resulting model is shown in Figure 12.

For each phase the following aspects should be defined:-

- Deliverables, tools, methods and inputs.
- Responsible persons and delegated responsibilities
- Required competencies and possible training requirements
- Procedures and work instructions
- Procedures for management of change
- Procedures for verfication and validation of the results.

The management plan should obviously avoid the formulation of incompatible goals.

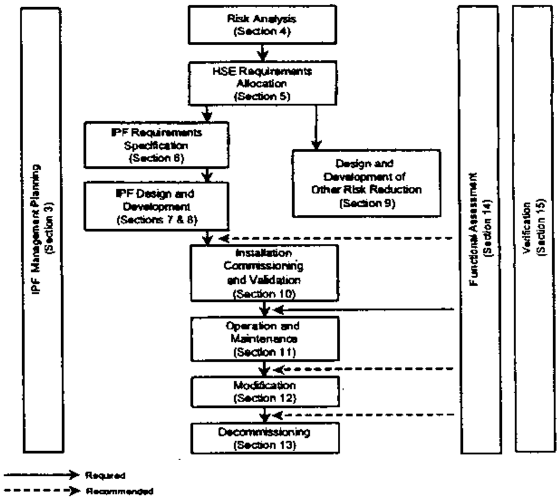


Figure 1, Lifecycle model as proposed by IEC 61511

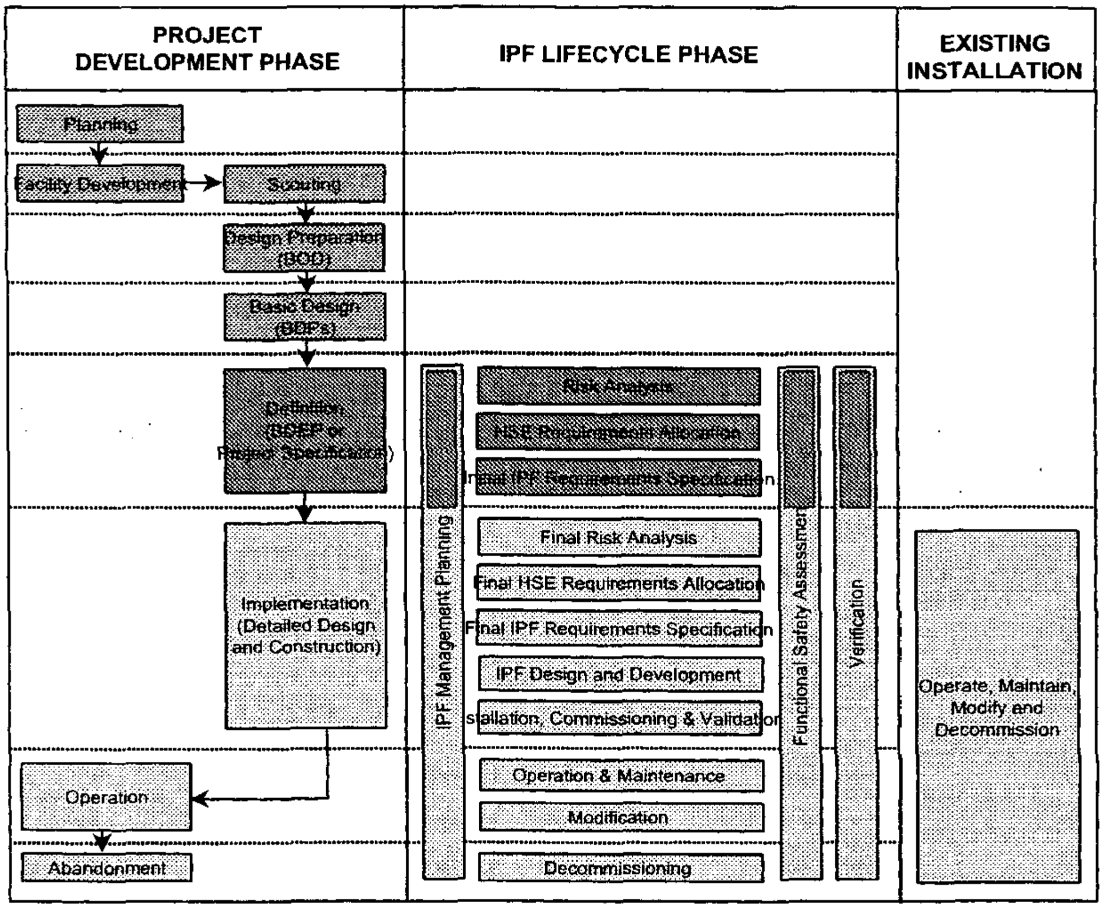

PROJECT DEVELOPMENT PHASE
IPF LIFECYCLE PHASE
EXISTING INSTALLATION
Planning
Facility Development
Scouting
Design Preparation (BOD)
Basic Design (BDPs)
Definition (BDEP or Project Specification)
Implementation (Detailed Design and Construction)
Operation
Abandonment
IPF Management Planning
Risk Analysis
HSE Requirement Allocation
Initial IPF Requirements Specification
Final Risk Analysis
Final HSE Requirements Allocation
Final IPF Requirements Specification
IPF Design and Development
Installation, Commissioning & Validation
Operation & Maintenance
Modification
Decommissioning
Functional Safety Assessment
Verification
Operate, Maintain, Modify and Decommission

Figure 2, Lifecycle as applicable to new construction projects

## 10 References

[1] International Electro technical Committee (IEC) IEC 61511 (draft) Functional safety of Safety Instrumented Systems for the Process Industry Sector
Part 1: Framework, definitions, system, hardware and software requirements
Part 2: Functional safety: Safety Instrumented Systems for the process industry sector - Informative
Part 3: Guidance for the determination of the required safety integrity levels - informative