

GUIDELINES
for
SAFETY INSTRUMENTED SYSTEMS
for the
THE PROCESS SECTOR

Authors: Arto Meskanen; Risto Heinonkoski; Ian Hitchen.

Disclaimer.

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use.

Introduction.

These guidelines were developed for use by the Agro division within Kemira Oyj, a large international company and aimed therefore specifically at the 'end user'. The guidelines are intended to provide a consistent approach for all end users within the division meeting, local regulatory requirements as well as the concepts inherent within the standards EN IEC 61508 and IEC 61511. Against this background the authors have provided the contained information as a general guidance to other 'end users' operating in the process sector.

SIPI61508: User Guidelines to Implementation of IEC 61508

LIST OF CONTENTS

Terminology

Background

Introduction

Determination of the Safety Integrity Levels

Hazard and Risk Analyses (phase 3)

Overall Safety Requirements (phase 4)

Safety Requirements Allocation (phase 5)

Correlation between SIL and PFD_{avg}

Case studies

Appendices:

Appendix 1: Guidance for the calibrated Risk Graph

Appendix 2: Application example

Terminology.

A comprehensive dictionary of terms related to the standard IEC 61508 is found in part 4 of the standard. Another glossary of terms used in automation & control is found in internet address: <http://www.simmons.demon.co.uk/Glossary.html>. Here, the most used terms are described:

ALARP – As Low As Reasonable Practical. A term applied to the reduction of risk by taking measures to reduce risk to persons (between intolerable and negligible levels) until the cost/effort of further measures is grossly disproportionate to the benefits they would deliver.

Demand Rate – The frequency with which a protective system is called upon to perform its protective function.

Diversity – Existence of different means of performing a required function (e.g. other physical principles or other ways of solving the same problem). [IEE/BCS report]

E/E/PES – Electrical/Electronic/Programmable Electronic System

ESD – Emergency Shutdown System. Usually implemented as an independent system from the process control system. For high safety integrity levels it is normal to avoid software based systems.

EUC – Equipment Under Control. Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

Fail Safe – A design property of an item, which prevents its failures from resulting in critical faults. [BS 4778 Part 3]

Failure – The termination of the ability of a system hardware element to perform a required function. (Note: hardware can fail but software can only have faults.)

Fault Tree – A logic diagram showing which fault modes of sub-items or external events, or combinations thereof, result in a given fault mode of the item. [BS 4778 Part 3]

Functional Safety – The ability of a safety related system to carry out the actions necessary to bring the plant to a safe state. [IEC 61508]

Harm – physical injury or damage to the health of people either directly or indirectly as a result of damage to property or the environment.

Hazard – potential source of harm

Hazardous situation – circumstance in which a person is exposed to hazard(s)

Hazardous event – hazardous situation which results in harm

Protective System - An instrument protective system used in SIL 1-3 applications. See [Safety Integrity Level](#).

Risk – combination of the probability of occurrence of harm and the severity of the harm

Tolerable risk – risk, which is accepted in a given context, based on the current values of society

PFD_{avg} – average probability of failure on demand of a safety-related protection system

Residual risk – risk remaining after protective measures have been taken

RRF = Risk reduction factor – the inverse of **PFD_{avg}**

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

SIPI61508: User Guidelines to Implementation of IEC 61508

Safety function – function to be implemented by an E/E/PE safety related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.

Safety Integrity – probability of a safety-related system performing the required safety functions under all the stated conditions within a stated period of time

Safety Integrity Level (SIL) – discrete level (one out of possible four) for specifying the safety integrity requirements of the safety functions allocated to the E/E/PE safety-related systems, where level 4 has the highest safety integrity and level 1 the lowest.

Safety Instrumented System (SIS) – a term not used by IEC 61508, but today generally used as a synonym for the term safety-related system

Safety-Related System (SRS) – a designated system that both

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

Background

The development of methods and guidelines for improving and unifying the realisation of safety instrumented systems within the Company was started in the form of a project in autumn 1997 which ran until 2000. In the first stage of the project, the current practices, and requirements set by authorities within each country where the company's production was sited, as well as needs for developing these practices were collected using a questionnaire. In September 1998, a seminar on Safety Instrumented Systems (SIS) was arranged where the present situation and the needs of development were discussed. The seminar resulted in a set of recommendations to the HSE team of The Company.

The HSE team discussed the recommendations and came out with the following scope definition for continuation of the project:

PROJECT SCOPE

DEVELOPMENT OF GUIDELINES AND MODELS FOR SAFETY INSTRUMENTED SYSTEMS

Define a common method for risk assessment and concepts to be used as the basis for defining safety instrumentation.

Recommend the Integrity-level to be used in automation in the different safety critical production- and handling processes in the division.

In co-operation with production teams:

- **prepare a list of safety critical equipment or units and recommend a model for**
 - **The level of instrumentation**
 - **Safety Instrumented Function v On-Stream (redundancy)**
 - **Testing and maintenance**

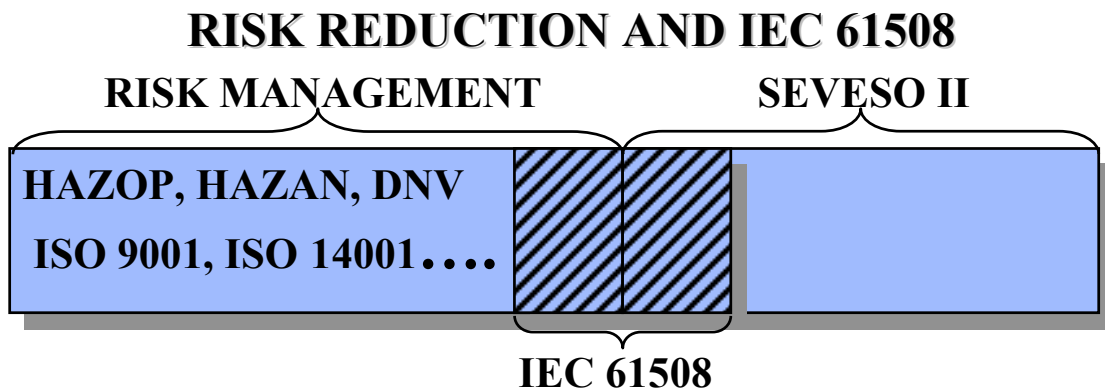
Prepare a training programme for the above.

Assign the Project Manager (Engineering Department) and Project Owner (HSE Department)

Introduction

An essential theme discussed at the company SIS seminar was the new standard IEC 61508: Functional Safety of electrical/electronic/programmable electronic safety-related systems. The conclusion of the seminar was that it shall form the basis of all recommendations and guidelines regarding safety instrumented systems within the Company.

The relation of IEC 61508 with other tools for risk management is illustrated by the following picture:



IEC 61508 IS A MANAGEMENT TOOL TO COVER PART OF THE TOTAL RISK REDUCTION. IT COVERS PART OF THE SEVESO II AND PART OF OTHER RISK MANAGEMENT AREAS

The Company has also developed a set of instructions called “Codes of Practice (COP)” for the safe production, storage, transport and sale of certain types of products. This guideline is not intended to replace any of the instructions included in these codes of practice but to supplement these by guiding the instrumentation engineering to meet the safety requirements of these codes.

The intention of this guideline is also to extract the essential procedures and recommendations of the IEC 61508 into a compact form (‘model solutions’) to facilitate their application to The Company’s processes.

The essential elements of the standard IEC 61508 are:

- Adoption of the safety lifecycle concept for systematic dealing with all design, realisation, maintenance and decommissioning aspects of the safety related automation.
- Definition of the management of functional safety at all phases of the lifecycle
- Definition of the requirements for assessing the functional safety at various phases of the lifecycle
- Definition of the requirements for documentation at all phases of the lifecycle.

The first target of the project was to define a common method for risk assessment and concepts for defining safety instrumentation.

This target is covered by the phases 1 to 5 of the overall safety lifecycle model, Figure 1 below.

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

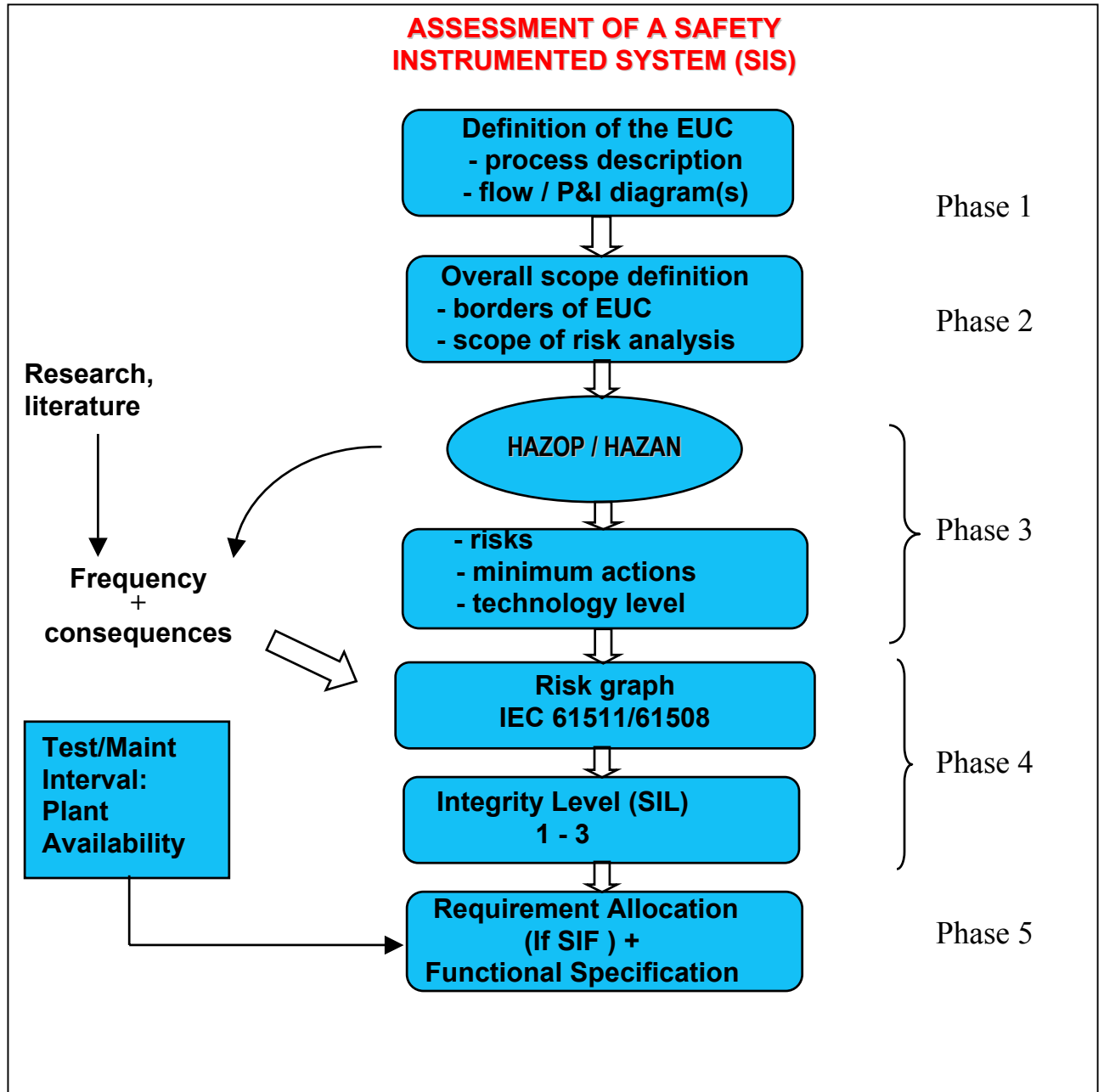


Figure 1 Method for assessment of safety instrumented systems

Determination of the Safety Integrity Levels.

The requirements of phases 1 to 5 in the lifecycle model are outlined below

The **first** phase is **Concept**, and includes sufficient familiarisation with the EUC and its environment (physical, legislative etc.) to enable the other phases of the lifecycle to be carried out. The familiarisation may utilise written process description, flow diagrams, P&I diagrams etc.

The **second** phase, **Overall scope definition**, means defining and documenting the borders of the EUC and the EUC control system. In addition to bordering the physical process, also the scope of the hazard and risk analysis is defined (process hazards, environmental hazards, etc.). As above, flow and P&I diagrams may be used for marking the EUC. If process shut down costs or possible equipment damages are exceptionally high, they may be also included in the hazard analysis and the additional protection in the SIS.

The **third** phase, **Hazard and risk analysis**, includes the following objectives:

- The actual determination of all hazards and hazardous events of the EUC (in all modes of operation) for all reasonably foreseeable circumstances including fault conditions and misuse Failures of the EUC control system shall be included in the analysis
- Determination of the event sequences leading to the hazardous events
- Determination of the EUC risks associated with the above hazardous events
- Determination of the likelihood of the hazardous events

The **fourth** phase, **Overall safety requirements**, includes the specification of the safety functions and the safety integrity requirement for each function for reducing the risk to the target level. This specification shall be done for each identified hazard.

All specified safety functions with their related safety integrity requirement form the overall safety requirement specification.

The **fifth** phase, **Safety requirements allocation**, means that the above specified safety functions are each designated specific E/E/PE safety related systems. Here, the normal engineering procedure of an organisation should always takes into account the requirements for the external risk reduction facilities like fire walls, bunds, drain systems, etc and the requirements for “other safety related systems such as relief valves, rupture disks, explosion relief panels. Hence, they are in this guideline considered as part of the plant.

The following figure illustrates the general concept of safety requirements allocation to the three subsystems. In the concepts of the standards, the risk assessment and SIL determination are then based on the remaining risk after the external risk reduction facilities and other safety related systems have been implemented, i.e. the leftmost box in the figure.

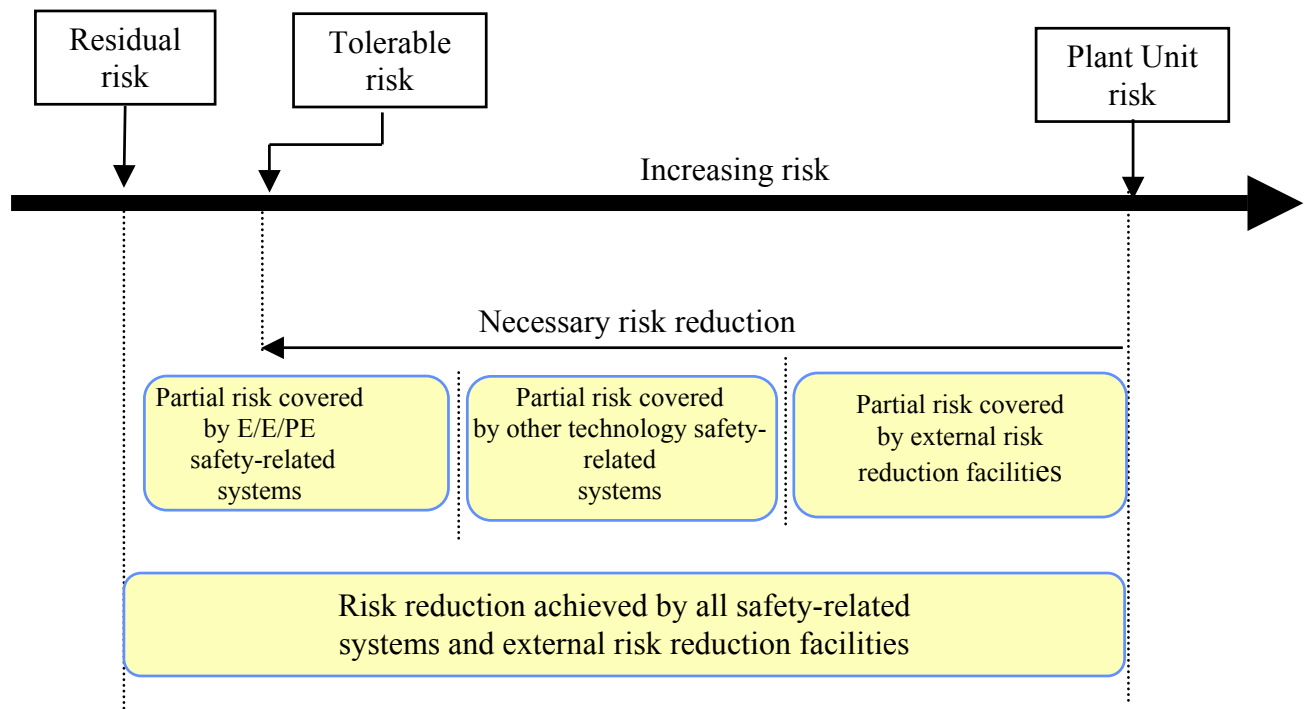


Figure 2: Risk reduction - general concepts (IEC 61508-2)

Hazard and Risk Analyses (phase 3)

The first and second phase summarised previously result in a description of the process reviewed and determine the parts requiring closer examination. In addition, the types of risks to be analysed are defined. This guideline may be applied to risks on people at the process site, the external community, and the environment.

Risks to production equipment resulting in economic losses may be included as well, if the potential economic losses are considered intolerably high.

When the scope has been defined, phase 3 is started.

The hazard and risk analysing methods used for a specific case depend on the type of EUC in question. The two most commonly used methods are Process Hazard Analysis (PHA) and Hazard and Operability study (HAZOP). Fault Tree Analysis (FTA) is most often used for analysing the possible routes through which a defined hazardous event can arise. Description of the above methods is outside the scope of this recommendation. Some general insight can however be obtained from the case example attached to this guideline. It is assumed that the persons involved in carrying out the determination of the required safety integrity of a safety-related system are familiar with these methods. A very good presentation of the methods is found in the book “HAZOP AND HAZAN – Identifying and Assessing Process Industry Hazards” by Trevor Kletz / Institution of Chemical Engineers, ISBN 0 85295 285 6.

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

Overall Safety Requirements (phase 4)

Analysing of the identified risks using the selected methods shall result in finding answers to at least the following questions:

- What are the consequences of each hazardous event?
(On-site / Off-site / Environmental impacts / Production losses)
- What is the likelihood of the hazardous event to take place?
- What is the required risk reduction for each hazardous event?
- What measures are available for removing each identified risk? The measures include use of external risk reduction facilities, use of E/E/PE safety related systems (SIS), and use of other technology safety related systems. The measures based on SIS are the safety functions that are actually the core of the whole procedure.

The specified safety functions and the corresponding safety integrity levels form together the overall safety requirements specification.

The required risk reduction can be determined either qualitatively or quantitatively. IEC 61508-5 contains examples of both methods. The quantitative method leads to rather laborious calculations and is not widely used. The qualitative method has already been applied to several cases within Kemira and is significantly less laborious. However, it has been blamed for its nonlinearity in relation to the parameter values.

This method leads to a unique value of the required safety integrity level (SIL), and is described in more detail later (**Graphical methods for determining SIL**).

Correlation between SIL and Risk Reduction:

Neither the qualitative nor the semi-quantitative method requires the numerical exact determination of the risk reduction factor for each safety function. However, after the parameters have been determined and the required SIL been found, the risk reduction factor (RRF) is simply the inverse of the PFD_{avg} found in table 2 for the SIL. For example, if the determined SIL is 2, the range of PFD_{avg} of the safety function is between 0.01 and 0.001. The corresponding range of RRF is then from 100 to 1000.

Safety Requirements Allocation (phase 5)

When the overall safety requirement and the technical measures for removing the risk have been determined **for each identified risk**, the safety requirement is allocated to the three subsystems as indicated by previous figure.

As mentioned before, the external risk reduction facilities include measures like firewalls, drain systems or bunds. These are measures always considered by project engineers in connection with safety critical processes, and fall outside the actual scope of this guideline. The same applies to the other safety related systems like relief valves and rupture disks. However, when determining the requirement for risk reduction by means of the E/E/PE safety related systems (SIS), the reduction carried out by measures in these two other categories shall be taken into account.

The required risk reduction by means of SIF is thus equal to (required total risk reduction / RRF of the external risk reduction facilities / RRF of the other technology safety related systems).

Graphical methods for determining SIL

The qualitative approach is based on a graphical method, called risk graph method.

So far, most of the applications within Kemira have utilised a general risk graph which was not specifically calibrated' for each application sector.

The semi-quantitative approach suggested by process industry is also based on a sector specific 'calibrated' risk graph. The risk graph and the related table are found in the appendices.

The Demand Mode:

The standard IEC 61508 identifies two demand modes: Low demand mode or High demand mode. Low demand mode means that the frequency of demands for the operation on the SIF is not greater than once a year or twice the proof-testing interval. Demands for the SIF to respond higher than this (or continuously) are High demand.

Based on above, the PFD_{avg} values, and the tables used for determining the safety integrity level in this guideline are selected for the **low demand mode**.

Correlation between SIL and PFD_{avg}

Although the qualitative and the semi-quantitative methods do not explicitly include the determination of the required PFD_{avg} value or RRF for a safety function, there is a direct correlation between the SIL and the PFD_{avg} . This correlation is given in Table 2 below:

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand = PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 2 – Safety integrity levels: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in low demand mode of operation (IEC 61508-1)

After the safety functions have been defined and allocated to the SIS, it is required that a full Functional Specification is developed. This guidance does not cover this aspect of the standard, but the following is provided for information:

Architectural requirements

First, it must be noted that **a safety integrity level is specified for each safety function**. The basic requirement of the standard is that the designed **safety function** fulfils the reliability of the **SIL** assigned to the function. A safety function consists of **a sensor subsystem, a logic subsystem, and a final element subsystem**. For each subsystem, the standard limits the possible architecture based on the technology used. The most essential limitations concern **fault tolerance and the selection of components**.

Checking the PFD_{avg} and the availability of the plant

In the design of industrial safety instrumented systems, the primary issue is safety. On the other hand, the SIS should not lower the availability of the plant to an unacceptable level. These requirements are in direct conflict with each other. Therefore, in addition of following the guidance of the standard regarding safety, also the availability of the plant needs to be considered, and the design revised until both requirements are satisfied.

General comments concerning design of SIS

The guidance given by IEC 61508 for realising a SIS is generic, whilst for the process industry a guidance has been produced as standard IEC 61511. However, it is still a requirement to follow specific Codes of Practice / Standards e.g. solutions for burners, boilers etc. and that those engaged in the life cycle must be competent to carry out their functionality.

There are several software tools available which encompass Hazard and Operability with Safety Integrity determination (either using calibrated Risk Graphs and/or LOPA) along with more specific tools for use in the SIF design and management phases.

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

SIPI61508: User Guidelines to Implementation of IEC 61508

Case studies.

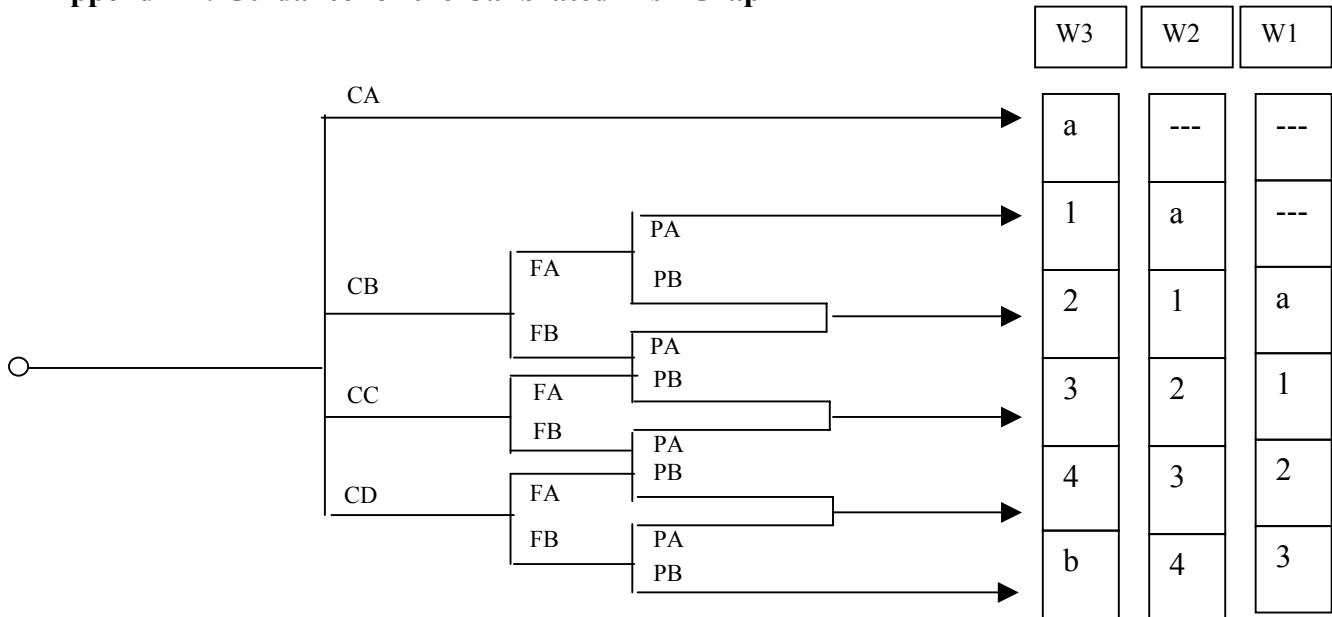
The concepts covered in this guide have been applied to several projects within the Company to test the concepts of the guide. One such trial application has been included in the appendices.

Appendices:

Appendix 1: Guidance for the calibrated Risk graph.

Appendix 2: Application Example

Appendix 1: Guidance for the Calibrated Risk Graph



The numbers 1 to 4 are the Safety Integrity Level (SIL) required for the identified Safety Instrumented Function (SIF) that is to be utilised to reduce the risk to a tolerable value. It also requires that the SIF is designed and managed in accordance with IEC 61508 and related guidelines such as IEC 61511.

The value of 'a' represents a possible safety related function which is has a Safety Integrity Level value less than the standard. A 'b' value means that the identified SIL value is greater than the standard and special means should be adopted to determine the actual requirements.

SIPI61508: User Guidelines to Implementation of IEC 61508

Risk parameter	Classification	Comments
<p>Consequence (C)</p> <p>Average number of Fatalities</p> <p>This can be calculated by determining the average numbers present when the area exposed to the hazard is occupied and multiplying by the vulnerability to the identified hazard.</p> <p>The Vulnerability will be determined by the nature of the hazard being protected against. The following factors can be used:</p> <p>V=0.01 Small release of flammable or toxic material</p> <p>V=0.1 Large release of flammable or toxic material</p> <p>V=0.5 As above but also a high probability of catching fire</p> <p>V=1 Rupture or explosion</p>	<p>C Minor injury</p> <p>A Range 0.01 to 0.1</p> <p>C Range > 0.1 to 1.0</p> <p>B Range > 1.0 to 10</p> <p>C</p> <p>C</p> <p>C</p> <p>D</p>	<p>The classification system has been developed to deal with injury and death to people.</p> <p>For the interpretation of CA, CB, CC and CD, the consequence of the accident and normal healing shall be taken into account</p> <p>Greater than 10 use quantified approach</p>
<p>Occupancy (F)</p> <p>This is calculated by determining the length of time the area exposed to the hazard is occupied during a normal working period.</p> <p>NOTE – If the time in the hazardous zone area is different depending on the shift being operated the maximum should be selected.</p> <p>NOTE – It is only appropriate to use FA where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up.</p>	<p>FA Rare to more often exposure in the hazardous zone. Occupancy less than 0.1</p> <p>FB Frequent to permanent exposure in the hazardous zone</p>	<p>See comment 1 above</p>
<p>Probability of avoiding the hazardous event (P) if the protection system fails to operate</p>	<p>PA Assumed to be 0.9 if all conditions in column 4 are satisfied</p> <p>PB Assumed to be zero if all the conditions are not satisfied</p>	<p>PA should only be selected if all the following are true:</p> <p>facilities are provided to alert the operator that the SIS has failed</p> <p>independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area</p> <p>the time between the operator being alerted and a hazardous event occurring exceeds 1 hour</p>
<p>Demand rate (W) given no protection system</p> <p>To determine demand rate it is necessary to consider all sources that will lead to a demand on the SIS. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designated and maintained according to IEC 61508, is limited to below the performance ranges associated with SIL1. For simple applications it is sufficient to sum the demand frequencies. For more complex systems it may be necessary to construct fault trees.</p>	<p>W 1 Demand rate less than 0.03 per year</p> <p>W 2 Demand rate between 0.3 and 0.03 per year</p> <p>W 3 Demand rate between 3 and 0.3 per year</p> <p>W 3 For demand rates higher than 3 per year higher integrity levels will be needed</p>	<p>The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS. Credit can be taken for relief valves providing these are fully sized for the expected duty</p> <p>If little or no experience exists of the process or the control system, or of a similar process or control system, the estimation of the W factor may be made by calculation. In such an event a worst case prediction shall be made. If the demand rate is very high e.g. 10 per year, the SIL has to be determined by another method or the risk graph recalibrated</p>

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

Appendix 2: An Application Example

INTRODUCTION.

This example is based on the work associated with a project to improve the safety of the Ammonia Nitrate plant ammonium nitrate solution (ANS) pumping facilities.

The intent of the project was to meet the Kemira Agro Code of Practice – Pumping of AN containing Solutions and Slurries.

Only those aspects of the project related to this guide have been included in this document.

SUMMARY

This is an example of an approach for the assessment of risk associated with the pumping of Ammonia Nitrate solution with no Safety Instrumented Systems.

The required Safety Integrity Level of the SIS was identified based on this risk assessment.

This SIL value is that average availability required of the SIS in order to provide the risk reduction needed to enable the Equipment Under Control to be operated at a ‘tolerable’ risk value.

The methodology employed is a mix of quantitative and qualitative assessment.

The quantitative part of the assessment uses failure rate and probabilities from various sources and ‘feel right’ experience.

The qualitative method uses the ‘calibrated’ risk graph of this guide to determine the Safety Integrity Level required from the Safety Instrumented Functions (as identified in the COP).

The following is not included in this guide :

Design, Implementation and Life Time Management of the SIS.

However, for information, the detailed design is based on the requirements of Kemira Ince I&E Engineering Standards which includes for on-line proof testing, non conformance reporting, and management of change.

SIPI61508: User Guidelines to Implementation of IEC 61508

Stage One.

The process requirements are defined in a Technological Scope.

This scope defined the modification required to the existing plant needed to meet the Kemira COP for the Pumping of AN Solutions.

Included in the scope are the process parameters, the basic control systems, the basic mechanical design and 'other risk reduction items' e.g. Relief Valves and the SIS identified in the COP.

This scope is amended / approved by the internal customer.

Stage Two.

A modification Engineering Flow Diagram (EFD) is produced from the approved Technological Scope. The boundaries of the EUC to be HAZOP are defined on a working copy of the EFD.

The HAZOP team was lead by a Chairperson trained / experienced in the techniques and their role is to guide the team.

Other members were - Plant Operations Supervisor, Project Technologist (Chemical Engineer), Automation (IE Engineer). All contributed to know how required to audit the EUC as plant / process. The methodology was based on the ICI format. (Annex2).

All pipes, vessels and tanks were identified and the results recorded (Annex3).

Action items requiring changes to the EFD form part of a revised Technological Scope which is then approved.

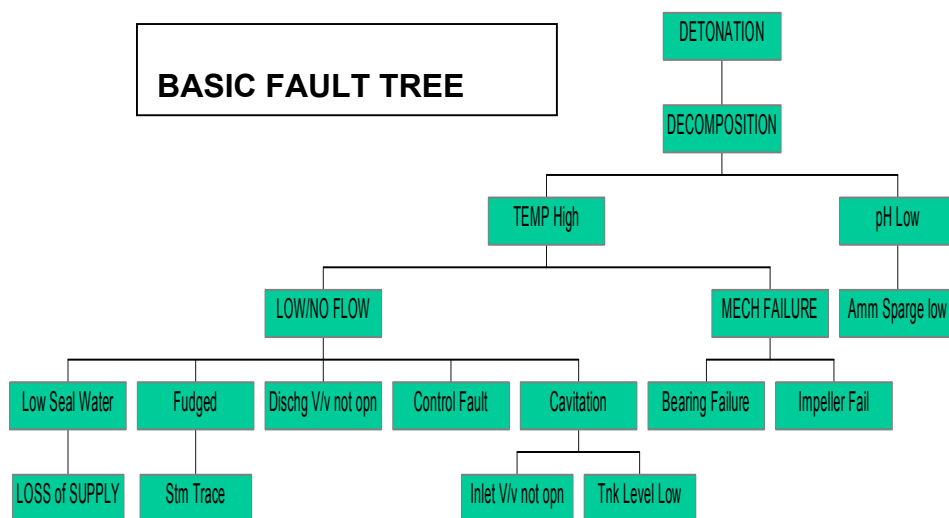
An Engineering Scope provides the information used for final cost estimating and the detailed design.

Stage Three

A team consisting of the Project Technologist, the customer Plant Technologist and the Project IE Engineer carried out a more detailed Risk Assessment as follows --

Basic Fault Tree:

The top event was identified as a detonation within the pump. This detonation may be contained but also could lead to injury / fatality. The fault tree is not considered absolute but gives a very good guidance to enable -



Hazard Rate Estimate:

The values used in are best estimate to provide an order of magnitude for use in the Qualitative Risk Graph.

The following were used in the fault tree analysis to provide **an order of magnitude** of the top event.

Low Seal Water 1/20 yrs.: Stm Trace 1/10yrs.: Hand V/v not open 1/10 yrs.: Control Fault 1/10 yrs.:

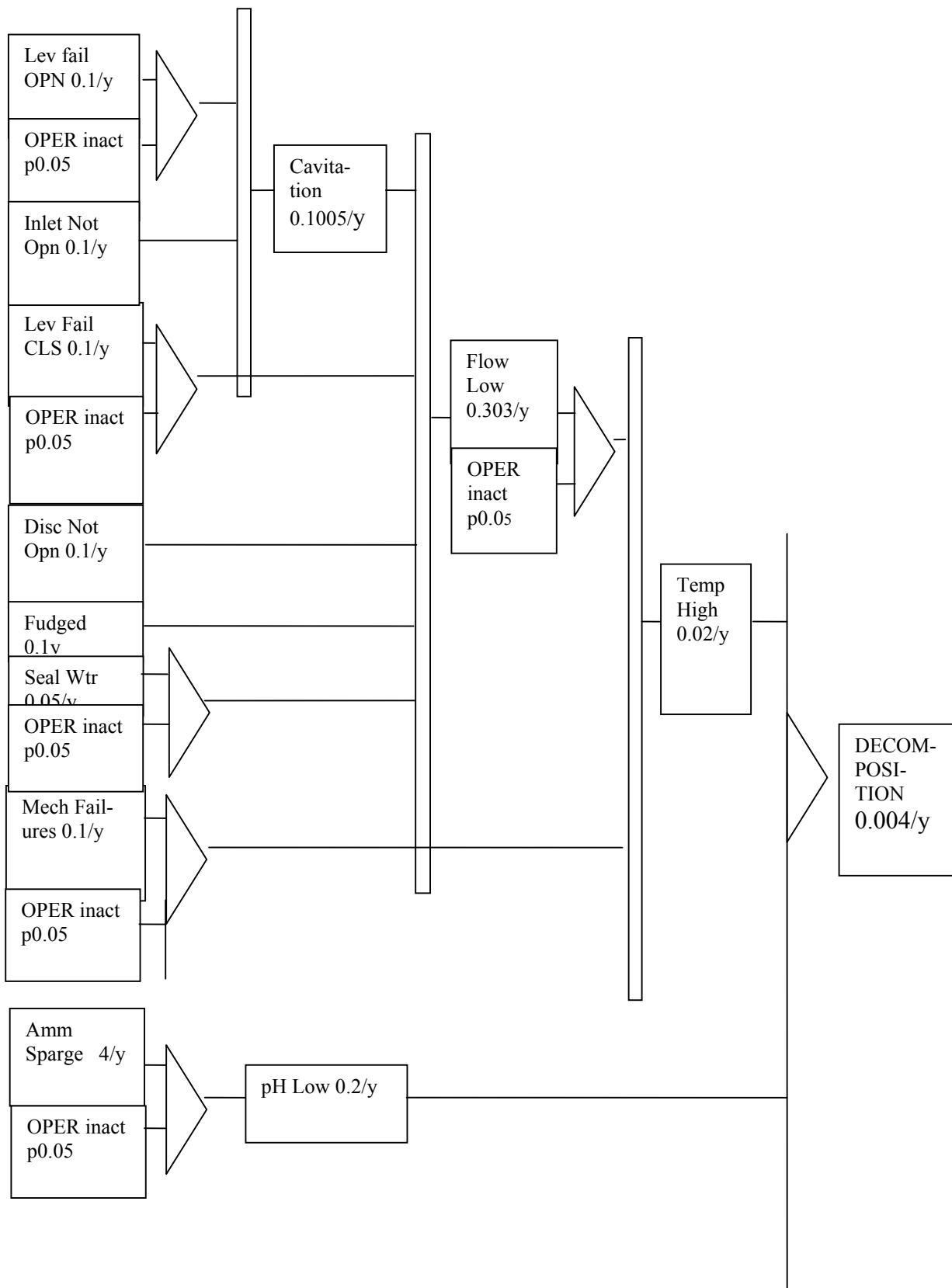
Low Tnk Lev 1/10yrs. Mech Fail 1/10 yrs.: Amm Sparge failure 4/ yrs.:

Operator lack of action to faults / alarms Prob. 0.05

Please note these are guidance values only and are based on plant experiences as 'Feel OK' values

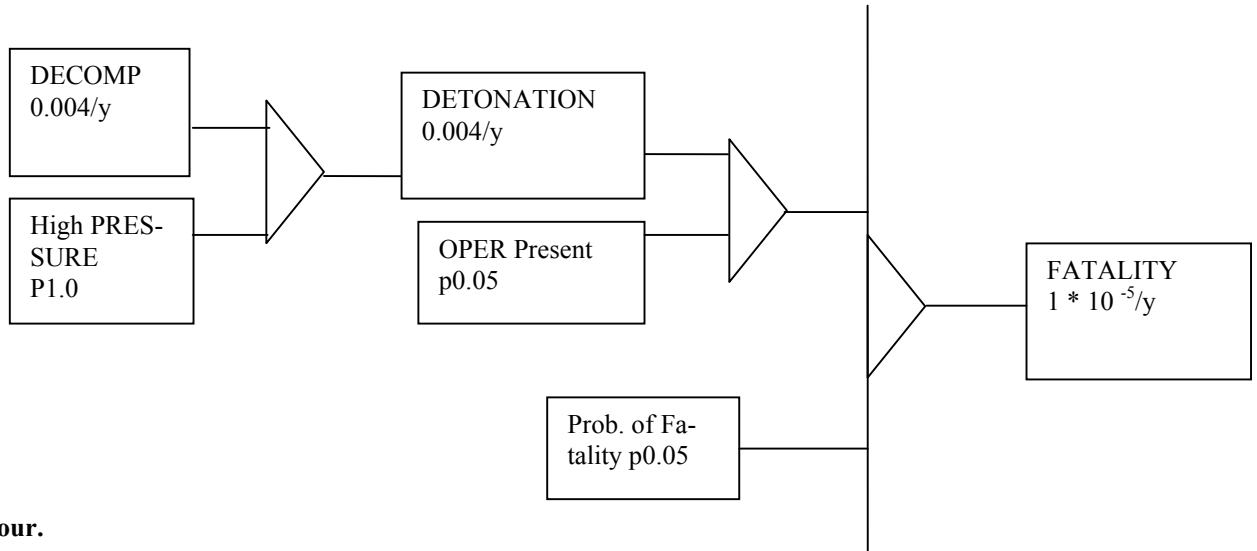
Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

SIPI61508: User Guidelines to Implementation of IEC 61508



Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

SIPI61508: User Guidelines to Implementation of IEC 61508



Stage Four.

The stage 3 results were used by the team in the semi-quantitative Risk Graph, forming part of this guide, to determine the SIL of the SIS for **personnel protection**.

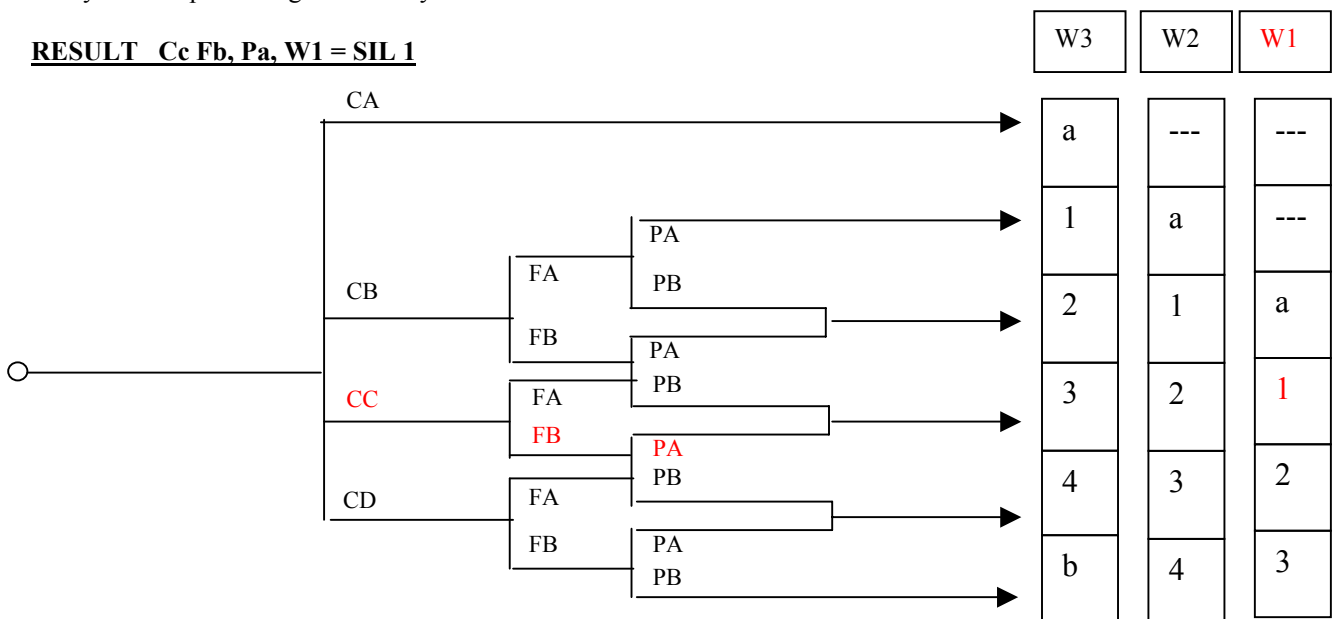
Risk Parameter **C** CONSEQUENCE.
 Vulnerability =1 Rupture /detonation
 Number of persons present =1: C = **Cc**

Risk Parameter **F** OCCUPANCY.
 PUMP OPERATED 24 hrs x 7dys SHIFT PERIOD 8 hrs , IN DANGER ZONE 4 x .5 hrs per shift =2.0
 Occupancy fraction 2.0/8 = 0.25: F = **Fb**

Risk Parameter **P** PROBABILITY OF AVOIDANCE
 Other alarms and operating procedures: **Pa**

Risk Parameter **W** HAZARD RATE
 Analysis from previous gives 0.004/yr: W = **W1**

RESULT Cc Fb, Pa, W1 = SIL 1



Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use

SIPI61508: User Guidelines to Implementation of IEC 61508

Stage Five.

Functional Specification.

The COP for pumping identifies the various SIF requirements for each type of pumping system. The pumping system to be employed in this application required a purging system to prevent build up of product at the back of the impellers.

COP Identified Safety Instrumented Functions.

TABLE 1

Ref	Measurement	Event	Result
1	Temperature	Impeller Damage	Local Hot Spot
2	Temperature	Expeller Damage	Local Hot Spot
3	Seal Wtr Flow	Too Little Seal Water	Cavitation, ANS in Confined space
4	Tank Level	Loss of Suction Head	Cavitation - Temp Rise
5a	ANS Flow	Out V/V Closed	ANS Confined – Temp Rise
5b		Plugged Disch Line	ANS Confined – Temp Rise
5c		LCV Closed	ANS Confined – Temp Rise
5d		In V/V Closed	Cavitation, - Temp Rise
5e		Motor Stopped	Rev Flow, Tank Spill
6	Motor Amps	As ref. 5 a to e	

Ref. 1&2 No diversity and thermal lag. Resistance type elements poor reliability at Ince. Use Type K t/c.

Ref. 3 Seal Water Flow Low Trip and diversity from temperature and ANS flow meter.

Ref. 4 Tank Level Low Trip and diversity from ANS Flow and Low Current (Power Curve flat).

Ref. 5a &5d Start-up Interlock - then low current and low flow trips

Ref. 5b ANS low flow and diversity of Low Amps

Ref. 5e Motor contactor status as logic input close valves

A functional logic was produced to represent the SIS requirements based on Kemira Ince Design and Engineering specification. This was approved by the internal customer.

A Trip and Alarm Review record is completed for each SIF sub-system, which records the design Trip and Pre-alarm values in Process and Instrumentation units it also records the SIL, the Testing Frequency and Maintenance Interval. It is also a record all deviations from this Kemira Ince IE approved standards together with the reasons for deviating.

This document is a 'life cycle' recording all updates of settings / category.

The SIS review involves:

Plant Technologist and / or Project Technologist; I.E. Design Engineer; Operation Supervisor

The principals of testing are defined in Kemira Ince Safety Manual. The requirements of this document are incorporated into the IE Design Standards.

For each Initiator there is a fully defined test procedure written in the Maintenance Management System. Hard copies are issued for approval, which are held as reference documents. The testing is scheduled into the MMS as defined in the review document.

Neither the owner Company nor the authors accept any responsibilities for the accuracy of the information provided or to any consequence of its use