ProSalus
SAFETY CONSULTANTS

Experts in Functional Safety

TÜVRheinland®

TÜV Functional Safety Program

FUNCTIONAL SAFETY ENGINEER

CERTIFICATION COURSE

SAFETY INSTRUMENTED SYSTEMS

www.prosalus.co.uk

TÜVRheinland®
ID: 145/09
FS Expert
S I S

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

FUNCTIONAL SAFETY ENGINEER CERTIFICATION COURSE IN SAFETY INSTRUMENTED SYSTEMS IEC 61511 AND IEC 61508

Slide 1- 1

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Objective of the FSE Certification Course

To provide attendees with a fundamental understanding of the principles of functional safety according to IEC 61511 and IEC 61508 with respect to the design and management of Safety Instrumented Systems (SIS) in the process industry

To assess the competency of the attendees by exam as the first step towards registration and certification in the TÜV Rheinland Functional Safety Program

Slide 1- 2

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Introductions

Welcome to the workshop

- **My background and experience**
- **About you?**
  - Your Name
  - A little background
  - What to do you want out of this Course
  - What does your company want out of this course

Slide 1- 3

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

- **Workshop Facilities & Etiquette**
  - In case of an emergency – exits and alarms
  - Toilets - location
  - Breaks – formal & feel free to stretch at any time
  - Tea & Coffee – help yourselves at any time
  - Feel free to ask questions at anytime
  - Please set mobile phones to silent so it doesn't effect your colleagues

Slide 1- 4

Function Safety Engineering

- **Duration**
  - 3 day course with homework
  - Exam on fourth day
- **Exam**
  - Four hour two part exam
  - Part 1 – 60 multiple choice questions
  - Part 2 –10 Open question
- **Working day**
  - 09:00 – 17:00
  - Lunch at 12:30 – 13:30

Slide 1- 5

Function Safety Engineering

FSE Course Contents

- Introduction to IEC 61508 and IEC 61511
- Functional Safety Management and the Lifecycle
- Competency Management and Assessment
- Process Hazard and Risk Assessment
- Risk Reduction and Safety Allocation
- Safety Requirements Specification
- Design and Development of the Safety Instrumented Function
- Software for Safety
- Safety Integrity Level Verification Calculation Methods
- Safety Integrity Level Determination
- SIL Determination for Fire and Gas Systems (ISA Methodology)
- Operations & Maintenance
- Exam

Slide 1- 6

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Today

- Introduction to IEC 61508 and IEC 61511
- Functional Safety Management and the Lifecycle
- Competency Management and Assessment
- Hazard and Risk Assessment
- Risk Reduction and Safety Allocation
- Safety Requirements Specification

Slide 1- 7

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Day 2

- Design and Development of the SIF
- Software for Safety
- Understanding Failure
- Failure Data and Sources
- Interpreting Failure Data
- Safety Integrity Level Verification Methods

Slide 1- 8

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Day 3

- Safety Integrity Level Determination
  - Risk Graphs
  - Layers Of Protection Analysis
- SIL Determination for Fire and Gas Systems
- Operations and Maintenance
- Exam Preparation

Slide 1- 9

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Introduction to Functional Safety

Slide 1- 10

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

What is Safety

- The condition of being safe
- Freedom from danger, risk, or injury
- Freedom from unacceptable risk
- Safety is the state of being "safe" (from Latin *Salus)*
- The condition of being protected from harm or any other event which could be considered non-desirable.

Slide 1- 11

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

What is Functional Safety (IEC 61511)

A part of the overall Process Safety approach

IEC61511-1 clause: 3.2.25
Part of the overall safety relating to the process and the Basic Process Control System which depends on the correct functioning of the Safety Instrumented System and other protection layers

Slide 1- 12

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

What is Functional Safety?

- A safety system is functionally safe if:
  - Random, common cause and systematic failures do not lead to malfunctioning of the safety system resulting in:
    - Injury or death of humans
    - Spills to the environment
    - Loss of equipment or production

Slide 1- 13

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Challenges in Achieving Functional Safety

The challenge is to design a system in such away as to prevent dangerous failures or to control them when they arise from:

- Incorrect specifications of hardware or software
- Omissions in the safety requirements specification
- Random hardware failure mechanisms
- Systematic hardware failure mechanisms
- Software errors
- Common cause failures
- Human error
- Environmental influences
- Supply system voltage disturbances

One of the key concepts to achieving FS is Safety Integrity Levels

Slide 1- 14

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

What is the Safety Integrity Level (SIL)

- SIL is a:
  - Qualitative measure of safety integrity in terms of the avoidance of systematic failures
  - Quantitative measure of safety integrity in terms of the hardware failures and fault tolerance
  - One of four levels of integrity
  - An order of magnitude risk reduction against a single hazard occurrence
- *SIL is not just an assessment of the loop hardware*

Slide 1- 15

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Safety Integrity Level

- Three important SIL properties to remember
  - Includes all of the safety instrumented function
  - The higher the SIL the more robust the requirements to achieve it
  - Includes hardware and systematic requirements

IEC 61511 Table 3 – Safety Integrity Levels: Probability of Failure on Demand (Demand Mode of Operation)

Safety Integrity Level (SIL)	Target average probability of failure on demand	Target Risk Reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10,000 - ≤100,000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1000 - ≤10,000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 – ≤1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 - ≤100

Slide 1- 16

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Safety Integrity Levels Continued

IEC 61511 Table 4 – Safety Integrity Levels: frequency of dangerous failures of the Safety Instrumented Function

(Continuous Mode of Operation)

Safety Integrity Level (SIL)	Target frequency o fdangerous failures to perform the safety instrumented function (per hour)
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Slide 1- 17

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

What is Functional Safety Engineering -

- Hazard Identification – Consequence / Frequency Analysis
- Targets of Tolerability / Acceptability of Risk – Safety Targets
- Risk Assessment / Risk Reduction / Safety Integrity Levels
- Engineering / Management Capability to a target Safety Integrity
- Lifecycle Processes to a target Safety Integrity
- Verification / Validation to a target Safety Integrity
- Understanding Change Management

FSE requires a Multi disciplined Approach to Safety

Slide 1- 18

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Introduction to the

Functional Safety Standards

Slide 1- 19

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

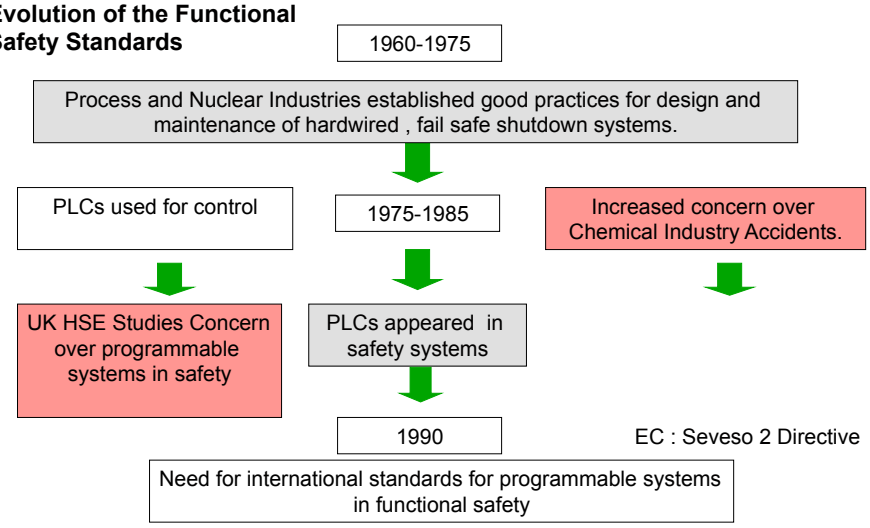
- Some guidance was available on designing instrument protective functions, ICI, Shell, BP etc
- Systematic issues not included in guidance
- Replacement of relays and solid state logic with software based logic systems raised issues with:
  - How to decide what systematic integrity was required
  - How to achieve and maintain required Hardware and software integrity
  - What had to be considered to achieve systematic integrity

Slide 1- 20

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Evolution of the Functional Safety Standards



Slide 1- 21

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Need for Internationally recognised standard for E/E/PES

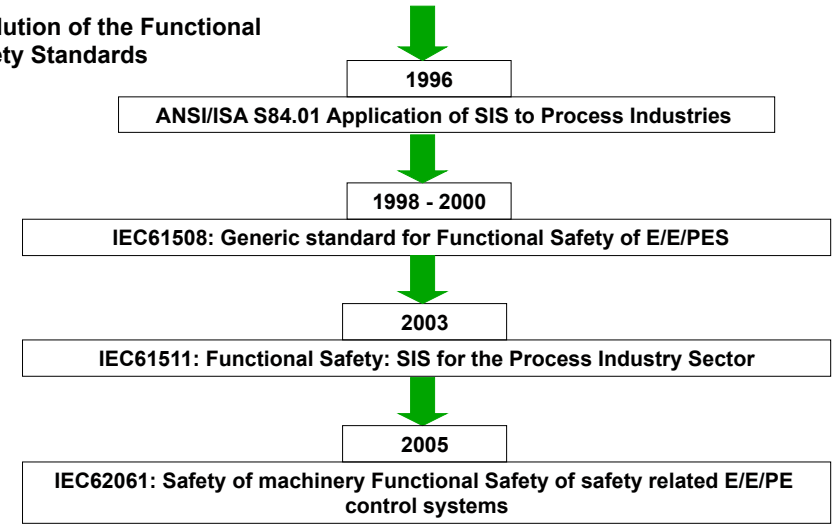
- By 1990: An urgent need for guidance, standard or code of practice for Functional Safety Engineering – SIS.
- Existing practice was based on solid state and German DIN 19250 with no provision for programmable systems.
- Systematic requirements not clearly identified
- Process Safety Management and Regulation changes include assessment and auditing of safety measures including Safety Insrumented Systems

Slide 1- 22

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Evolution of the Functional Safety Standards



Slide 1- 23

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Functional Safety Standards used in the Process Industry

- **IEC 61508:** Functional safety of electrical/electronic / programmable electronic safety-related systems
- **IEC 61511 / ANSI/ISA 84.00.01 Modified:** Functional Safety: safety instrumented systems for the process industry sector
- **IEC 62061:** Safety of Machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
- **ISO 13849:** Safety of Machinery – Safety-related parts of control systems – General principles of design and validation
- **EN 50402:** Functional Safety requirements for fixed gas detection systems
- **ISO 13702:** Requirements and guidelines for the control and mitigation of fire and explosions on off-shore oil and gas installations
- **ISO 10418:** Analysis, design, installation and testing of surface protection systems

Slide 1- 24

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

IEC61511-1 Figure 2 Relationship between IEC 61511 and IEC 61508

Slide 1- 25

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

IEC 61508

Title: Functional safety of electrical/electronic/programmable electronic safety-related systems –

Part 0: Introduction to functional safety
Part 1: General requirements
Part 2: Requirements for electrical / electronic /programmable electronic systems
Part 3: Software requirements
Part 4: Definitions and abbreviations
Part 5: Examples of methods for the determination of safety integrity levels
Part 6: Guidelines on the application of IEC 65108-2 and IEC 61508-3
Part 7: Overview of techniques and measures

Slide 1- 26

Function Safety Engineering

IEC 61508 Generic Standard for all Industry Applications

The Scope of IEC 61508 applies to:

- Any safety related device or system based on electrical/ electronic / programmable electronic (E/E/PE) Technology
- Any Safety related systems in any industry sector including Process, Nuclear, Oil & Gas, Exploration, Sub Sea, Aerospace, Military , Railway, Motor Industry, Shipping e.g. pipe laying vessels etc
- Industries where no sector specific functional safety standard exists
- Applicable World wide (subject to individual country acceptance)

Slide 1- 27

Function Safety Engineering

IEC 61511

Title: Functional Safety- Safety Instrumented Systems for the Process Industry Sector

Part 1: Framework, definitions, system hardware and software requirements

Part 2: Guidelines for the application of IEC 61511-1

Part 3: Guidance for the determination of the required Safety Integrity Levels

Slide 1- 28

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

IEC 61511

Part 1: Mandatory requirements for work procedures, records, hardware, software, testing, maintenance, assessment. Based on safety lifecycle framework.

Part 2: Extensive guidance on Part 1 - methods and design features to achieve required levels of safety integrity.

Part 3: Guidance on methods of determining the required Safety Integrity Level for any Safety Instrumented Function. Quantitative (e.g. FTA method), Semi Quantative (e.g LOPA method) and qualitative methods (e.g. risk graph method).

Slide 1- 29

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

IEC 61511 Functional Safety for the Process Industry Sector

The Scope of IEC 61511 applies to:

- Chemicals, Tank Storage, Pharmaceutical, Non Nuclear Power, Utilities Industry, Oil and Gas Production and Exploration, Bio Plants……
- Safety Instrumented Systems – normally pre certified / approved / assessed
- Legacy Safety Instrumented Systems
- Pipe to Pipe Standard (Sensor to Final Element)
- Excludes Operating, Source and Embedded Software (Full Variability Language FVL)
- Not for device certification
- ANSI/ISA 84.00.01-2004 (IEC 61511 Modified) USA implementation with Grandfather clause

Slide 1- 30

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

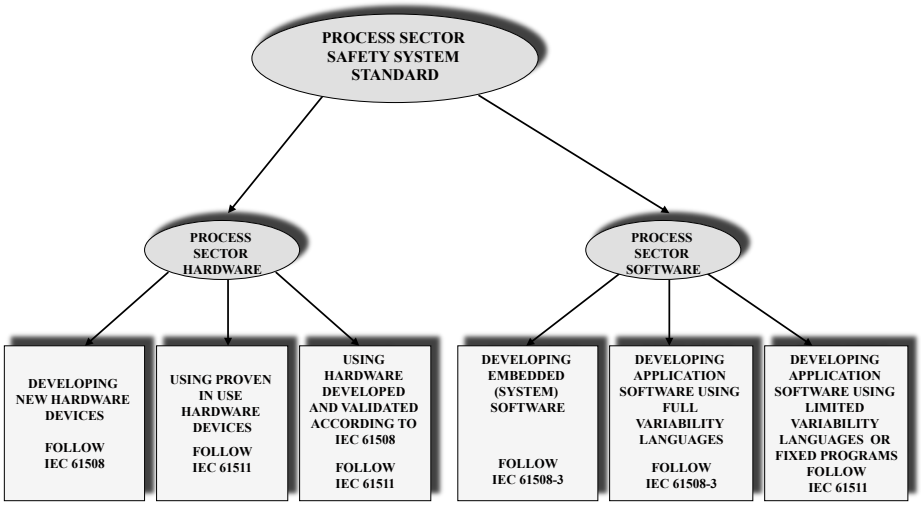
Additional Informative Guidance:-

- EEMUA 222 – Guide to the Application of IEC 61511 to safety instrumented systems in the UK process industries;
- Norsok OLF070 – Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry;
- EI/IP – Guidance on assessing the safety integrity of electrical supply protection;
- CASS - Guide to Functional Safety Capability Assessment;
- ISA-TR84.00.02-2002 – Parts 1 to 5 – SIF – SIL Evaluation Techniques;
- ISA-TR84.00.02-2002 – Guidance for Testing of Process Sector SIFs
- CDOIF– Guideline Demonstrating Prior Use
- IChemE – Using risk graphs for SIL Assessment – a user guide for ChemEng
- EI Draft – Guidance on SIL Determination
- EI Draft – Guidance on Quantified Human Reliability Analysis

Slide 1- 31

ProSalus SAFETY CONSULTANTS

Function Safety Engineering



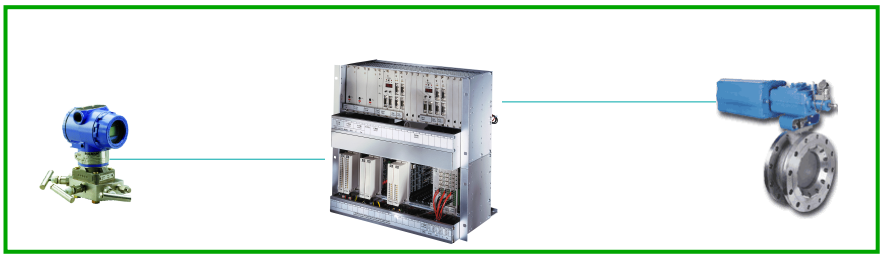
IEC 61511-1 Figure 3 - Relationship between IEC 61511 and IEC 61508

Slide 1- 32

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Scope of a Safety Instrumented Function



Sensor **Logic Solver** **Final Element**

(Hardware and Software)

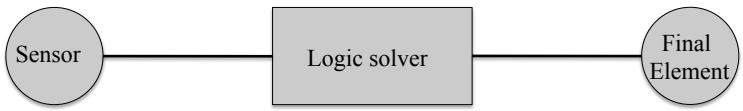
Slide 1- 33

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Safety Instrumented Functions

A SIF is always formed from three sub systems



Initiators
Pressure Transmitter
Temperature Transmitter
etc

Final Elements
Shut off Valve
ESD Valves
Vent Valves
Pumps
etc

Slide 1- 34

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Safety Instrumented Functions

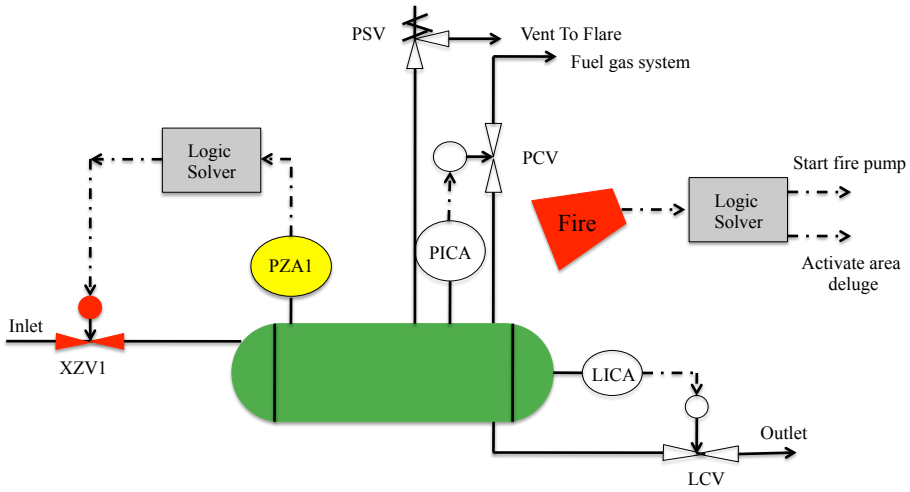
- Safety Instrumented Systems (SIS) are one of the most widely used active risk reduction techniques that form part of the preventative protection layers
- A SIS is made up of individual Safety Instrumented Functions (SIF)
- A SIF contributes to the overall risk reduction for an identified hazard
- Overall risk reduction is made up of many layers (safeguards) that are identified during the hazard study
- The cause / consequence pair identified during the hazard study helps determine the amount of risk reduction required
- An Instrument SIF helps to prevent / reduce the frequency of a hazardous event
- A F&G SIF helps to mitigate / reduce the consequences of a hazardous event

Slide 1- 35

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Typical Safety Instrumented Functions (Preventative & Mitigative)



Slide 1- 36

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Safety Instrumented Functions

A SIF protects against a single hazard is identified during a hazard study

A Safety Instrumented System (SIS) is made up of several SIF loops

A SIF can be:

- a single initiator and several final elements;
- a single final element and several initiators

The SIF Functional, Integrity and logical relationship between Inputs & Outputs is captured in the Safety Requirements Specification (SRS)

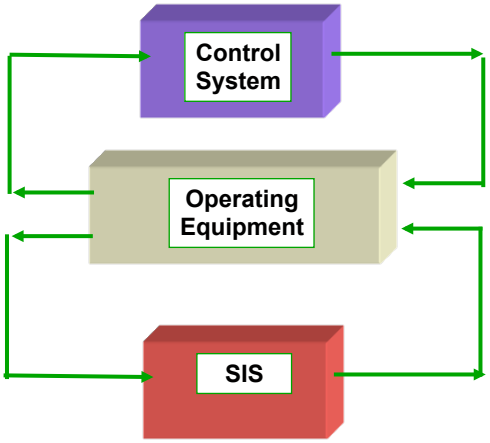
Slide 1- 37

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Safety Instrumented Systems act independently of the process or its control system to try to prevent a hazardous event.

The SIS achieves risk reduction by reducing the frequency (likelihood) of the hazardous event
The amount of risk reduction allocated to the SIS determines its "target Safety Integrity Level" i.e. SIL



Slide 1- 38

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Introduction to Regulatory Compliance

Slide 1- 39

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

So why do we need Functional Safety Standards

- Because we don't learn from our mistakes
  - Disasters keeping repeating – Trevor Kletz – "Lessons from Disaster" (ISBN 0 85295 307 0)
- Prescriptive regulations and standards need support form risk / goal based regulations and standards to work effectively when dealing with complexity or novel approaches e.g. API RP 14C
- Latest regulatory approach is risk based goal orientated approach (e.g. In the UK - HASAWA – COMAH – SMS - QRA – Competency)
- A risk based approach needs well trained and competent engineers who are aware and knowledgeable about safety (HSE 2007 – Management of Competency Systems)

Slide 1- 40

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Hazardous Events that emphasis the need for Safety Standards

- **Flixborough, UK, 1974 –** Accelerated the introduction of the HASAWA and subsequently the Control of Major Incident Hazards
- **Seveso, Italy, 1976 –** Introduction of the SEVESO Directive I & II – Implemented in the UK through the Control OF Major Accident Hazards Regulations (COMAH)
- **Piper Alpha, UK 1987 –** Leads to the HSE taking responsibility for Offshore safety and the introduction of the Offshore Installations (Safety Case) Regulations & Offshore Installations (Prevention of Fire & Explosion, and Emergency Response) Regulations (PFEER)
- **Buncefield, UK, 2005 –** Process Safety Leadership Group (PSLG) Report - Safety & environmental standards for fuel storage sites leading to increased focus on Functional Safety Management

Slide 1- 41

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

BP Refinery, Texas City Tx: 23 March 2005

Slide 1- 42

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

BP Refinery, Texas City – Refinery Explosion

2010 Agreement between OSHA and BP (Texas City Incident) –

BP shall complete a Safety Instrumented System Lifecycle Management to more completely implement the SIS Standard (ANSI/ISA S84.00.01-2004) at the Refinery and cover the following subject matters:

(a) Policies, Procedures, and/or Standards
(b) Competency Requirements
(c) Training Requirements
(d) Documentation Requirements
(e) Roles and Accountabilities of Departments and Individuals; and
(f) Compliance Assurance and Auditing Protocols

BP agrees to pay the full amount of the remaining proposed penalties -$50,610,000.00

Slide 1- 43

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Buncefield, UK: 11 December 2005

Slide 1- 44

Function Safety Engineering

Government guidance and the Process Safety Leadership Group (PSLG) Guidance

- The Buncefield incident investigation team has the published eight reports providing findings and recommendations for use within the process industries.
- The report from the PSLG provides guidance on the application of functional safety management system
- Complements existing guidance on Safety Management Systems already provided in the SEVESO directive and other Process Safety Management guidance, regulations and standards

Slide 1- 45

Function Safety Engineering

The guidance states that for a Hazard Installation an Functional Safety Management System must be in place and contain for each phase in the Safety Instrumented System lifecycle:-

- Safety planning, organisation and procedures;
- Identification of roles and responsibilities of persons;
- Competence of persons and accountability;
- Implementation and monitoring of activities;
- Procedures to evaluate system performance and validation including keeping of records;

Slide 1- 46

Function Safety Engineering

PSLG Guidance continued:-

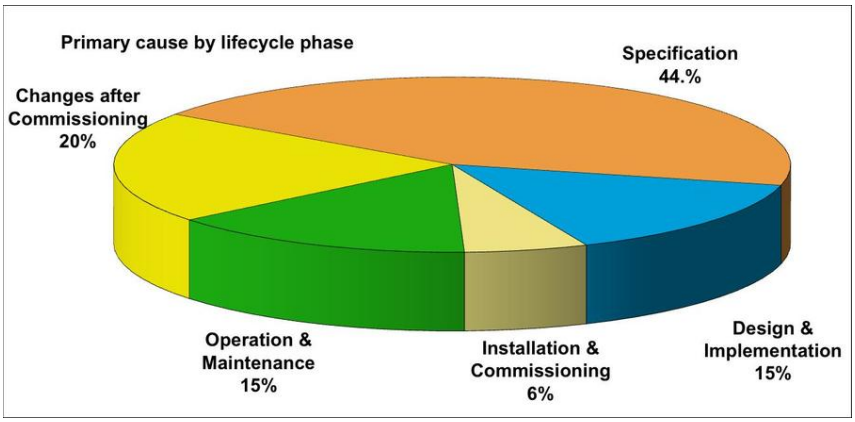
- Procedures for operation, maintenance, testing and inspection;
- Functional safety assessment and auditing;
- Management of change;
- Documentation relating to risk assessment, design, manufacture, installation and commissioning;
- Management of software and system configuration

▪The focus of the guidance supports previous HSE research into the causes of systematic failures

Slide 1- 47

Function Safety Engineering

Incidents Caused by Control and Safety System Failures



HSE UK : "Out of Control" Figure 10 (*ISBN 978 0 7176 2192 7)*

Slide 1- 48

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

HSE Summary: Analysis of Incidents

- Majority of incidents could have been anticipated if a systematic risk-based safety lifecycle approach had been been applied
- Safety principles are independent of the technology
- Situations often missed through lack of systematic approach
- Need to verify that the specification has been met
- Over dependence on single channel of safety
- Failure to verify and validate the software
- Poor consideration of human factors
- Inadequate specification of the safety requirements because of :
  - poor hazard analysis
  - inadequate assessment of the impact of failure modes of the control system

Slide 1- 49

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

HSE Health & Safety Executive

Regulatory Compliance

Every employer MUST comply:

•Every employer shall make a **Suitable and sufficient** assessment of the risks to the health & safety of his employees …and of persons not in his employment

•Every employer shall make and give effect to such risk reduction arrangements as are arrangements **as are appropriate**…..

Slide 1- 50

ProSalus SAFETY CONSULTANTS

Function Safety Engineering

Hierarchy of UK Health and Safety Regulations

Health and Safety at Work Act 1974

Employer and Employee Duties, OSH Standards, Enforcement and Penalties

EU Seveso II Directive

Process Safety Management

COMAH
Control of
Major Accident Hazard

DSEAR (ATEX)
Dangerous Substances
and Explosive
Atmospheres

PUWER
Provision and Use of
Work Equipment

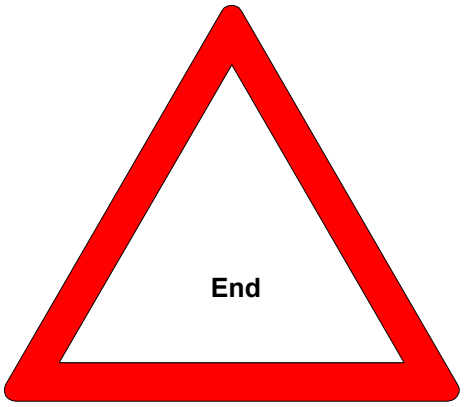
MHSWR
Management of Health &
safety at Work

Machinery
Directive

Slide 1- 51

ProSalus SAFETY CONSULTANTS

Function Safety Engineering



Slide 1- 52

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Management
And
The Safety Life Cycle

Slide 2 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Why should safety be documented?**
  - Safety has to be demonstrated and evidence supplied
  - Safety must be auditable and traceable
  - Safety needs verifiable information
  - Regulators need to see safety is under control
  - Regulator requires that safety documentation can be reproduced
  - Evidence must be securely stored and backed up
  - Safety Documentation will be used through out the plant lifetime

FSM can now be approved / certified by Third parties such as

TUV Rheinland

Slide 2 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Safety life-cycle goals (Clause 6.2.3)

1. ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both function and safety integrity requirements;
2. ensure proper installation and commissioning of the safety instrumented system;
3. ensure the safety integrity of the safety instrumented functions after installation;
4. maintain the safety integrity during operation (for example, proof testing, failure analysis);
5. manage the process hazards during maintenance activities on the safety instrumented system.

Slide 2 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Purpose of Functional Safety Management Systems

- The purpose of the FSM system is to clearly describe the processes adopted by an organisation to assure the suitability and continuing functional integrity of safety instrumented systems essential to ensure the safety of hazardous processes
- The FSM approach based on the IEC 61511-1 lifecycle framework is considered to be one of the most effective means of recording how to generate, review, implement, verify and thereafter audit, revise and manage so as to achieve effective functional safety life-cycle operation of safety instrumented functions.

Slide 2 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **FSM procedures are required to increase the probability of avoiding systematic failures**
  - Typically due to human error so procedures are proven to work
  - Guidance on the application of the techniques and measures to avoid systematic failures is given in:
    - IEC 61508-2 – Annex B Tables B1-B5
    - IEC 61508-3 - Annex B Tables A1-A10
  - Guidance on assessing Software systematic capability is given in:
    - IEC 61508-3 – Annex C
  - Techniques and measures are given for each phase of the lifecycle
  - Techniques and measures need to be appropriate to Target SIL

Slide 2 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 2 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Scope of Functional Safety Management Systems

- It is important not to confuse FSM with the Site Safety Management System (SMS) which details how the business manages safety and meets its regulatory and legislative responsibilities
- FSM supports the overall site safety performance and an integral part of the site SMS
- FSM compliance should also be included in Key Performance Indictors, Process Safety Indicators, and Risk Analysis
- IEC 61511-1 life cycle framework - equipment, software and management systems that comply with IEC 61508 will also comply with IEC 61511 simplifying project procurement and planning for obsolescence for legacy systems.

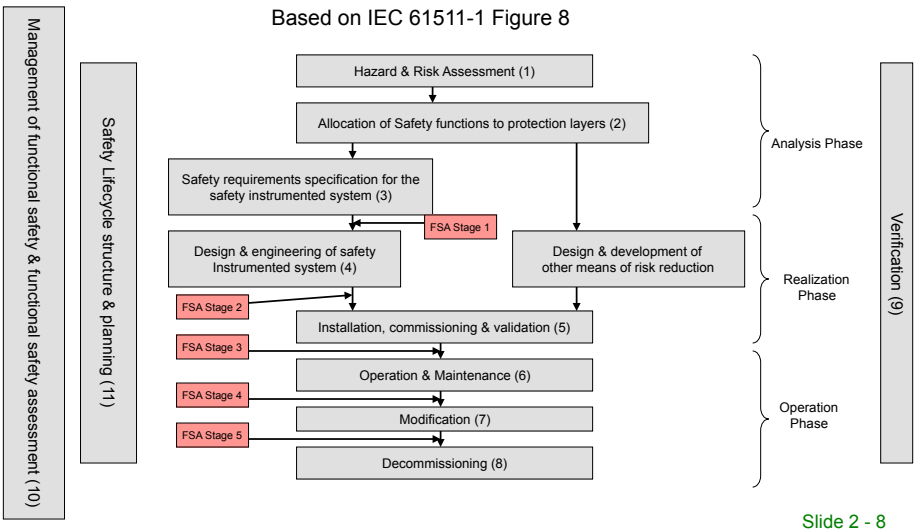
Slide 2 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Lifecycle Concept

Based on IEC 61511-1 Figure 8

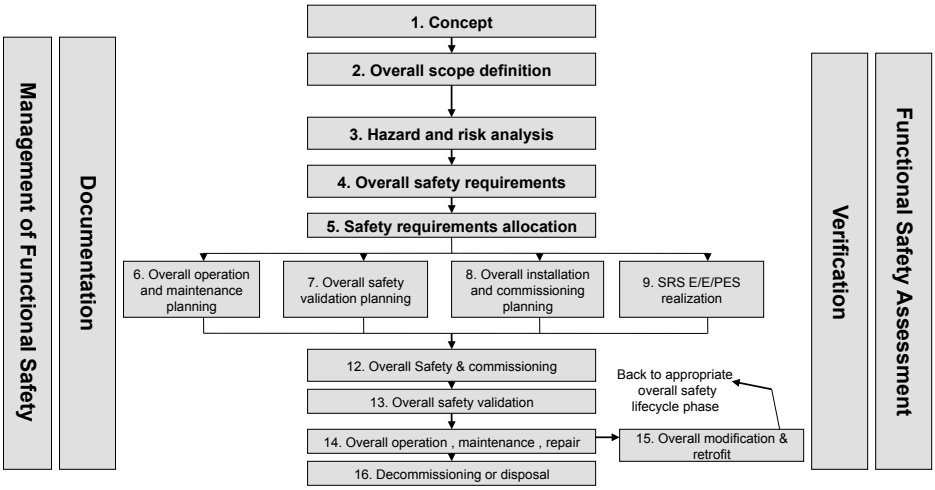


Slide 2 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Lifecycle Concept



Slide 2 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical contents for an IEC 61511 FSM System

1. Functional Safety Policy
2. Management Of Functional Safety
3. Functional Safety Life-Cycle
4. Verification
5. Process Hazard and Risk Assessment
6. Allocation Of Safety Functions
7. Safety Requirements Specification
8. Design and Development
9. Application Software
10. Factory Acceptance Testing
11. Installation and Commissioning
12. Validation
13. Operation and Maintenance
14. Modification
15. Decommissioning
16. Information and Documentation
17. Product Supply and Safety Manual

Slide 2 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Management of Functional Safety

- **Requirements:**
  - **General:**
    - Defined policy and strategy for achieving safety
    - Defined functional safety indicators (PSM – HSG254)
      - Leading & Lagging Indicators
    - Safety Management System (HSG65)
  - **Organisational Competence:**
    - Responsible persons, departments & organizations
      - Identified for each of the lifecycle phases
      - Competency assurance at each stage (HSE – CMS / IET Guidance)
        - Knowledge, training, experience and application
        - Knowledge of legal and safety regulations
        - Understanding of hazards and consequences
        - Understanding of novelty and complexity of technology

Slide 2 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Policy

- Commitment to promote sound integrity management under the umbrella of IEC 61511
- Policy to design, build, install, commission and service the SIS in accordance with IEC 61511
- Strategy to communicate, promote and monitor a FS conscious attitude by the methodical implementation of formal FSM procedures.
- Commitment to carry out FS Audits and Competency Assessment.
- Success can be measured in terms of achieved system functional safety and achieving the SIL throughout the life of the SIS .
- FS system must be systematically audited and reviewed and all personnel, working on or responsible for safety related systems, are required to adhere to the procedures

Slide 2 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Management of Functional Safety

- **Requirements**
  - **Implementing and monitoring procedures**
    - PHA Procedure
    - Safety Requirements Template / Checklist
    - Functional Safety Management Plant Template
    - Design Procedures
    - Hardware / Software Verification Procedure
    - Hardware / Software Validation Procedure
    - Functional Safety Assessment Procedure
    - Functional Safety Audit Procedure
    - Change Management, Software Modification & Impact Analysis
  - **Software configuration management – IEC 61511**
    - Planning and procedures for
      - Software Compliance – e.g. IEC 61131
      - Application Software Development
      - Software Integration - Module & Firmware

Slide 2 - 13

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical Safety Lifecycle Documentation

Phase	Information
All phases	Safety plan, plans for each phase of the lifecycle, IEC 61508 table of Techniques & Measure
Hazard and risk analysis & Allocation of Safety Functions	HAZOP, SIL Determination, LOPA, ETA, FTA, QRA, COMAH etc reports
Safety Requirements	Specification with all safety functions and their functional and integrity requirements, cause and effects
Design & Engineering	SIS design, FDS, SDS, SMDS, HFT,GA, Control and logic philosophy, SLD, circuit diagrams, manuals, reliability analysis etc
Installation and commissioning	Checklists, Integration, FAT, SAT specification and reports, Installation and commissioning plans and functional checklists
Safety validation	Functional safety Assessment, Verification and Validation report
Operation and maintenance	Functional Testing, Inspection and Maintenance Logs, FS audit reports
Modification and Decommissioning	Change management / modification request, impact analysis reports,

Slide 2 - 14

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Verification & Validation, Assessments, Audits

- **Verification - (IEC 61511 Clause 7)**
  - Verification is carried out after each lifecycle phase
    - Check of values used in LOPA
    - Check of failure data used and calculations undertaken
    - Check of SFF and correct Hardware Fault Tolerance applied
- **Validation - (IEC 61511 Clause 15)**
  - Validation is a phase in the lifecycle
  - Validation is carried out at the end of the Project / Modification, before hazards are present in the process
  - Validation verifies that the SRS has been met
- **Functional Safety Assessment (FSA) - (IEC 61511 Clause 5.2.6)**
  - Assesses that the FS lifecycle plan has been correctly implemented
  - 5 assessment stages during the lifecycle – Stage 3 mandatory
  - Must be carried out with sufficient independence to meet the target SIL

Slide 2 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Verification Report

- Scope & boundaries of verification
  - What is being verified – (e.g. checking PFD calculations)
  - Information that verification is to be carried out against – (e.g. SIL target)
- Who is verifying – (person, competence & level of independence)
- Procedures, measures and techniques to used for verification activity – (e.g. FTA to check RBD)
- Tools and supporting analysis – (e.g. failure data, confidence levels)

Slide 2 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Verification Report cont'd

- How will non conformances be handled – (e.g. action log / priority)
- Declaration of pass/fail criteria - (e.g. Tolerances)
- How failure / non-compliance will be managed

- Typical example:
  - Loop Calculations
  - Correct software test methods for target SIL (61508 tables)

Slide 2 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Validation Report

- Scope & boundaries of Validation
  - What is being validated – Description of SIS & associated devices
  - IEC 61511 Clause 15 requirements addressed and included in SRS
  - Information that validations is to be carried out against – SRS, Cause & Effects, function charts etc
- Who is validating – person, organisation, competence & level of independence
- Procedures, measures and techniques to used for validation activity – e.g. loop testing, calibration procedures, simulation of application software
- Tools and supporting analysis – e.g. test instruments calibrated to traceable standard

Slide 2 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety (SIL) Validation Report cont'd

- How will non conformances be handled – e.g. action log / priority
- Tools & techniques appropriate for Target SIL
  - IEC 61508-2 – Table B.5
  - IEC 61508-3 – Table A.7
- Declaration of pass/fail criteria - e.g. SRS not met, logic not as per Cause & Effect. Timing requirements not met
- Typical example:
  - Completed Loop test procedure
  - Correct software test methods for target SIL (61508 tables)

Slide 2 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 2 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 2 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Clause 15 - Validation activities must include:

1. SIS performs in all operating modes as identified in the SRS;
2. Adverse interaction of BPCS or other systems has no affect on SIS;
3. SIS properly communicates & Computations are correct;
4. Sensors, logic solver, & final elements perform in accordance with SRS;
5. SIS documentation is consistent with the installed system;
6. Confirmation that SIF performs as specified on invalid PV values;
7. The proper SD sequences activate with correct annunciation / display;
8. SIS reset , bypass, start up overrides & manual SD functions perform as SRS;
9. The proof-test intervals are documented in the maintenance procedures;
10. Diagnostic alarm functions perform as required;
13. Confirmation that the SIS performs as required on loss of utilities & returns to the desired state on reset;
14. Confirmation that the EMC immunity, has been achieved.

Slide 2 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Assessment IEC 61511 Clause 5.2.6

Investigation, based on evidence, to judge the functional safety achieved by one or more protection layers

As a minimum 1 FSA must be carried out at Stage 3 prior to hazards being present

To be compliant with the requirements of IEC 61511 FSA should be carried out at the following stages of a project:

- **Stage 1** - After HRA, Protection Layers identified and SRS complete
- **Stage 2** - After SIS design
- **Stage 3** – After Installation, pre-commissioning, validation & operation and maintenance procedures have been developed.
- **Stage 4** - After gaining experience in operating and maintenance
- **Stage 5** - After modification and prior to decommissioning of a SIS

Slide 2 - 23

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Functional Safety Assessment must confirm

- The PHRA has been carried out (Clause 8);
- The PHRA recommendations have been implemented or resolved;
- MOC procedures are in place and have been implemented;
- The recommendations arising from previous FSA have been resolved
- The SIS is designed, constructed and installed in accordance with the SRS, any differences having been identified and resolved;
- The SIS safety, operating, maintenance and emergency procedures are in place;
- The SIS validation planning is appropriate and the validation activities have been completed;
- Employee training has been completed and appropriate information about the SIS has been provided to the O&M personnel;
- Plans or strategies for implementing further FSAs are in place.

Slide 2 - 24

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical Information required for FS Assessment

- Results for previous FS assessments & HRAs
- Risk Targets and Risk Reduction measures implemented
- Allocated Safety Requirements for Protection Layers
- Safety Requirements and Cause and Effects
- Identified SIFs and Verification Data
- Verification & Validation Reports (Inspections, FAT, SAT, Commissioning)
- Functional Safety Management Procedure
- SIS Operation and Maintenance Reports & Procedures
- Details of SIS Modification and Impact Analysis
- Development & production tools used (S/W simulation, Test equipment)
- Operating history including data to be used for Prior use arguments
- Safety Instrumented - Supplier list

Slide 2 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Audits

- Similar techniques required as for Quality Auditing
- Could be managed by Quality Department if checklist developed
- Audits that Functional Safety Management procedures are being correctly implemented not technical content
- Six monthly for a new systems / Annual for mature systems
- Auditor must be sufficiently independent from people doing the work
- Non Conformances need to be prioritised and actioned
- Recording and follow-up critical

Information required for FS Audit

- FSMP – Responsible Departments / Persons
- FSM & Competency management Procedures
- Results from previous Audits

Slide 2 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Level of Independence Requirements
IEC 61508-1 Tables 4 & 5

Minimum Level of Independence	Consequences or Safety Integrity Level/Systematic capability			
	1 / A	2 / B	3 / C	4 / D
Independent person	X	X1	Y	Y
Independent Department	-	X2	X1	Y
Independent Organization	-	-	X2	X

X2 applies depending on previous experience, degree of complexity, novelty of design, technology

Slide 2 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Management of Change (Clause 5.2.6.2.2 & 17)

- A modification procedure needs to be included in FSM
- Impact Analysis needs to be carried out to assess impact on FS
- Review documentation – where in the lifecycle does impact have an effect on safety possibly even back to Phase 1 - PHRA
- We need to understand the impact of change – such as:
  - Replace a safety component with a different manufacturer (No assessment required for like for like replacement)
  - How much retesting is required (modular design reduces impact of retesting)
  - Need to consider verification and revalidation requirements
  - Update all impacted documentation with change
- Competent Authority to sign off

Slide 2 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Functional Safety Capability Gap Analysis**
  - Requirement to identify weaknesses / gaps in the FSM system
  - Based on the concept of Targets Of Evaluation (TOES) first introduced in the CASS guidelines (www.cass.uk.net)
  - Adapted for IEC 61511 FSM requirements
  - Assesses the current status of an organisations – plans, procedures and work instructions
  - Maps FSM to IEC 61511 Part 1 requirements and relevant industry guidance as appropriate
  - Provides recommendations for improvements
  - Determines current Functional Safety Capability

Slide 2 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Scope of FS Gap Analysis**
  - Functional Safety Policy
  - Functional Safety Procedures
  - Functional Safety Life Documentation
  - Other company procedures were appropriate e.g. training records, disaster recovery procedures
  - Records of all activities concerned with Functional Safety
  - Include IEC 61508-1/2/3 and 6 were appropriate
  - Competency Management System must be included

Slide 2 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

FUNCTIONAL SAFETY MANAGEMENT SYSTEM – MAPPING TABLE TO STANDARDS					
T.O.E. Number/Description		Procedures and Controls Required to Comply	IEC61511 Refs. (Clause. Para)	Auditors Comments	Action
1.	General Requirements	Functional Safety Management System	5.2.1	Company does not currently operate an informal FSM based on the 61511 standard.	1. Develop a formal methodology document, based on the existing QMS procedures to capture Company functional safety processes 2. Review the existing QMS procedure against the 61511 lifecycle requirements and develop or modify procedures to ensure all clause are adequately addressed
2.	General Requirements	Functional Safety Policy Statement	5.2.1.1	No formal statement and strategy document in place at the time of the audit	3. Prepare statement to include top level strategy / approach to FS

Typical FS gap analysis record sheet

Slide 2 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- The mapping leads to recommendations to either update, revise or introduce new procedures and work instructions and systems to improve compliance
- Changes to existing systems should be implemented through a:
  - Roll out exercise through out the organisation
  - Series of workshops / toolbox talks to keep staff up to date
- Must include competency testing and assessment of staff that will be directly interfacing with the SIS including operations, maintenance and engineering.

Slide 2 - 32

ProSalus SAFETY CONSULTANTS

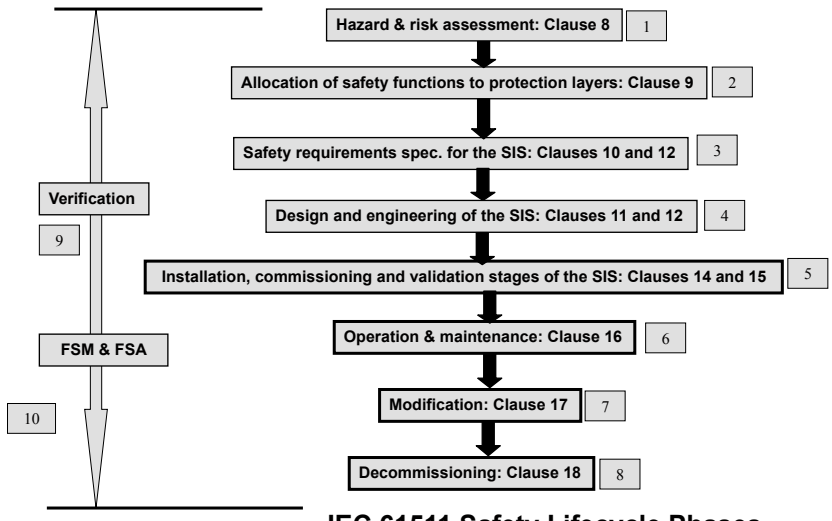
Functional Safety Engineering

Example of the Planning Process

Slide 2 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



IEC 61511 Safety Lifecycle Phases

ProSalus Limited

Slide 2 - 34

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

EEMUA 222 Competency Assessment Form Lifecycle Phases 1 to 3

Safety lifecycle phase	Competence requirements	Range statement (specifies the context)	Competence components (assessment is against these components)	Assessor comments and evidence	Gaps and closure actions	Gap management actions
1. Hazard and Risk Analysis	Can fully participate in hazard identification, hazard analysis, hazard and operability (HAZOP) studies, and computer/control HAZOP (CHAZOP) studies.	For SIS equipment and hazards associated with plants *X, Y and Z*.	1.1 Understands principles of hazard identification, hazard analysis and HAZOP and CHAZOP studies. 1.2 Understands where hazards may be introduced by the SIS. 1.3 Has experience of participating in hazard identification, hazard analysis or HAZOP and CHAZOP studies.	*(Record verbal and written evidence of meeting competence component requirements)*	*(List identified gaps against competence requirements for the role and actions to close gaps e.g. training, alternative work experience)*	*(State how each gap will be managed until the candidate is re-assessed as competent for the role, e.g. seek approval of AN Other, supervised by a competent person)*
2. Allocation of Safety Functions to Protection Layers	Can effectively allocate safety functions to SIS, other technology and procedural protection layers as carried out in LOPA studies.	For the technologies and operational processes on plants *X, Y and Z*.	2.1 Understands the effectiveness of different types of protection layers and appropriate credit that can be taken for each. 2.2 Has experience of allocating safety functions to protection layers. 2.3 Has experience of participating in or leading SIL determination using LOPA. 2.4 Is familiar with use of SIL determination software, if appropriate.			
3. Safety Requirements Specification for the SIS	Can develop safety requirements specification for the SIS.	For the technologies and hazards associated with plants *X, Y and Z*.	3.1 Knows and understands how to develop functional specifications. 3.2 Knows and understands how to develop integrity specifications. 3.3 Has experience of developing a Safety Requirements Specification including role statements and functional and integrity specifications for SIS in accordance with IEC 61511			

Slide 2 - 35

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 2 - 36

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Safety Competency Assessment (FSCA)

Slide 2 - 37

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **HSE Competency Management System Guidance**
  - Compliance is Mandatory
  - 4 Phases: Plan, Design, Operate, Audit and Review
  - 15 Principles to consider
- **HSE/BCS/IET competencies guidelines**
  - levels of competence
  - functions and 'jobs'
  - example requirements
  - Assessment
- **Continuing Professional Development (CPD)**
  - Requirement for Professional Institutes

Slide 2 - 38

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Competency Programs**
  - **Institutes** - objective to set (members) apart from others in the field
  - **Functional Safety Certified Engineer** - TUV based schemes, with international membership based around examination and Functional Safety experience
  - **HSE Competency Management Scheme** - Based on Institute of Railway Signalling Engineers (IRSE) - well-established scheme, focused on industry requirement
  - **HSE/IET/BCS in the UK** - general competencies for safety practitioners based on IEC 61508 - largely workplace/experience based self assessed
  - **EEMUA 222 -** Based on process industry requirements

Slide 2 - 39

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Guidelines published by IET from HSE/IET/BCS study**
  - focuses on electrical, electronic and programmable electronic systems
- Competencies of four types
  - technical skills
    - e.g. hazard analysis, report writing
  - behavioural skills
    - e.g. personal integrity, interpersonal skills, problem solving, attention to detail
  - underpinning knowledge
    - e.g. domain (application area) knowledge
  - underpinning understanding
    - e.g. principles of safety and risk

ProSalus Limited

Slide 2 - 40

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Structure of the Guidelines

- The guidelines are organised around functions
  - these are 'job functions', not system functions
    - e.g. independent safety assessment (ISA)
- Competency levels
  - three levels are distinguished *within* each function
    - supervised practitioner
      - *work always checked by a practitioner or expert*
    - practitioner
      - *capable of working alone or supervising others*
    - expert
      - *can take overall responsibility, and work in novel situations*
- Guidance on operation of a competency scheme
  - mapping to organisation
  - assessing individuals

ProSalus Limited

Slide 2 - 41

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functions in the Guidelines

- Initial set of 'job functions'
  - C1 ~corporation functional safety management (CFM)
  - C2 ~ project safety assurance management (PSM)
  - C3 ~ safety-related system maintenance and modification (SRM)
  - C4 ~ safety-related system or services procurement (SRP)
  - C5 ~ independent safety assessment (ISA)
  - C6 ~ safety hazard and risk analysis (HRA)
  - C7 ~ safety requirements specification (SRS)
  - C8 ~ safety validation (SV)
  - C9 ~ safety-related system architectural design (SAD)
  - C10 ~ safety-related software realisation (SSR)
  - C11 ~ safety-related hardware realisation (SHR)
  - C12 ~ human factors engineering (HF)

ProSalus Limited

Slide 2 - 42

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Sets of Competencies

- For each function, competencies are divided into
  - function related
    - which apply to the function as a whole
      - *e.g. ISA 14 Principles of functional safety assurance*

    Has a knowledge and understanding of the principles of functional safety assurance and can relate them to a typical safety lifecycle model
  - task related
    - which apply to individual tasks within the function
      - *e.g. ISA 5 Reviewing safety documentation*

        Accurately and systematically review documents, supported by discussions to clarify ambiguities and understanding where necessary, to obtain evidence to support a judgement on whether a system has satisfied its functional safety requirements
- Criteria are then set out against these competencies

ProSalus Limited

Slide 2 - 43

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Sample Criteria

ISA 5 Reviewing safety documentation		
Accurately and systematically reviews documents, supported by discussions to clarify ambiguities and understanding where necessary, to obtain evidence to support a judgement on whether a system has satisfied its functional safety requirements		
Supervised Practitioner	Practitioner	Expert
Has successfully performed review work requiring a high degree of accuracy	Can illustrate with e.g. review reports, witness testimonies how inaccuracies omissions and deficiencies have been identified in reviewing safety-related system documentation as part of independent safety assessments	Can illustrate through review procedures and review records, how actions have been taken to ensure the accuracy of design reviews carried out as part of independent safety assessments. Can illustrate how insufficient accuracy in reviewing documentation has led to uncertainty with regard to a safety assessment
In this case, relatively clear progression of capability		

ProSalus Limited

Slide 2 - 44

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Assessment

- Guidelines identify six evidence types
  - assignment and/or project records (AP)
    - engineers log books
  - workplace observation (WO)
    - usually evidence from supervisor/line manager
  - competence test (CT)
    - might be test on content of relevant standards
      - *e.g. CASS assessment*
  - witness testimony (WT)
    - more general 'testimonial' than workplace observation
  - oral (OR)
    - response to questions at the assessment meeting
  - documentary evidence (DC)
    - e.g. project reports or papers

ProSalus Limited

Slide 2 - 45

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Adapting for an Organisation

- The guidelines acknowledge that this needs to be done
  - suggested process
    - identify a responsible person (presumably at least expert CFM)
    - this person audits the organisation to identify
      - *safety related functions (in the safety process, not in products)*
      - *staff carrying out safety work*
      - *who else should be included*
  - it is expected that some 'jobs' in a given organisation will mix functions in the guidelines
    - the responsible person should modify the criteria to match the organisation and document the results
    - this may mean moving functions
      - *e.g. moving (copying) testing from safety validation (SV) to human factors engineering (HF) if safety-related human interface tests are carried out*
    - function related competencies may also need to be moved

ProSalus Limited

Slide 2 - 46

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Assessment

- Assessment process (scheduled) managed by responsible person
  - assessors allocated for individuals
  - with support of 'technical experts' if necessary
- Assessments are done through meetings
  - 10-15 minutes per task or function related competency
  - expected outcomes
    - assessment
      - *profile against competency statement for function*
    - recommendations
      - *e.g. training*
    - information to help in team building
- Assessment scheme kept under review
  - to improve the scheme, as necessary

ProSalus Limited

Slide 2 - 47

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Competency Statement: ISA5 Reviewing safety documentation		
Summary of evidence provided including context	Evidence Type	OR
Gave presentation on recent project situation where it was found during review of the safety documentation that the treatment of software failures in system fault was consistently incorrect.		
	Expert	
	Practitioner	✓
	Supervised Practitioner	

ProSalus Limited

Slide 2 - 48

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Assessment Summary															
Experienced analyst, but needs more training in planning and eliciting information															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Total
Expert					■			■				■				3
Practitioner	■	■		■	■	■	■	■	■	■		■	■	■	■	13
Supervised Practitioner	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	15

In order to obtain expert level the candidate requires:

1 Training in preparation of safety assessment plans and maintaining plans through the lifetime of the project

2 Experience in collecting information from all relevant stakeholders

Date for next assessment	dd/mm/yyyy

ProSalus Limited

Slide 2 - 49

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Observations

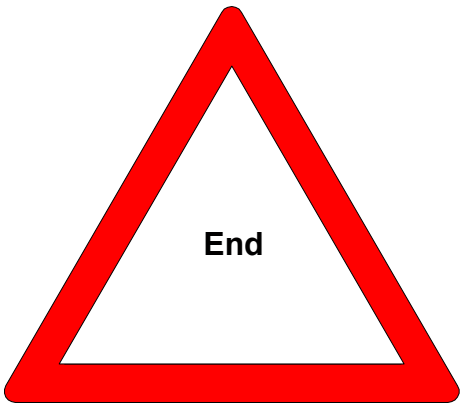
- Individual skills and competencies are important
  - perhaps more so in safety than other areas, due to the difficulty of validating analyses
  - particularly crucial for ISA, due to importance of role
- HSE/IET/BCS guidelines are quite comprehensive
  - but need to be interpreted for specific 'jobs' in companies
- HSE guidelines now in place and are a mandatory requirement

ProSalus Limited

Slide 2 - 50

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 2 - 51

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard

And

Risk Assessment

IEC 61511 Phase 1

Slide 3 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Requirements – Clause 8

A hazard and risk analysis shall be carried out on the process and its associated equipment. It shall result in:

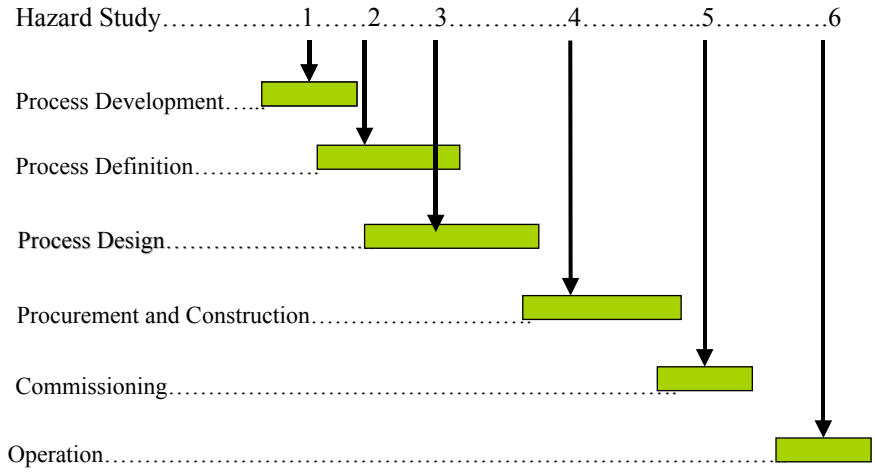
1. a description of each identified hazardous event and the factors that contribute to it (including human errors);
2. a description of the consequences and likelihood of the event;
3. Consideration of conditions such as normal operations, start up, shutdown, Maintenance, upsets, ESD
4. the determination of requirements for additional risk reduction necessary to achieve the required safety;
5. a description of the measures taken to reduce or remove hazards and risk;
6. a description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates and any credit taken for operational constraints or human intervention;
7. Allocation of the safety functions to layers of protection taking into account the impact of common cause failures between safety layers
8. identification of those safety functions applied as SIFs

Slide 3 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard Studies

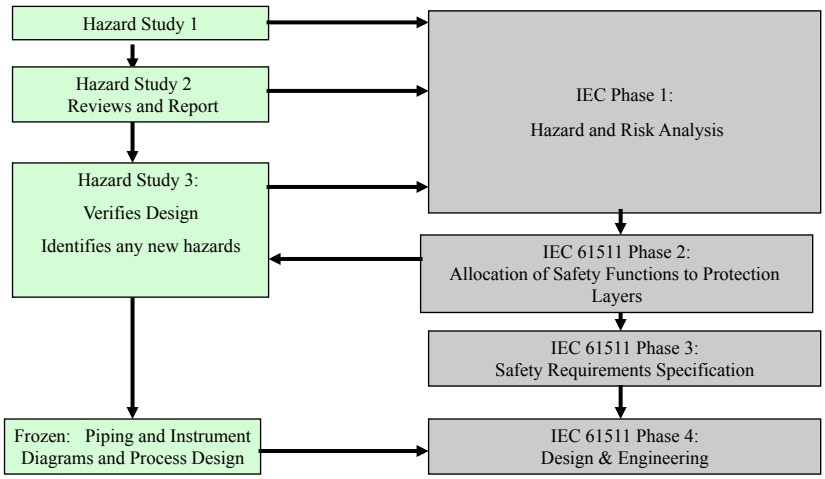


ProSalus Limited Slide 3 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Activity Model: Hazard Studies and Safety Lifecycle Phases



ProSalus Limited Slide 3 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard Study 1

- Identify hazards associated with the process.
- Identify major environmental problems and assess suitability of proposed sites
- Criteria for hazards, authorities to be consulted, standards and regulations, codes of practice.
- Collect/review information on previous hazardous incidents.

Also known as: Concept and definition phase hazard study or Screening Level Risk Analysis (SLRA)

ProSalus Limited Slide 3 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

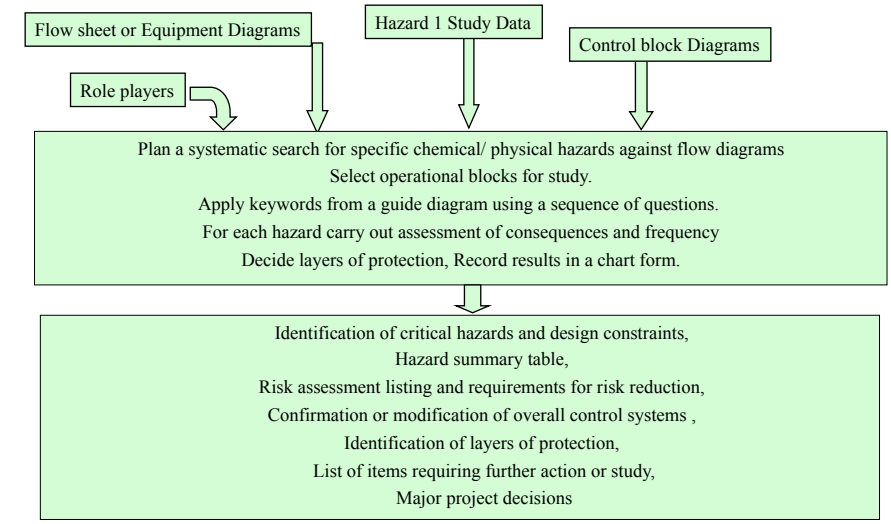
Process Hazard Study 2

- Examine plant items and equipment on process flow sheet and identify significant hazards
- Identify areas where redesign is appropriate
- Assess plant design against relevant hazard criteria
- Prepare environmental impact assessment

ProSalus Limited Slide 3 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 3 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Measures to prevent or eliminate causes

Measure	Reduce hazard due to
Pressure/temperature reduction in process	High energy levels, stresses
Minimize equipment, piping, seals and joints	Leaks
Design for containing maximum pressure	Rupture/bursting
Provide pressure relief system	Rupture/bursting
Location/layout/spacing	Interactions/confined spaces
Operational alarms	Wrong operating conditions
Automatic protection systems (SIS)	Wrong operating conditions, dependency on human response

ProSalus Limited

Slide 3 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Measures to mitigate or reduce consequences

Measure	Mitigate Consequences of
Containment/bunding/safe disposal	Uncontrolled dispersion, contamination
Rapid leak detection	Leaks leading to gas cloud /liquid pool
Rapid fire detection	Runaway Fire
Control room/occupied buildings design for pressure shocks	Injury to occupants
Toxic refuge (Gas safe room)	Toxic vapour exposure
Fire protection/dispersion aids – water jets	Spread of fire
Fire fighting facilities	Uncontrolled fire
Off site vent/ Relief discharges	Uncontrolled emissions
Isolation of stages and units	Migration of fires Feeding of fires from other units
Emergency procedures	Uncontrolled responses Chaotic evacuation
Emergency shutdown systems	Slow response to hazardous event. Dependency on human factors

ProSalus Limited

Slide 3 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard study level 3

- Critical examination of plant operations on completed design
- Identifies detail hazard, control and operability problems.
- Reviews existing safety measures
- Often uses Hazard and Operability study (HAZOP) method
- Should be completed before detailed design/ procurement begins

ProSalus Limited

Slide 3 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Overall HAZOP Study procedure

Definition Phase
Scope & objectives-- Responsibilities--Select team

Preparation Phase
Plan--Collect Data--Choose recording method
Estimate time required- Arrange the schedule

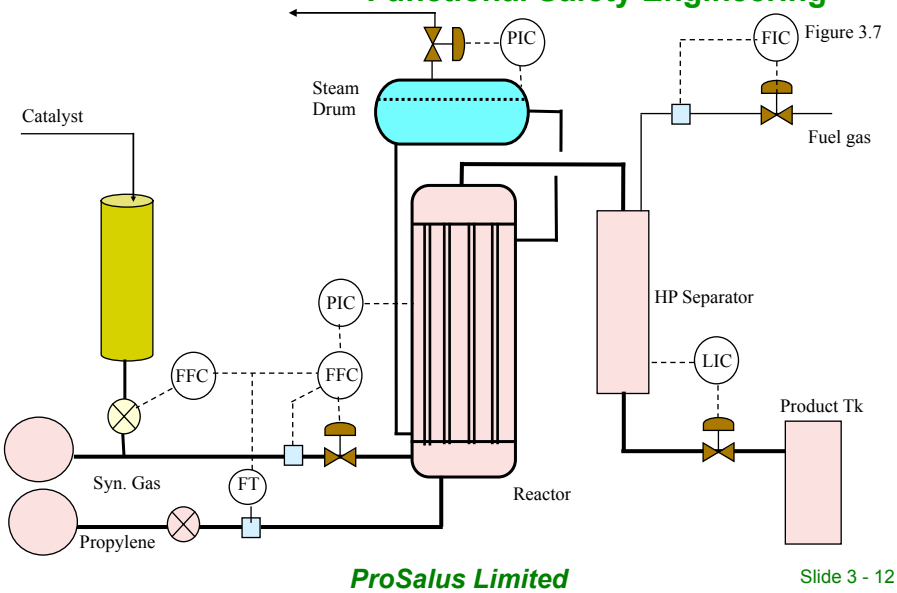
Examination Phase
Divide system into elements--Examine element for deviations from design intent
Identify possible deviations, cause, consequences, protection needs
Agree actions -repeat for each element

Reporting and Follow-up Phase
Record on worksheets--Sign off records--Produce report
Follow up actions - Restudy where needed- Issue final report

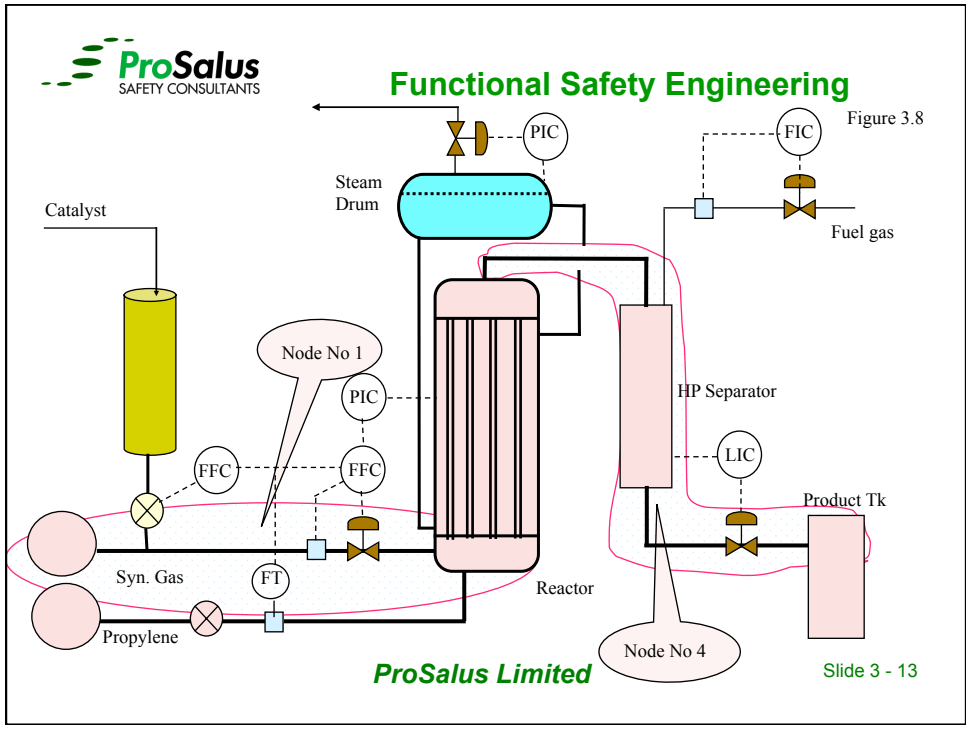
ProSalus Limited Slide 3 - 11

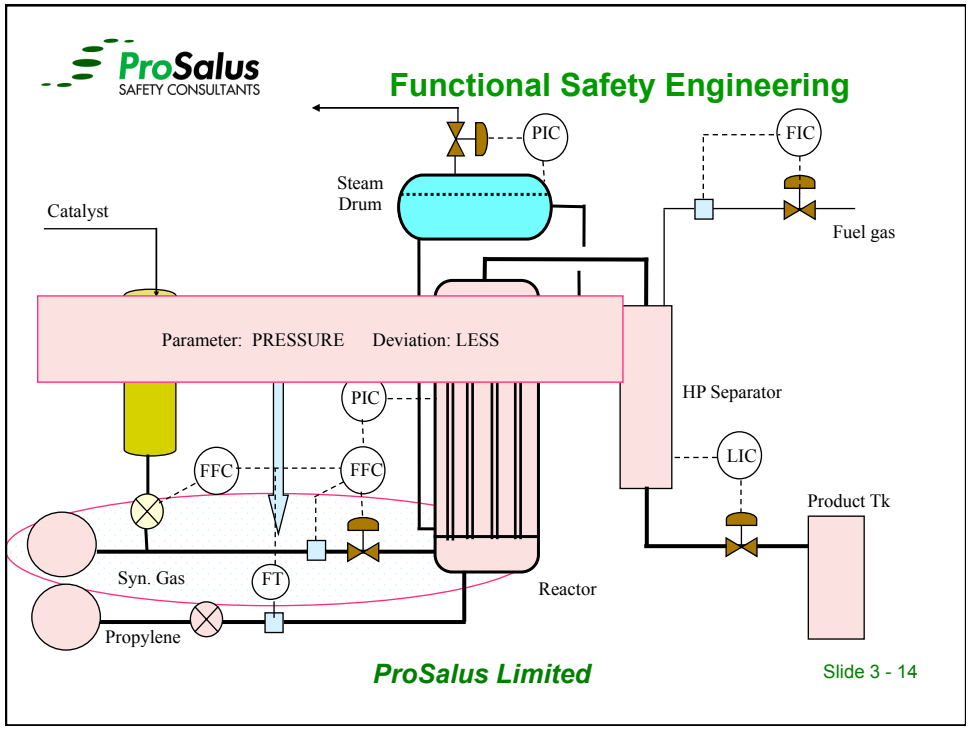
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited Slide 3 - 12





ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Line by Line Study

- Obtain a description of the intended normal modes of operation from the designer.
- Apply a series of prompts using keywords to stimulate thinking by the whole team about deviations from normality.
- Record those deviation conditions that are possible and are likely to have a significant consequence in terms of hazards or damage to the plant or severe loss of production.
- Record the corresponding actions required of the design team or the plant management as appropriate.

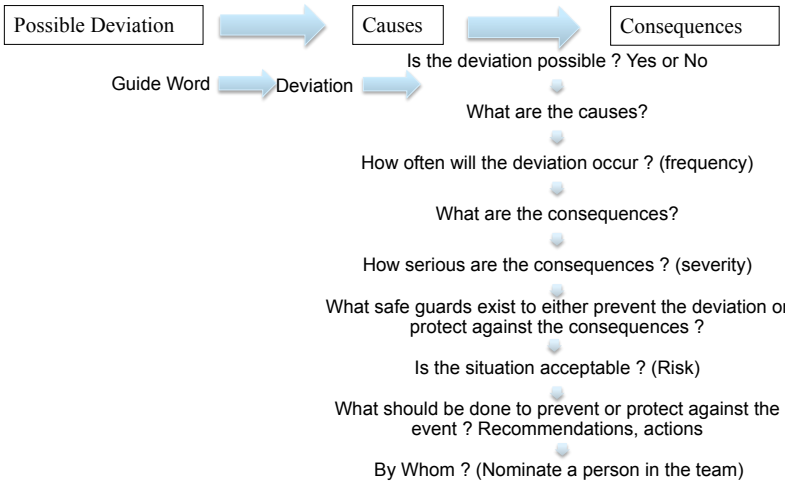
ProSalus Limited

Slide 3 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Causes and consequences



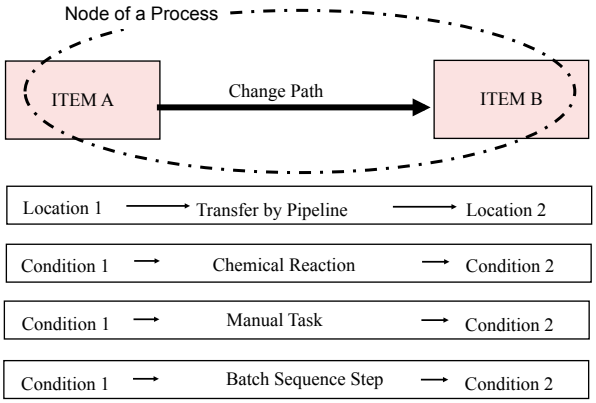
ProSalus Limited

Slide 3 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Change Path Concepts



ProSalus Limited

Slide 3 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Generating deviations

Basic Guidewords

Guideword	Meaning
NO or NOT (or none)	None of the design intent is achieved
MORE (more of, higher)	Quantitative increase
LESS	Quantitative decrease
AS WELL AS (more than)	Qualitative modification or additional activity occurs
PART OF	Only some of the design intent is achieved.
REVERSE	Logical opposite of design intent
OTHER THAN	Complete substitution – another activity takes place.

ProSalus Limited

Slide 3 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Derived Guidewords for Process Studies

Parameter	Guidewords that can give a meaningful combination
Flow	Non; more of; less of; reverse; elsewhere, as well as
Temperature	Higher; lower
Pressure	Higher; lower; reverse.
Level	None; higher; lower
Mixing	Less; more; none.
Reaction	Higher (rate of); lower (rate of); none; reverse; as well as.
Phase	Other; reverse; as well as.
Composition	Part of; as well as.
Communication	None; part of; more of; less of; other; as well as.

ProSalus Limited

Slide 3 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Creating Deviations

Combining guidewords with elements generates deviations, some of which are credible and some are not credible.

Guideword + Element → Possible Deviation

The multi disciplined (Process, Operations, Maintenance etc) HAZOP study team has the task of deciding what elements are applicable and then deciding what deviations are credible for each element

ProSalus Limited

Slide 3 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of guideword/element matrix for process example

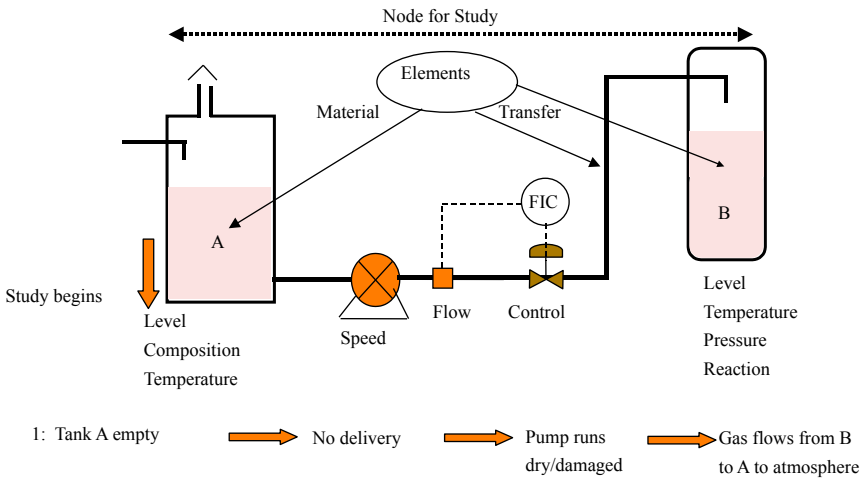
Element (parameter)	Guidewords								
	No	More	Less	Rev.	Part of	As well as	Where else	Early/ late	Other
Tank A Level	X	X	X						
Tank A Comp		X	X			X			
Flow in pipe	X	X	X	X		X			
Temp in pipe		X	X						
Pressure in pipe	X	X	X						X

ProSalus Limited

Slide 3 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 3 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Examples of Element First Examination Method

Part : Transfer of acid from A to B	Element: Tank A	Parameter: Level	
Deviation	NONE	**Meaning/effect:**	Tank is empty
Is it possible	YES		
Causes	1:No supply	2: Extraction exceeds inflow.	3:
How often?	Monthly	Monthly	
Consequences	1: No transfer	2: Pump damage	
Severity	Nil	Moderate+ Loss of production	
Safeguards	Operational	None	
Acceptable risk	N/A	NO	
What should be done		Low level detection and interlock on pump	
Action:	Specify safety trip	Process and Instrument engineers.	

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Causes of Deviations

The cause of a deviation will nearly always be due to a failure of some kind

- Hardware: Equipment, piping, instrumentation, design, construction, materials
- Software: Procedures, instructions, specifications
- Human: Management, operators, maintenance
- External: Services (steam, power), natural (rain, freezing), sabotage.

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Evaluating EUC Risks

- Safeguards will probably be in place …
- How do we describe the risks ?
  - Pretend there are no safeguards
  - Identify deviations and causes
  - Identify consequences, again without protection.
  - Recognize the protection measures provided (describe the safeguards)
  - Decide if the protection measures are good enough.

ProSalus Limited Slide 3 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hazard Study 4 - Purpose

Reservation review verifying that the provisions in all previous studies are fully implemented and that the installation has been implemented as per the design intent

- **Key Aspects**
  - Hazard review after construction is substantially completed but before hazardous materials are introduced to the plant
  - Check that equipment and installation is as per design intent
  - Check that previous Hazop Study actions are closed out
  - Emergency Plan and Operating and maintenance instructions / procedures have been handed over and are in place
  - Safety manual handed over
  - Staff training and competency assessments are complete

ProSalus Limited Slide 3 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hazard Study 5 - Purpose

Safety Health and Environmental audit of constructed plant before introducing hazardous materials to provide an opportunity for those responsible for personal safety, employee health and environmental protection on the site to satisfy themselves that the detailed implementation of the project meets the company, statutory and legislative requirements.

- **Key Aspects**
  - Hazard Review to ensure that safety, health and environmental management systems and procedures are in place
  - Process Safety Indicators have been identified and added to SMS
  - SIFs have been added to Site Risk Control Systems
  - Emergency Plan and Operating and maintenance instructions / procedures have been handed over and are in place are operational

ProSalus Limited Slide 3 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hazard Study 6 - Purpose

Ongoing review through out the plant life time to confirm that design has been fulfilled opposite SHE aspects and compare plant operational experience with assumptions made in hazard studies. First review will include confirmation that all documentation is available and in place.

- **Key Aspects**
  - First review 6 -12 months after plant operation
  - Validation that all documentation has been updated
  - Modifications made during commissioning and start up have not altered the risk profile
  - Validation of compliance to conditions of consent
  - Validation of employee occupational health monitoring

ProSalus Limited Slide 3 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

HAZOP Examples

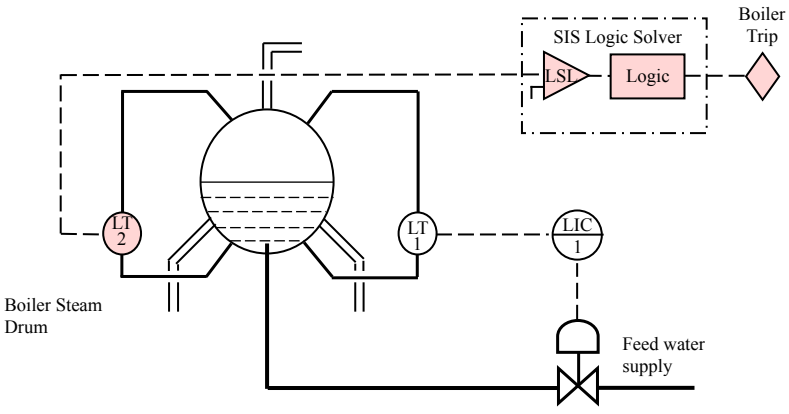
ProSalus Limited

Slide 3 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of a safeguard in place: Boiler drum level



ProSalus Limited

Slide 3 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Worksheet Example for Drum Level Hazard

Part : Boiler feedwater to drum	Element: Drum	Parameter: Level	
Deviation	LESS	Meaning/effect:	Drum level runs very low or empty
Is it possible	YES		
Causes	1:Loss of feedwater supply	2: Instrument fault, sensor reads high	3: Control valve fails shut
How often?	1 per yr	0.2 per yr	0.1/yr
Consequences	1: Boiler tubes overheat and rupture		
Severity	Severe. Risk of injuries	Severe: Damage to boiler	
Safeguards	Low feedwater pressure alarm	Low level trip system	
Acceptable risk	subject to satisfactory assessment		
What should be d one	Risk assessment to check safeguard performance		
Action:	Prepare safety requirements spec.	Determine target SIL rating of trip and alarm	

ProSalus Limited

Slide 3 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Complementary Hazard Study Techniques

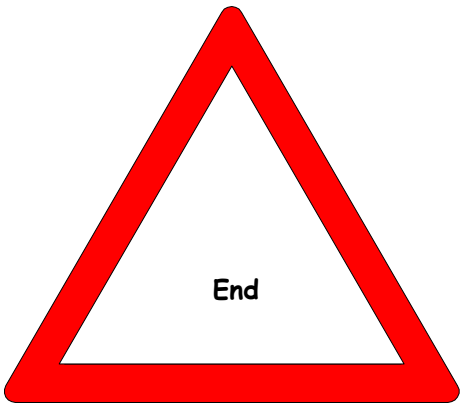
- Mechanical Plant, Instrumentation and Machines – FMEA, FMECA & FMEDA
- Electrical systems – E-HAZOP / Sneak Analysis
- Control systems - CHAZOP
- Alarm systems – Alarm Review – EEMUA 191
- Operation & Maintenance Tasks – Hierarchical Task Analysis
- Human HAZOP - Predictive Human Error Analysis (PHEA)

ProSalus Limited

Slide 3 - 32

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 3 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Reduction, Safety Allocation And Safety Requirements Specification

Slide 4 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Reduction

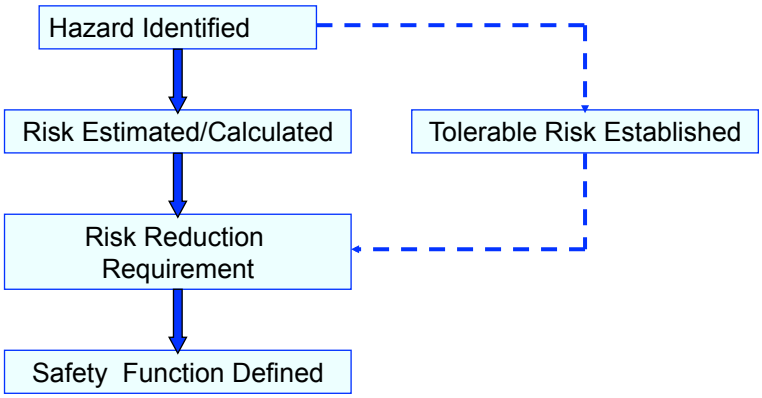
- At this point we know
  - We have identified the hazards
  - The cause / consequences pairs of the hazards
  - The likelihood or frequency of the hazards
- **Now we need to ask ourselves**
  - What is our Risk Target / Tolerability Criteria
  - Do we need to reduce the risk to make it As Low As Reasonably Practicable “ALARP”?
  - If so how much risk reduction is required?
  - Do we need a SIF to fill the gap to meet the Risk Target?

ProSalus Limited Slide 4 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Reduction: Design Principles



ProSalus Limited Slide 4 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Perception

- **There are different levels of risk:**
  - **High Consequence Low Frequency**
    - E.g. being struck by lightning 14 million to 1
  - **Low Consequence High Frequency**
    - E.g. office work – paper cuts etc
- Beware low frequency / high Consequence events
  - **Tolerable Risk**
    - Lies between negligible and unacceptable
    - The ALARP Region also requires consideration of reasonable practicability, established good practice & cost / Benefit Analysis
    - HSE – "Reducing Risks, Protecting People" (R2P2) and website for additional ALARP & CBA Guidance

ProSalus Limited Slide 4 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Individual Risk

ProSalus Limited Slide 4 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fatal Accident Rate - FAR

ProSalus Limited Slide 4 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Societal Risk

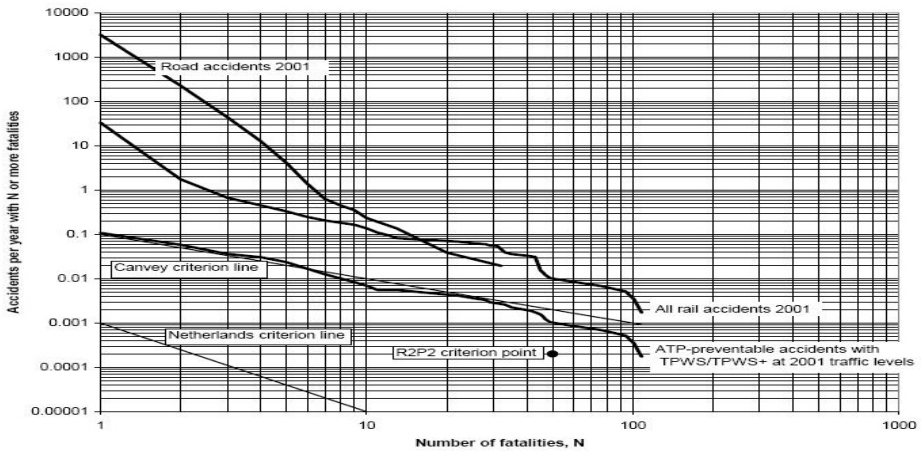
ProSalus Limited

Slide 4 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Figure 4: Transport FN-curves for 2001 and FN-criteria



Example FN – Curve Slide courtesy of UK HSE

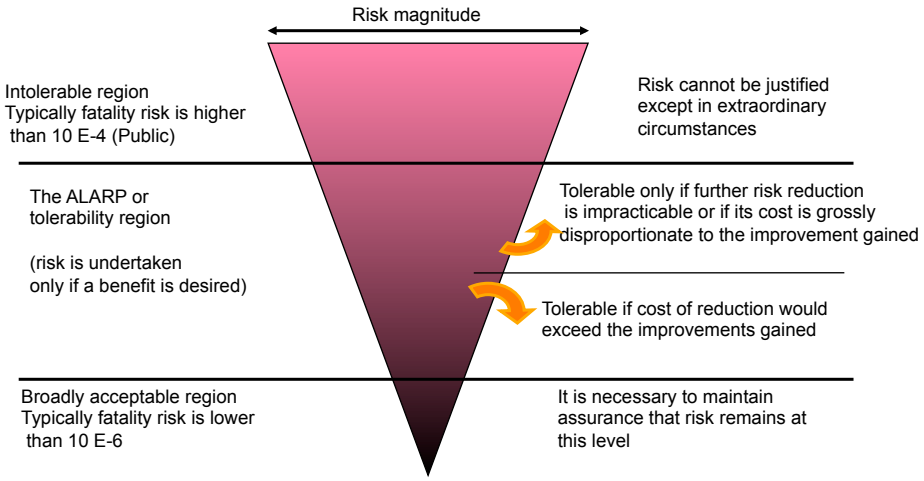
ProSalus Limited

Slide 4 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ALARP boundaries for individual risks: Typical values.



ProSalus Limited

Slide 4 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Government Tolerable - Risk Criteria Summary

	Maximum acceptable risk to the public
UK	1×10^{-4}
Hong Kong	1×10^{-5}
Netherlands	1×10^{-6}
Australia	1×10^{-6}

ProSalus Limited

Slide 4 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

As Low As Reasonably Practicable (HSE)

- The concept of "Reasonably Practicable" is fundamental to the setting of Health& Safety goals rather than being prescriptive.
- In most cases can be achieved by implementing existing "good practice" e.g. IEC 61511 for Safety Instrumented Systems
- For high hazard scenarios a more formal decision making technique is required, that could include event trees, fault trees, fire and gas modeling possibly complied as a safety case or safety report that includes cost benefit analysis, sensitivity analysis and optioneering
- Reasonably Practicable means (Edwards v NCB [1949]) weighing the risk against the sacrifice needed to further reduce it always weighting the decision in favour of H&S because the presumption is always that the risk reduction measure should be implemented

ProSalus Limited Slide 4 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Cost Benefit Analysis (HSE)

- Benefits can include: reduction in risk to workers & the public; cost of avoidance of contamination, environmental damage, site evacuation; deployment of emergency services
- Typical costs of prevention of H&S impact on people are (HSE)
  - Fatality - £1,336, 800 (x2 for cancer)
  - Permanent injury - £207,200
  - Serious injury - £20,500
  - Slight - £300
- Typical Disproportion factors (HSE) "rules of thumb"
  - 3 for risks to workers
  - 2 for low risks to members of the public
  - 10 for high risk scenarios i.e. multiple fatalities

ProSalus Limited Slide 4 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

CBA Worked Example (HSE)

- Consider a chemical plant with a process that if it were to explode could lead to:
  - 20 fatalities
  - 40 permanently injured
  - 100 seriously injured
  - 200 slightly injured
- The rate of this explosion is 1 in 100,000 per year.
- The plant has an estimated lifetime of 25 years.

- How much could the company reasonably spend to eliminate (reduce to zero) the risk from the explosion?
- If the risk of explosion were to be eliminated the benefits can be assessed to be:

Fatalities:	20	x £1,336,800	x 1x10-5	x 25 yrs	= £6684
Permanent injuries:	40	x £207,200	x 1x10-5	x 25 yrs	= £2072
Serious injuries:	100	x £20,500	x 1x10-5	x 25 yrs	= £512
Slight Injuries:	200	x £300	x 1x10-5	x 25 yrs	= £5
Total benefits =					**= £9,283**

- The sum of £9,283 is the estimated benefit of eliminating the major accident explosion at the plant on the basis of avoidance of casualties. (This does not include discounting or take account of inflation)
- For a measure to be deemed not reasonably practicable, the cost has to be grossly disproportionate to the benefits.
- This is taken into account by the disproportion factor (DF). In this case, the DF must reflect that the consequences of the explosion are high. Therefore based on HSE guidance a DF of 10 is considered reasonable
- Therefore it would be reasonably practicable to spend up to somewhere in the region of **£93,000 (£9300 x 10)** to eliminate the risk of an explosion on the plant.

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Overview

Of Formal

Risk Analysis Techniques

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Management can be applied in three ways

- Reduce the consequences to an acceptable level, or
- Reduce the frequency to an acceptable level, or
- Reduce the overall risk to an acceptable level

Risk Analysis Techniques

- **Risk Analysis** is the systematic use of available information to identify hazards and to estimate the risk to individuals, groups (societal), assets or the environment
- **Risk Estimation** is the process used to produce a measure of the level of risk for the hazard being analysed and consists of:
  - Frequency Analysis
  - Consequence Analysis
- **Risk Evaluation** is the judgement as to whether the risk is tolerable taking into account a countries risk criteria and other factors such as environmental and socio-economic aspects

ProSalus Limited Slide 4 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Typical Risk Analysis Techniques used in the Process Industry

- Event Tree Analysis
- Failure Mode and Effect Analysis & Criticality Analysis
- Fault Tree Analysis
- Hazard and Operability Studies (HAZOP)
- Human Reliability Analysis
- Preliminary Hazard Analysis (HAZID)
- Reliability Block Diagrams
- Consequence Models
- Sneak Analysis

ProSalus Limited Slide 4 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Frequency Analysis

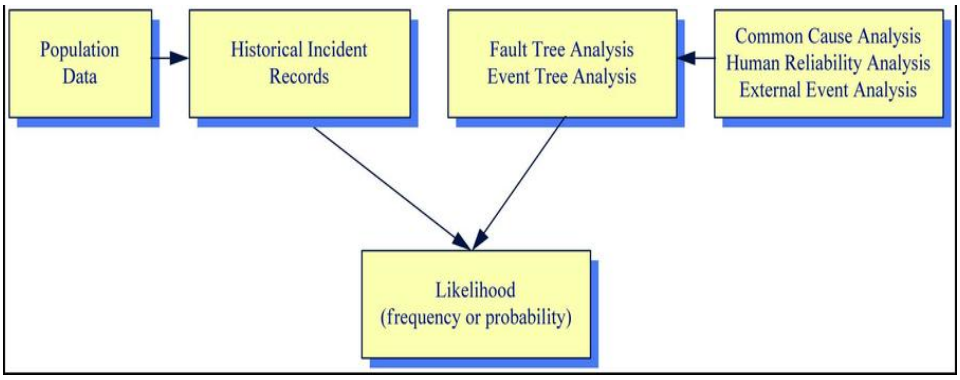
- Used to estimate the likelihood of each identified hazardous event
- Three approaches are commonly used to estimate frequencies:
  1. Use relevant historical failure data e.g. OREDA, AIChem, Faradip
  2. Frequency of event derived from analytical techniques e.g. ETA, FTA
  3. Use of expert judgement

ProSalus Limited Slide 4 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Frequency Analysis (DNV)

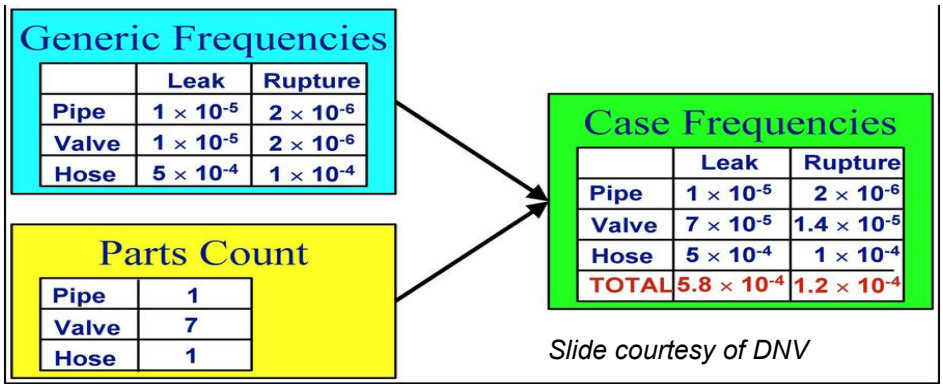


ProSalus Limited Slide 4 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Failure Case Frequency Calculation Method Based on Historical data Method



Slide courtesy of DNV

ProSalus Limited Slide 4 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Consequence Analysis

- Used to estimate the likely impact on individuals, populations (societal), property or the environment should the undesired event identified during hazard identification occur
- Usually an estimate of the number of people (receptors), located in different environments at different distances from the source of the event

  that might be either killed, injured or seriously affected by the event
- Events usually comprise of
  - Release of toxic materials
  - Fires
  - Explosions
  - Projectiles
- Further information - Guidelines for Chemical Process QRA CCPS publication ISBN 0 8169 0720 X

ProSalus Limited Slide 4 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Consequence Analysis

Discharge Models

↓

Dispersion Models

↓

Flammable and Toxic Effect Models

Slide courtesy of DNV

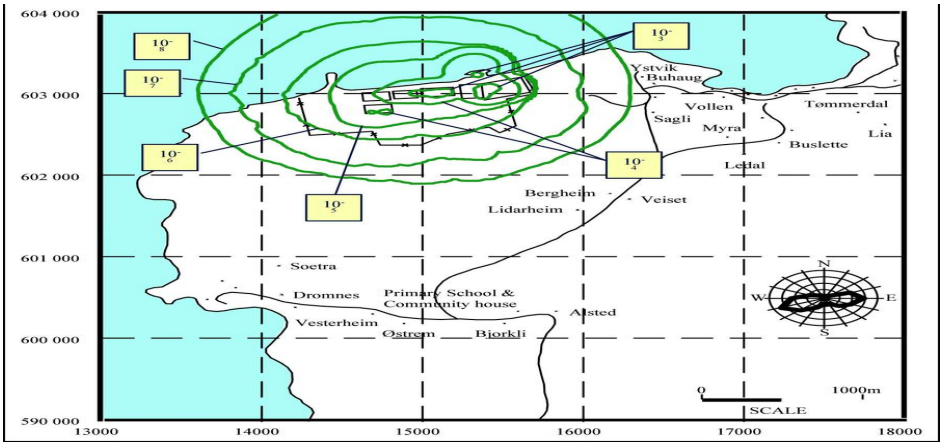
ProSalus Limited

Slide 4 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of presenting Risk Contours



Slide courtesy of DNV

ProSalus Limited

Slide 4 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of a presenting Fire Model

Slide courtesy of DNV

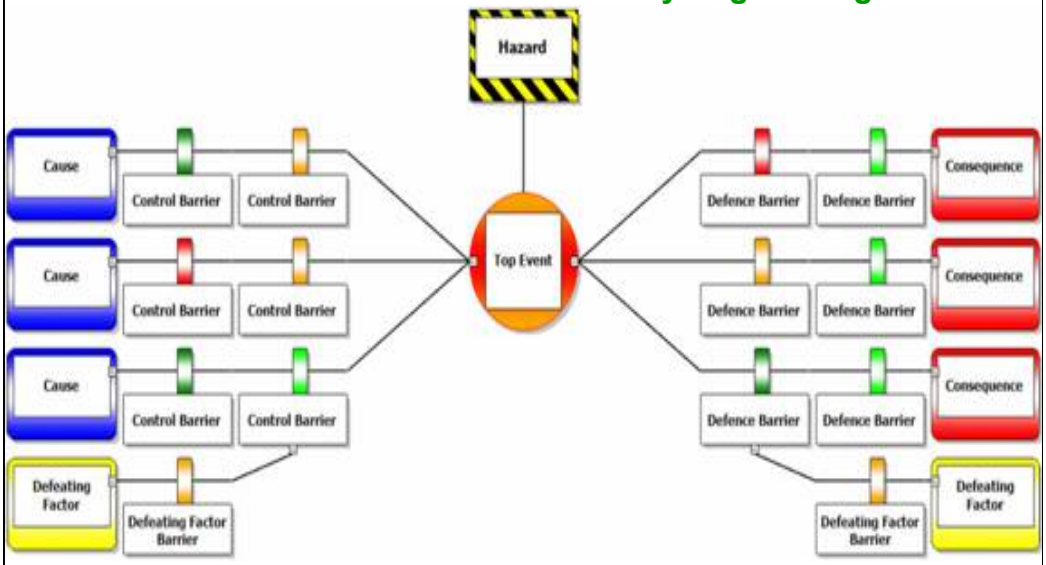
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Bow Tie Diagram**
  - Simple Graphical means to illustrate the relationship between
    - Major risk / hazard / undesirable event
    - Its causes / threats
    - Its consequences
    - The associated prevention and mitigation controls
  - Helps demonstrate how major risks are controlled
  - Supports the Safety case
  - Can be Qualitative or Semi Quantitative

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 4 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511
Safety Allocation
and
Risk Reduction Analysis Techniques

ProSalus Limited

Slide 4 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Introduction to Risk Reduction

- Risk Reduction can be achieved through any of the techniques which impact on the reduction of risk
- Risk can be spread across several techniques usually termed safety allocation:
  - Process design – focus's on inherent safety;
  - Technical Safety – focus's on passive protection measures
  - Functional Safety – focus's on active protection measures
  - Procedures & Process Safety Management
- All of these activities can form a part of the ALARP argument

ProSalus Limited Slide 4 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Impact of Risk Reduction Techniques

- Process design – reduction in severity of consequences and frequency of occurrence factors
- Mechanical design – reduction in severity of consequences and frequency of occurrence factors
- Layout design - reduction in severity of consequences and frequency of occurrence factors
- Control System design - frequency of occurrence factors
- Alarms - frequency of occurrence factors
- SIS design - frequency of occurrence factors
- F&G design - reduction in severity of consequences

ProSalus Limited Slide 4 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Risk Reduction Analysis techniques can be:**
  - Qualitative: everything expressed in words
  - Quantitative: everything expressed in numbers
  - Semi- quantitative: a mixture of words and numbers

ProSalus Limited Slide 4 - 29

ProSalus SAFETY CONSULTANTS

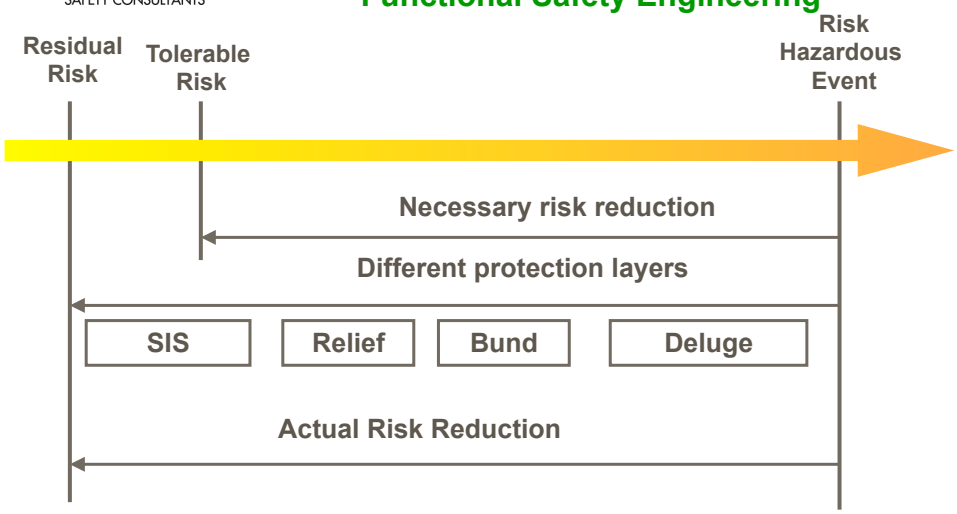
Functional Safety Engineering

- **IEC 61511 Risk Reduction Analysis techniques**
  - Simplified Risk Models
  - Fault tree analysis (FTA)
  - Event tree analysis (ETA)
  - Layer of protection analysis (LOPA)

ProSalus Limited Slide 4 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



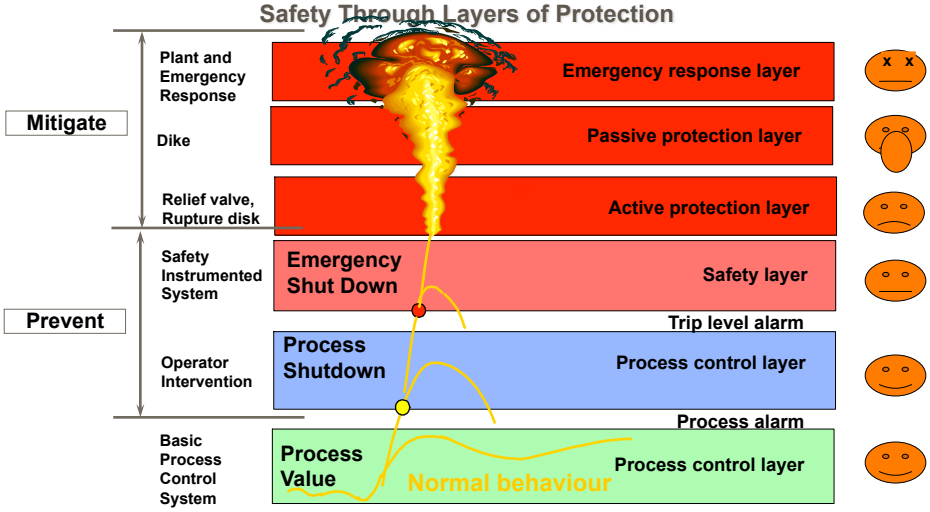
ProSalus Limited

Slide 4 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Through Layers of Protection



ProSalus Limited

Slide 4 - 32

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Simplified Risk Reduction Terms and Equations for use in Low Demand mode Applications

Ft = Tolerable Risk Frequency
Fnp = Unprotected Risk Frequency
Fp = Protected Risk Frequency

The Risk Reduction Factor:
RRF = Fnp / Ft

Safety Availability:
SA% = (RRF-1) x 100 / RRF

Probability of Failure on Demand:
PFDavg = 1 / RRF = ΔR = Ft / Fnp

ProSalus Limited Slide 4 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Simple Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1per 100000 yrs	IV	IV	IV	IV

ProSalus Limited Slide 4 - 34

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of applying the Risk Matrix Technique

A chlorine electrolyser plant presents a major leak hazard due to loss of pressure control.

The estimated frequency of occurrence is once per 10 years.

The estimated consequence without any protective measures is that the operating team of 3 people will be likely to suffer serious injury or they may be killed.

ProSalus Limited Slide 4 - 35

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Use the information given above and the Risk Matrix table below to classify the given risk and its frequency

Using this table, decide the maximum tolerable risk frequency to reduce the risk to class 3 (considered to be acceptable)

Calculate the target risk reduction factor, PFDavg values and safety availability required from the proposed Safety Instrumented System to achieve the tolerable risk frequency

State the target safety integrity level required from the SIS by reference to the SIL tables

ProSalus Limited Slide 4 - 36

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

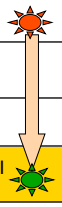
Slide 4 - 37

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1per 100000 yrs	IV	IV	IV	IV

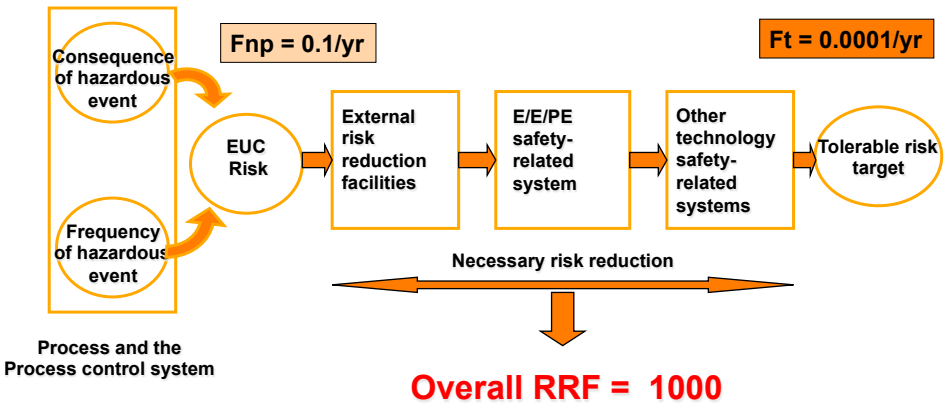


ProSalus Limited

Slide 4 - 38

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



Overall RRF = 1000

ProSalus Limited

Slide 4 - 39

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

PFDavg = 0.001

SIL = 2

Risk Reduction Factor: RRF = Fnp/Ft = .1/.0001 = 1000

The PFDavg required is 1/RRF = 1/1000 = $1x10^{-3}$

Safety availability = (RRF - 1)/RRF = 999/1000 = 0.999 or 99.9%.

The SIL table shows the required PFDavg is in the range 10^{-2} to 10^{-3} and therefore:

The required Safety Integrity Level is 2

ProSalus Limited

Slide 4 - 40

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Integrity Levels

Target failure measures (PFDavg) for a safety function operating in a low demand mode of operation

SIL	PFD	Safety Availability	Risk Reduction
4	0.0001 - 0.00001	0.9999 – 0.99999	10000 - 100000
3	0.001 – 0.0001	0.999 – 0.9999	1000 - 10000
2	0.01 – 0.001	0.99 – 0.999	100 – 1000
1	0.1 – 0.01	0.9 – 0.99	10 - 100

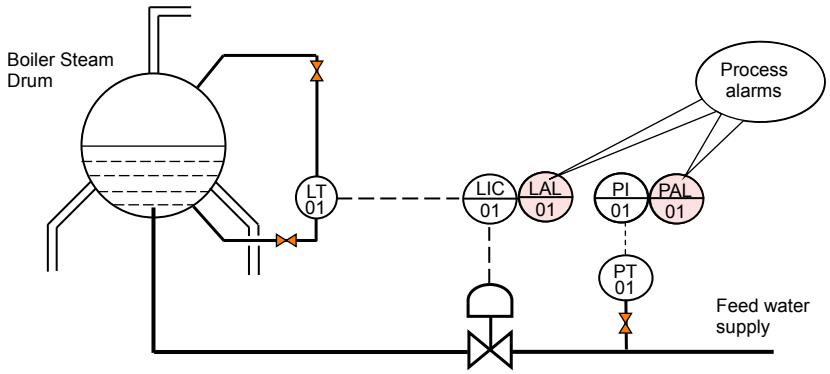
ProSalus Limited Slide 4 - 41

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of applying a Simplified Risk Model

Target RRF Determined as = 1000



HAZOP Study has identified a hazard of low level in Boiler drum leading to possible tube rupture and potential burn injury or possible fatality of 1 person with a frequency of once per year.

ProSalus Limited Slide 4 - 42

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I	I	I	II
1 per 10 years	I	I	II	III
1 per 100 years	I	II	III	III
1 per 1000 years	II	III	III	IV
1 per 10000 yrs	III	III	IV	IV
1per 100000 yrs	IV	IV	IV	IV

ProSalus Limited

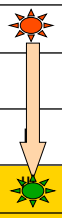
Slide 4 - 43

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Risk Matrix Table

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	minor injury	prod loss
1 per year	I		I	II
1 per 10 years	I		II	III
1 per 100 years	I		III	III
1 per 1000 years	II		III	IV
1 per 10000 yrs	III	III	IV	IV
1per 100000 yrs	IV	IV	IV	IV



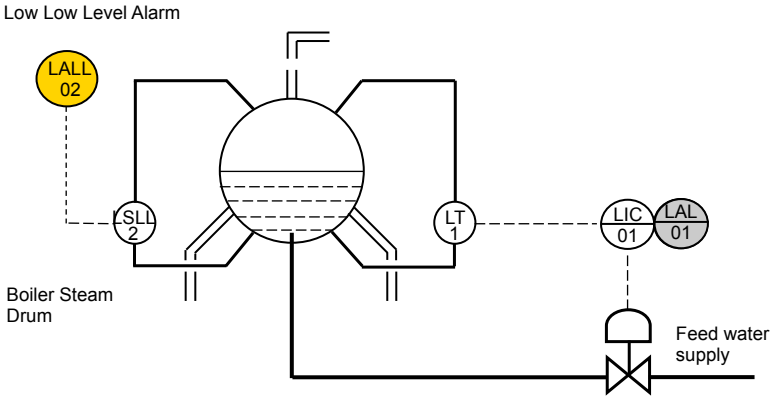
ProSalus Limited

Slide 4 - 44

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Stage 1 – Consider an Independent Alarm Function



ProSalus Limited

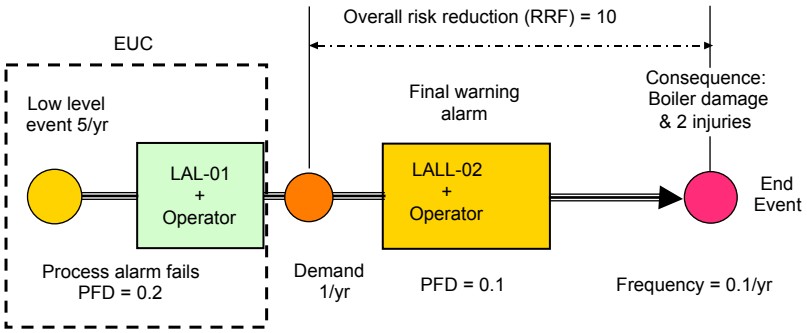
Slide 4 - 45

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk reduction model for Independent Alarm Function.

RRF = 1/PFD



Low level in drum 5 times per year operator misses process LAL once per year, assume 1 demand on IAF per year.

We must consider operator as well and therefore limit alarm to 0.1 in line with IEC 61511-3 guidance

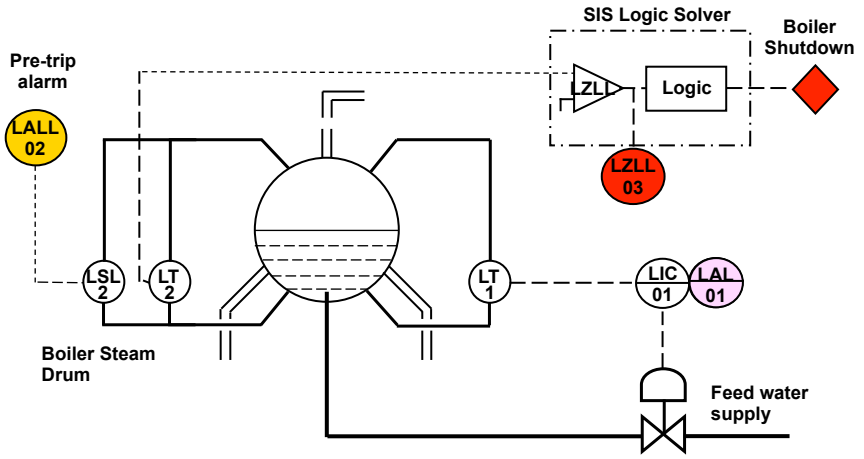
ProSalus Limited

Slide 4 - 46

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Low drum level protection with pre-trip alarm and SIF



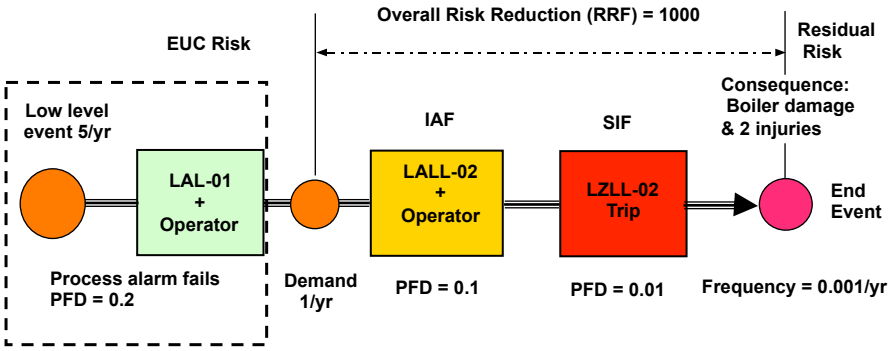
ProSalus Limited

Slide 4 - 47

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Reduction Model for Boiler Trip



Target RRF is 1000 therefore combined IAF (RRF = 1/0.1 = 10) x SIF (RRF = 1/0.01 = 100) = 10 x 100= 1000

ProSalus Limited

Slide 4 - 48

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **Fault Tree Analysis**
  - It is a top down technique
  - It starts with an undesired top event and from there we try to find out all different ways the top event can occur
  - It can be used to find any combination of events or failures that can cause the TOP event
  - It is a verification technique

ProSalus Limited Slide 4 - 49

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **What is fault tree analysis about?**
  - The causes of the TOP event are connected through logic gates in a tree format
  - Most common technique for casual analysis in risk and reliability studies, specially in the nuclear, aerospace and defence industries
  - Can be performed qualitative as well as quantitative

ProSalus Limited Slide 4 - 50

ProSalus SAFETY CONSULTANTS

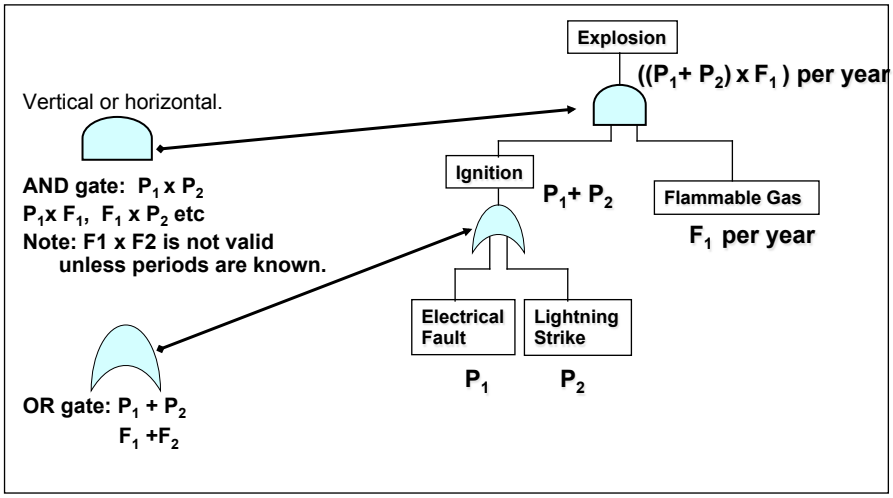
Functional Safety Engineering

- **The FTA Process**
  - Define scope of project
  - Define the top event
  - Develop the fault tree using gates
  - Identify Cut Sets (combination of base events that can cause the top event to occur)
  - Add Numerical values (Failures & Probabilities)
  - Document results

ProSalus Limited Slide 4 - 51

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

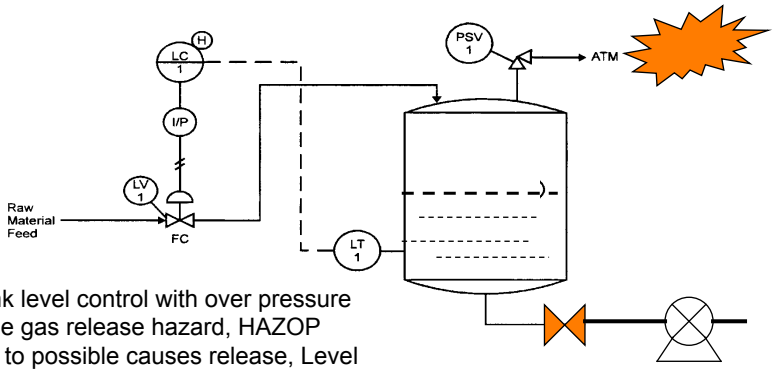


ProSalus Limited Slide 4 - 52

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of applying Fault Tree Analysis to a Risk Reduction



Basic tank level control with over pressure flammable gas release hazard, HAZOP identifies to possible causes release, Level control failure or operator error closing outlet valve when required open

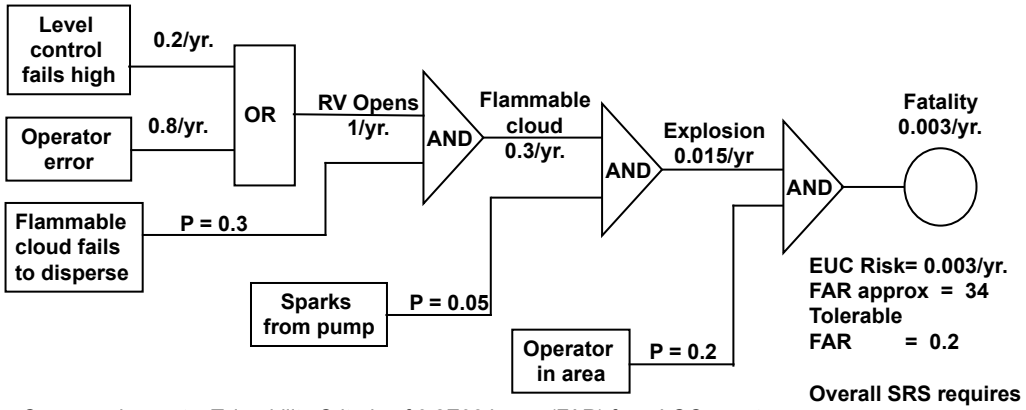
ProSalus Limited

Slide 4 - 53

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree for Tank Loss of Containment Example



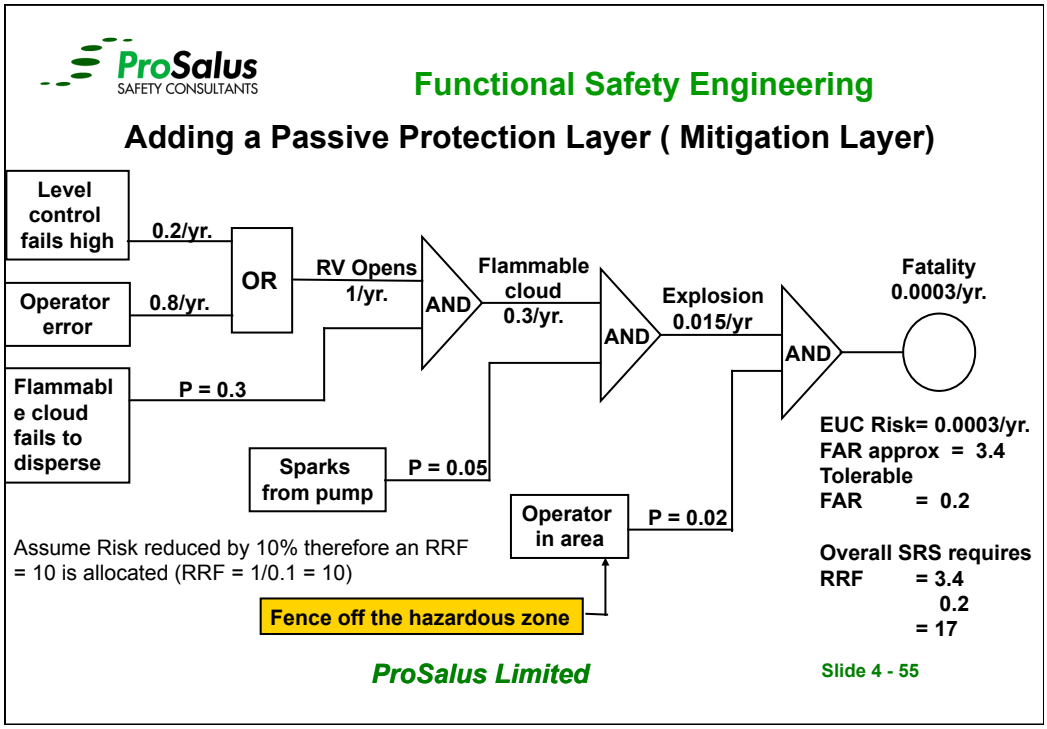
EUC Risk= 0.003/yr.
FAR approx = 34
Tolerable
FAR = 0.2

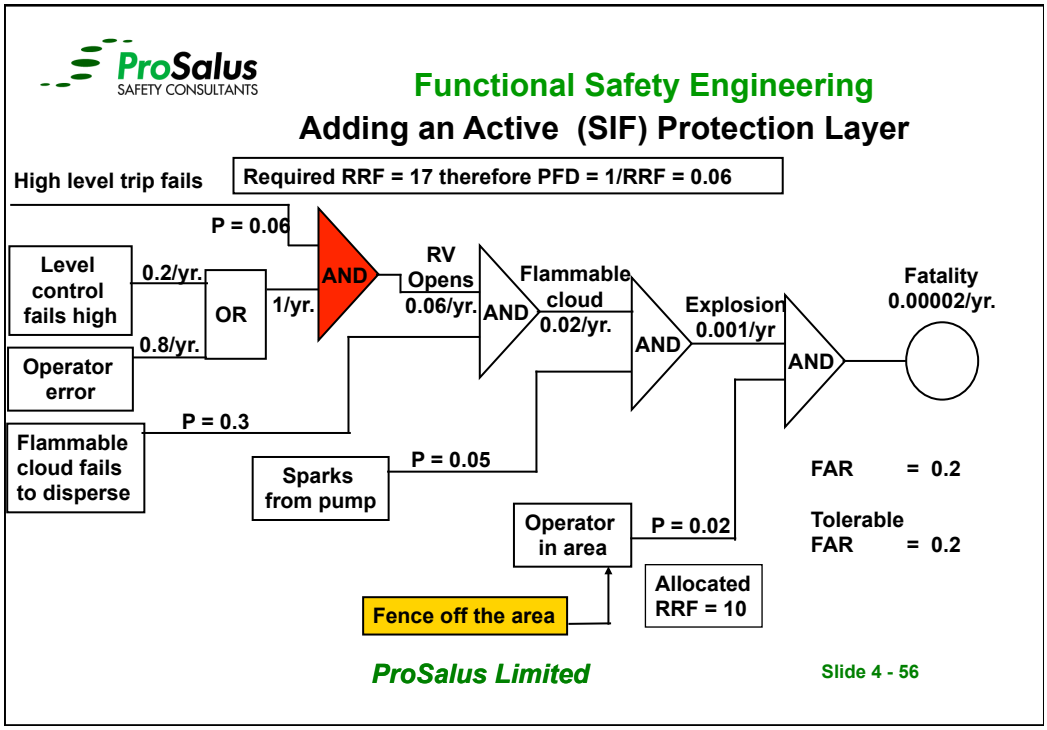
Overall SRS requires
RRF = 34 / 0.2
= 170

Company has set a Tolerability Criteria of 0.2E08 hours (FAR) for a LOC event leading to a possible fatality (assume 24/7 operation & 8760 hours = 1 year)

ProSalus Limited

Slide 4 - 54





ProSalus SAFETY CONSULTANTS

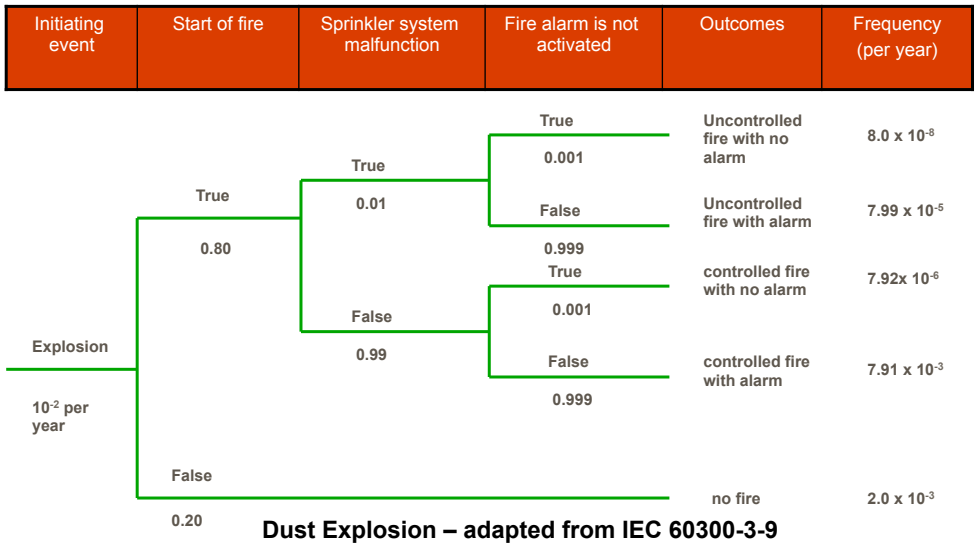
Functional Safety Engineering

- **Event Tree Analysis**
  - Helps us understand the consequences of events
  - Models an initiating event and the time sequence of event propagation to the potential consequences
  - Can be used qualitatively as well as quantitatively
  - Can be developed independently or in combination with fault tree analysis

ProSalus Limited Slide 4 - 57

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



Dust Explosion – adapted from IEC 60300-3-9

ProSalus Limited Slide 4 - 58

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

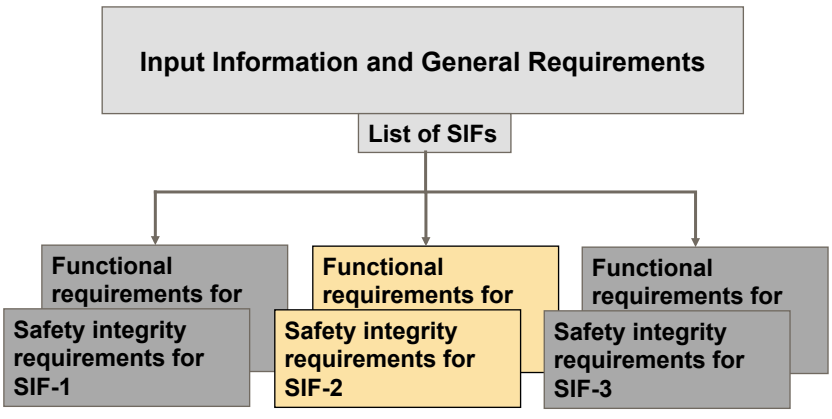
Safety Requirements Specification

Slide 4 - 59

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Requirements Specification



ProSalus Limited

Slide 4 - 60

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Integrity Requirements for a SIF

- The SIL of a SIF has been selected during the SIL determination study:
  - Risk Graph, LOPA, Risk matrix
  - SIL 1, 2 or 3
- This information must now be communicated to the design team to ensure the design meets the SIF safety integrity requirements during implementation implementation
- This is communicated by the Safety Requirements Specification (SRS) which is the basis of the SIS validation

ProSalus Limited Slide 4 - 61

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Functional Requirements for a SIF

- Functional requirements are derived from the hazard study and typically captured in the:
  - Piping & Instrument Diagrams
  - Cause & Effect Matrix
  - SIS Philosophy document
  - Functional Logic Diagram
- This information is communicated to the design team via the SRS to ensure required functionality is implemented
- This functionality is translated into the Functional design Specification (FDS) which is the basis of the SIS design

ProSalus Limited Slide 4 - 62

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Requirements Specification

- The SRS must prepared before commencing any design work
- Be based on the guidance in IEC61511-1/2 Clause 10 & 12
- Expressed and structured in such a way that it is:
  - Clear;
  - Precise;
  - Verifiable;
  - Maintainable;
  - Feasible
- Written to aid comprehension by those who are likely to utilize the information at any phase of the lifecycle

ProSalus Limited Slide 4 - 63

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Framework for the SRS

The SRS contains the functional and integrity requirements for each SIF and should provide sufficient information to design and engineer the SIS and include statements on the following for each SIF:

•Description of the SIF;

•Common cause failures;

•Safe state definition for the SIF;

•Demand rate;

•Proof test intervals;

•Response time to bring the process to a safe state;

•SIL and mode of operation (demand or continuous);

•Process measurements and their trip points;

•Process output actions and successful operation criteria;

•Functional relationship between inputs and outputs;

ProSalus Limited Slide 4 - 64

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Framework for the SRS

- Manual shutdown requirements;
- Energizing or de-energizing to trip;
- Resetting after a shutdown;
- Maximum allowed spurious trip rate;
- Failure modes and SIS response to failures;
- Starting up and restarting the SIS;
- Interfaces between the SIS and any other system;
- Application software;
- Overrides / inhibits / bypasses and how they will be cleared;
- Actions following a SIS fault detection

Non-safety instrumented functions may be carried out by the SIS to ensure orderly shutdown or faster start-up. These must be separated from the SIFs.

ProSalus Limited Slide 4 - 65

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example SRS Template

ProSalus Limited Slide 4 - 66

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example SRS Template

ProSalus Limited

Slide 4 - 67

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example SRS Template

ProSalus Limited

Slide 4 - 68

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example SRS Template

ProSalus Limited

Slide 4 - 69

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example SRS Template

ProSalus Limited

Slide 4 - 70

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree Analysis Exercise

ProSalus Limited

Slide 4 - 71

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Practical exercise no: 1 Fault Tree Analysis

This practical exercise requires attendees to construct a fault tree diagram using the basic principles introduced in this module. It uses an example of a simple reactor with automatically controlled feeds that has the potential to cause a serious risk to plant personnel.

Once the basic fault tree has been drawn, the model is to be adjusted to incorporate a safety-instrumented system and to demonstrate the resulting risk reduction.

ProSalus Limited

Slide 4 - 72

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor. An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls leading to sudden loss of oxidant feed.

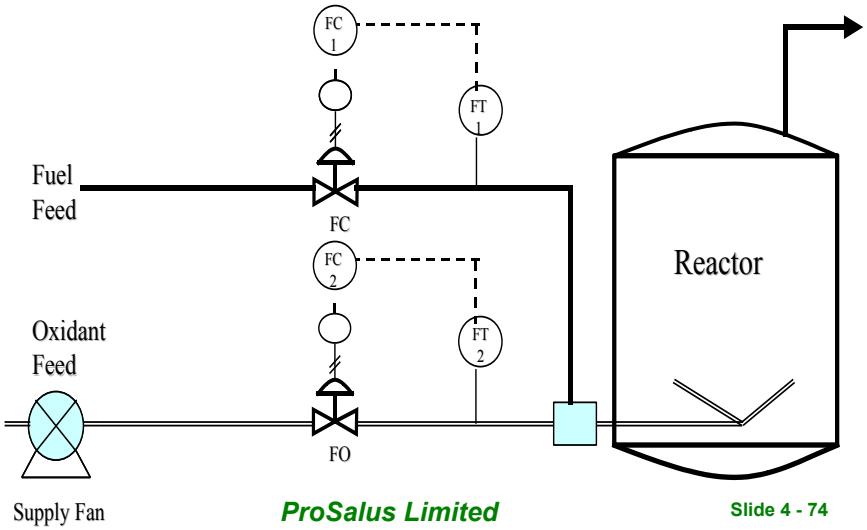
A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this Safety Instrumented function is FFSH- 03

ProSalus Limited Slide 4 - 73

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

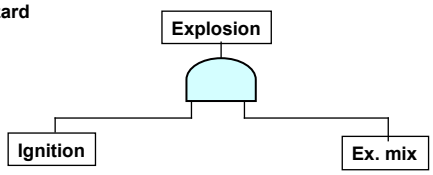


ProSalus Limited Slide 4 - 74

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault tree for basic hazard

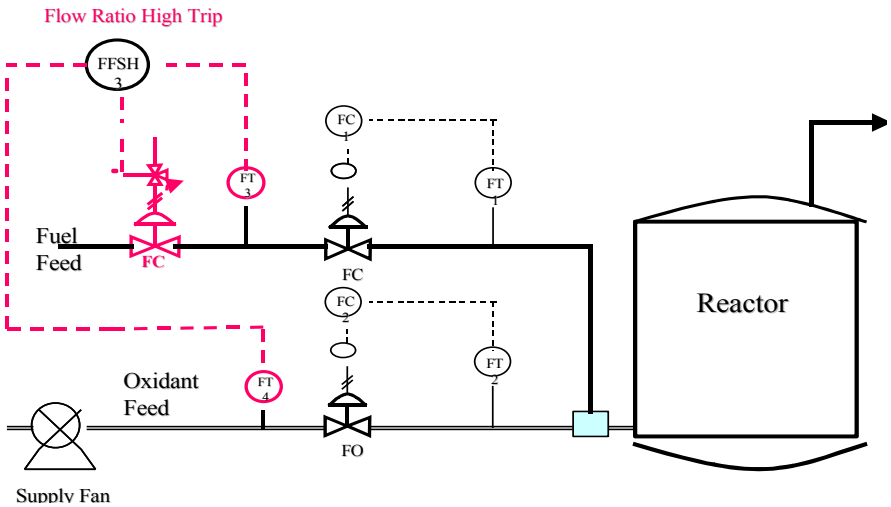


ProSalus Limited

Slide 4 - 75

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



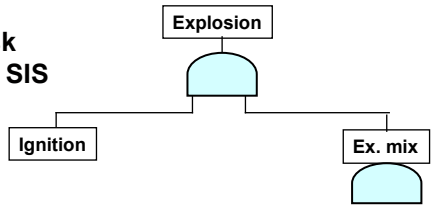
ProSalus Limited

Slide 4 - 76

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault tree for risk reduction using SIS

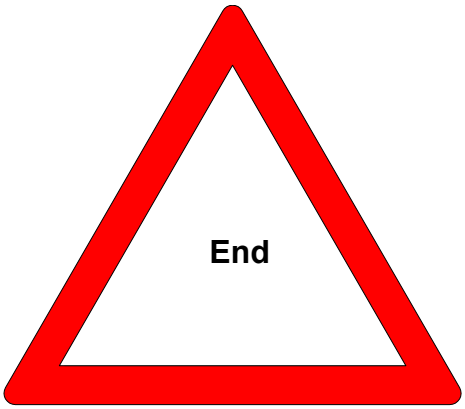


ProSalus Limited

Slide 4 - 77

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 4 - 78

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Instrumented System

Design and Development

Slide 5 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Achieving the target SIL

- Selection of Components and Sub Systems
- Design to achieve the target PFD average
- Design for safe behaviour on detection of a fault
- Ensure functional independence from BPCS
- Comply with fault tolerance requirements
- Design to reduce common cause failures
- Provide secure interfaces between components

ProSalus Limited

Slide 5 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Selection of Components and Subsystems

Two paths to Functional Safety Compliance:

1. All components and subsystems in the SIF loop are designed and tested in accordance with IEC 61508-2/3

   OR

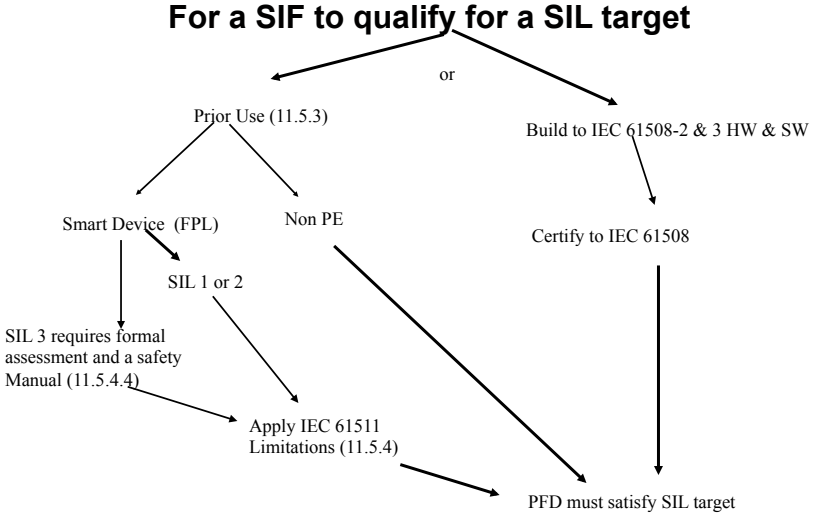
2. Evidence based on IEC 61511 “Prior Use” to demonstrate suitability of the SIF for a maximum target SIL2

ProSalus Limited Slide 5 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

For a SIF to qualify for a SIL target



ProSalus Limited Slide 5 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Requirements for Device to be IEC 61511 "Proven–in-use"

- Evidence that the instrument is suitable for SIF
- Consider manufacturer's QA systems
- PES devices need formal validation – IEC 61508-3 Annex A Table A.7 as starting point
- Performance record in a similar profile
- Adequate documentation
- Volume of experience, > 1 yr exposure per case.

Collect the records of every fault, failure, Inspection, proof test, partial test and maintenance event per instrument.

ProSalus Limited Slide 5 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The approved safety instrument list

- Each instrument that is suitable for SIF
- Update and monitor the list regularly
- Add instruments only when the data is adequate
- Remove instruments from the list when they let you down
- Adequate details: Include the process application

Managed by maintenance team and data fed to procurement

ProSalus Limited Slide 5 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Selection of Components and Subsystems

- **IEC 61508 General requirements _**
  - Component developed to relevant IEC 61508 Part 2 & 3 requirements
  - Safety Manual provided for specific component IEC 61508-2 Annex D
    - Functional Specification, Hardware / software configuration
    - Constraints and limitations on use identified during analysis (FMEDA)
    - Failure Modes for device and device diagnostics (Specifically those device failure modes not detected by diagnostics)
    - Failure Rates and Hardware Fault Tolerance
    - Type classification A or B, Systematic capability
    - Proof test, operating and maintenance requirements.
    - Calibration and set up features identified.

Slide 5 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Selection of Components and Subsystems

- **Field Devices**
  - 'An initiator or final element used as part of a SIS shall not be used for control purposes where failure of the control system would cause a demand on the protection system except when an analysis has been carried out to confirm that the risk is acceptable'
  - De-energize to trip is the preferred action.
  - Energize to trip shall apply a continuous end-of-line monitor such as pilot current to ensure continuity.
  - Smart sensors shall have write protection enabled.
  - Must be suitable for the installed environment
    - i.e. Corrosion, temperature, humidity etc.

ProSalus Limited

Slide 5 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Sharing of Sensors with BPCS

When possible do not share sensors because it:

- Violates the principles of independence
- Potential for a high level of common mode failure
- Cannot not be considered a separate layer of protection
- Creates maintenance and change control issues

Separation Rules: Field Sensors IEC 61511 Part 1 : 11.2.4

ProSalus Limited Slide 5 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Selection of Components and Subsystems

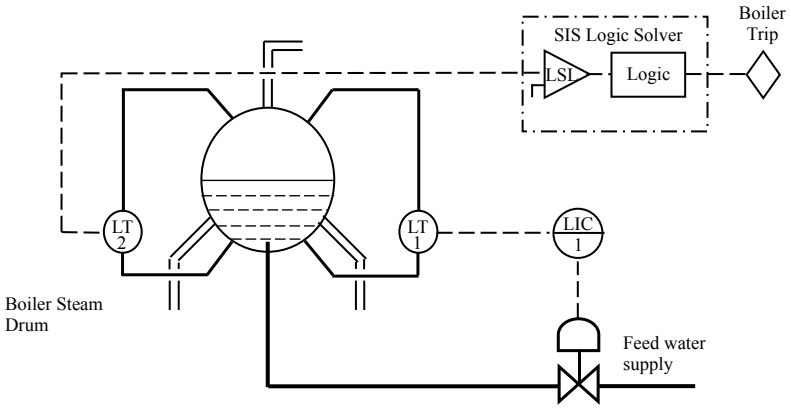
- **Field sensors**
  - If a sensor is used for both BPCS and SIS then common mode failure considerations must be assessed
  - Sensor diagnostics must be capable of placing the process in a safe state if a CMF occurs
  - The Hardware Fault Tolerance requirements are met
  - Separate sensors with identical or diverse redundancy will normally be required for SIL 3 & SIL 4 depending on the SFF.
  - If SIS sensors are connected to a BPCS suitable isolator / splitters must be used and meet the target SIL requirements.

ProSalus Limited Slide 5 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Separate Sensors for Control and Trip FTA Example



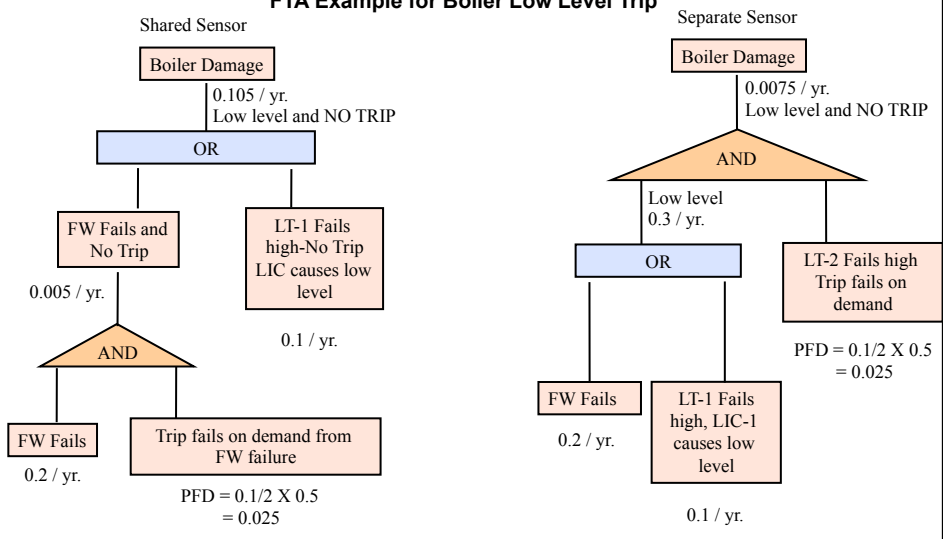
ProSalus Limited

Slide 5 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

FTA Example for Boiler Low Level Trip



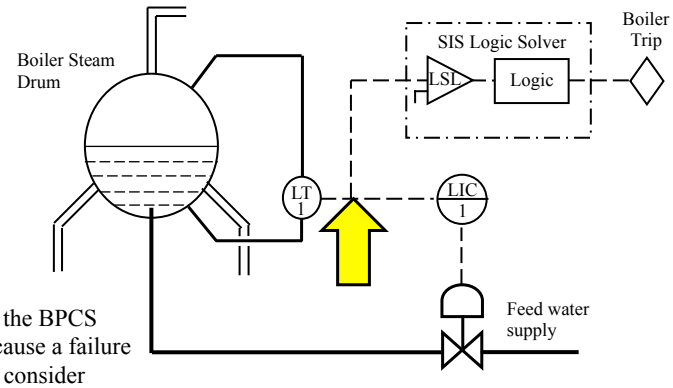
ProSalus Limited

Slide 5 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Shared Sensor for Control and Trip



Failure of the BPCS must not cause a failure in the SIS consider Splitter unit that is functionally safe

ProSalus Limited

Slide 5 - 13

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Selection of Components and Subsystems

- **Control and shutdown valves**
  - A single valve may be used for both BPCS and SIS provided that:
    - A failure of the valve cannot cause a demand on the SIF
    - Diagnostic coverage on the valve and SIF will ensure safe reaction to a dangerous failure and common mode failure requirements are met.
    - Hardware Fault Tolerance requirements are met
  - SIL 3 and SIL 4 will normally require separate identical or diverse valves

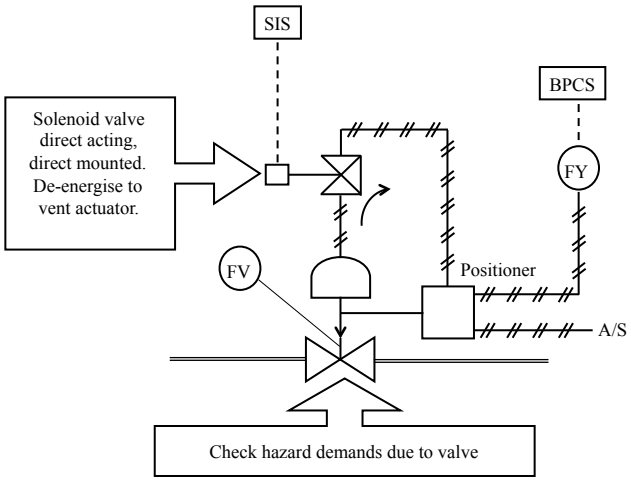
ProSalus Limited

Slide 5 - 14

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Arrangement for Tripping of Shared Control Valve SIL 1



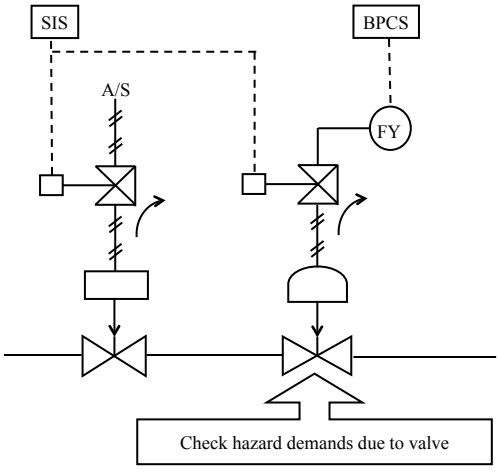
ProSalus Limited

Slide 5 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Diverse Separation of Control and Shutdown Valves SIL 2 & 3



ProSalus Limited

Slide 5 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Selection of Components and Subsystems

- **SIS Logic solver**
  - Functional separation between BPCS and SIS
  - Will have internal diagnostics to detect dangerous faults
  - Can be PES, Solid State or Relay
  - When there are a large number of outputs then it shall be necessary to determine if any foreseeable failures or combination of failures can lead to an hazardous event

ProSalus Limited Slide 5 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Considerations

Types of Failure

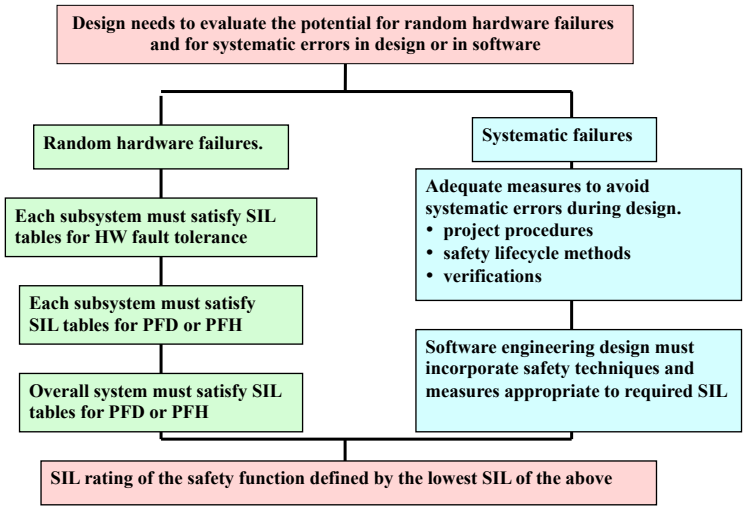
- The Integrity of a SIF is dependent on how often it fails dangerously.
- There are two main types of failure which need to be addressed:
  - Systematic failures;
  - Random hardware failures

ProSalus Limited Slide 5 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Considerations to meet the target Safety Integrity Level



ProSalus Limited

Slide 5 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Failures

- A failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or the manufacturing process, operational procedures, documentation or other relevant factors:
  - Safety requirements specification;
  - Design;
  - Manufacture;
  - Installation;
  - Operation;
  - Maintenance
- Usually due to a human error, design fault-wrong component, incorrect specification error in software program, error in testing.

ProSalus Limited

Slide 5 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic failures

- A single systematic fault can cause failure in multiple channels of a redundant system.
- Systematic failures, by their very nature, cannot be accurately predicted because the events leading to them cannot be easily predicted.
- Functional safety standards protect against systematic faults providing rules, methods and guidelines to prevent design errors.
- A system implemented using such methods should be relatively free of systematic errors.

ProSalus Limited Slide 5 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Random Failures

- A failure occurring at a random time, which results from one or more of the possible component degradation mechanisms.
  - Random failures rates can be predicted with reasonable accuracy depending on the quality of the data
    - E.g. Generic, Industrial or Site failure rate data
      - Safe failures
      - Dangerous failures

ProSalus Limited Slide 5 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Random Failures

- **Failure Rate data:**
  - Number of failures per unit / component as either:
    - A constant failure rate;
    - An average failure rate over a period / mission time
- **Dangerous failures are those that prevent success when there is a demand:**
  - Fails to operate when required i.e. valve fails to close
  - Worse are dormant failures – undetected dangerous failures
  - Potential consequences due to failure to prevent hazard occurring
- **Safe failures are spurious or nuisance failures:**
  - Spurious or nuisance shutdown no demand from process to trip
  - Downtime due to fault detection and restart
  - Loss of production / profits

ProSalus Limited Slide 5 - 23

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 / 61511 Modes of Operation

- Three modes to consider:
  - Low
  - High
  - Continuous
- Most process plant SIFs are ‘low demand mode’

ProSalus Limited Slide 5 - 24

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Demand Modes

- **Low demand mode:**
  - An infrequent demand rate on a protective system;
  - No greater than once per year
  - Use Probability of Failure of Demand average (PFDavg)
- **High demand:**
  - The demand rate is greater than once per year
  - Use average frequency of dangerous failure (PFH)
- **Continuous demand**
  - Dangerous failure will lead to a potential hazard without any further failure
  - Use average frequency of dangerous failure (PFH).

ProSalus Limited Slide 5 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Demand modes

Demand mode-61511	Continuous mode - 61511	
Low demand - 61508	High demand - 61508	Continuous - 61508
Use PFD_{avg}	Use probability of failure per hour	Use probability of failure per hour
Take credit for proof testing	No credit for proof testing	No credit for proof testing
Take credit for automatic diagnostics	Take credit for automatic diagnostics	No credit for automatic diagnostics

ProSalus Limited Slide 5 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Average Probability of Failure on Demand

- A statistical probability or chance that a system will not perform its intended function when demanded.
- Valid for ‘low demand mode’ operation only

Average frequency of dangerous failure

- The average frequency of a dangerous failure of system to perform the specified safety function over a given period (PFH).
- Valid for ‘high demand and continuous mode’ operation only
- When the system is the ultimate layer PFH is calculated from unreliability F(t) = 1-R(t) approximates to F(t)/T & 1/MTTF
- When the system is not the ultimate layer PFH is calculated from unavailability U(t) and approximates to 1/MTBF

Slide 5 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Understanding Types of Failures

For a low Demand System SIFs can fail in two ways:

- Dangerous failure (hidden, covert or un-revealed)
  - Loss of protective function, but not aware until demand
  - Failure rate can be reduced by hardware fault tolerance (e.g. 1oo2 or 1oo3
  - Diagnostics can also be used.
- Safe failure (revealed, evident – mostly economic)
  - Spurious or nuisance trip or alarm
  - No loss of protection
  - Spurious failures can be reduced by “revealed failure robustness” (e.g. 2oo2 or 2oo3)

ProSalus Limited

Slide 5 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Which type of failures have impact on the SIF?

Many failures do not influence the safety function at all, and so they are not considered anymore. Example: Display, Keypad, HART communication).

In safety engineering we need to differentiate between safe and dangerous failures,
and, if they are detectable or not (undetectable).

Safe failures impact on the SIF's availability, but not on the safety function.

Dangerous failures are split into detected and undetected.

Dangerous detected failures are detectable by diagnostic and will raise a diagnostic alarm or trip system into a safe state.

Slide 5 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Understanding Types of Failure

	(**D**etectable)	(**U**ndetectable)
(**S**afe)	λ_{SD}	λ_{SU}
(**D**angerous)	λ_{DD}	λ_{DU}

Depending on the kind of evaluation safe and detectable failures can force a system to go into the safe state.

λ_{SD} Signal cable to transmitter cut, Signal is 0 mA, central controller detects it: Safe!	λ_{SU} Output transistor becomes defective, signal ≥ 20 mA, central controller triggers (maintaining) gas alarm: Safe!
λ_{DD} Dangerous RAM-failure, being detected during automatic cyclic RAM-test, controller detects failure: Safe!	λ_{DU} Loss of measuring function without indication: **Unsafe – dangerous!**

The Dangerous Undetectable failure (λ_{DU}) is in the main focus of the SIL-consideration.

Slide 5 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Considerations

- Improving reliability and integrity
  - Hardware fault tolerance;
  - Multiple devices:
    - 1oo2, 1oo3 etc.
- Avoidance of nuisance or spurious trips:
  - Voted multiple devices
    - 2oo2, 2oo3 etc.

ProSalus Limited Slide 5 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Diagnostic Capability

- Ability of a sub system to automatically detect dangerous failures and take a action by:
  - Bringing the process to a safe state
  - Alerting the operator to take action – the diagnostic alarm should be included in the SIS in this case
- Thus when considering dangerous failures:
  - λ_{dd} = those dangerous failures that are detected by diagnostics:
  - λ_{du} = those dangerous failures that remain undetected by diagnostics and are only detected during Proof Testing

ProSalus Limited Slide 5 - 32

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Diagnostic Coverage

- The Diagnostic Coverage (DC) of a component or sub system is defined as the ratio of the average rate of dangerous detected failures of the component or sub system to the total average dangerous failure rate of the the component or sub system
- DC normally determined by FMEDA
- For pre certified or pre approved equipment the DC is included on the certificate of conformance

$$\textbf{Diagnostic Coverage} = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}}$$

ProSalus Limited Slide 5 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Considerations - Sensor Diagnostics

- Do not confuse with proof testing
- Integral to the device, designed in after OEM FMEDA has been completed to determine potential diagnostic mechanisms
- Must ensure diagnostic output is used and either trips the SIF or operator is trained to understand requirements of diagnostic alarms or NO credit for diagnostics should be taken in calculations
- Could compare trip transmitter value with related variables when practicable but not a secure method and puts more pressure on operator
- Diagnostic alarm test must be included in proof test to ensure operator awareness stays high

ProSalus Limited Slide 5 - 34

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Valve Diagnostics

Failure Mode	% Contribution to dangerous failures	%Detection by partial closure test	% Of Dangerous Faults Detected
Actuator spring breakage or jamming	20	70	14
Solenoid fails to vent	5	50	2.5
Positioner fails to trip	5	100	5
Hoses kinked or blocked	10	100	10
Valve stem or rotary shaft stuck	40	70	28
Actuator linkage fault	5	70	3.5
Seating failures of valve causing high leakage. Due to erosion or corrosion	10	0	0
Foreign bodies or sludge preventing full closure	5	0	0
Total	100%		63%

ProSalus Limited Slide 5 - 35

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Methods for Valve Diagnostics

- On–line functional testing
- Limit switch discrepancy / mismatch alarm
- Position feedback
- Partial closure testing – manual or automatic
- Smart Positioner – certified safety Positioner

ProSalus Limited Slide 5 - 36

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectural Constraints

Subsystem Safety Integrity

ProSalus Limited

Slide 5 - 37

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectural Constraints and Hardware Fault Tolerance

Hardware Fault tolerance:

Hardware fault tolerance is the ability of a system to continue to be able to undertake the required safety function in the presence of one or more dangerous faults in hardware. Hence a fault tolerance level of 1 means that a single dangerous fault in the equipment will not prevent the system from performing its safety functions.

From the above it follows that a fault tolerance level of zero implies that the system cannot protect the process if a single dangerous fault occurs in the equipment.

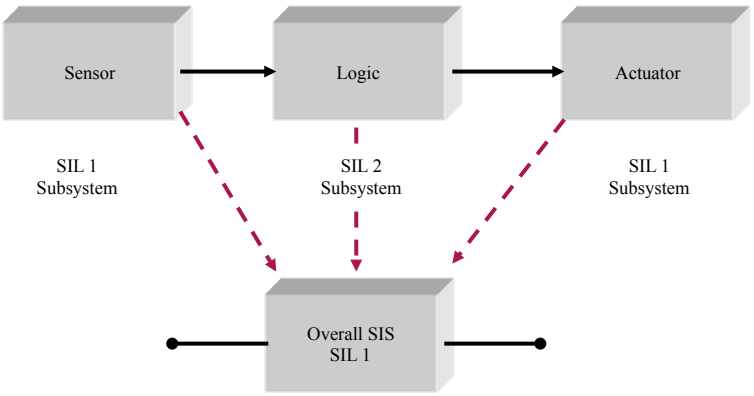
ProSalus Limited

Slide 5 - 38

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIL of the overall SIS is defined by the lowest SIL of the subsystems



ProSalus Limited

Slide 5 - 39

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safe Failure Fraction

- The Safe Failure Fraction (SFF) of a sub system is defined as the ratio of the average rate of safe plus dangerous detected failures of the sub system to the total average failure rate of the sub system
- SFF normally determined by FMEDA
- For pre certified or pre approved equipment the SFF is included on the certificate of conformance

$$\text{Safe Failure Fraction} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

ProSalus Limited

Slide 5 - 40

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectural Constraints

- IEC 61508 places an upper limit on the SIL that can be claimed for any SIF on the basis of the HFT of the subsystems that it uses.
- Limit is a function of
  - Device Type A or B
    - The degree of confidence in the behaviour under fault conditions
  - Safe Failure Fraction
    - Hardware fault tolerance

ProSalus Limited Slide 5 - 41

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Classification of Equipment

IEC 61508 defines two types of equipment for use in SIS:

- Type A: Simple Devices: Non PES – where failure modes and fault behaviour are well defined and there is dependable failure data
- Type B: Complex Devices: Including PES - where failure modes and fault behaviour are not well defined and there is insufficient dependable failure data
- Fault tolerance rating of B is less than A for equivalent SFF

ProSalus Limited Slide 5 - 42

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Table 2
Minimum hardware fault tolerance of type A sub systems

SIL	Minimum HW Fault Tolerance			
	SFF<60%	SFF 60% to 90%	SFF>90%	SFF>99%
1	0	0	0	0
2	1	0	0	0
3	2	1	0	0
4		2	1	1

For devices with well defined failure modes,
predicable behaviour and field experience.
Normally excludes PES

ProSalus Limited Slide 5 - 43

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Table 3
Minimum hardware fault tolerance of type B sub systems

SIL	Minimum HW Fault Tolerance			
	SFF<60%	SFF 60% to 90%	SFF>90%	SFF>99%
1	1	0	0	0
2	2	1	0	0
3		2	1	0
4			2	1

For devices with some none defined failure modes
OR unpredictable behaviour
OR insufficient field experience

ProSalus Limited Slide 5 - 44

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511-1 Table 6
Minimum hardware fault tolerance of sensors, final elements & non PES logic

SIL	Minimum HW Fault Tolerance
1	0
2	1
3	2
4	Special requirements: See IEC 61508

The following summarized conditions apply for SIL 1,2 and 3 :
Increase FT by 1 if instrument does not have fail safe characteristics
Decrease FT by 1 if instrument if the device complies with the following.

- The hardware is selected on the basis of prior use (IEC 61511 11.5.3)
- The device allows adjustment of process related parameters only, for example, measuring range, upscale or downscale failure detection.
- The adjustment of the process related parameters of the device is protected, for example jumper, password.
- The function has a SIL requirement of less than 4.

Alternatively tables 2 and 3 of IEC 61508 may be applied if the SFF can be calculated

ProSalus Limited Slide 5 - 45

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architecture rules for PES logic solvers
IEC 61511-1 Table 5
Minimum hardware fault tolerance of PE logic solvers

SIL	Minimum HW Fault Tolerance		
	SFF<60%	SFF 60% to 90%	SFF>90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements: See IEC 61508		

Alternatively tables 2 and 3 of IEC 61508 may be applied with an assessment

ProSalus Limited Slide 5 - 46

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Minimum Architectures for Fault Tolerance of Type A and B Sub-Systems for 60% to 90% SFF

	Simple Devices (Non PES) Type A		Complex Devices Type B	
Safety Integrity.	Min. Fault tolerance.	Minimum Architecture	Min. Fault tolerance.	Minimum Architecture
SIL 1	0	1oo1	0	1oo1
SIL 2	0	1oo1	1	1oo2 or 2oo3
SIL 3	1	1oo2 or 2oo3	2	1oo3
SIL 4	2	1oo3	Special requirements apply, see IEC 61508	

ProSalus Limited

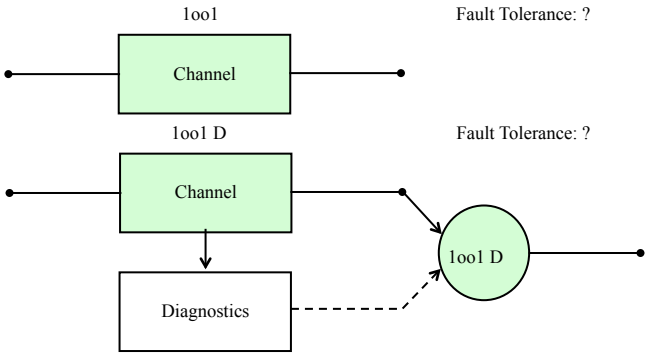
Slide 5 - 47

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectures for Safety Systems - 1oo1 Single channel

1oo1D has a higher safe failure fraction than 1oo1 but is still not able to protect the plant if a fault remains hidden



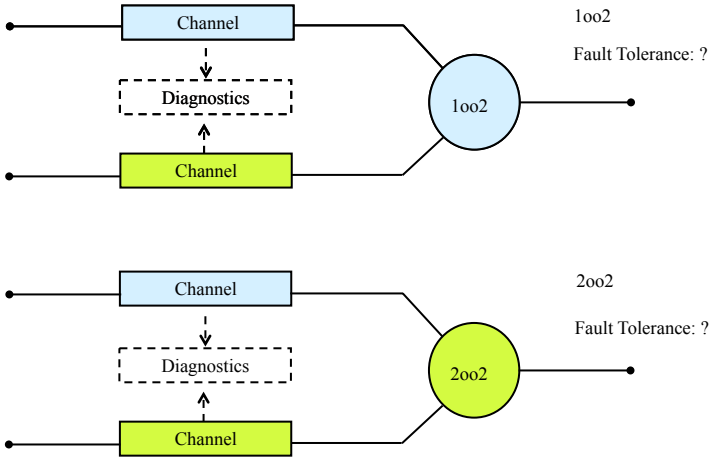
ProSalus Limited

Slide 5 - 48

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectures for Safety Systems - 1oo2 v 2oo2



ProSalus Limited

Slide 5 - 49

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Performance attributes of sub-system architectures

Sub system structure	Fault tolerance	Selection Guide
1oo1	0	Use if both PFD and nuisance trip targets are met.
1oo2	1	2 Sensors installed, 1 required to trip. PFD value improved, nuisance trip rate doubled. Often suitable for SIL 2
2oo3	1	3 Sensors installed, 2 required to trip. PFD improved over 1oo1, nuisance trip rate dramatically reduced.
1oo1D	0	Internal and external diagnostics used to improve safe failure fraction. Alternative to 1oo2 for SIL2
1oo2D	1	As for 1oo1D but able to tolerate 1 fault and revert to 1oo1D during repair. Meets SIL 3 if safe failure fraction exceeds 90%. Does not satisfy diversity for SIL3 if sensors are identical. Reduces spurious trip rate, good alternative to 2oo3
1oo3	2	3 Sensors installed, 1 required to trip. PFD improved over 1oo2 but not by much unless diverse instruments are used. Nuisance trip rate may be a problem. Likely to be used for SIL 2 or 3.
2oo4	2	Configured as two voting pairs of 1oo2D. Very high performance when used in logic solvers. Achieves SIL 3 performance with 1 pair off line for repair.

ProSalus Limited

Slide 5 - 50

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safe Failure Fraction - Issues

- Optimistic claims for dangerous failures that can be detected by diagnostics
- FMEDA is considered best practice for assessing dangerous failures that can be detected by diagnostics
- If the detected failure claim is to optimistic then the safety integrity will be compromised due to the reduction in Hardware fault tolerance

ProSalus Limited Slide 5 - 51

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause & Common Mode Failures

- A CCF occurs when a single fault results in the corresponding failure of multiple components.
- Common mode failures are a subset of common cause failures'
  - *"A common-mode failure (CMF) is the result of an event (s) which because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundancy system, leading to the defined system failing to perform its intended function".*

ProSalus Limited Slide 5 - 52

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failures in Sensors

- Wrong specification
- Hardware design errors
- Software design errors
- Environmental stress
- Shared process connections
- Wrong maintenance procedures
- Incorrect calibration

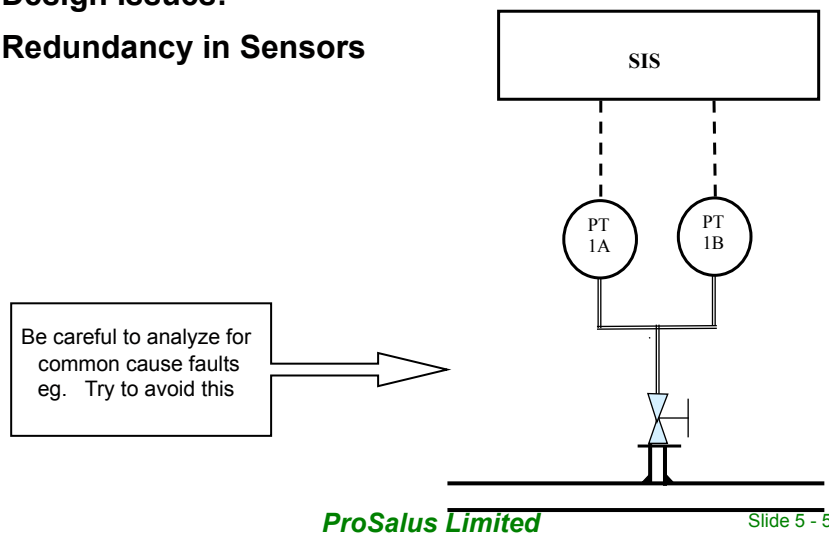
ProSalus Limited Slide 5 - 53

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Issues:

Redundancy in Sensors



ProSalus Limited Slide 5 - 54

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failures (IEC 61508)

- IEC 61508 Part 6 Annex D –Method for quantifying CCF
- 2010 version updated and based on PDS methodology
- Based on the following factors from IEC 61508-6 Table D.1 to D5:
  - Separation/segregation;
  - Diversity/redundancy;
  - Complexity/design/application/experience;
  - Assessment/analysis & feedback of data;
  - Procedures/human interface;
  - Competence/training/safety culture;
  - Environmental Control;
  - Environmental Testing.

ProSalus Limited

Slide 5 - 55

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 5 - 56

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 5 - 57

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 5 - 58

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Slide 5 - 59

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failures (IEC 61508)

- Using the IEC 61508 Part 6 Annex D β-factor model
  - Common Cause failure rate is $\lambda_D\beta$
  - Where diagnostics are available overall CCF rate is

$$\lambda_{DU}\beta + \lambda_{DD}\beta_D$$

  - Using Table D1, D2, D3 and D4
  - β - $S = X + Y = \beta_{int}$ for a 1oo2 System
  - β_D - $S_D = X (Z+1) + Y = \beta_{D\ int}$ for a 1oo2 System

ProSalus Limited

Slide 5 - 60

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failures

- Apply Table D5 for systems with levels of redundancy greater than 1oo2 , table based on PDS Method
- IEC 61508-3, Annex D, Table D.4 for 1oo2
  - *0.01 –0.1 for field equipment;*
  - *0.005 –0.05 for programmable electronic systems*

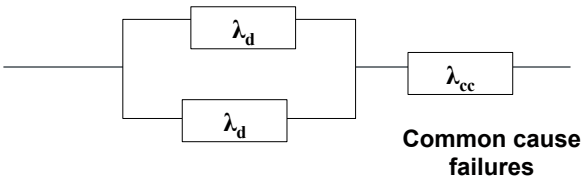
ProSalus Limited Slide 5 - 61

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failures – Systems Diagram 1oo2

- Consider a simple 1oo2 redundant subsystem



λ_d = total dangerous failure rate
λ_{cc} = total common cause failure rate
$\lambda_{cc} = \beta\lambda_d$
Where β = the common cause failure factor

ProSalus Limited Slide 5 - 62

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failure Calculation - Example

$\lambda_{cc} = \lambda_{common\ cause}$

$\lambda_{cc} = \beta\lambda_d$

Where:

λ_d =0.05 failures / year

$\beta = 0.1$

Therefore

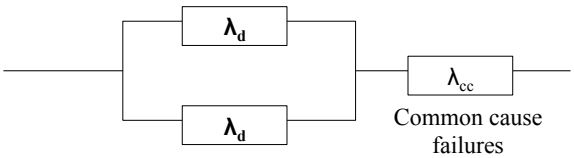
λ_{cc}= 0.1 * 0.05 = 0.005 failures / year

ProSalus Limited Slide 5 - 63

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Common Cause Failures – Systems Diagram 1oo2



$$PFD_{avg} = \frac{(\lambda_d)^2 \times T^2}{3} + \frac{\lambda_{cc} \times T}{2}$$

Common Cause failure should be shown as an additional 1oo1 block in the RBD or as an input to an OR gate in an FTA and then summed with the 1oo2 block to calculate overall sub system PFDavg

ProSalus Limited Slide 5 - 64

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Considerations - Field Devices Summary

- Safety Related Instruments must well proven
- Smart instrumentation treated as PES – Type B
- Separation, Redundancy, Diversity design issues
- Increased Diagnostic Coverage for improved SFF to reduce HFT requirements
- For SIL 1 and SIL 2 - justifiification of suitability on “prior use”.
  - Requires evidence of previous usage in safety.
  - SIL 3 requires formal assessment (IEC 61511 11.5.4.4)
  - “ Prior use” does not help if the instrument is new to your company unless the vendor can assist with Client data

ProSalus Limited Slide 5 - 65

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Safety Component Selection

- Use Safety Certified / approved components to IEC 61508 wherever possible as this aids in the verification in terms of failure data, component type, safe failure fraction, available diagnostics
- Make sure Safety Manual is supplied with device / component.
- Ensure application and usage complies with vendor’s safety manual.
- If you have records of the same instrument being used for an extensive period in safety applications you can document your own “Prior use” justification up to SIL 2 only.
- Insist on verifiable data from Vendor / system supplier for the device / component either based on FMEDA, returns data or acelerated testing.

ProSalus Limited Slide 5 - 66

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Application Software

Slide 5 - 67

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Software Safety Topics

- Software for Safety
- Software Verification & Systematic Errors
- Software Management & Quality Assurance
- Software Safety life cycle
- Software Safety Requirements
- Certification and compliance

ProSalus Limited

Slide 5 - 68

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Software for Safety

- SIS software must have a proven QA/C (Testing) and FSM record
- Software comes in two parts: Embedded and Application
  - Both parts require software QA/C & FS management procedures
  - Embedded software including development tools QA/C & FS management procedures and software construct should to be 3rd party certified to IEC 61508-3 with a report of limitations of use
  - Application tools should be certified for use with the OEM software package
  - Development of Application software to follow IEC 61511-1 figures 12 Software development lifecycle table 7 and comply with IEC 61131 software language requirements.

ProSalus Limited Slide 5 - 69

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Software Verification & Systematic Errors

- IEC 61508-3 safety approved embedded / operating system and check versions are certified for use with hardware and application package
- IEC 61508-3 precertified software modules (Function Blocks)
- OEM approved application package matched to system hardware and software versions.
- IEC 61511 Clause 12 for QA and FSM procedures for application software when using IEC 61508 compliant systems
- IEC 61511 Software Validation by Testing against Requirement Specification and cause and effects
- Software verification complicated – 61508 requires formal analysis & traceability (61508-7 Annex D)

ProSalus Limited Slide 5 - 70

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Software Management and Quality Assurance

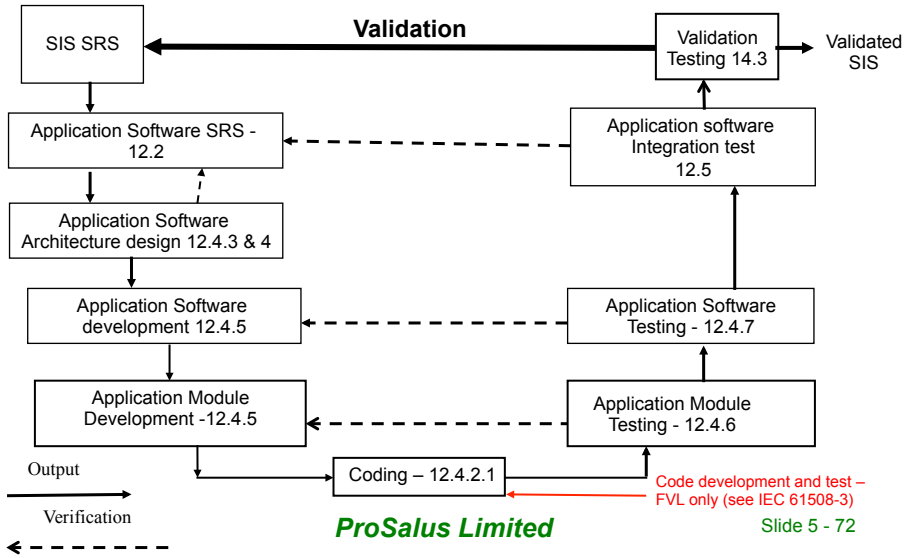
- Management of Software Quality & Testing replaces reliability analysis
- Software Quality Assurance practices are well established.
- IEC 61508-6 Annex E Safety Manual requirements for Software Elements
- Software Safety Life Cycle in IEC 61508-3 Annex G for detailed guidance on software lifecycles and IEC 61511 clause 12
- IEC 61508-6 Annex E for example guidance on the application of the IEC 61508-3 software safety integrity tables

ProSalus Limited Slide 5 - 71

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Software Safety Lifecycle: V model



ProSalus Limited Slide 5 - 72

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Application Software Life Cycle Requirements

- Application Software Safety Requirements Specification
- Features and facilities required of the application language
- Features to facilitate safe modification of the application
- Architecture of the application software
- Requirements for support tools, user manual and application languages
- Software development methods
- Software module testing
- Software integration testing
- Integration testing with the SIS subsystem

Continues through to Validation, Operation, Proof testing and Inspection.

ProSalus Limited Slide 5 - 73

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ProSalus Limited Slide 5 - 74

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ProSalus Limited

Slide 5 - 75

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ProSalus Limited

Slide 5 - 76

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ProSalus Limited

Slide 5 - 77

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Part 3 Overview

Slide 5 - 78

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Safety Certified PES Logic Solvers

- TUV Publish a list of type certified systems on website
- Ensure hardware and software versions are as per certificate
- Check Test report for any limitations on use
- Software representation complies with IEC 61131 requirements
- Within the use of LVL software there is the possibility to create user defined function blocks, however they must be constructed and tested as FVL software modules to avoid human or specification errors
- Certification can be directed at specific applications e.g. furnace control, HIPPS or for other typical process applications

ProSalus Limited Slide 5 - 79

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Software Verification

- Software verification complicated – 61508 requires formal analysis & traceability (61508-7 Annex D)
- Difficult and costly to test all foreseeable combinations of logic not normally considered in process applications reliance on SRS and C&E testing
- The failure modes are unpredicatable in presence of hardware faults.
- Re-use of old software in new applications (also known as SOUP…software of uncertain pedigree - Refer HSE guidance RR 336/2001 & 337/2001

ProSalus Limited Slide 5 - 80

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Table A.1 – Software safety requirements specification (see 7.2)

TECHNIQUE/MEASURE *	REF	SIL1	SIL2	SIL3	SIL4
Computer-aided specification tools	B.2.4	R	R	HR	HR
Semi-formal methods	Table B.7	R	R	HR	HR
Formal methods	B.2.2, C. 2.4	-	R	R	HR
Note 1 – The software safety requirements specification will always require a description of the problem in natural language and any necessary mathematical notation that reflects the application. Note 2 – The table reflects additional requirements for specifying the software safety requirements clearly and precisely.					
* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/ measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measure has to be satisfied.					

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Table A.3 – Software design and development: (see7.4.4)

TECHNIQUE/MEASURE *	REF	SIL1	SIL2	SIL3	SIL4
1 Suitable programming language	C.4.5	HR	HR	HR	HR
2 Strongly typed programming language	C.4.1	HR	HR	HR	HR
3 Language subset	C.4.2	-	-	HR	HR
4a Certified tools and Certificated translators	C.4.3	R	HR	HR	HR
4b Tools and translators: increased confidence from use	C.4.4	HR	HR	HR	HR
* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/ measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measure has to be satisfied.					

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Table A.4 – Software design and development: detailed design (see 7.4.5 and 7.4.6

TECHNIQUE/MEASURE *	REF	SIL1	SIL2	SIL3	SIL4
1a Structured methods	C.2.1	HR	HR	HR	HR
1b Semi-formal methods	Table B.7	R	HR	HR	HR
1c Formal design and refinement methods	B2.2.2, C.2.4	-	R	R	HR
2 Computer-aided design tools	B.3.5	R	R	HR	HR
3 Defensive programming	C.2.5	-	R	HR	HR
4 Modular approach	Table B.9	HR	HR	HR	HR
5 Design and coding standards	C.2.6, Table B.1	R	HR	HR	HR
6 Structured programming	C.2.7	HR	HR	HR	HR
7 Use of trusted/verified software elements (if available)	C.2.10	R	HR	HR	HR

* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measure has to be satisfied.

ProSalus Limited

Slide 5 - 83

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Scope of compliance required for logic solver software products

- SIS Logic Solver and I/O certified for use at the relevant SIL
- All of the programming languages supported by the logic solver with any special safety functions and function blocks to be certified for compliance at the relevant SIL.
- All restrictions and operating procedures required by the certifying organization to be stated in the user documentation.
- Methodology for on-line testing using overrides to be approved by the certifying organization.

ProSalus Limited

Slide 5 - 84

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Software Proven in Use - IEC61508-7 B.5.4 Field experience

For field experience to apply *(very difficult in reality – different firmware versions and missing FSM of the software)*

- unchanged specification;
- 10 systems in different applications;
- 100000 operating hours and at least one year of service history.

This documentation must contain at least

- the exact designation of the system and its components, including version control for hardware;
- the users and time of application;
- the operating hours;
- the procedures for the selection of the systems and applications procured to the proof;
- the procedures for fault detection and fault registration as well as fault removal.

ProSalus Limited Slide 5 - 85

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

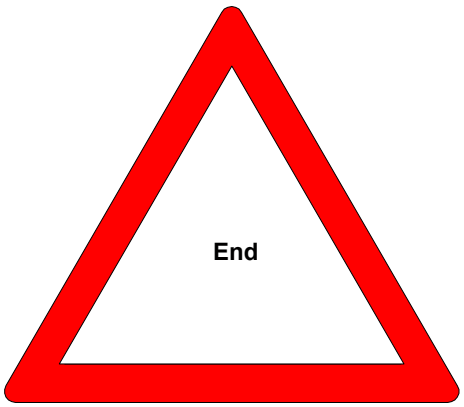
Summary

- Software safety integrity is achieved through IEC 61511-12 software life cycle and company software quality assurance procedures
- IEC 61508-3 is targeted at new PES devices but can be applied as necessary for end user support, but requires detailed knowledge
- Certified software packages provide a secure platform for the end user to execute an application.
- Vendor's training and safety manual requirements must be applied
- IEC 61511-2 Clause 12 provides additional support but is informative only

ProSalus Limited Slide 5 - 86

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 5 - 87

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIL Verification

Slide 6 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Types of Failures - Recap

- Sub Systems can fail because of:
  - Random hardware failures
  - Common cause hardware failures
  - Systematic failures
- Any of these failures drives the SIF into a specific state:
  - Safe failures λ_s = Safe undetected failure rate λ_{su} + Safe detected failure rate λ_{sd}
  - Dangerous failures λ_d = Dangerous undetected failure rate λ_{du} + Dangerous detected failure rate λ_{dd}

Slide 6 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Failures - Recap

- **Definition: A hidden fault in design or implementation such:**
  - Software design
  - Specifications
  - Operating manuals
  - Maintenance or test Procedures, etc
- **IEC 61508 approach:**
  - Measures to avoid systematic failures ((tables in 61508-2/3 Annex A/B))
  - Probabilistic calculations for Software can be done (61508-7 Annex D)

Slide 6 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hardware Verification Approaches:

- **IEC 61511-2 approach:**
  - Follow Methodology in IEC 61508-2 & 3 Annex B for hardware systematics
  - Hardware Verification – IEC 61508 or ISA simplified approach allowed
- **IEC 61508-6 approach:**
  - Techniques and Measures to control systematic hardware failures (tables in 61508-2/3 Annex A/B)
  - Hardware Verification (PFD or PFH Calculation)
- **ISA-TR84.00.02-2002 approach:**
  - Detailed Technical Report on 5 Parts - Simplified Equations, FTA, Markov Analysis

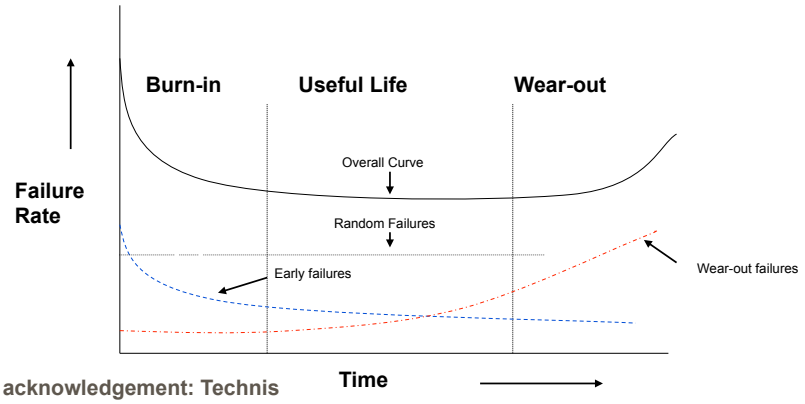
Slide 6 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Random Hardware Failures - Introduction

The Bathtub Curve & Assumed Constant Failure rate



Slide acknowledgement: Technis

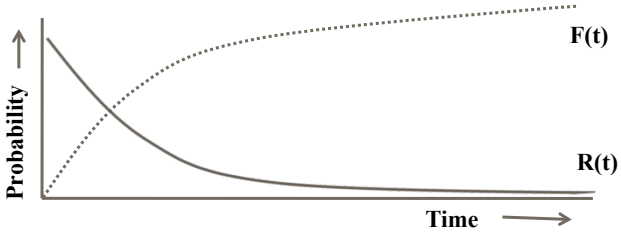
Slide 6 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Simplified Exponential Distribution - Background

- IEC 61508 / 61511 equations assume a Constant failure rate = λ
- Therefore the exponential distribution can be simplified to -
- Reliability rate – $R(t) = e^{-\lambda t}$
- Unreliability rate – $F(t) = 1 - R(t)$
- Unreliability rate – $F(t) = 1-e^{-\lambda t}$ (Cumulative Probability of failure)
- If λt is small (<0.1), then $1-e^{-\lambda t}$ approximates to λt



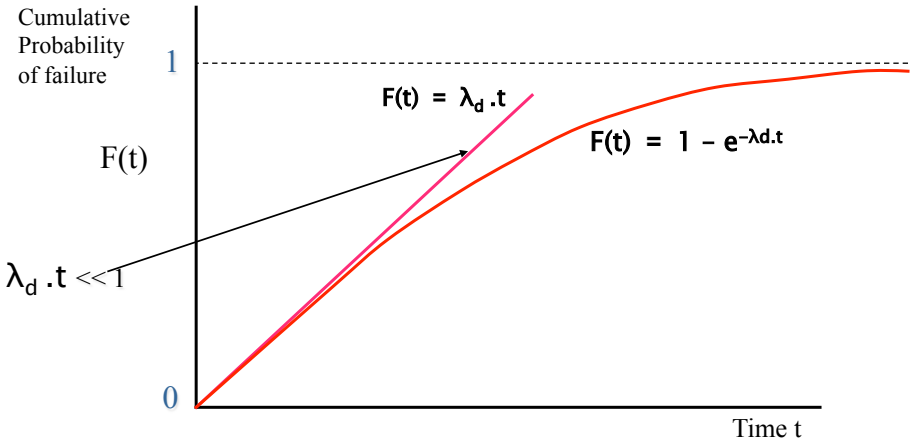
For a detailed discussion of the simplification refer to Reliability, Maintainability & Risk" Smith – ISBN 978-0-7506-6694-7

Slide 6 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Cumulative Probability of Failure – Linear Assumption



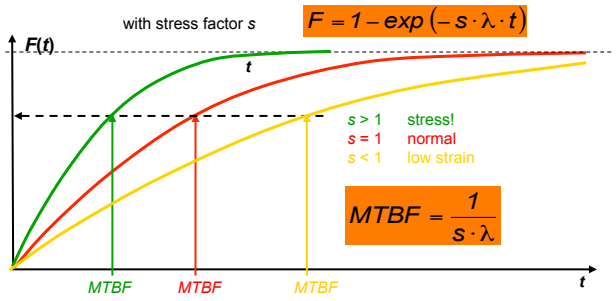
Slide 6 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The effects of Stress on component Failure - Background

The probability of failure changes under different stress conditions:

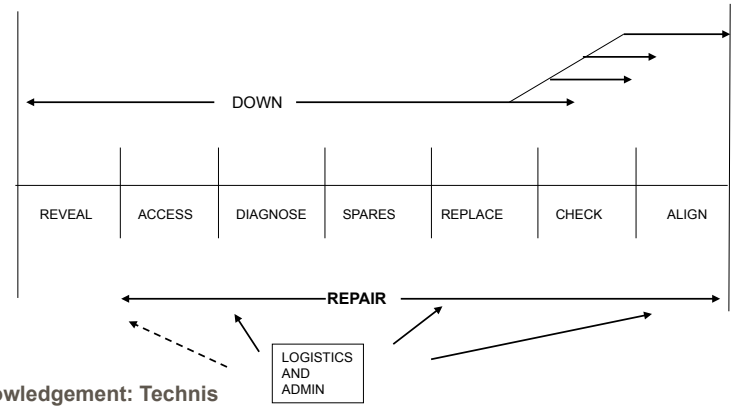


Slide 6 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Considering the Mean Time To Repair (MTTR)



Slide acknowledgement: Technis

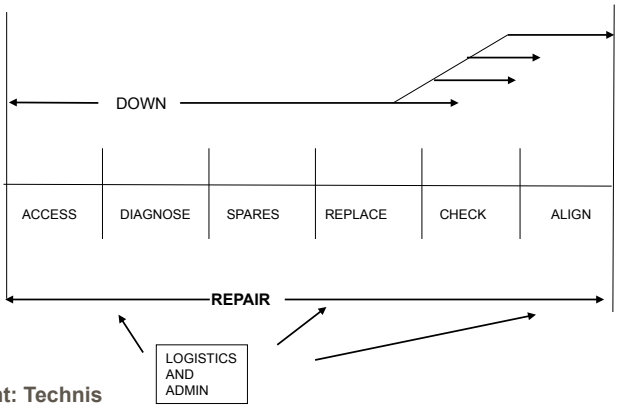
Slide 6 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Considering the Mean Repair Time (MRT)

MRT does not include the time to detect the failure



Slide acknowledgement: Technis

Slide 6 - 10

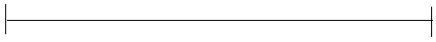
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Considering the MEAN DOWN TIME (MDT)

Of any unit:

MRT + (Proof Test Interval)/2



Of a System with two Redundant Units:

MRT + (Proof Test Interval)/3

Slide acknowledgement: Technis

Slide 6 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Definitions - Unavailability and Availability - Background

For a 1oo1 System - 10 yrs MTBF; annual proof test interval (PTI) means:

Assume 1/MTBF = λ (when << 1) = 1/10 = 0.1

MDT = MRT + PTI/ 2 = 0.5 (Assuming MRT is small e.g. 4 hours)

Thus Unavailability = 0.5 yr x 0.1 pa = 5% = PFD = 0.05

Unavailability ≡ λ MDT (Approximation when λ is small)

UNAVAILABILITY is similar to PFDavg

NB: actually λ MDT / (1 + λ MDT) (For when λ is large)

NB: Availability = 1 – Unavailability

NB: Availability = MTTF / (MTTF + MTTR)

NB: MTBF = MTTF + MTTR

Slide 6 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Understanding Types of Failure Rate Data

- Generic Data
- Industry specific data
- Site specific data

The type of data used affects the accuracy of the prediction

Slide 6 - 13

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Examples of Failure Data Sources

- US MIL Handbook 217
- UK BT HRD
- Lees “Loss Prevention in the Process Industries”
- AIChemE – Process Equipment Reliability Data Book
- OREDA, PDS, SINTEF Data Book (Offshore)
- Exida Safety Data Handbook
- Manufacturers FMEDA Reports
- UK MoD Def Stan 00-41
- UKAEA (SRD)
- Faradip
- Various Consultants data banks RMC, DNV, DJS
- SN 29500

Slide 6 - 14

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of using Failure Rate Data - Faradip

	PER MILLION HOURS		
Gas pellister 1010(fail .003)	5.00	10	30
Detector smoke ionization	1.00	6.00	40
Detector ultraviolet	5.00	8.00	20
Detector infra red (fail .003)	2.00	7.00	50
Detector rate of rise	1.00	4.00	12
Detector temperature	0.10	2.00	.
Detector flame failure	1.00	10	200
Detector gas IR (fail .003)	1.50	5.00	80

Failure modes (proportion)		
Rate of rise	Spurious 0.6	Fail 0.4
Gas pellister	Spurious 0.3	Fail 0.7
Infra red	Spurious 0.5	Fail 0.5
Smoke (ionize) & UV	Spurious 0.6	Fail 0.4

Slide acknowledgement: Technis

Slide 6 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Estimating Confidence Levels for Failure Data

"*Reliability, Maintainability & Risk" Smith – ISBN 978-0-7506-6694-7*

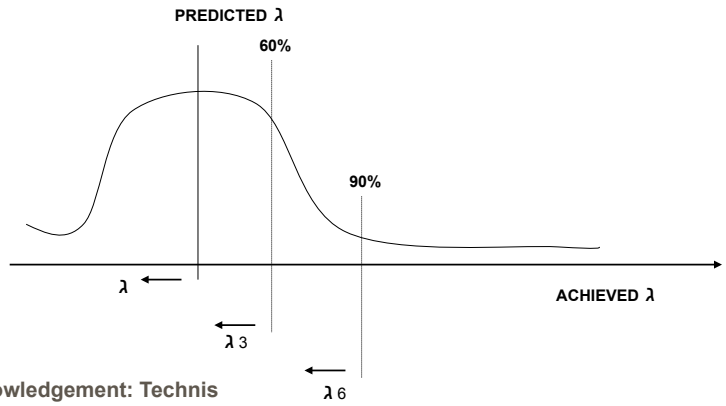
- Smith proposes rules of thumb for estimating the confidence level for:
  - Generic Data
  - Industry specific data
  - Site specific data

Slide 6 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Increasing Confidence Levels when Using Generic Data



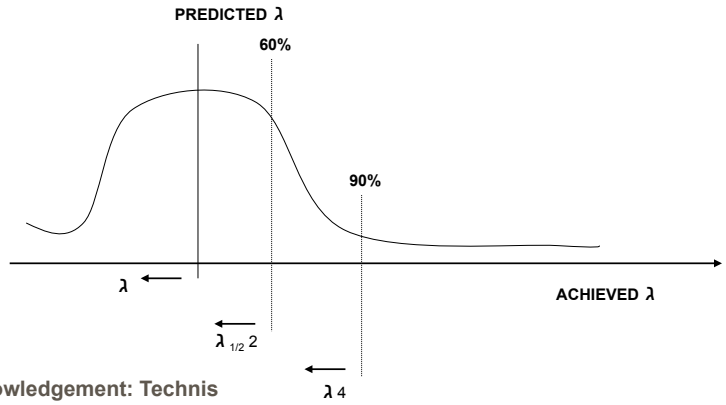
Slide acknowledgement: Technis

Slide 6 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Increasing Confidence Levels when Using Industry Data



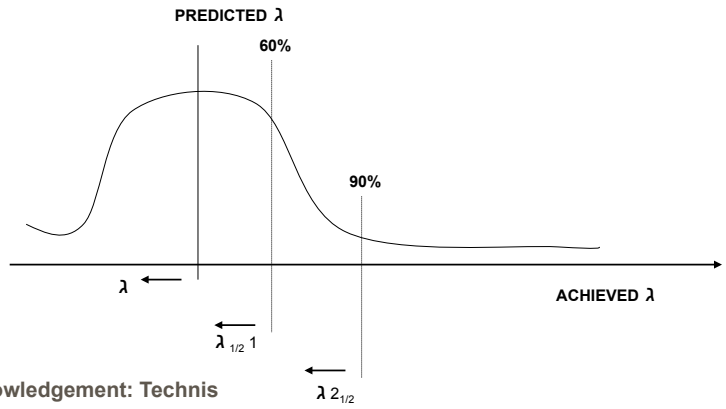
Slide acknowledgement: Technis

Slide 6 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Increasing Confidence Levels when Using Site/Company Data



Slide acknowledgement: Technis

Slide 6 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Failure Mode, Effect Analysis (FMEA)

Slide 6 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Failure Modes and Effect Analysis (FMEA)

- Purpose – to study the results or effects of item failure on system operation and to classify each potential failure according to its severity
  - First formal applications in1960 in the aerospace industry
  - First of all it is a design technique
  - But is also a verification technique
  - It can be used for products, systems and processes
  - Is a single failure mode analysis technique
  - Does not consider multiple failures at the same time
  - Common cause or systematic failures are not addressed
  - Is a bottom-up technique

Slide 6 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

FMEA can be adjusted to the problem or needs at hand

- FMEA – Failure modes and effects analysis
  - Basic technique (BS EN 60812)
  - DOD MIL-STD-1629A
- FMECA – Failure mode, effect, and critically analysis
- Functional FMEA
- Maintenance FMEA
- Process FMEA
- Software FMEA
- FMEDA – Failure modes, effects and diagnostic analysis

Slide 6 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

FMEA Process

- The following steps are important
  - Define the system and scope of the analysis
  - List all sub systems and components
  - Identify failure modes
    - Determine rates of occurrence
    - Determine Locatability
  - Identify effects of failure
    - Determine severity
    - Determine detectability – Locatability – Fault Coverage (FD/FL)
    - Criticality Analysis

Slide 6 - 23

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Failure Mode & Effect Aanalysis

Severity Classification

1 Fault leading to an Unsafe Failure which is not detected by the system diagnostics
2 Fault leading to an Unsafe Failure which is detected by the system diagnostics
3 Fault leading to a Safe Failure which is not detected by the system diagnostics
4 Fault leading to a Safe Failure which is detected by the system diagnostics

Identification	Function	Failure Modes	Operational Mode	Failure Effects		Detection Method	Compensating Provisions	Severity Class	Remarks
				Local	End				
Temperature Controlled Reference Coils	Provide reference against which measured values can be compared	Fibre Break	Normal	No Profile	Incorrect Trace	Normal operation reports break and location	Redundant DTS 800 M4 Unit	4	Requires replacement of Optics Module. One instance in fault reports.
Fibre Switch	Allows single laser to connect to multiple fibres	Switch dirty	Normal	Source attenuated	Degraded trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	Unit can be cleaned
Receiver	Detects Back scattered light	Surface Degradation	Normal	Reduction in output	Degraded Trace	QA Zone allocated for Signal Level Below threshold	Redundant DTS 800 M4 Unit	4	Long term gradual failure
Laser (Inc AOD)	Generate Light source for transmission through fibre sensors	Reduction in Power	Normal	Source attenuated	Degraded Trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	Most recorded fault
AOD Driver	Provides pulsing function of laser	Incorrect Pulse - Believable	Normal	Close to correct emission profile	Potential error in temperature value	QA Zone allocated to monitor Standard Deviation. Periodic Function Test.	Redundant DTS 800 M4 Unit	2	Include trace analysis for this fault in periodic site Function Test.
Breakout PCB	Provides power distribution for Optics Module	Incorrect Voltage to other circuits	Normal	Module supply out of spec	Degraded Trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	Most sensitive module is processor which will shut down switching outputs to safe state.
Main Amp	Amplifies Optics Module output for processing	Incorrect Gain	Normal	Incorrect signal to Averager	Incorrect Trace	QA Zone allocated for Signal Level Below threshold	Redundant DTS 800 M4 Unit	4	Does not affect reported values, but signal could be biased. Detectable during periodic FunctionTest. Reference signal offset as per measured signal.
Temperature Control PCB Assembly	Controls temperature of laser, receiver, reference coil and AOD.	Temperature sensor fault	Normal	Incorrect control level	On Ref Coil, trace will be offset	Functional Test by applying shock low temp to field sensor.	Redundant DTS 800 M4 Unit	1	Trip threshold is against an absolute level. This fault could mean that the absolute threshold is not reached therefore no trip. However, there are no reports of this failure mode in fault records.
Optics Interface PCB Assembly	Gain and offset to main amp plus HV supplies to APD's	Incorrect gain & offset to Main Amp.	Normal	Incorrect signal to Averager	Incorrect Trace	QA Zone allocated for Signal Level Below threshold	Redundant DTS 800 M4 Unit	4	Does not affect reported values, but signal could be biased. Detectable during periodic FunctionTest. Reference signal offset as per measured signal.
Averager PCB Assembly	Accumulates data and generates average	A/D Converter Fail	Normal	No Output	No Trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	
Power Supply	Provides power & regulation to system modules	Output Too Low	Normal	Some Modules Failing	Degraded or No Trace	Alarm handoff from UPS to serial interface. QA Zone allocated for Signal / Noise ratio above threshold.	UPS with battery pack. Redundant DTS 800 M4 Unit	4	
Memory PCB Assembly	Stores OS, Application and data.	Data Corrupted	Normal	Wrong results	Inconsistent Data, incorrect operation of relays	QA Zones set up for inconsistency checking	Redundant Unit	4	
Processor PCB Assembly	Perform mathematical analysis on returned signals	Incorrect Calculation	Normal	Incorrect result	Inconsistency in Trace	QA Zone detects abnormal trace.	Redundant DTS 800 M4 Unit.	2	Project uses redundant pair. One processor in error would lead to discrepancy between units detected by safety logic solver, but possibly only when trip condition occurs.
Output Module	Provide powered outputs to interposing relays to external logic solver	Contacts stick closed	Normal	Fail to open on demand from processor	Failure to transfer status to safety system	Voting in comparison with redundant 800 DTS system in external safety logic solver. Comparison with fault relay status.	Redundant DTS 800 M4 Unit. Selection of relays with low fail rates	1	Original on-board relays now removed and replaced by external high quality relays incorporating Hermetic seal and gas filled can.

Slide 6 - 24

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree Analysis (FTA)

Slide 6 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

WHAT IS FAULT TREE ANALYSIS

- An analysis method to identify causes for an assumed failure (top event)
- Deductive method – focuses on top event
- Logical structure
- Considers Equipment failures & Human errors
- Identify possible causes for a system failure
- Predict:
  - Reliability
  - Availability
  - Failure frequency
- Identify system improvements
- Predict effects of changes in design and operation

Slide 6 - 26

ProSalus SAFETY CONSULTANTS

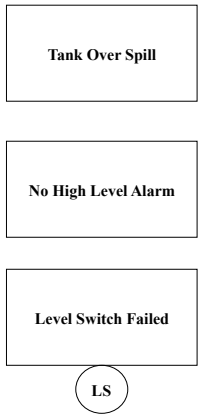
Functional Safety Engineering

Fault Tree Symbols

TOP

INTERMEDIATE

BASIC



- Basic event data are normally failure frequencies.
- Conversion to probability depends on whether failure is revealed or unrevealed.

Slide 6 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree Symbols- 2

LOGIC GATES:

OR gate

Output occurs if any of the input events happen

AND gate

Output occurs only when all the input events happen

TRANSFER gate

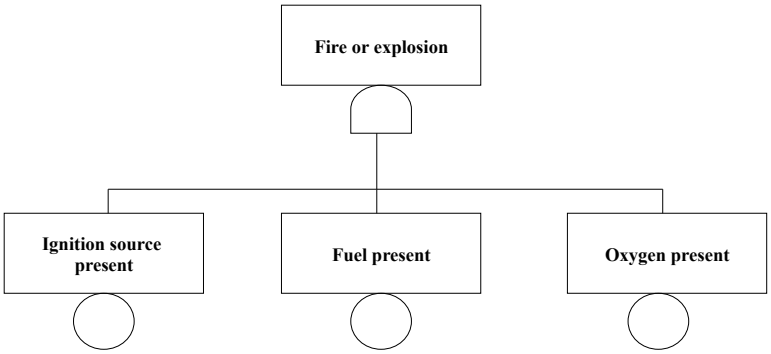
Indicates that part of this fault tree is developed elsewhere

Slide 6 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

AND gate example



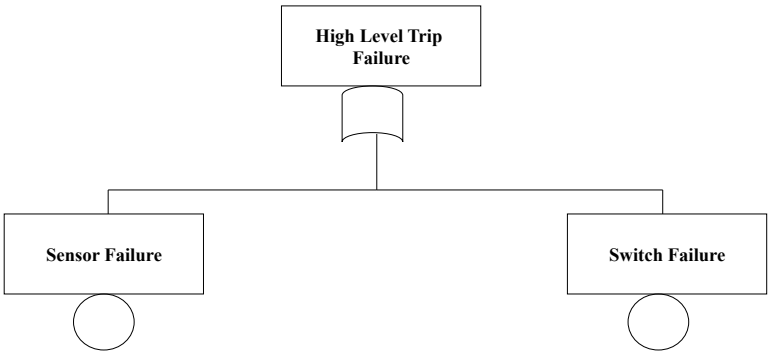
Output event occurs only when all the input events happen

Slide 6 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

OR gate example



Output event occurs in any of the input events happen

Slide 6 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process

STEP 1 - System Definition

STEP 2 - Understanding the system

STEP 3 - Defining the top event

STEP 4 - Constructing the fault tree

STEP 5 - Qualitative Analysis

STEP 6 - Gather failure rate data

STEP 7 - Quantitative Analysis

Slide 6 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process- 2

Step 1 - System Definitions

- Mark-up system drawing and check off items
- Initial equipment configuration
  - Which valves open/closed / Which pumps on/off?

Step 2 - Understanding the System

- Un-allowed events (considered not possible)
- Existing events (considered certain)
- Other assumptions

Step 3 - Top Event Identification

- Requires precise definition - Use HAZOP, FMEA, experience etc
- Vague or poorly defined top events often lead to a poor analysis
- Example: - 'Compressor Fire' is too general use 'Fire in the oxygen compressor enclosure during normal operation' is good

Slide 6 - 32

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 3

Step 4 - Fault Tree Construction

- Begin at top event
- Determine the intermediate faults/causes that result in the top event
- If the basic causes can be determined immediately from the top event then the problem is too simple for FTA
- Identify the logic gate that defines the relationship of those causes to the top event.
- **HOW FAR TO GO?**
  - A branch is of no further interest
  - A branch is known to have very low probability
  - You have reached the stage of individual component failures for which no data is available

Slide 6 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 4

STEP 5 – Fault Tree Reduction (Qualitative Analysis)

- A cut set is any combination of basic events which will cause the top event.
- Cut sets are calculated by Boolean algebra (for complex fault trees many thousands of cut sets may be produced – therefore only simple trees are produced and quantified by hand?.
- Cut sets are used to quantify fault trees.

- 1st Order - 1 Event causes top entry
- 2nd Order - 2 Events needed top entry
- 3rd Order - 3 Events needed top entry

Slide 6 - 34

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Boolean Algebra

1. AND (A and B) = A.B
2. OR (A or B) = A+B
3. NOT (A) $= \overline{A}$
4. XOR (A and B) $= A.\overline{B} + \overline{B}.A$

1. A+A = A
2. A + 1 = 1
3. A + 0 = A
4. A.A = A
5. A.1 = A
6. A.0 = 0
7. A+A.B = A
8. $A + \overline{A} = 1$
9. $A.\overline{A} = 0$
10. $\overline{A.B} = \overline{A}+\overline{B}$
11. $\overline{A+B} = \overline{A}.\overline{B}$

Slide 6 - 35

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 5

Step 6 – Gathering Failure Data

- Need data on basic event frequencies/probabilities.
- Site historical data is preferred when not available take from reliability database such as Faradip etc
- Engineering judgment needed when data is sparse

Step 7 – Fault Tree Quantification

- Calculation of top event frequency or probability
- How often? = Frequency
- Chance of failure on demand = Probability

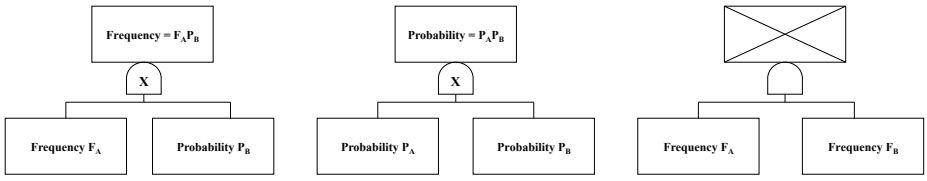
Slide 6 - 36

ProSalus SAFETY CONSULTANTS

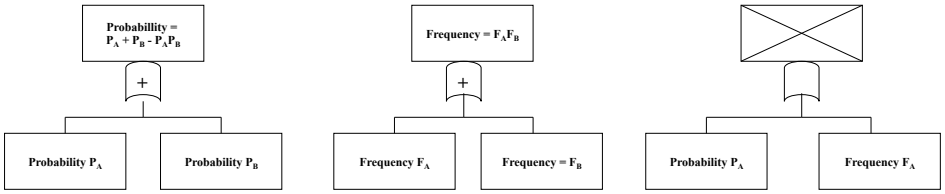
Functional Safety Engineering

AND Gate

Gate By Gate Calculation



OR Gate



Slide 6 - 37

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Rules For Quantification

1 All branches must be independent

2 Decide if top event probability (P) or frequency (F) is required

3 Obtain failure data and convert to probability if required.

Revealed Failure: P = F x Repair Time
Unrevealed Failure: P = 0.5 x F x Test Interval

4 OR Gates (Add)
All inputs must be same type as output

5 AND Gates (Multiply)
P_a x P_b = P; F_a x P_b = F; F_a x F_b not permitted

Slide 6 - 38

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 6

Common Mode/Dependent Failures

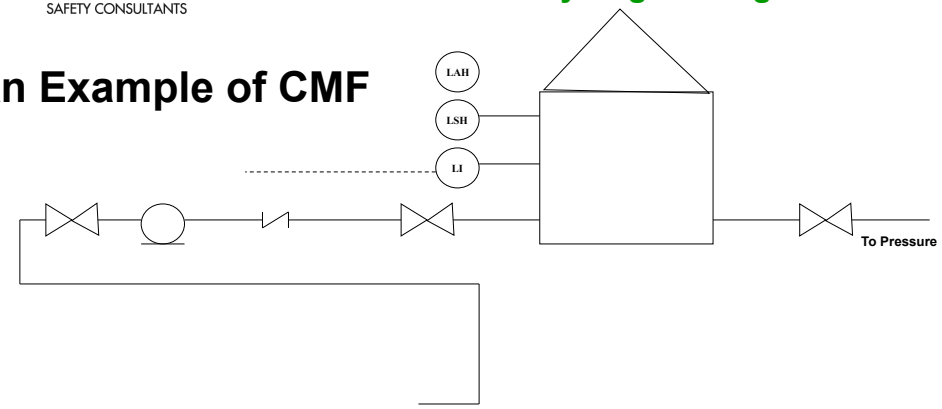
- Quantification assumes all events independent
- CMF causes a number of things to fail simultaneously
- CMF can cause serious errors in results if not included in fault tree
  - Defeats redundancy and/or diversity
  - Can involve both initiating event and mitigating systems

Slide 6 - 39

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

An Example of CMF



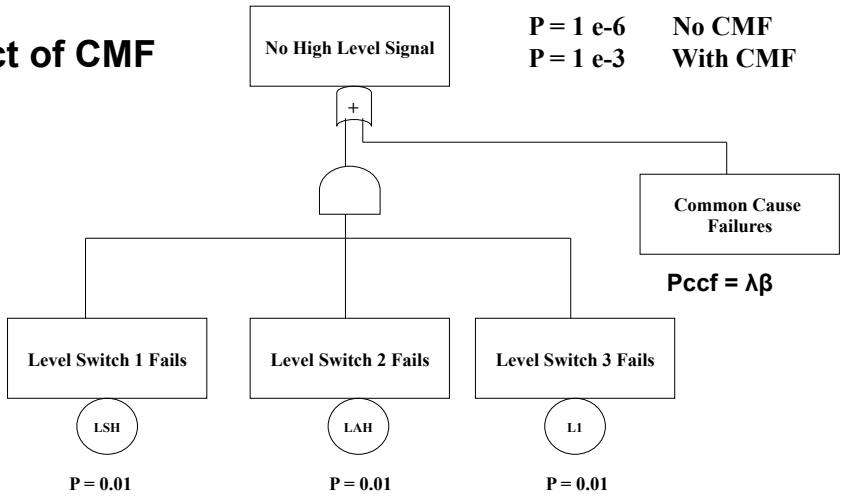
- **Danger of overfilling tank, with potential to overpressure tank. Protect with 3 independent high-level shutdown systems?**

Slide 6 - 40

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Effect of CMF



Slide 6 - 41

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

STRENGTHS OF FTA

- Widely used
- Theory well developed
- Many published texts and papers
- Large number of engineers trained in FTA
- Complimentary information available from:
  - Qualitative and
  - Quantitative analysis
- Visually easy to understand

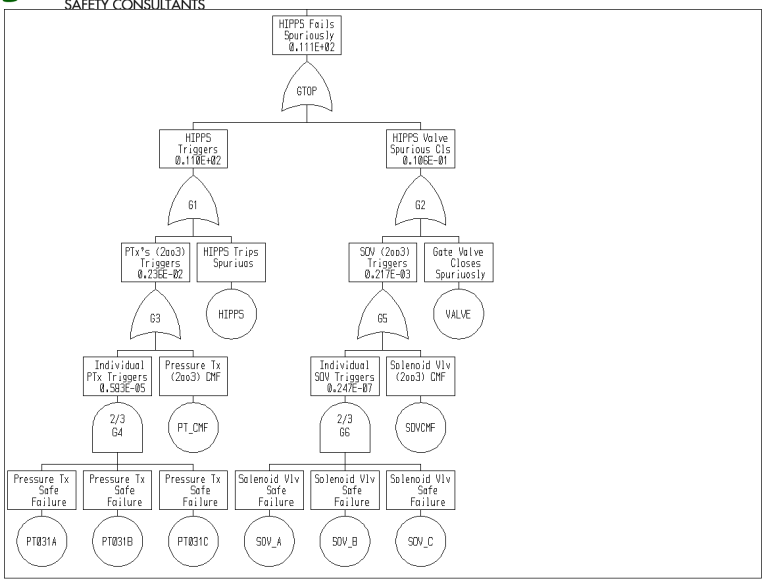
Weakness of FTA

- Very time consuming
- Errors if paths missed
- Error prone if manual
- Substantial experience needed
- Poor treatment of time dependence

Slide 6 - 42

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



FTA SIL Verification Example

Slide 6 - 43

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectures for Low Demand mode of Operation

Based on ISA.TR84.00.02-2002

Slide 6 - 44

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ISA TR 84.00.02 (Part 1 & 2) Simple Formulas– Basic of terms

β	The fraction of undetected failures that have a common cause
λ_{DCCF}	$\beta\lambda_D$
λ_D	Dangerous failure rate
λ_{DD}	Detected dangerous failure rate
λ_{DU}	Undetected dangerous failure rate
$MTTR$	Mean time to repair
PFD_{AVG}	Average probability of failure on demand
T_i	Proof – test interval
λ_s	Safe failure rate
DC	Diagnostic Coverage DC = λ_{DD}/λ_D
T_{ia}	Auto Diagnostic Test Interval

Slide 6 - 45

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ISA TR 84.00.02 (Part 1 & 2) Simple Formulas - Approximation

	1oo1	1oo2	1oo3	2oo2	2oo3
PFDavg	$\frac{1}{2}\lambda_d T_i$	$\frac{1}{3}\lambda_d^2 T_i^2$	$\frac{1}{4}\lambda_d^3 T_i^3$	$\lambda_d T_i$	$\lambda_d^2 T_i^2$
STR	λ_s	$2\lambda_s$	$3\lambda_s$	$2\lambda_s^2 MTTR$	$6\lambda_s^2 MTTR$

λ_d = Dangerous failure rate

λ_s = Revealed failure rate

T_i = Test interval

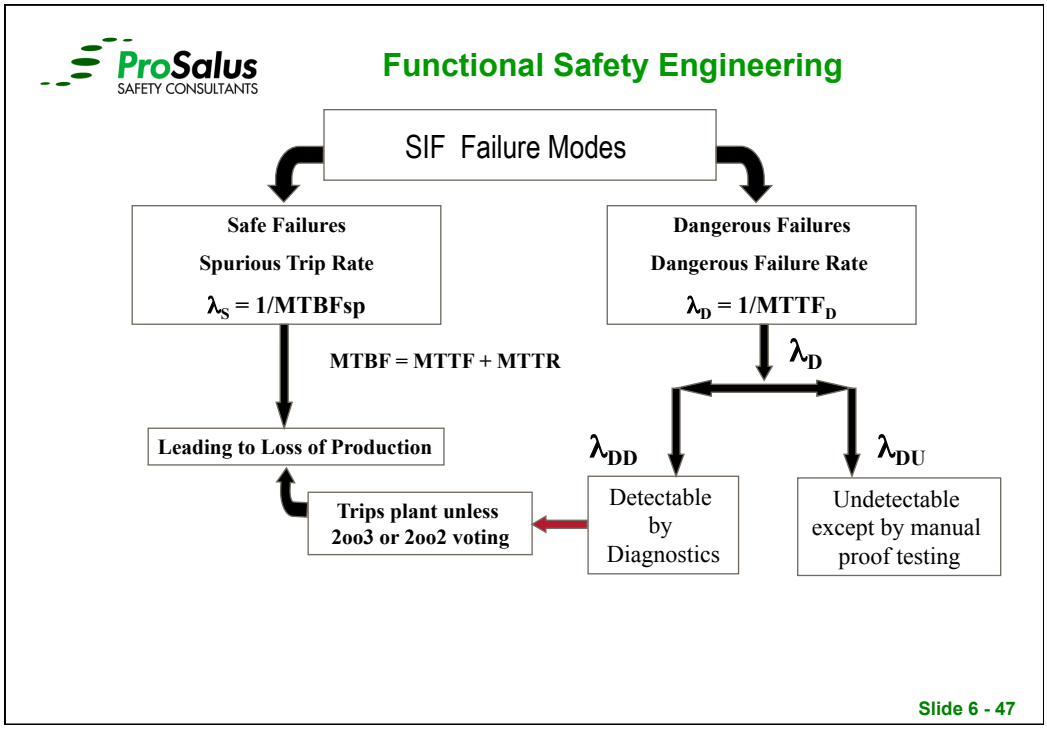
MTTR = Mean Time to repair

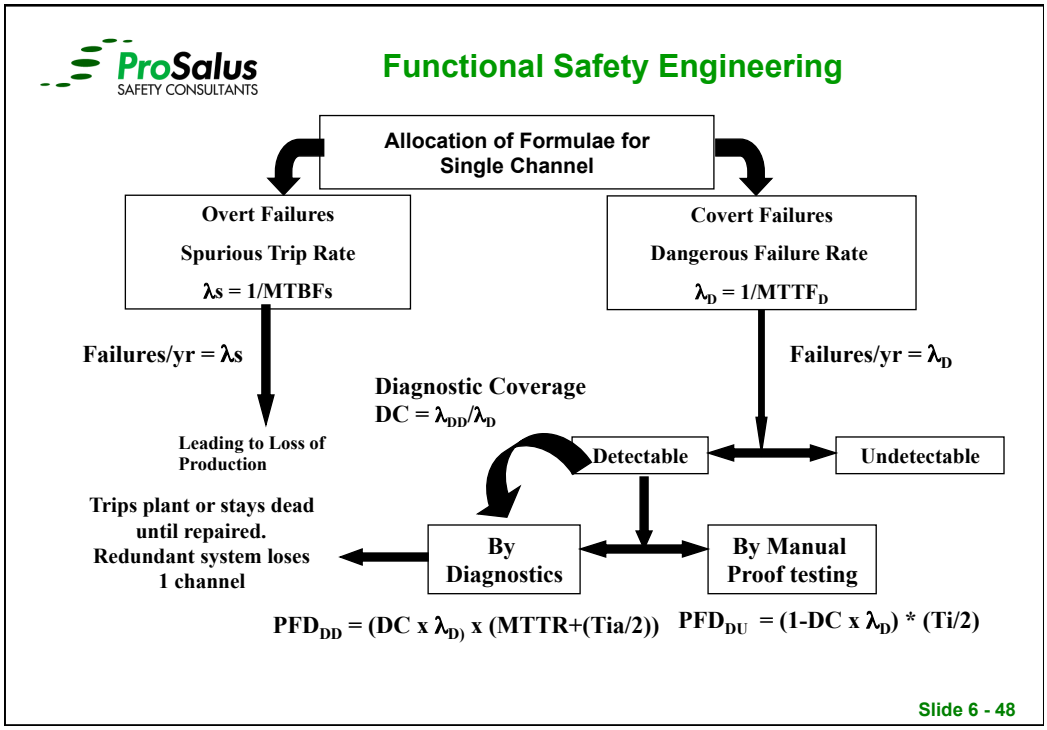
Table showing the most basic simple formula's.

These formula's do not take into account:

- Test coverage factor
- Maintenance interval
- Test duration
- Override during repair
- CCF (Beta Factor)
- Systematic failure rate

Slide 6 - 46





ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

PFD_{avg} Calculations According to ISA.TR84.00.02-2002

The PFD_{avg} is determined by calculating the PFD for all of the components in each SIF loop and combining these individual values to obtain the overall SIF loop PFD_{AVG} value. This is expressed by the following:

$$PFD_{SIF} = \Sigma PFD_{s} + \Sigma PFD_{Ls} + \Sigma PFD_{FE}$$

Where,

PFD_{FE} is the final element PFD_{avg} for a specific SIF,

PFD_{S} is the sensor PFD_{avg} for a specific SIF,

PFD_{LS} is the logic solver PFD_{avg},

PFD_{SIF} is the PFD_{avg} for the specific SIF in the SIS.

Slide 6 - 49

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Determining the PFD_{avg} (ISA.TR84.00.02-2002)

The procedure for determining the PFD_{avg} is as follows:

1.Identify each sensor that detects the process condition that could lead to the event the SIF is protecting against

Only those sensors that prevent or mitigate the designated event are included in PFD calculations.

2.List the $MTTF^{DU}$ for each sensor.

3.Calculate the PFD for each sensor configuration using the $MTTF^{DU}$ and the appropriate equation with consideration for redundancy.

Slide 6 - 50

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

System Equations (ISA.TR84.00.02-2002)

The following equations cover the typical configurations used in SIF configurations. To see the derivation of the equations listed, refer to ISA–TR84.0.02–Part 5.

Converting MTTF to failure rate, λ:

$$\lambda^{DU} = 1 \setminus MTTF^{DU}$$

Equations for typical configurations:

$$\textbf{1oo1}\ PFD_{avg} = [\lambda^{DU} \times TI/2] + [\lambda^{D}_{F} \times TI/2]$$

Where λ^{DU} is the undetected dangerous failure rate
λ^{D}_{F} is the dangerous systematic failure rate, and
TI is the proof test interval

Slide 6 - 51

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Failures (ISA.TR84.00.02-2002)

ISA equations model the systematic failure λ^{D}_{F} as an error that occurred during the specification, design, implementation, commissioning, or maintenance that resulted in the SIF component being susceptible to a random failure.

Systematic failures are rarely modeled for SIF Verification calculations due to the difficultly in assessing the failure modes and effects and the lack of failure rate data for various types of systematic failure.

However, these failures are extremely important and can result in a significant impact to the SIF performance, this is addressed through lifecycle process that incorporates design and installation concepts, validation and testing criteria, and management of change and are intended to to be a defense systematic failures..

Slide 6 - 52

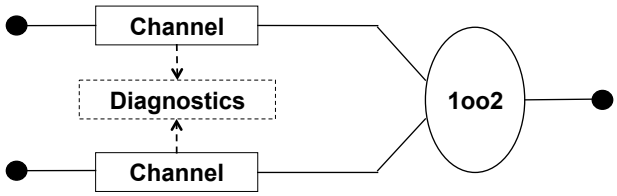
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 (ISA.TR84.00.02-2002)

1oo2 - System

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.



1oo2 physical block diagram

Slide 6 - 53

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 (ISA.TR84.00.02-2002)

$PFD_{avg} = [((1-\beta) \times \lambda^{DU})^2 \times TI^2/3] + [(1-\beta) \times \lambda^{DU} \times \lambda^{DD} \times MTTR \times TI] + [\beta \times \lambda^{DU} \times TI/2] + [\lambda^{D}_{F} \times TI/2]$

For simplification, 1 – β is generally assumed to be one, which yields conservative results. Consequently, the equation reduces to

$PFD_{avg} = [(\lambda^{DU})^2 \times TI^2/3] + [\lambda^{DU} \times \lambda^{DD} \times MTTR \times TI] + [\beta \times \lambda^{DU} \times TI/2] + [\lambda^{D}_{F} \times TI/2]$

Where MTTR is the mean time to repair
λ^{DD} is dangerous detected failure rate, and
β is fraction of failures that impact more than one channel of a redundant system (CCF).

The second term represents multiple failures during repair. This factor is typically negligible for short repair times (typically less than 8 hours). The third term is the common cause term. The fourth term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate λ_s = Safe failure rate channel 1 (λ_{s1}) + Safe failure rate channel 2 (λ_{s2})

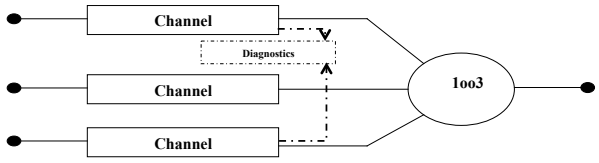
Slide 6 - 54

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo3 (ISA.TR84.00.02-2002)

1oo3 – System
This architecture consists of three channels connected in parallel, such that either channel can process the safety function. Thus there would have to be dangerous failure in all three channels before a safety function failed on demand.



1oo3 physical block diagram

$$PFD_{avg} = [(\lambda^{DU})^3 \times TI^3/4] + [(\lambda^{DU})^2 \times \lambda^{DD} \times MTTR \times TI^2] + [\beta \times (\lambda^{DU} \times TI/2)] + [\lambda^{D}_{F} \times TI/2]$$

The second term accounts for multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term and the fourth term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate $\lambda_s = 3\lambda_s$

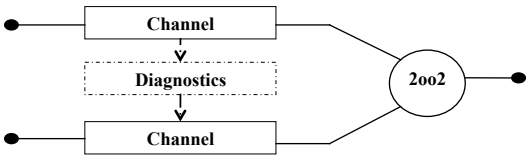
Slide 6 - 55

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo2 (ISA.TR84.00.02-2002)

2oo2 – System
This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.



2oo2 physical block diagram

$$PFD_{avg} = [\lambda^{DU} \times TI] + [\beta \times \lambda^{DU} \times TI] + [\lambda^{D}_{F} \times TI/2]$$

The second term is the common cause term and the term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate $\lambda_s = 2\lambda_s^2 MTTR$

Slide 6 - 56

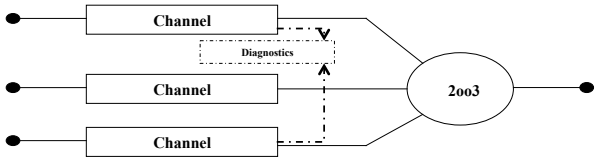
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo3 (ISA.TR84.00.02-2002)

2oo3 – System

3 channels in parallel with majority voting such that the output state does not change if only 1 channel changes.



2oo3 physical block diagram

$PFD_{avg} = [(\lambda^{DU})^2 \times (TI)^2] + [3\lambda^{DU} \times \lambda^{DD} \times MTTR \times TI] + [\beta \times \lambda^{DU} \times TI/2] + [\lambda^{D}_{F} \times TI/2]$

The second term in the equation represents multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term. The fourth term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate $\lambda_s = 6\lambda_s^2 MTTR$

Slide 6 - 57

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The simplified equations **in** ISA.TR84.00.02-2002 without the terms for multiple failures during repair, common cause and systematic errors reduce to the following for general use

1oo1

$PFD_{avg} = \lambda^{DU} \times TI/2$

2oo2

$PFD_{avg} = \lambda^{DU} \times TI$

1oo2

$PFD_{avg} = [(\lambda^{DU})^2 \times TI^2]/3$

2oo3

$PFD_{avg} = (\lambda^{DU})^2 \times TI^2$

1oo3

$PFD_{avg} = [(\lambda^{DU})^3 \times TI^3]/4$

2oo4

$PFD_{avg} = (\lambda^{DU})^3 \times (TI)^3$

Slide 6 - 58

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Implementation

- Calculating the PFD of the function
- The PFD of each subsystem/element is calculated for (1oo1, 1oo2 etc.) for the:
  - Initiator
  - Logic solver
  - Final element
- The total PFD for the combination is then calculated

Slide 6 - 59

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Impact of Proof Testing

The Probability of Failure for 1oo1 element = $\frac{1}{2}\lambda_d T_i$

Therefore if the Proof test interval is increased then the PFDavg will also increases proportionally, likewise if the proof test is decreased the PFDavg will also decreases proportionally

Slide 6 - 60

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Impact of Maintenance

The simplified formula for PFDavg = $\frac{1}{2}\lambda_d T_i$

- Assumes that the element is in the 'as new condition'
- Testing does not cover every aspect (coverage factor < 1)
  - E.g. we do not know the internal condition of a valve
- Only periodic 'bench type' maintenance can bring elements back to an 'as new condition'

- ***The PFDavg will increase without routine maintenance***

Slide 6 - 61

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Impact of Imperfect Proof Test and Maintenance

- At the Maintenance Interval the element is maintained and returned to the as new condition:
  - For 1oo1 System:

$$PFD_c = (\frac{1}{2}\lambda_d T_i C + \frac{1}{2}\lambda_d T_m (1 - C))$$

Where:
λd = Total unrevealed or dangerous failure rate (per/year)
Ti = Total interval (years)
C = The Proof test coverage factor
Tm = Maintenance interval; interval at which the device is maintained to as new condition (years)

Slide 6 - 62

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Calculation

For a simplified 1oo1 system:

$$PFDavg = \tfrac{1}{2}\lambda_d T_i$$

Dangerous undetected failure rate λ is 10^{-6} h^{-1} (1 failure in 114 years)

Proof test Ti is annual (every 8760 hours),

So the

$$PFD_{avg} = 0.5 \cdot 10^{-6} \cdot 8760 = 4.38 \cdot 10^{-3}.$$

Slide 6 - 63

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

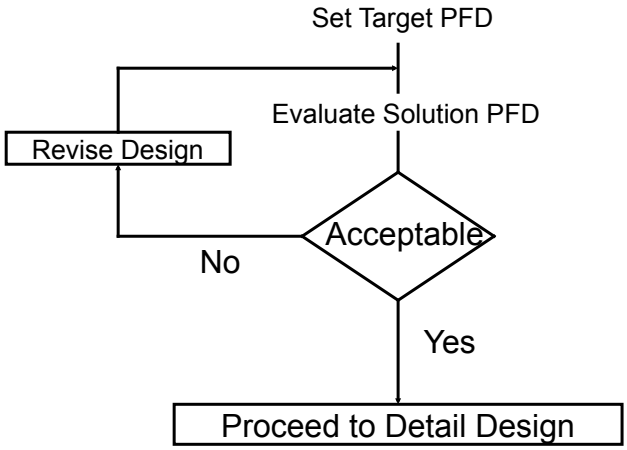
Design Example

Slide 6 - 64

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design Iteration for Target PFD

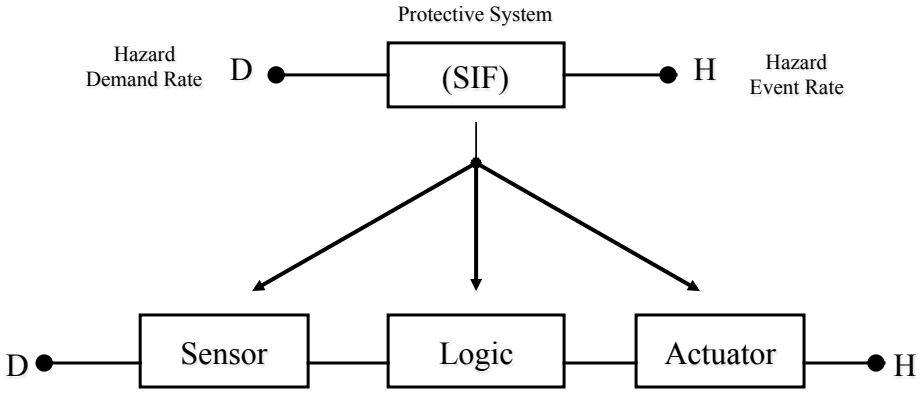


Slide 6 - 65

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 1



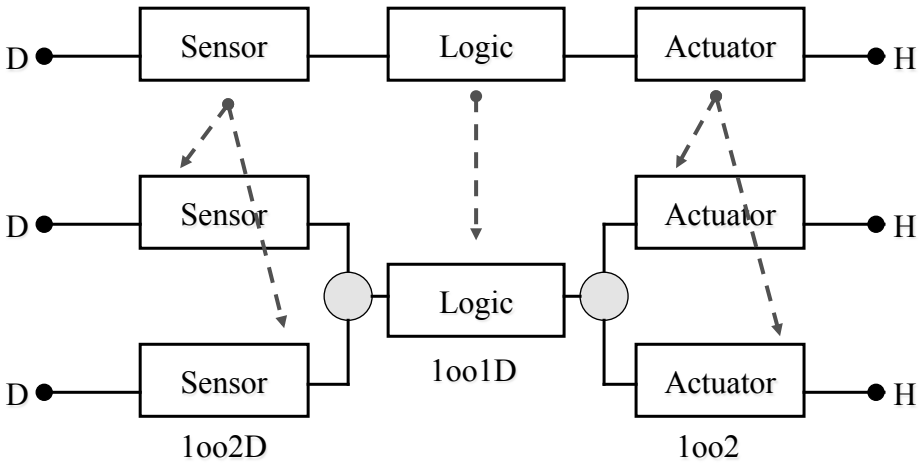
Slide 6 - 66

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 2, identify channels in each stage

Example:Dual channel sensors and actuators, single channel logic

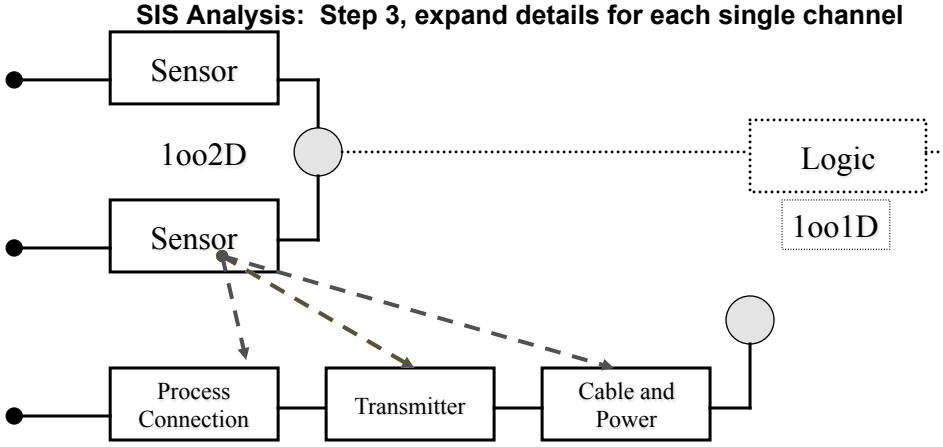


Slide 6 - 67

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 3, expand details for each single channel

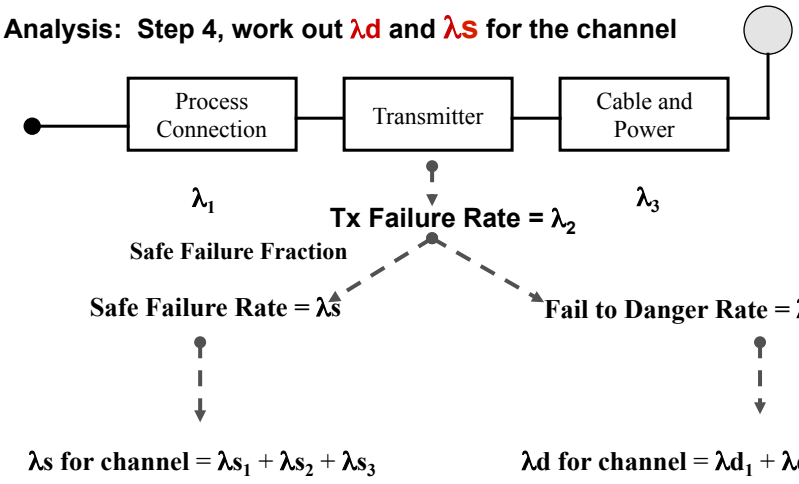


Slide 6 - 68

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 4, work out λd and λs for the channel

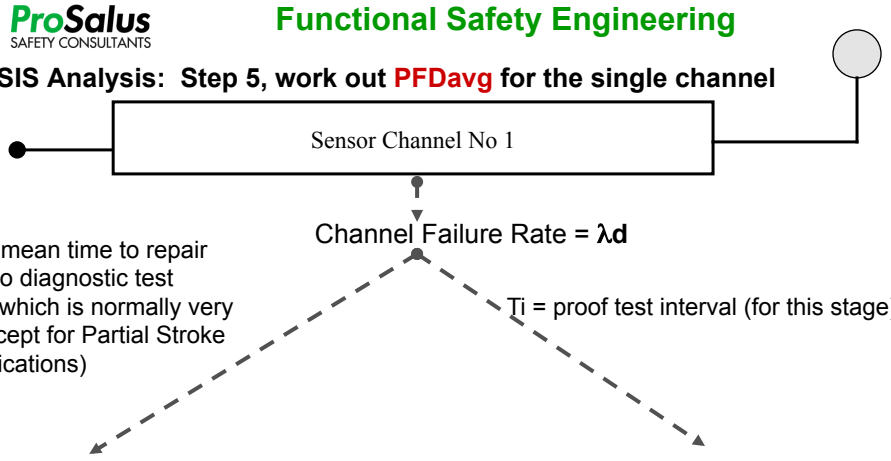


Slide 6 - 69

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 5, work out PFDavg for the single channel



MTTR = mean time to repair
Tia = auto diagnostic test interval (which is normally very small except for Partial Stroke test applications)

Ti = proof test interval (for this stage)

PFDa = DC x λd x (MTTR+(Tia/2)

Portion detected by auto diagnostics

PFDb = (1-DC) x λd x Ti/2)

Portion detected by manual proof tests

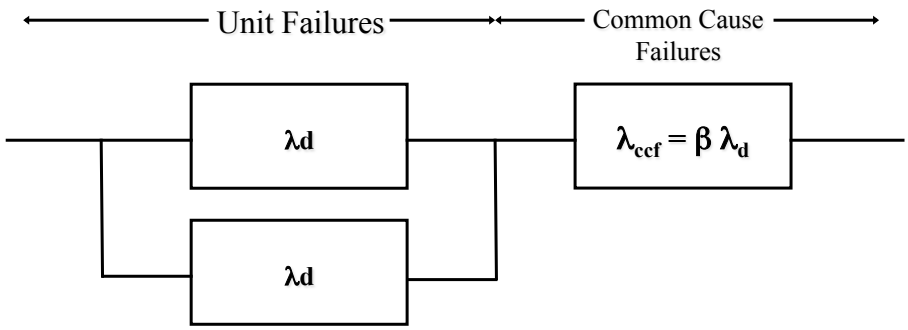
PFDavg = PFDa + PFDb

Slide 6 - 70

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Beta Factor: Common Cause Failures in redundant SIS channels



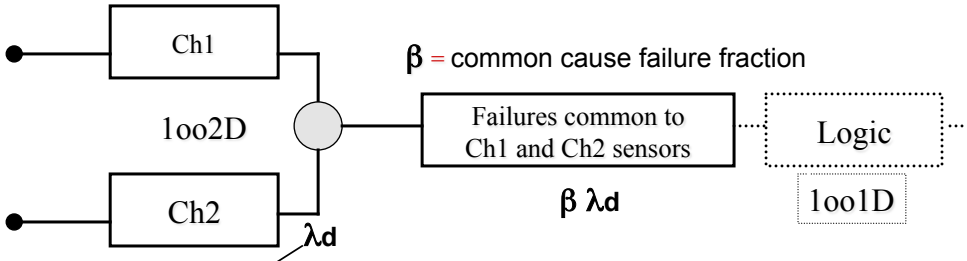
Example: 1002 with common cause failure RBD block

Slide 6 - 71

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 6, find the PFDavg for the 1002D sensor group: Break out the common cause failure fraction for the redundant channels and calculate PFDavgs for each portion



Redundant section:
PFDavg =
((DC x λd)² x (MTTR+Tia)²)
+ (((1-DC x λd) x Ti)²)/3

+

Common cause section
PFDavg =
((DC x (β x λd)) x MTTR)
+ ((1-DC x (β x λd) x Ti/2)

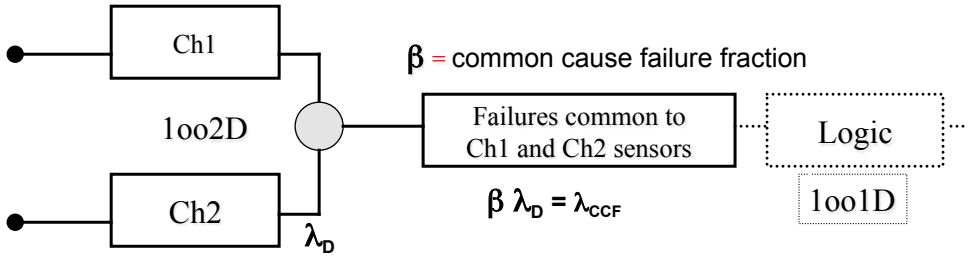
Slide 6 - 72

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example

DC = 70%, λd = 0.01/yr, MTTR = 48 hrs, Tia = 100 msec, Ti = I yr, β = 10%



1002D PFDavg = ((0.7 x 0.01)^2 x (0.0055)^2) + (((1-0.7 x 0.01) x 1)^2)/3 = 3.00E-06 **+** **CCF PFDavg =** ((0.7 x (0.1 x 0.01)) x 0.0055) + ((1-0.7 x (0.1 x 0.01) x ½) = 1,54E-04

1002D PFDavg + CCF PFDavg = 3.00E-06 + 1,54E-04 = 1,57E-04

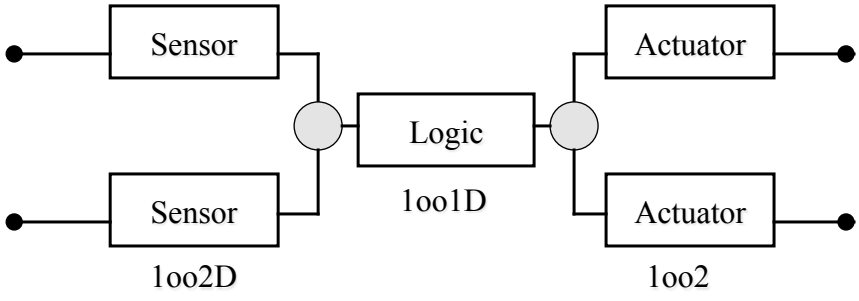
Slide 6 - 73

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 7, repeat steps 3 to 6 for each stage

Example:Dual channel sensors and actuators, single channel logic



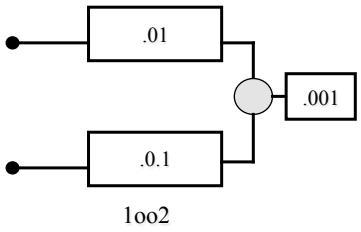
PFDavg for sensors **+** **PFDavg for Logic solver** **+** **PFDavg for actuators**

Slide 6 - 74

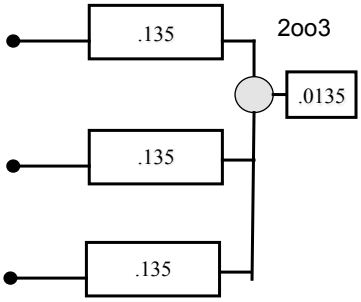
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Reducing Spurious Trip Rate



Dual Sensors Spurious
= (2 x 0.01) + (0.1 x 0.01)
= 0.021 trips per yr



2oo3 Sensors Spurious
= 6x λs^2 (MTTR)+ $\beta \lambda s$
= (6 x 0.135^2 x 8/8760) +(0.1 x 0.135)
= 0.00001 + 0.0135
= 0. 01351 trips per yr

Slide 6 - 75

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example evaluation of Diagnostic Coverage for Valve

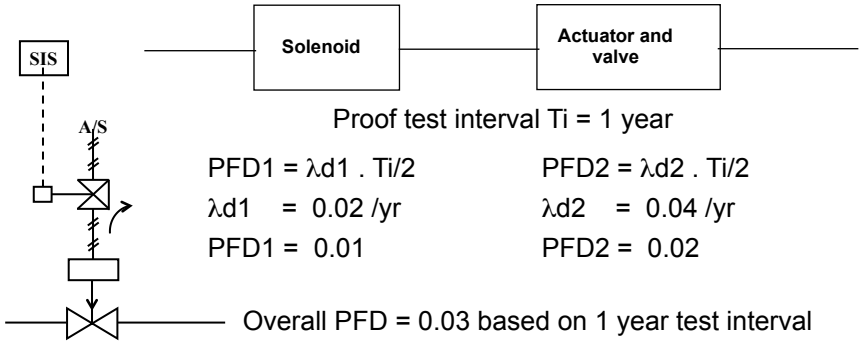
Failure Mode	% Contribution to dangerous failures	%Detection by partial closure test	% Of Dangerous Faults Detected
Actuator spring breakage or jamming	20	70	14
Solenoid fails to vent	5	50	2.5
Positioner fails to trip	5	100	5
Hoses kinked or blocked	10	100	10
Valve stem or rotary shaft stuck	40	70	28
Actuator linkage fault	5	70	3.5
Seating failures of valve causing high leakage. Due to erosion or corrosion	10	0	0
Foreign bodies or sludge preventing full closure	5	0	0
Total	100%		63%

Slide 6 - 76

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design example: SIL 2 single or double valve decision
Step 1 Single valve with solenoid



Proof test interval Ti = 1 year

PFD1 = λd1 . Ti/2 PFD2 = λd2 . Ti/2

λd1 = 0.02 /yr λd2 = 0.04 /yr

PFD1 = 0.01 PFD2 = 0.02

Overall PFD = 0.03 based on 1 year test interval

Qualifies for SIL 1 only

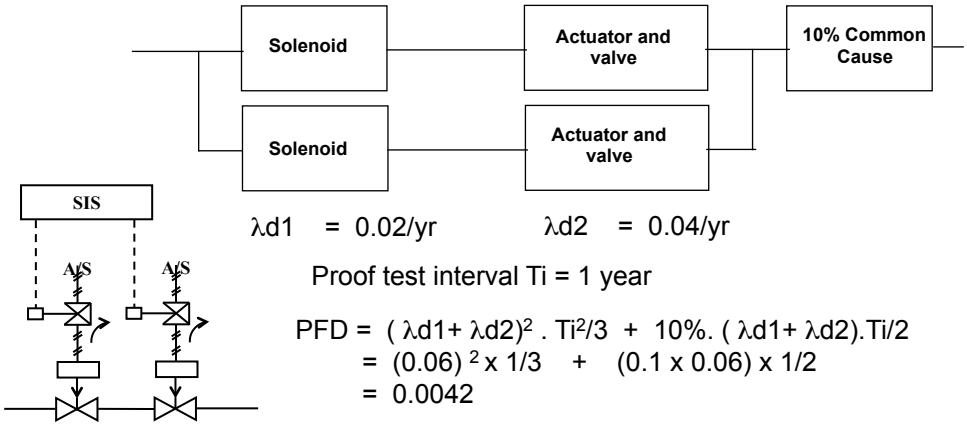
Reliability diagram for single tripping valve

Slide 6 - 77

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 2 : Reliability diagram for 1oo2 tripping valves



λd1 = 0.02/yr λd2 = 0.04/yr

Proof test interval Ti = 1 year

PFD = $(\lambda d1+\lambda d2)^2 . Ti^2/3 + 10\%. (\lambda d1+\lambda d2).Ti/2$

= $(0.06)^2$ x 1/3 + (0.1 x 0.06) x 1/2

= 0.0042

Overall PFD = 4.20E-03 based on 1 year test interval

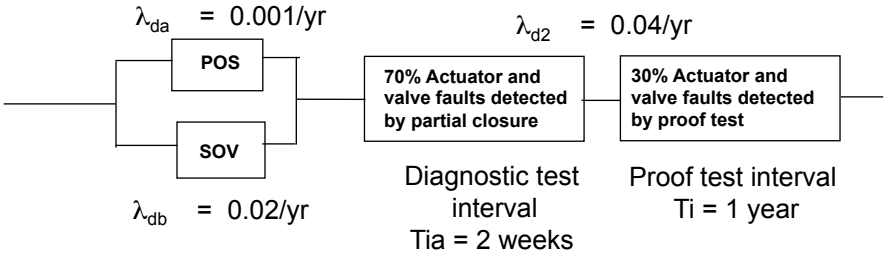
Qualifies for SIL 2 with adequate margin for sensors and logic

Slide 6 - 78

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Reliability diagram for single tripping valve with Smart Positioner and Partial Closure Testing



$PFD_1 = \lambda_{da} . \lambda_{db} . Ti^2/3$
$PFD_1 = (0.001 \times 0.02) \times 1^2/3$
$PFD_1 = 6.60E\text{-}06$

$PFD_2 = .7\lambda_{d2} . Tia/2$
$PFD_2 = (0.7 \times 0.04) \times 0.038/2$
$PFD_2 = 5.32E\text{-}04$

$PFD_3 = 0.3\lambda_{d2} . Ti/2$
$PFD_3 = (0.3 \times 0.04) \times 1/2$
$PFD_3 = 6.00E\text{-}03$

Overall PFD = 6.54E-03 based on 1 year test interval
Qualifies for SIL 2 with adequate margin for sensors and logic

Slide 6 - 79

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Conclusion for design example

Option 1:

to meet the SIL 2 target: Install 2 block valves and proof test once every 2 years

Option 2:

to meet the SIL 2 target: Install 1 block valve with smart Positioner PS testing every 2 weeks. Proof test once every year.

NB : Both options must satisfy SIL architecture constraints.

Slide 6 - 80

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Commentary on Diagnostic claims for Valves

One attraction of high diagnostic coverage is the improvement in safe failure fraction.

Improved SFF allows reduced Fault Tolerance under IEC 61508. If you can establish high Safe Failure Fraction (SFF) using a smart Positioner you can reduce the number of valves needed to meet a SIL target.

Responsibility remains with end user to justify reduced FT requirements by showing diagnostic coverage and SFF are calculated. Vendors will be keen to assist!

IEC 61508-2 clause 7.4.4.5 should be consulted. See also IEC 61508-6 Annex C

Slide 6 - 81

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Query: Can Diagnostic Coverage of the valve qualify as improved SFF?

Answer: Only if test interval does not add significantly to MTTR and only if safe response or immediate repair is assured. (see 61508-6 annex B).

In practice diagnostic test interval must be at least Ti/10 and should be less than 1 week . (see 61508 annex D table D3). Calculations are required.

If Yes does this mean we can claim > 90% SFF for the valve subsystem?

Answer: Yes

Does this qualify for reduced redundancy?

Answer: Yes it does if PFD figures are satisfied.

Slide 6 - 82

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SUMMARY

Commonly manufacturers of components and subsystems have no influence on the SIL of the complete safety related system.

SIL-rating of a subsystem makes no sense – in the best case this is an indicator that it would be suitable / has the capability to be part of a *SIL* rated system.

Always the PFDavg or PFH of the safety related system has to be calculated.

Additionally requirements for the avoidance of systematic failures have to be met – 61508 Systematic Capability.

The standard requires an assessment of functional safety capability – Management, Design, Change Control, Implementation, Competency, Operations & Maintainance.

Certificates are not mandatory, and there is no law yet requiring SIL-certificates.

Slide 6 - 83

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Practical Exercise No: 2

SIL Verification Practical

Slide 6 - 84

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Exercise No: 2 – SIL Verification

Task 1 Calculate the single channel PFDavg and spurious trip rate for the high temperature trip example. Draw a single channel reliability block diagram and calculate using the failure rates in the table the PFDavg and the spurious trip rate for each sub system and the overall system using a proof testing interval of 6 months.

Assume the system uses 2 relays, 1 relay in the sensor subsystem and 1 relay in the logic solver subsystem, The trip actuation uses a solenoid valve and to vent the air cylinder on a valve that will drive open and release quench water into the reactor.

Task 2: Redraw the RBD and calculate the PFDavg and spurious trip rate for the SIF using the second diagram showing 3 high temperature transmitters on a reactor configured 2oo3 on the basis of proof testing every 6 months, Beta Factor 10% and MTTR of 24 hours.

The 3 temperature transmitters each transmit to a trip amplifier device that acts as a high temperature trip device leading to a single channel actuation as in task 1

Slide 6 - 85

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

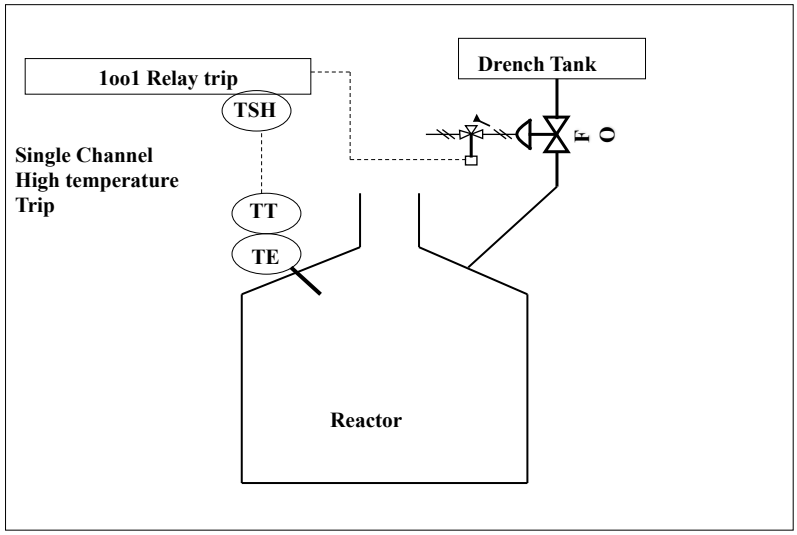
Table of fault rates for the Devices

Channel Device	Fail-safe rate per year	Fail –danger rate per year
TE…element	1.5	0.20
TT .Transmitter	0.5	0.05
Cable/terminals	0.01	0.00
TSH….trip amplifier/switch	0.5	0.1
Relay (each)	0.05	0.002
Solenoid Valve	0.04	0.02
Trip Valve	0.4	0.1

Slide 6 - 86

ProSalus SAFETY CONSULTANTS

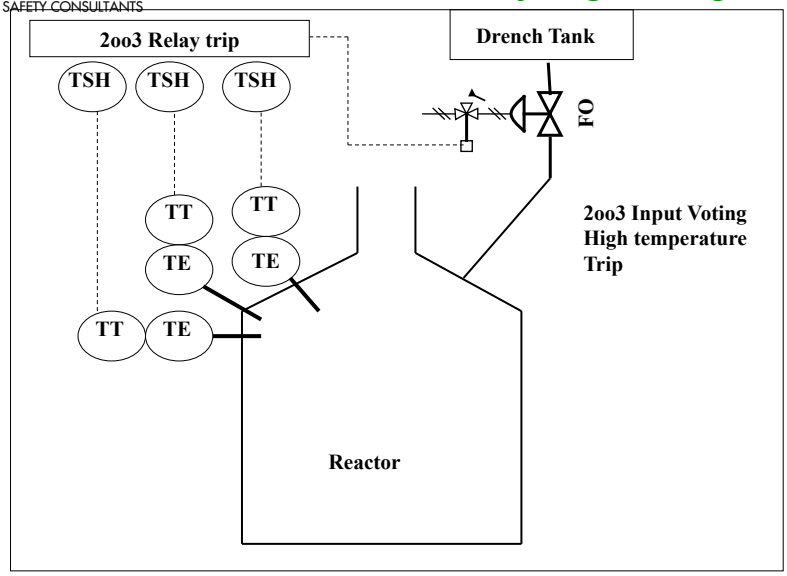
Functional Safety Engineering



Slide 6 - 87

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



Slide 6 - 88

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectures for Low Demand mode of Operation

Based on Reliability Block Diagrams

IEC 61508 2010 Part 6

Slide 6 - 89

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Part 6 Low demand mode – Index of terms

β	The fraction of undetected failures that have a common cause
β_D	The fraction of those failures that are detected by the diagnostic tests, the fraction that have a common cause *(β = 2 x β_D)*
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal 0.5 λ (assumes 50 % dangerous failures and 50 % safe failures)
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)
MTTR	Mean rime to restoration (hour)
PFDG	Average probability of failure on demand for the group of voted channels
T_1	Proof – test interval (h)
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all components in the channel of the subsystem)
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)

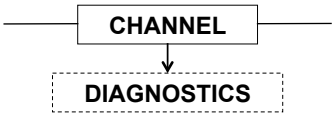
Slide 6 - 90

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

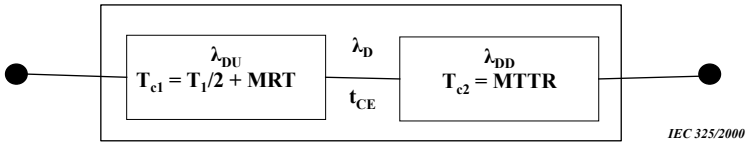
IEC 61508 Part 6 – Low Demand Mode

B.3.2.2.1 1oo1 – System: Single channel where any dangerous failure leads to failure of the safety function when a demand arises.



IEC 324/2000

Figure B.4 - 1oo1 Physical Block diagram



IEC 325/2000

Figure B5 – 1oo1 Reliability Block Diagram

Slide 6 - 91

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo1 – System cont'd

Figure B.5 shows that the channel can be considered to comprise of two components, one with a dangerous failure rate λ_{DU} & the other with a dangerous failure rate λ_{DD}. It is possible to calculate the channel equivalent mean down time t_{CE}, adding the individual down times from both components, t_{c1} and t_{c2}, in direct proportion to each component's contribution to the probability of failure of the channel:

$$t_{CE} = \lambda_{DU} / \lambda_D(T_1 / 2 + MRT) + \lambda_{DD} / \lambda_D \, MTTR$$

For every architecture, the detected dangerous failure rate and the undetected dangerous failure rate are given by

$$\lambda_{DU} = \lambda_D(1\text{-}DC) \; ; \qquad \lambda_{DD} = \lambda_D DC$$

For a channel with down time t_{CE} resulting from dangerous failures

$$PFD = 1 - e^{-\lambda_D t_{CE}}$$
$$\approx \lambda_D t_{CE} \qquad \text{since } \lambda_D t_{CE} << 1$$

Hence, for a 1oo1 architecture, the average probability of failure on demand is

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Slide 6 - 92

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 Channels

B.3.2.2.2 1oo2 - System

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

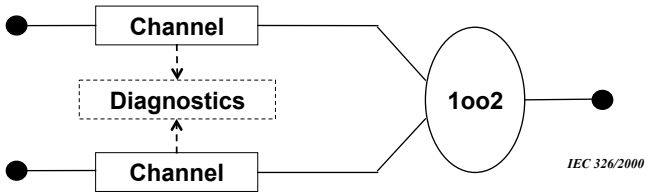


Figure B.6 – 1oo2 physical block diagram

Slide 6 - 93

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 Channels cont'd

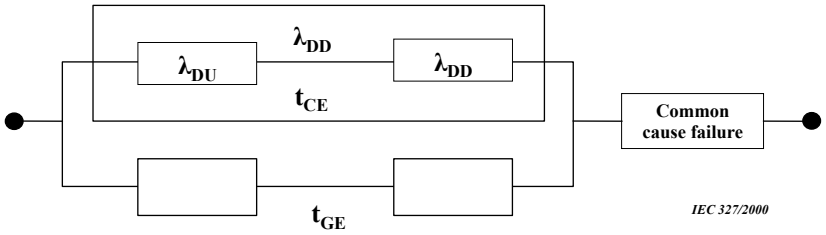


Figure B.7 – 1oo2 reliability block diagram

Figures B.6 and B.7 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1, but now it is necessary to also calculate the system equivalent down time t_{GE}, which is given by

$$t_{GE} = \lambda_{DU} / \lambda_D \, (T_1 / 3 + MRT) + \lambda_{DD} / \lambda_D \, MTTR$$

The average probability of failure on demand for the architecture is

$$PFD_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \, (T1 / 2 + MRT)$$

Slide 6 - 94

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo2 Channels

B.3.2.2.3 2oo2 – System

This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

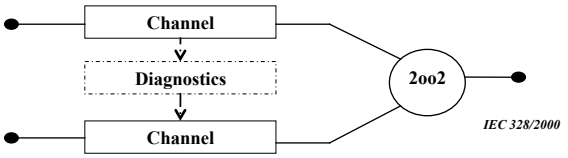


Figure B.8 – 2oo2 physical block diagram

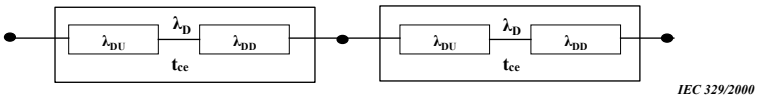


Figure B.9 – 2oo2 reliability block diagram

$$PFD_G = 2\lambda_d t_{ce}$$

Slide 6 - 95

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2D Channels

B.3.2.2.4 1oo2D – System

During normal operation, both channels need to demand the safety function before it can take place. In addiction, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by the other channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated between the channels, either channel can determine the state of the other channel via a means independent of the channel.

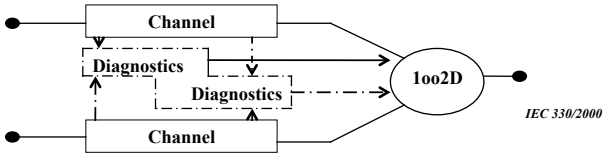


Figure B.10 – 1oo2D physical block diagram

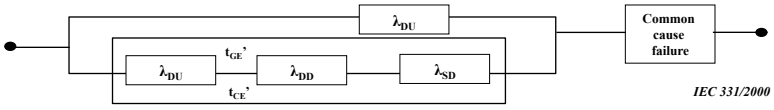


Figure B.11 – 1oo2D reliability block diagram

Slide 6 - 96

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2D cont'd

The detected Safe failure rate for every channel is given by

$$\lambda_{SD} = \lambda_S DC$$

Figures B.10 and B.11 contain the relevant block diagrams. The values of the equivalent mean down times differ from those given for the other architectures in B.3.2.2 and hence are labelled t_{CE}' and t_{GE}'. Their values are given by:

$$t_{CE}' = (\lambda_{DU} (T_1 / 2 + MRT) + (\lambda_{DD} + \lambda_{SD}) MTTR) / (\lambda_{DU} + (\lambda_{DD} + \lambda_{SD}))$$

$$t_{GE}' = T_1 / 3 + MRT$$

The average probability of failure on demand for the architecture is:

$$PFD_G = 2(1 - \beta)\lambda_{DU}((1 - \beta)\lambda_{DU} + (1 - \beta_D)\lambda_{DD} + \lambda_{SD})\, t_{CE}'\, t_{GE}' + 2(1\text{-}K)\, \lambda_{DD} t_{CE}' + \beta\lambda_{DU} (T1/2 + MRT)$$

Slide 6 - 97

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo3 Channels

B.3.2.2.5 2oo3 – System

Three channels in parallel with majority voting such that the output state does not change if only one channel changes. It is assumed that any diagnostic testing would report faults only and not change the output state.

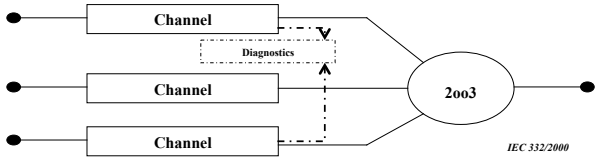


Figure B.12 – 2oo3 physical block diagram

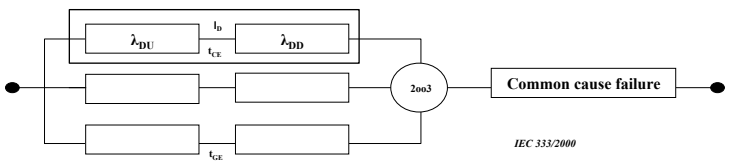


Figure B.13– 2oo3 reliability block diagram

Slide 6 - 98

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo3 cont'd

Figures B.12 and B.13 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1 and the value of t_{GE} is as given in B.3.2.2.2 , The average probability of failure on demand for the architecture is:

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(T1/2 + MRT)$$

B.3.2.2.6 1oo3 – System

Three channels in parallel with a voting arrangement such that the output state follows 1oo3 voting. It is assumed that any diagnostic testing would report faults only and not change the output state. The RBD is as the 2oo3 case but with 1oo3 voting with the value of t_{CE} is as given in B.3.2.2.1 and the value of t_{GE} is as given in B.3.2.2.2 The average probability of failure on demand for the architecture is:

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(T1/2 + MRT)$$

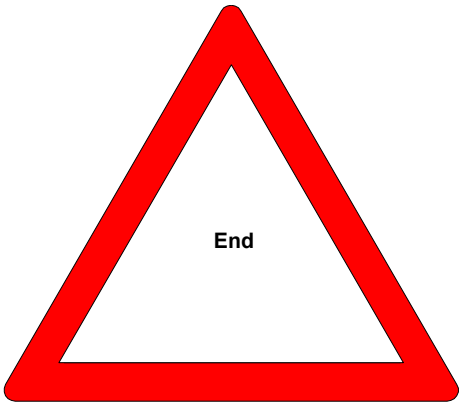
Where

$$t_{G2E} = \lambda_{DU} / \lambda_D (T_1 / 4 + MRT) + \lambda_{DD} / \lambda_D \, MTTR$$

Slide 6 - 99

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



Slide 6 - 100

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Practical SIL Determination Methods based on IEC 61511

ProSalus Limited Slide 7 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

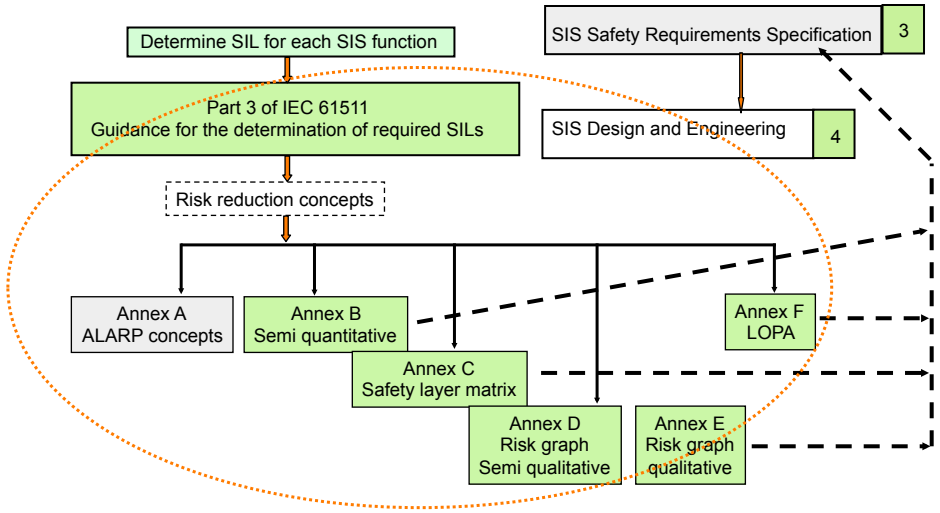
Target Safety Integrity Level (SIL) of a SIF

- The target SIL of the SIF is critical to the SRS
  - To ensure the design is appropriate to the risk contribution required to prevent the hazard from occurring
- IEC 61511-3 provides guidance on determination methodologies
- CCPS also offers guidance on the LOPA method
- These methods can be quantitative, semi quantitative or qualitative methods

ProSalus Limited Slide 7 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited Slide 7 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIL Determination by Risk Graph

ProSalus Limited Slide 7 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Risk Graph Assessment Team

- Competent, Experienced team with relevant site experience and knowledge of the process to be assessed
- Based on the Process to be assessed the team should include:
  - Independent Facilitator & Scribe (Could be Process Safety Engineer)
  - Process design experience
  - Operations experience
  - Maintenance experience & equipment knowledge
  - Safety representative
  - Control & Instrument representative
  - Other specialists as required (Electrical, Mechanical, Equipment vendor)

ProSalus Limited Slide 7 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Graph

- Determination Tool Based on Calibrated Risk Parameters (IEC 61511-3):
  - Demand Rate (W)
  - Consequence (C)
  - Occupancy (F)
  - Probability of Avoidance (P)
- Mandatory to consider Personal Safety and Environment consequences
- Optional to consider Asset consequences / business needs
- Now considered a screening tool for significant risk SIFs
- Tend to be conservative
- Can be Qualitative or Semi Quantitative

ProSalus Limited Slide 7 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk graph: general scheme

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Personal Safety Risk Graph

- Based on the IEC61511-3 Methodology (Also guidance in IEC 61508-5, Annex D)
- Calibrated in terms of potential loss of life
- All four risk parameters (W, C, F, P) considered:
  - The Frequency of Demand with no SIS installed
  - Consequences in terms of fatalities or serious injury with no SIS installed
  - Personal exposure to the hazard in terms of occupancy
    - Duration is normally assessed as less than 10% or more than 10% of working time
  - Probability of Avoidance
    - Avoidance factors such as SIS failure alarm, manual shutdown & evacuation

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk graph: Semi Quantitative Parameters

Parameter	Range of values
Consequence: C Number of Fatalities Guidance as follows: Multiply no of people present when area is occupied by vulnerability. Vulnerability factors guide: V =0.01 small release of flammable or toxic material V = 0.1 Large release V = 0.5 As above but high probability of fire or highly toxic V = 1 Rupture or explosion.	C_A = Minor injury C_B = Range 0.01 to < 0.1 C_C = Range 0.1 to < 1.0 C_D = Range > 1.0

ProSalus Limited Slide 7 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk graph: Semi Quantitative Parameters

Parameter	Range of Values
Occupancy (F) This is calculated by determining the length of time the area exposed to the hazard is occupied during a normal working period Avoidance (P) Possibility of avoiding the hazardous event if the protection system fails to operate.	F_A = Rare to more often exposure in the hazardous zone. Occupancy less than 0.1 F_B = Frequent to permanent exposure in the hazardous zone. P_A = Possible to avoid Should only be selected if all the following are true: Facilities are provided to alert the operator that the SIS has failed Independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to safe area The time between the operator being alerted and a hazardous event occurring exceeds 1 hour
	P_B = Not possible to avoid. Applies if any of P_A conditions are not met

ProSalus Limited Slide 7 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk graph: Semi Quantitative Parameters

Parameter	Range of Values
Demand rate (W). The number of times per year that the hazardous event would occur in the absence of the SIS under consideration	W_1 = Demand rate less than 0.1 demand per year W_2 = Demand rate between 0.1 demand and 1 demand per year W_3 = Demand rates higher than 1 demand and 10 demands per year

ProSalus Limited Slide 7 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Demand Rates (W)

Demand rates are generally determined by:

- Control system failure
- Equipment Failure such as pumps, valves, blockage etc
- Human error;
- During abnormal operating conditions e.g. start up;
- Environmental conditions;
- Utility failure e.g. electrical, instrument air, cooling water etc.

ProSalus Limited Slide 7 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Graph: Environmental Impact

ProSalus Limited Slide 7 - 13

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

General environmental consequences

ProSalus Limited Slide 7 - 14

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Asset Loss graph

- The severity of the consequence are calibrated:
  - In terms of Financial loss
  - The financial consequences must be calibrated in terms of what would occur if no SIS installed
  - Beware of over extending the financial loss as the leads to high SIL values were the SIS would have had no impact

ProSalus Limited Slide 7 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Graph: Asset Loss

ProSalus Limited Slide 7 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

General asset consequences (Not in IEC 61511)

ProSalus Limited Slide 7 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

A credit is an Order of Magnitude (SIL1)

- Don't take credit for the control system when it was the cause of the demand
- Don't take credit for the SIS which the SIF under assessment forms a part of
- Don't take a credit for frequency of occupancy when there is uncertainty in the location of operations / maintenance
- Don't take a credit for avoidance unless all of the criteria can be met
- A SIF can protect against more than one hazard, assess each hazard in turn and take the worse case SIL

ProSalus Limited Slide 7 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Target Integrity Level

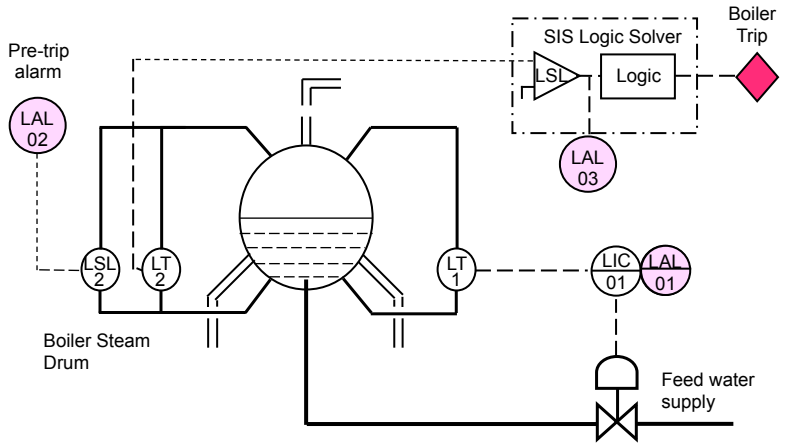
- The target integrity of a SIF is determined from the highest of the three assessment:
  - Safety
  - Environment
  - Asset
- Target Integrity level = maximum (SIL, EIL, AIL)
- The SIF must be designed to achieve the highest target Integrity Level

ProSalus Limited Slide 7 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Boiler Drum with pre-trip alarm and SIS trip Example



ProSalus Limited Slide 7 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Risk Parameters:

SIL Classification by Risk Parameters Chart

C – Extent of Damage

- C_A: Slight injury
- C_B: Severe irreversible injury to one or more persons or death of a person
- C_C: Death of several persons
- C_D: Catastrophic consequences multiple deaths

F – Frequency & Exposure time

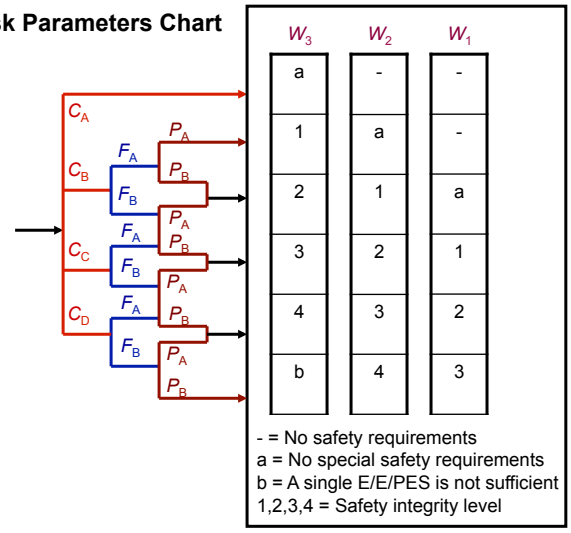
- F_A: Seldom to relatively frequent
- F_B: Frequent to continuous

P – Hazard Avoidance / Mitigation

- P_A: Possible under certain conditions
- P_B: Hardly possible

W – Occurrence Probability

- W_1: Very low
- W_2: Low
- W_3: Relatively high



ProSalus Limited

Slide 7 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIL Classification by Risk Parameters Chart: Example

Risk Parameters:

C – Extent of Damage

C – Extent of Damage

- C_A: Slight injury
- C_B: Severe irreversible injury to one or more persons or death of a person
- C_C: Death of several persons
- C_D: Catastrophic consequences multiple deaths

F – Frequency & Exposure time

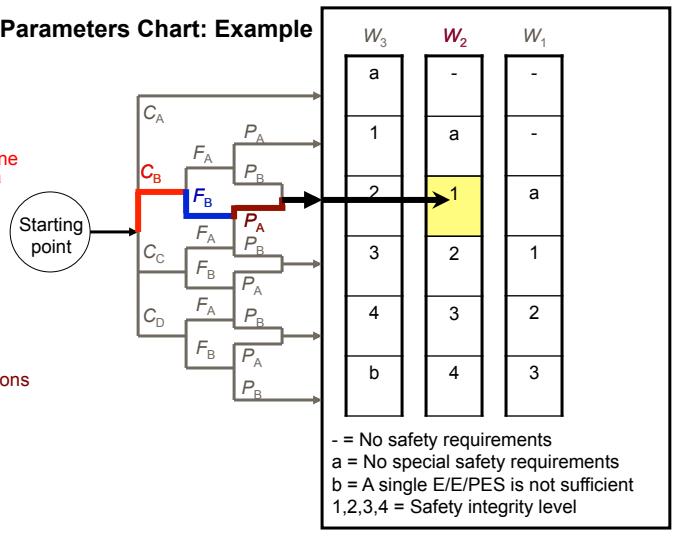
- F_A: Seldom to relatively frequent
- F_B: Frequent to continuous

P – Hazard Avoidance / Mitigation

- P_A: Possible under certain conditions
- P_B: Hardly possible

W – Occurrence Probability

- W_1: Very low
- W_2: Low
- W_3: Relatively high



ProSalus Limited

Slide 7 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Practical Exercise No: 3

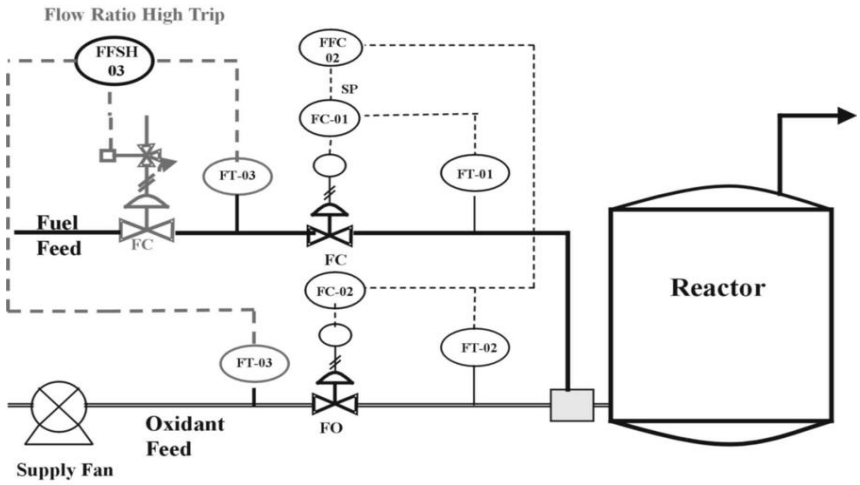
Determination of SIL by Risk Graph

ProSalus Limited

Slide 7 - 23

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 7 - 24

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Exercise No: 3 - Determination of SIL by Risk Graph

This practical exercise requires participants to determine the required SIL of a proposed safety-instrumented system using the basic principles and risk graphs and calibration parameters for safety, environment and asset loss described in this module

The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor. An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls Sudden loss of oxidant feed.

A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this function is FFSH- 03

ProSalus Limited Slide 7 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Assume that the following information has been decided for the reactor.

The total frequency of the events leading to an explosive mixture is approximately once every ten years.

The consequence of the explosion has been determined to be a vessel rupture causing death or serious injury to 1 person

The occupancy in the exposed area is less than 10% of the time and is not related to the condition of the process.

The onset of the event is likely to be to be fast with a worst-case time of 10 minutes between loss of oxidant and the possible explosion.

The material released from an explosion is not harmful to the environment.

The reactor will cost in excess of £250, 000 to replace.

Determine the target SIL = , EIL = , AIL =

Determine the overall target integrity for the SIF =

ProSalus Limited Slide 7 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ProSalus Limited

Slide 7 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Layers of Protection Analysis

(LOPA)

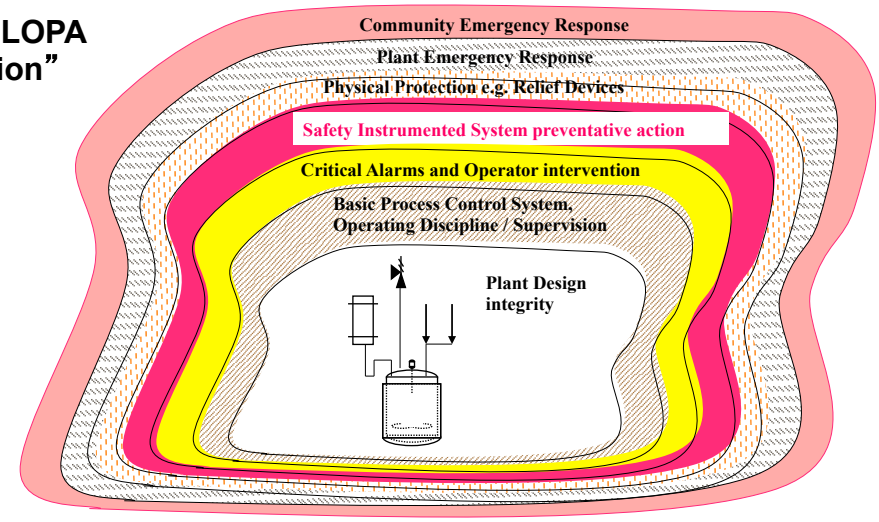
ProSalus Limited

Slide 7 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The LOPA "Onion"



ProSalus Limited Slide 7 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

- **What is LOPA**
  - Usually developed from HAZOP introduced in 2001 per IEC 61511
  - Assessment usually hazard scenario based (i.e derived from HAZOP)
  - It is a modified version of ETA usually based on the CCPS simplified process risk assessment approach and is considered a semi quantitative type analysis.
  - For "Buncefield Type" scenarios (Storage Tanks) are more Quantitive approach is required
  - For IEC 61511 analyses each hazard cause / consequence pair were a SIF has been identified as a safe guard during HAZOP
  - Can be applied to general PRA without SIF assessment
  - Requires Tolerability Risk Criteria to be established for site under assessment

ProSalus Limited Slide 7 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 - Mapping HAZOP Data to LOPA Data

ProSalus Limited Slide 7 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The LOPA Process:

1. Define the unwanted Impact
2. Determine and list all of the initiating events
3. Determine and list all of the layers of protection
4. Quantify the frequency of the initiating events
5. Quantify the effectiveness of the layers of protection
6. Calculate the resultant frequency of the unwanted impact

ProSalus Limited Slide 7 - 32

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

LOPA Worksheet

ProSalus Limited Slide 7 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

How LOPA works

		Example
	Risk Tolerance Criteria (freq.)	10^{-7}
→	Initiating Event Frequency	10^{-1}
→	Conditional Modifier (Ignition Frequency)	10^{-1}
→	PFD of 1st IPL (BPCS)	10^{-1}
→	PFD of 2nd IPL (Mechanical PRV)	10^{-2}
→	SIL (1-3) for SIS_1	$10^{-?}$

SIS Required. SIL = $10^{-7}/(10^{-1}*10^{-1}*10^{-1}*10^{-2}) = 10^{-2}$

ProSalus Limited Slide 7 - 34

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Part 3 Annex F.4 Severity Levels

Table F.2 Impact event severity levels

Severity Level	Consequence
Minor (M)	Impact initially limited to local area of event with potential for broader consequence, if corrective action not taken
Serious (S)	Impact event could cause serious injury or fatality on site or offsite
Extensive (E)	Impact event that is five or more severe times than a serious event

ProSalus Limited Slide 7 - 35

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Personnel Risk Tolerance Criteria

ProSalus Limited Slide 7 - 36

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Environmental Risk Tolerance Criteria

ProSalus Limited

Slide 7 - 37

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Commercial Risk Tolerance Criteria

ProSalus Limited

Slide 7 - 38

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Impact Event Description & Initiating Cause

- The HAZOP is reviewed to identify all cause / consequence pairs which have a SIF included in the safeguards for the hazard scenario
- The Impact event description is the HAZOP Consequence for the hazard scenario under review
- Initiating Cause description is the HAZOP Cause for the hazard scenario under review
- These two descriptions are entered into the LOPA record sheet

ProSalus Limited Slide 7 - 39

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 2 – Example Initiating events - (e.g. cause from HAZOP)

ProSalus Limited Slide 7 - 40

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Use Conditional Modifiers

- Use of conditional modifiers can be contentious they must be specific to the site under assessment and require to be determined by analysis. Typical conditional modifiers are:
  - Probability of ignition
  - Probability of exposure
  - Probability of Injury

ProSalus Limited Slide 7 - 41

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 4 Identification of IPLs

- Identify BPCS protective function, If any
- List any Alarms and the operator response (written procedure required)
- Record qualifying pressure relief devices
- Document Other Safety Related Systems
  - Management Practices
  - Human Actions
  - Machine Protection Systems

ProSalus Limited Slide 7 - 42

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

General Rule of Independence

To be Independent, a layer of protection shall prevent an unsafe scenario from progressing regardless of the initiating event or the performance of another layer of protection.

Given events A and B, A is independent of B if, and only if, the probability of A is unchanged by the occurrence of B.

Two events (A and B) are independent if the probability that they both occur is the product of their separate probabilities: P(A and B) = P(A) * P(B).

ProSalus Limited Slide 7 - 43

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ProSalus Limited Slide 7 - 44

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Basic Rules for BPCS and Alarms
If a BPCS (whole loop) is an IE, no credit is taken for the BPCS or Alarm IPL unless they are independent systems.
If BPCS and Alarm IPLs use the same sensor, you can take credit for one IPL only.
The Alarm IPL requires a formally recorded and auditable operator action to prevent the scenario.
If a sensor failure is the IE, BPCS and Alarm IPL are not valid credits if they require the failed sensor to function.
If a final element failure is the IE, BPCS and Operator action on Alarm IPL are not valid credits if they require the failed final element to function.
If a BPCS logic solver is an IE, no credit is taken for the BPCS or Alarm IPL, unless they are independent systems
If an Alarm is an IPL, the operator must have time to prevent the scenario. No credit shall be taken if the operator has less than 10 minutes to respond. May be able to take credit if this is a recognized case in the Emergency Response plan.
Maximum of only one (1) BPCS and one (1) Alarm IPL credit are allowed for a case.
Sharing of BPCS and SIS elements may be allowed when there is evidence of adequate independence. (see rules for sharing SIS elements by the BPCS)

ProSalus Limited Slide 7 - 45

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 5 - Mitigation

- Relief devices
- Flares
- Containment
- Other Safety Related Protection Systems

Then go on to consider Safety Instrumented Systems
if you still have protection gaps

ProSalus Limited Slide 7 - 46

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Rules for Pressure Relief Devices

1 The Pressure Relief Device either protects or it doesn't. Partial credit is not allowed.

2 If the Pressure Relief Device discharges to the atmosphere creating a 2nd hazard (to people, the environment or equipment), no credit is allowed. If the release to the atmosphere has an acceptable risk, credit may be taken

3 If the Pressure Relief Device discharges to a flare, tank, or scrubber, credit is taken

4 This is not a tool for deciding "No Overpressure Protection Device Needed".

ProSalus Limited Slide 7 - 47

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 6 address SIS Requirements

List Safety Instrumented Functions if required.

The SIL of the SIF is the numerical value needed to "Close the Gap".

ProSalus Limited Slide 7 - 48

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Basic Rules for SIS

1 SIS entries are considered last and then only if necessary to close the protection gap
2 A non-zero, positive value in the Protection Gap column indicates a SIS is needed.
3 The required SIL of the SIS is the value which closes the Protection Gap
4 A SIL value greater than 3 should not be allowed. Additional non-SIS IPL's are required. - or there is something wrong with the process
5 A zero or negative value in the Protection Gap column indicates a SIS is not needed.
6 A SIS with a SIL of 2 or 3 can be replaced with a combination of lower SIL provided they are independent from each other.

SIL 1 + SIL 1 = SIL 2 ; SIL 1 + SIL 2 = SIL 3

7 Two (2) SIS IPL's used in the same case require separate sensors, logic solver and final element. Independent paths through the same SIS logic solver must be used.

ProSalus Limited Slide 7 - 49

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 7

- Completely document scenario, Initiating event, IPLs. Justify and address Uncertainties and Sensitivities.
- Document the SIS requirements AND the requirements for the other Mitigation Systems

ProSalus Limited Slide 7 - 50

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example

Determination of SIL by LOPA

ProSalus Limited Slide 7 - 51

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example - Determination of SIL by LOPA

This practical exercise requires participants to determine the required SIL of a proposed safety-instrumented system using the basic principles and LOPA parameters described in this module

A Tank Overfill hazard has identified by the HAZOP team, two causes have been identified:

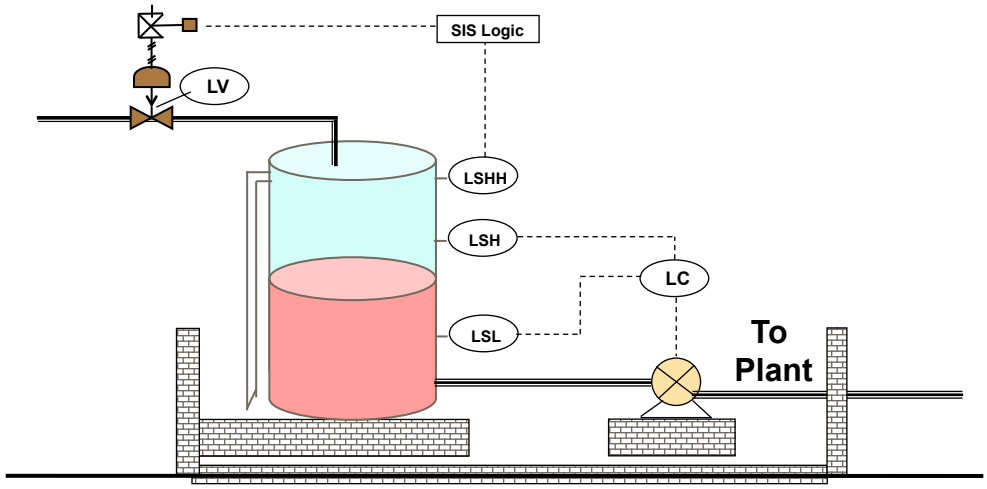
- Pump failure: 2.0 per year
- Level Control Failure: 0.1 per year

Determine the required target SIL for personnel safety of the High Level Shut Off to the tank if the tolerable risk for the hazard is 1.0E-05

ProSalus Limited Slide 7 - 52

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 7 - 53

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

LOPA Worksheet for Pump Scenario

ProSalus Limited

Slide 7 - 54

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

LOPA Worksheet for Level Control Scenario

ProSalus Limited

Slide 7 - 55

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Practical Exercise No: 4

Determination of SIL by LOPA

ProSalus Limited

Slide 7 - 56

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Exercise No: 4 - Determination of SIL by LOPA

This practical exercise requires participants to determine the required SIL of a proposed SIS using the basic principles and LOPA parameters described in this module

Liquid is transferred manually to a holding tank before delivery to the plant, the operator must stop the pump at 75% Tank Level.

A Tank Over pressurisation hazard has been identified by the HAZOP team, two causes have been identified:

- Operator fails to stop pump : 0.1 per year
- Level Control Failure: 0.1 per year

Determine the required target SIL for personnel safety of the High Pressure Vent SIF to Flare

ProSalus Limited Slide 7 - 57

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Exercise No: 4 - Determination of SIL by LOPA

The tolerable risk for the hazard is 1.0E-05

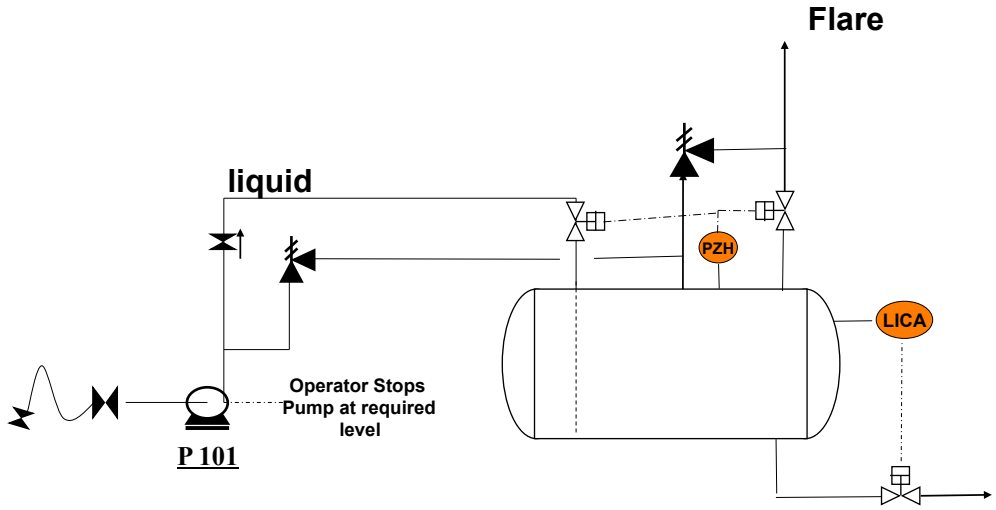
The Holding tank has a relief valve installed which is sized for full flow and vented to Flare

The process design is not considered to be fit for purpose

ProSalus Limited Slide 7 - 58

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 7 - 59

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

LOPA Worksheet

ProSalus Limited

Slide 7 - 60

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIL Determination

For

Fire and Gas Systems

ISA-TR84.00.07

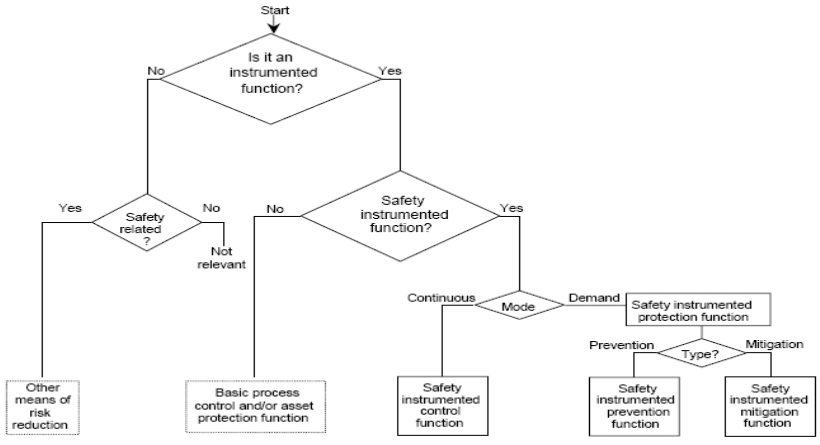
ProSalus Limited

Slide 7 - 61

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Relationship Between Protection Functions



ProSalus Limited

Slide 7 - 62

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIPF verses SIMF

- FGS detect loss of containment by directly measuring the presence of the released material (gas concentration) or effects of their release (thermal radiation) to initiate mitigative actions such as:
  - Plant evacuation alarm
  - Deluge systems
  - Fire water or spray systems
  - Water curtains
- Instrument functions detect changes in process conditions without a LOC and take preventative actions to eliminate the consequence from occurring
- IEC 61511 is based on the concept that the SIF eliminates the consequence and this is why the use of performance based design methodologies for SIMF are not currently the norm in the process industries

ProSalus Limited Slide 7 - 63

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Assessing Fire and Gas Systems (FGS)

- FGS design can be implemented using a
  - Prescriptive approach using national consensus standards, codes, and / or industry guidelines. (NFPA 72)
  - Risk-based approach, including the concept of designing to a targeted performance level, with an associated integrity and an acceptably-low probability of failure on demand

.

- However, it is difficult to apply the IEC 61511 lifecycle approach in practice due to the following three factors.

ProSalus Limited Slide 7 - 64

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Factors affecting FGS Assessment

- Factor 1 - IEC 61511 techniques are suited for specific hazards that can be adequately defined using HAZOP and LOPA as an input to the risk assessment process. FGS reduce the risk of general hazards (e.g., leaks from a variety of equipment), and these hazards are difficult to define and analyze with precision without using more-advanced risk analysis techniques, such as gas dispersion modeling or fire modeling

- Factor 2 - FGS do not prevent a hazardous condition, but – rather – they mitigate the effects of the hazard. The FGS system typically reduces the magnitude and severity of a hazard instead of completely eliminating it which is a requirement of IEC61511

ProSalus Limited Slide 7 - 65

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Factors affecting FGS Assessment

Factor 3 - In addition to failure of components that could render the system unavailable, a significant cause of FGS ineffectiveness is due to inadequate positioning of FGS sensors to detect the hazardous condition. Even if very high SIL targets can be achieved in FGS design and testing (in terms of low average probability of failure on demand of the instrumented function), sufficient reduction in risk will not occur unless detector placement and coverage is very high.

Therefore, the detector placement and coverage problem requires study with the same quantitative rigor as average probability of failure on demand.

ProSalus Limited Slide 7 - 66

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Factors affecting FGS Assessment - Final Elements

Another significant cause of FGS ineffectiveness is due to the incapability of the mitigation final elements (e.g. fire water system, foam deluge, water curtain, ventilation system) to perform their function with a high probability of success.

Effectiveness of the mitigation function is dependent on:

- stopping the process and removing the hazardous material
- applying fire water with the appropriate flow and spray characteristics
- Initiating alarms to enable personnel to get to safety

ProSalus Limited Slide 7 - 67

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ISA-dTR84.00.07 Performance-based FGS Analysis Procedure

1
2
3
4
5
6
7
8
9

ProSalus Limited Slide 7 - 68

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

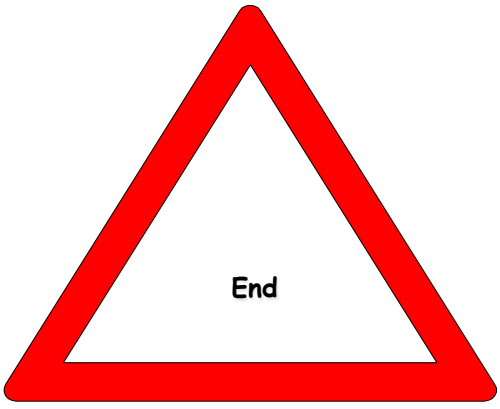
Conclusions on FGS Assessment

- FGS assessment requires advanced techniques for analysis not normally considered part of the C&I Function more related to Process Safety / Technical Safety Function and covered by the QRA
- Significant cause of FGS ineffectiveness is inadequate positioning of detectors and final elements and only calculating the PFD of the system components is not rigorous enough
- RRF only achieved if detector placement & coverage is high
- RRF is also dependent of capability of Final Element (Fire water etc)
- SIL is insufficient to properly define the design basis for FGS SIF
- Design basis based on performance criteria –
  - Percentage Detector Coverage
  - Percentage Mitigation Effectiveness
- Remember relevant standards must be applied (e. g. EN 54 / NFPA 72)

ProSalus Limited Slide 7 - 69

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited Slide 7 - 70

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Operations and Maintenance

of

Safety Instrumentation Systems

ProSalus Limited

Slide 8 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Using the Safety Instrumented System

- Installation and commission – IEC 61511 Clause 14
- Validation – IEC 61511 Clause 15
- Operation & Maintenance – IEC 61511 Clause 16
- Modifications – IEC 61511 Clause 17

ProSalus Limited

Slide 8 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Safety life-cycle goals (Clause 6.2.3)

1. ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both function and safety integrity requirements;
2. ensure proper installation and commissioning of the safety instrumented system;
3. ensure the safety integrity of the safety instrumented functions after installation;
4. maintain the safety integrity during operation (for example, proof testing, failure analysis);
5. manage the process hazards during maintenance activities on the safety instrumented system.

ProSalus Limited Slide 8 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Installation and Commissioning

- **Installation and commissioning must be**
  - **Carried out according to plan**
  - **Documented Evidence of**
    - **Installation and commissioning activities**
    - **Failure resolution**
    - **Retest**

ProSalus Limited Slide 8 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Installation and Commissioning

- **System / Equipment Suppliers**
  - Supply documentation as per 61508 / 61511 requirements to ensure SIS is installed and commissioned correctly
- **Operators**
  - Follow Installation and Commissioning Plan
  - Tested in accordance with Commissioning Procedure
  - Safety Manual requirements included in O&M Procedures

ProSalus Limited Slide 8 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Validation Plan

- **Operator Requirement to assure**
  - **Integrity requirement achieved**
  - **Functional requirements achieved**
  - **Basis of validation is the safety requirements specification**

ProSalus Limited Slide 8 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Validation Report

- **Documented Evidence of:**
  - **Validation activities completed**
  - **All Safety Instrumented Functions validated**
  - **Tools used during validation**
  - **Results of the validation**
  - **Any discrepancies**
    - **SIS Fit for Purpose**

ProSalus Limited Slide 8 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The SIS Validation activities must include as a minimum the following:

- SIS performs in all operating modes as identified in the SRS;
- Confirmation that adverse interaction of the BPCS and other connected systems do not affect the proper operation of the SIS;
- SIS properly communicates (where required) with the BPCS or any other system or network;
- Sensors, logic solver, and final elements perform in accordance with the SRS;
- SIS documentation is consistent with the installed system;
- Confirmation that the SIF performs as specified on invalid process variable values;
- The proper shutdown sequence is activated;
- The SIS provides the proper annunciation and proper operation display;

ProSalus Limited Slide 8 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The SIS Validation activities - continued:

- The SIS reset functions perform as defined in the SRS;
- Bypass functions operate correctly;
- Start-up overrides operate correctly;
- Manual shutdown systems operate correctly;
- The proof-test intervals are documented in the maintenance procedures;
- Diagnostic alarm functions perform as required;
- Confirmation that the SIS performs as required on loss of utilities (for example, electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the SIS returns to the desired state;
- Confirmation that the EMC immunity, as specified in the SRS, has been achieved.

ProSalus Limited Slide 8 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Operation and Maintenance

- Key to maintaining the SIL over plant life time
- O&M procedures must include Safety Manual requirements
- Estimated repair times included in SIL verification
- Proof Test Intervals included in SIL verification
- Critical to plant safety that these are completed to schedule

ProSalus Limited Slide 8 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Operator Requirements

- Procedures in place for
  - SIF Maintenance
  - Repair activities
  - Change control / modifications
  - Functional Safety Assessment
- Periodic Functional safety audits

ProSalus Limited

Slide 8 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Modification Documentation

- Documentation includes
  - The modification or retrofit request
  - The impact analysis
  - Re-verification and re-validation of data and results
  - All documents affected by the modification and retrofit activity

ProSalus Limited

Slide 8 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Impact Analysis

- An impact analysis includes
  - An assessment on what impact the change has
  - Hazard and risk analysis to applicable phases of the lifecycle
  - Guarantee of functional safety at all times
  - Result of the impact analysis determines whether the modification will be authorized

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Override Procedures

- Maintenance overrides are not problem as long as you guarantee the safety function
- Things to think about
  - Is there a procedure?
  - Are people informed?
  - Is the override time limited?
  - Do you lock out/tag out the area?

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Why do proof testing?

Keeps the PFD within the design targets

OHSA requirements in USA

IEC 61508 and 61511 compliance

PFDavg increases with test interval …so without testing the PFDavg rises above limits and SIL falls to ZERO.

ProSalus Limited

Slide 8 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Proof testing: Key points

- Use a documented procedure
- Test entire SIF
- Test intervals based on the Safety Requirements Specification
- Review the test interval after operational experience
- Full testing after any changes
- Description of all tests performed
- keep records to certify the tests and inspections have been performed.

ProSalus Limited

Slide 8 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Valve on-line testing methods

- Problem is to test the ability of the valve to close off flow or release pressure as per function
- The need for final process test may be reduced if duty levels are not severe.
- The testing of solenoid and ability to move the valve covers a large portion of potential faults.
- Partial closure testing (Tia = PTI/10) and physical inspections at higher frequencies , leaving full closure tests to once per year or greater.
- Define the testing facilities needed during the design stage.

ProSalus Limited

Slide 8 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Inspection Programme guidance from IEC 61511 Part 2

16.3.2 Inspection

As stated in IEC 61511-1, inspecting the SIS is different from proof testing. Whereas a proof test is ensuring the SIS will operate properly, a visual inspection is required to validate the mechanical integrity of the installation.

Normally, the inspection is done at the same time as the proof test but it may be done at a more frequent interval if desired..

ProSalus Limited

Slide 8 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Maintenance Management Programme (IEC 61508)

Some useful guidelines in these standards on how maintenance response and reporting activities can assist in building an accurate record of SIS reliability.

From Phase 14 of the safety life cycle model in IEC 61508-1 see next 3 diagrams, based on fig 7, 8 and 9

These procedures lead to analysis of performance problems and may lead to modifications. Management of change M.O C. procedures then apply…see following slides

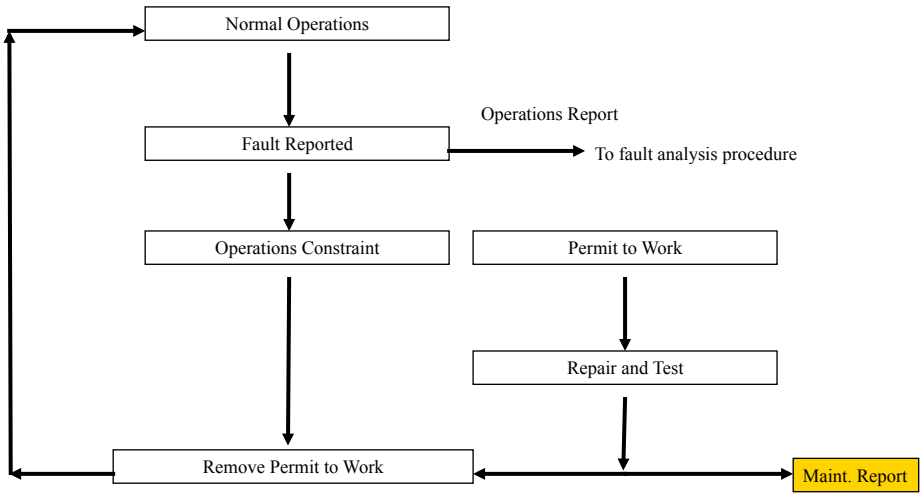
ProSalus Limited

Slide 8 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Revealed faults procedure: response to reported fault.



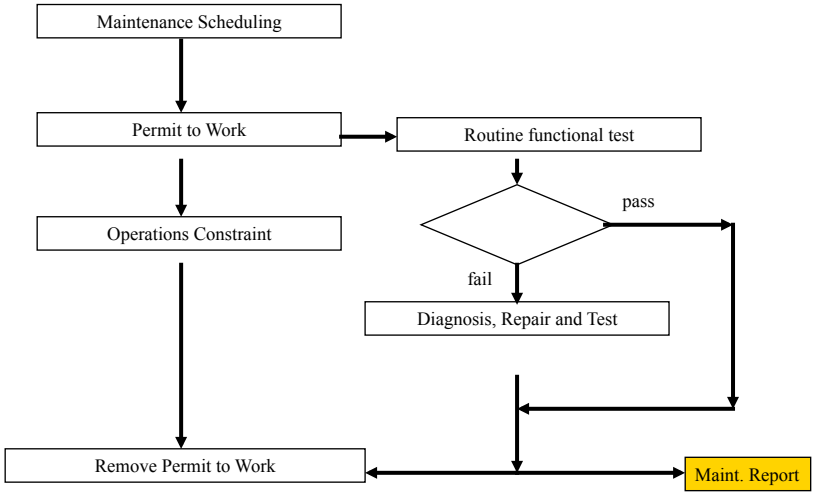
ProSalus Limited

Slide 8 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Unrevealed faults procedure: Proof testing



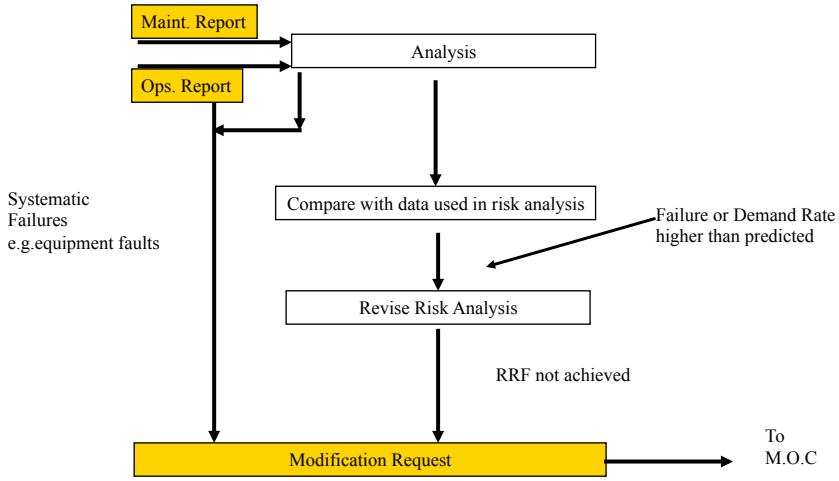
ProSalus Limited

Slide 8 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Evaluation of maintenance and proof testing reports



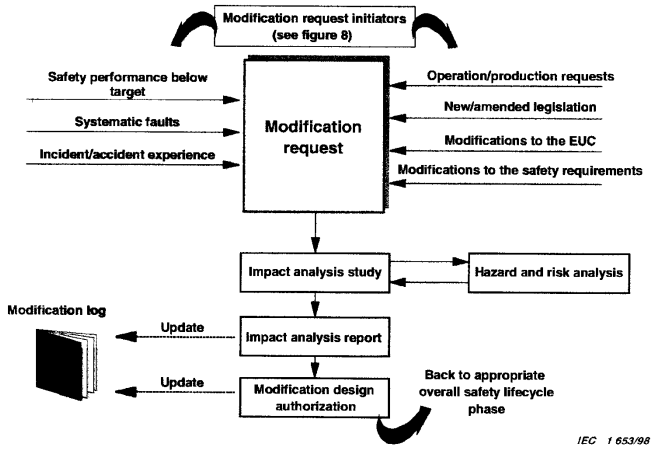
ProSalus Limited

Slide 8 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Modification Procedure Model



ProSalus Limited

Slide 8 - 23

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Summary

- Management of Change critical to Process Safety
- MOC and Maintenance is a Key Performance Indicator
- Proof Test Integral to maintaining SIL Capability

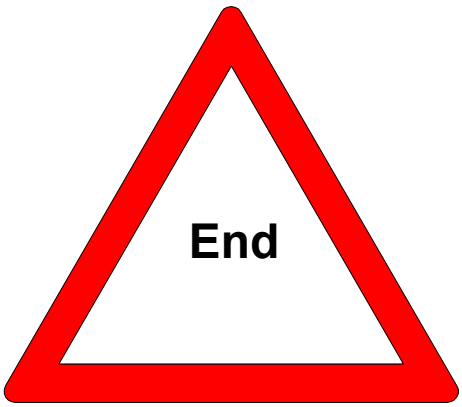
Thanks for your attendance and any Questions

ProSalus Limited

Slide 8 - 24

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 8 - 25

FUNCTIONAL SAFETY ENGINEER
CERTIFICATION COURSE
Exercise Solutions

The following slides are arranged by practical number and consist of question items followed by answer items.

Practical exercise no: 1

Fault trees

This practical exercise requires attendees to construct a fault tree diagram using the basic principles introduced in module 3.

It uses an example of a simple reactor with automatically controlled feeds that has the potential to cause a serious risk to plant personnel. Once the basic fault tree has been drawn, the model is to be adjusted to incorporate a safety-instrumented system and to demonstrate the resulting risk reduction.

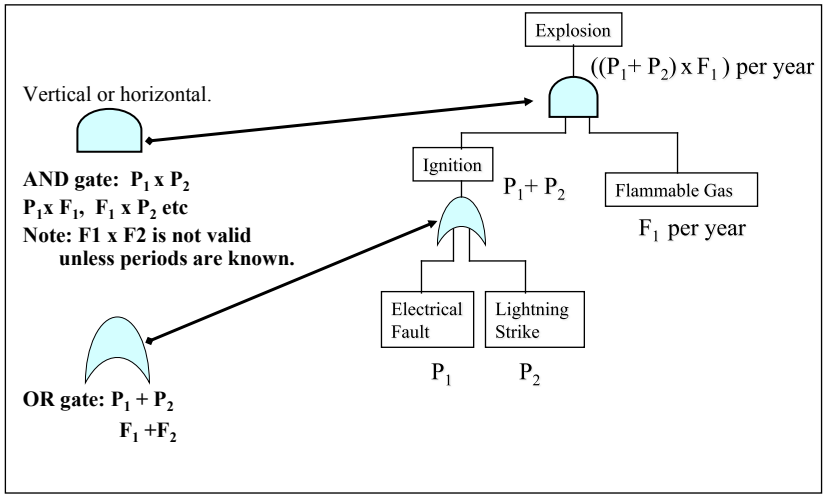
The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor.

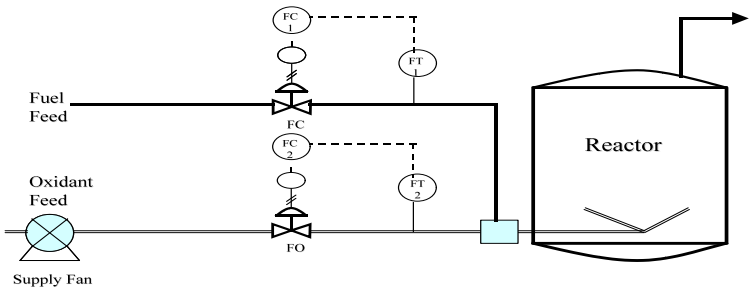
An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

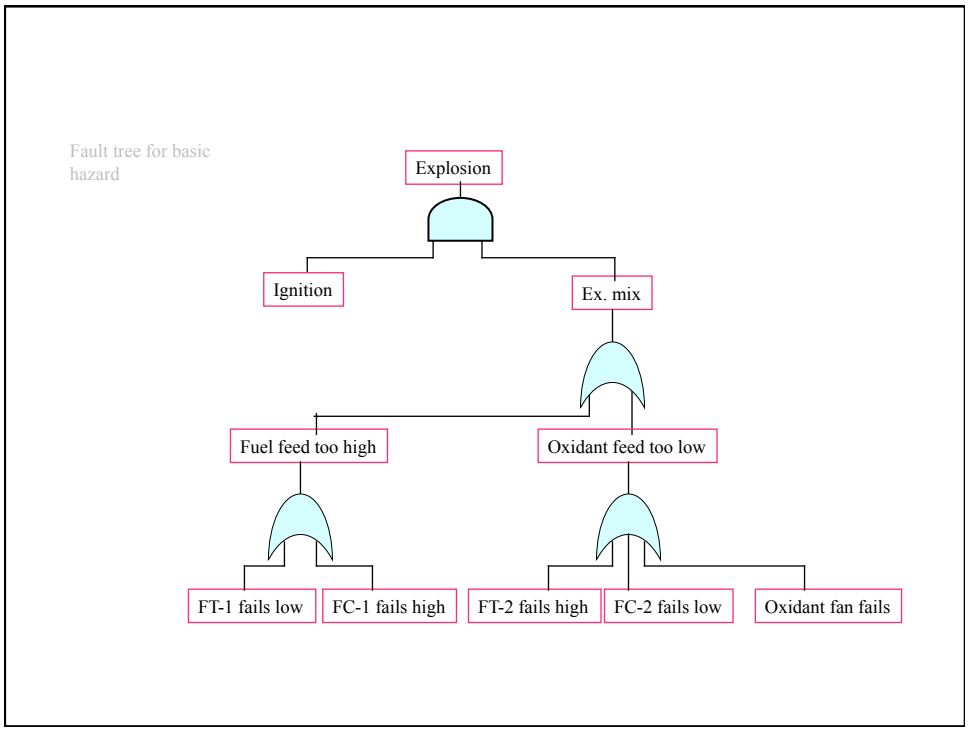
Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls leading to sudden loss of oxidant feed.

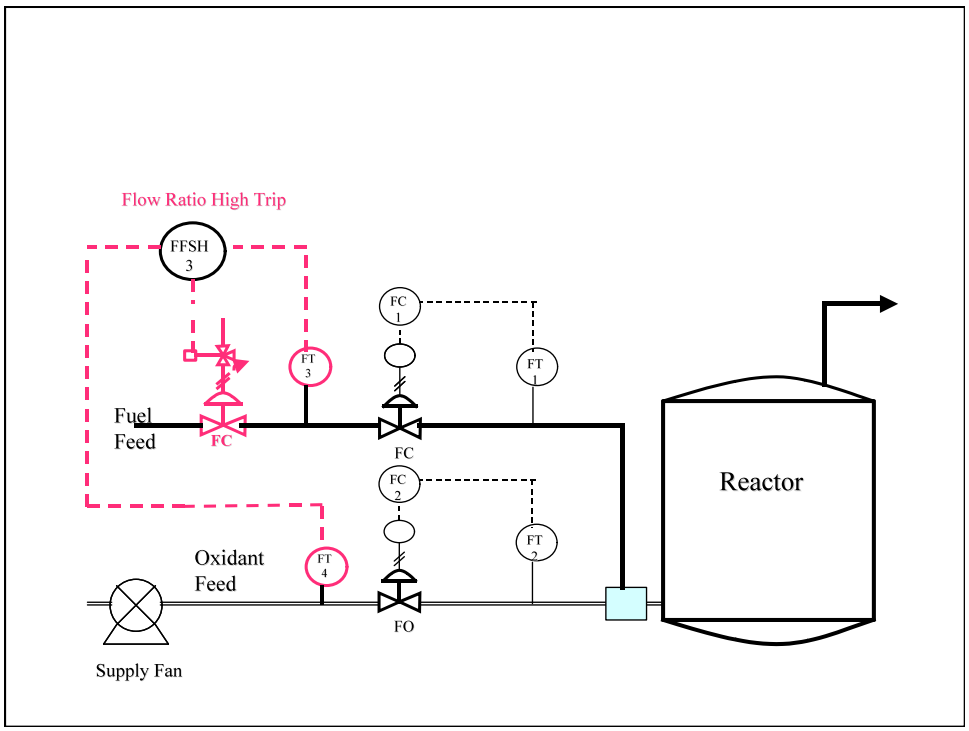
A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this SIF is FFSH- 03

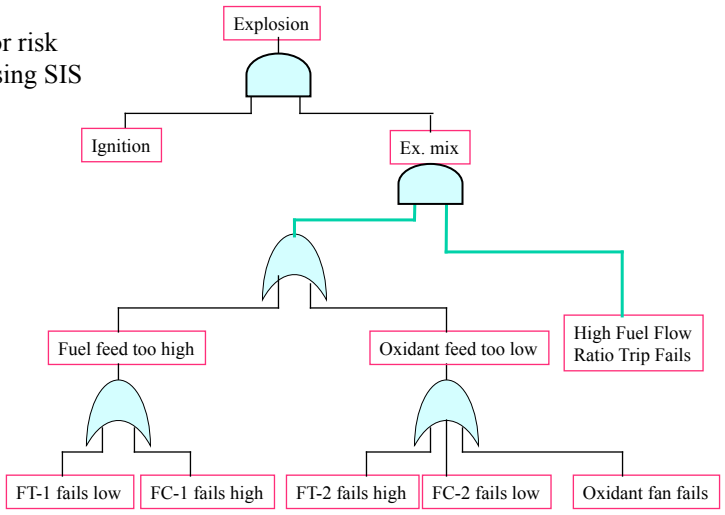








Fault tree for risk reduction using SIS



Exercise No: 2 – SIL Verification

Task 1 Calculate the single channel PFDavg and spurious trip rate for the high temperature trip example. Draw a single channel reliability block diagram and calculate using the failure rates in the table the PFDavg and the spurious trip rate for each sub system and the overall system using a proof testing interval of 6 months.

Assume the system uses 2 relays, 1 relay in the sensor subsystem and 1 relay in the logic solver subsystem, The trip actuation uses a solenoid valve and to vent the air cylinder on a valve that will drive open and release quench water into the reactor.

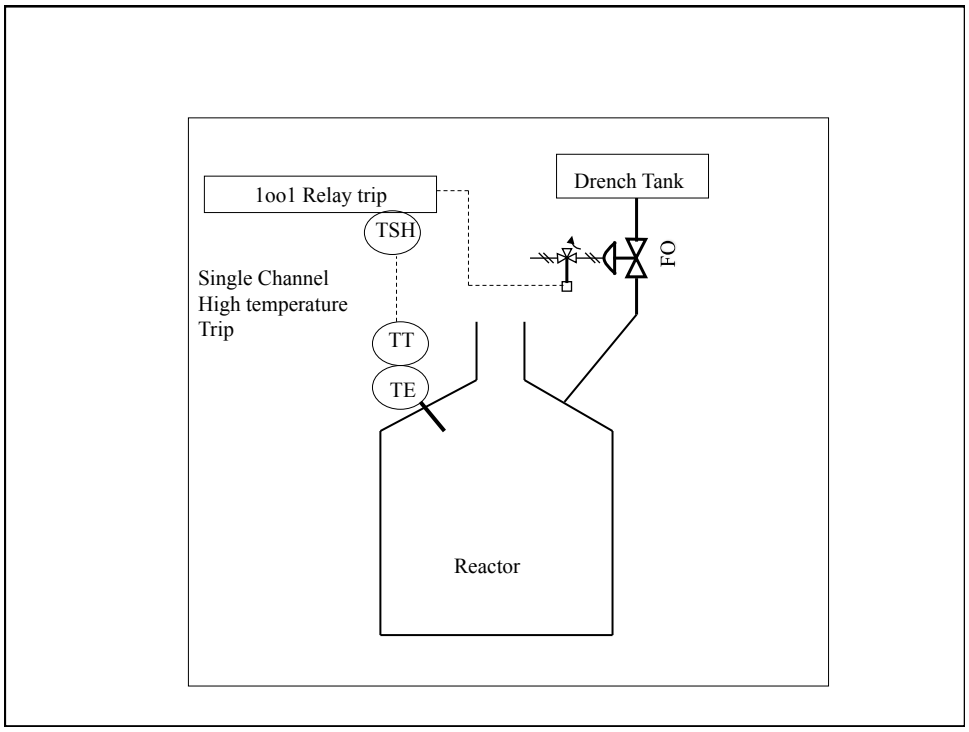
Task 2: Recalculate the PFDavg and spurious trip rate for the SIF using the second diagram showing 3 high temperature transmitters on a reactor configured 2oo3 on the basis of proof testing every 6 months, Beta Factor 10% and MTTR of 24 hours.

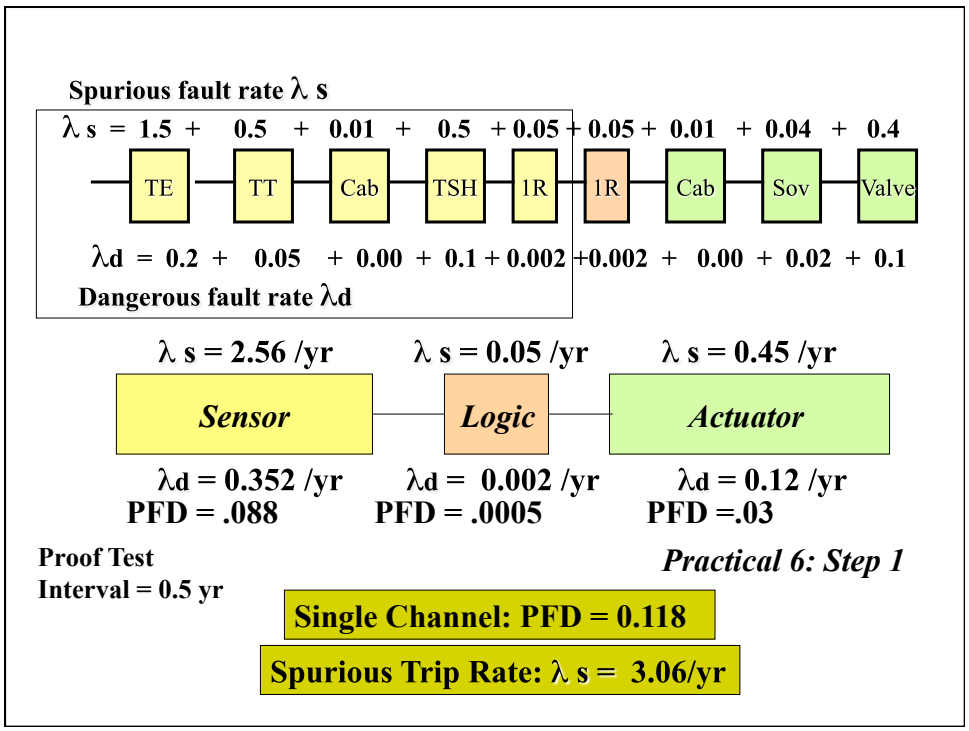
The 3 temperature transmitters each transmit to a trip amplifier device that acts as a high temperature trip device leading to a single channel actuation as in task 1

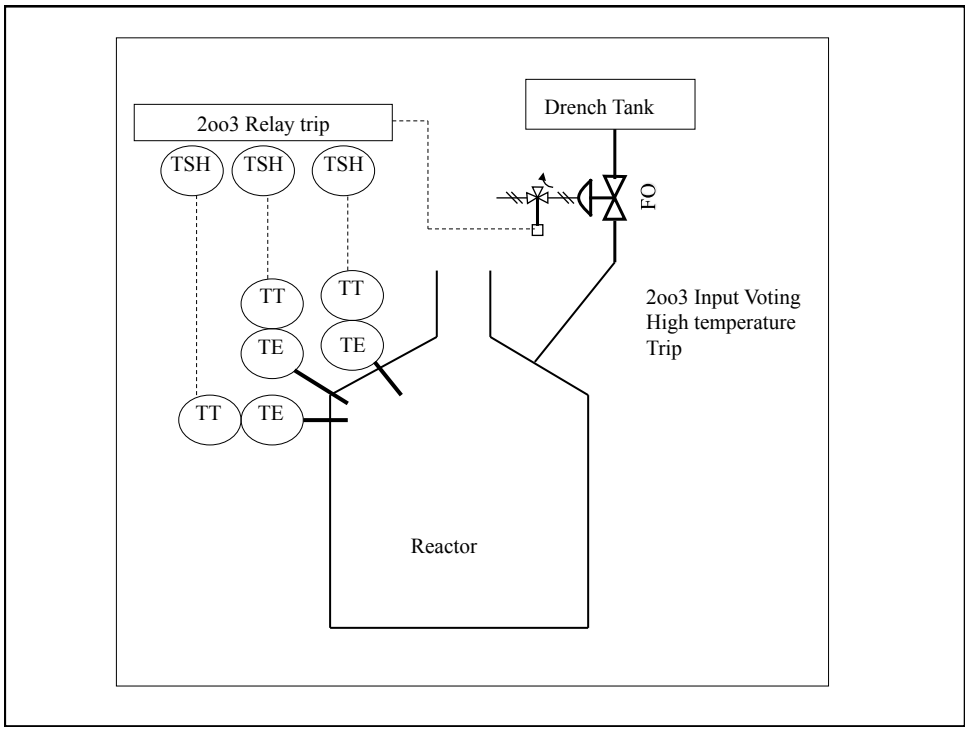
Table of fault rates for the Devices

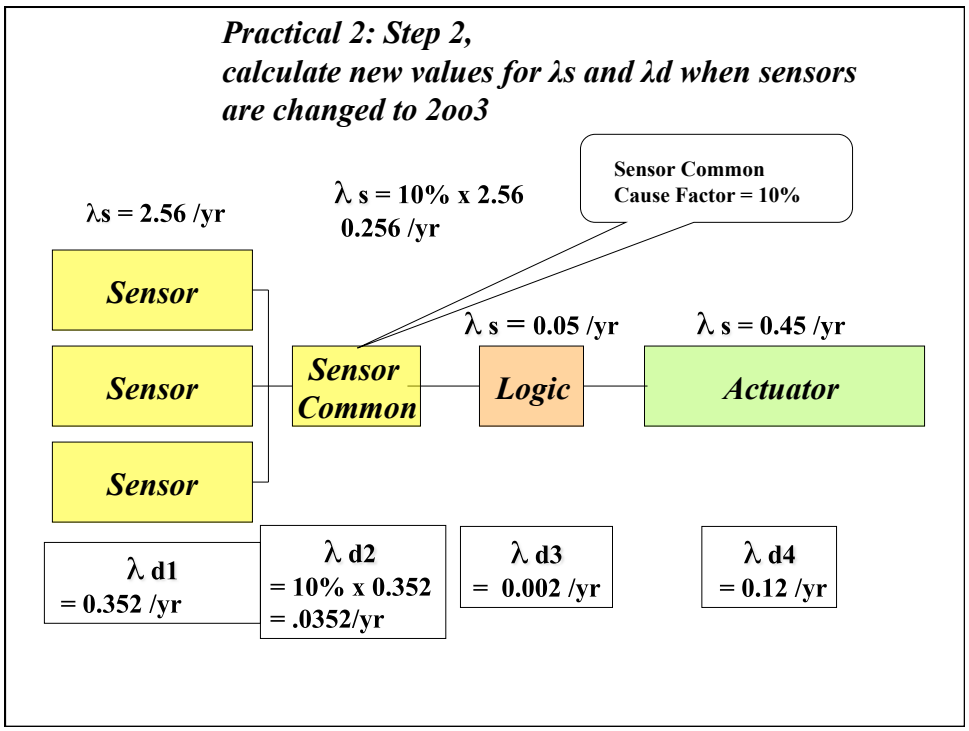
Channel Device	Fail-safe rate per year	Fail –danger rate per year
TE…element	1.5	0.20
TT .Transmitter	0.5	0.05
Cable/terminals	0.01	0.00
TSH….trip amplifier/switch	0.5	0.1
Relay (each)	0.05	0.002
Solenoid Valve	0.04	0.02
Trip Valve	0.4	0.1

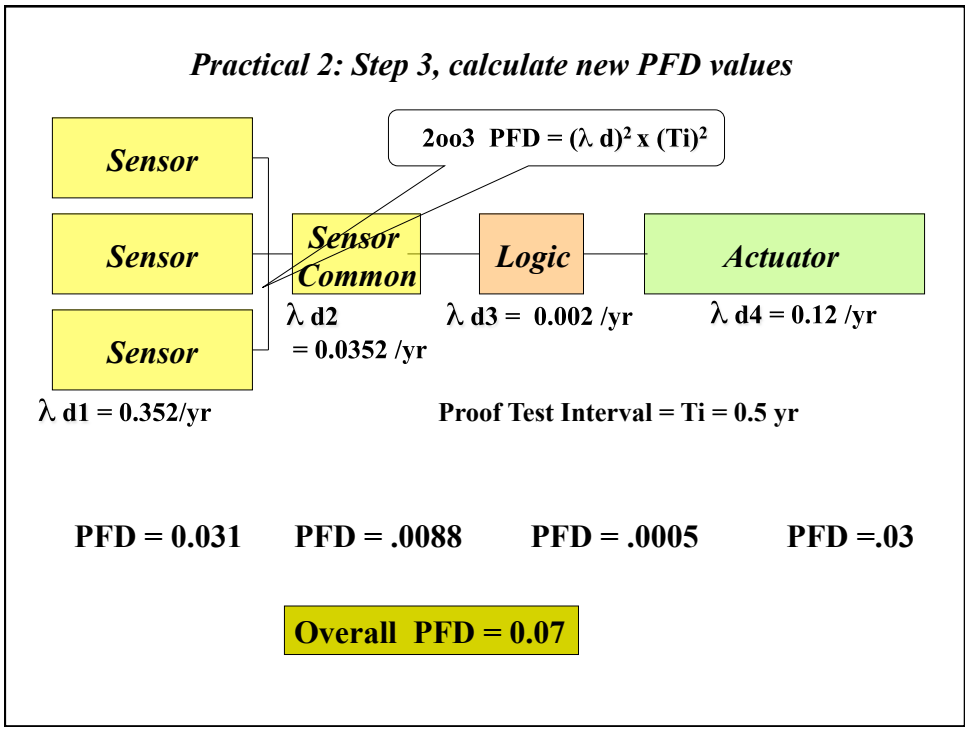
3/4/11

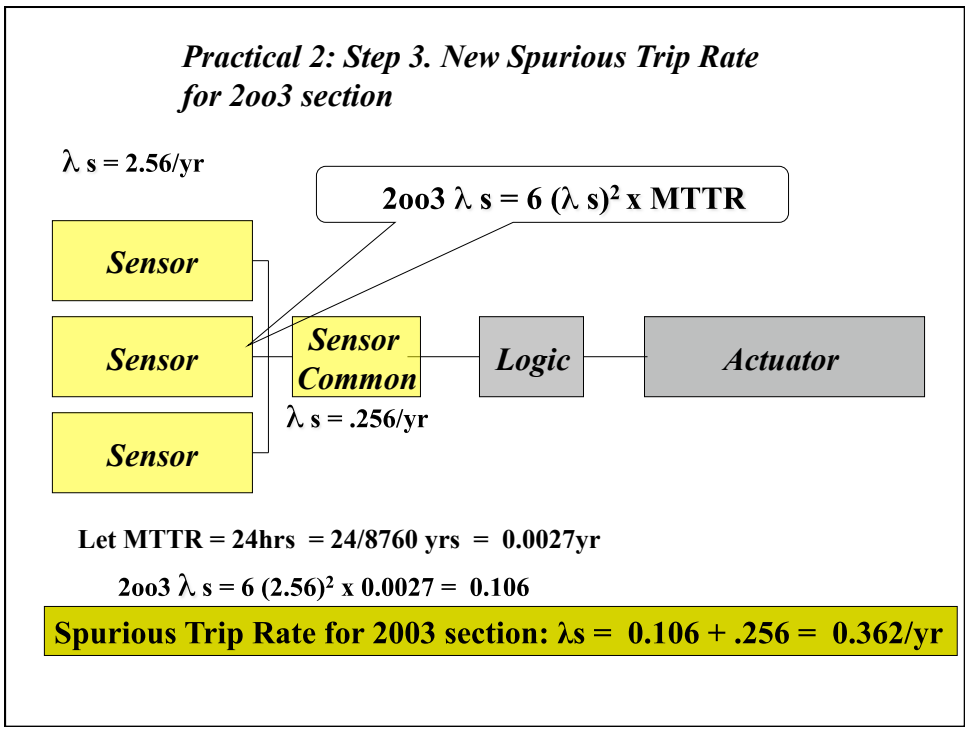


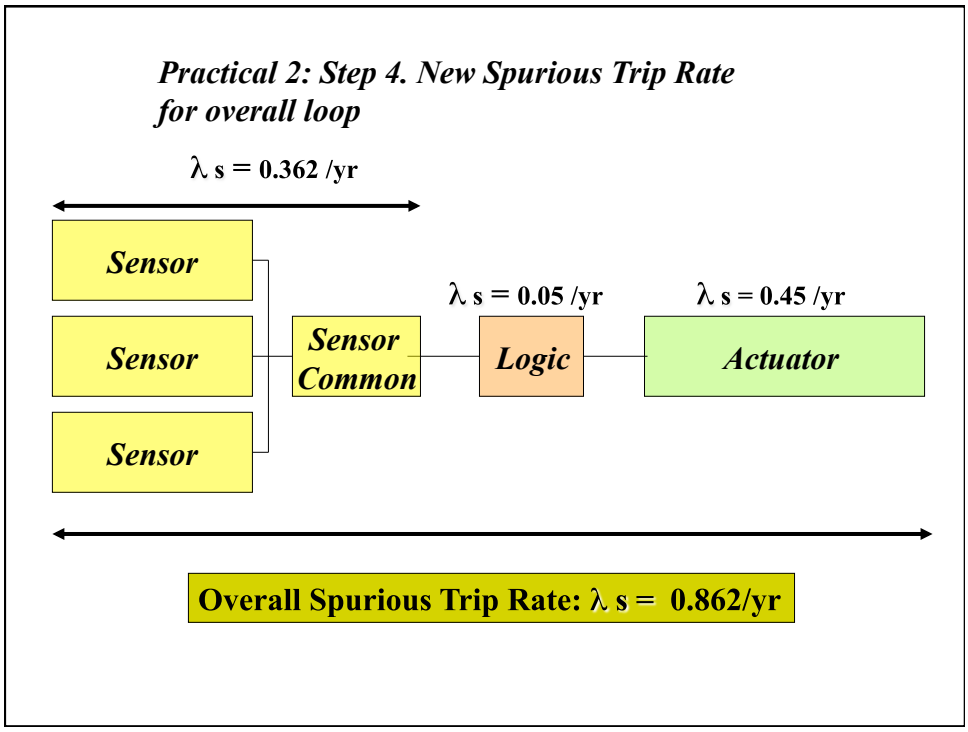


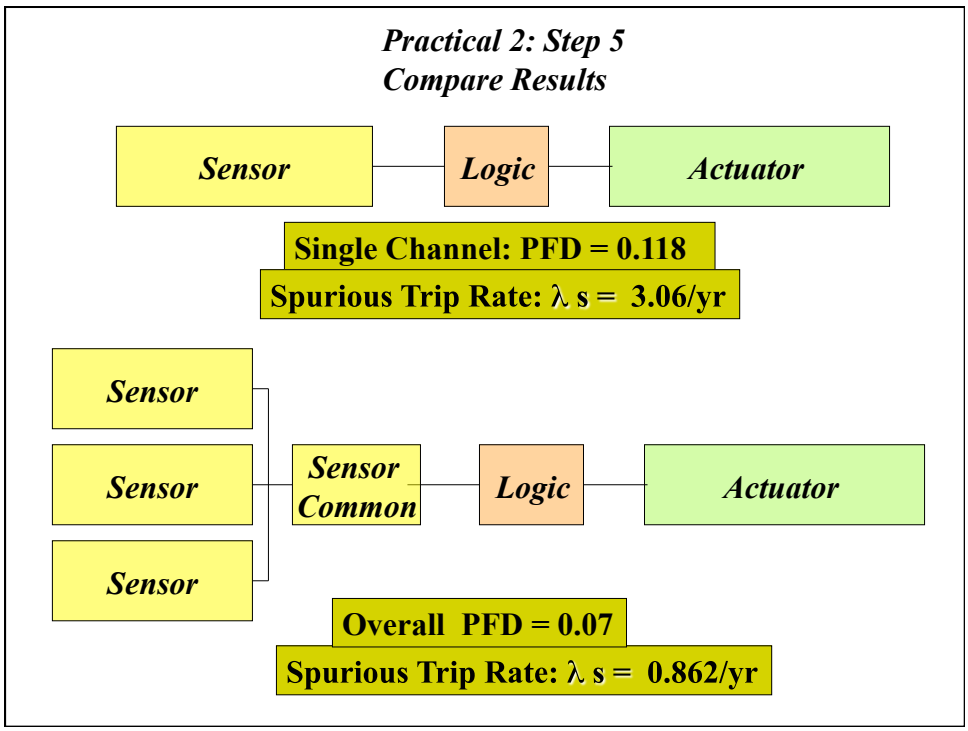












Exercise No: 3 - Determination of SIL by Risk Graph

This practical exercise requires participants to determine the required SIL of a proposed safety-instrumented system using the basic principles and risk graphs and calibration parameters for safety, environment and asset loss described in this module

The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor. An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls leading to sudden loss of oxidant feed.

A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this function is FFSH- 03

Assume that the following information has been decided for the reactor.

The total frequency of the events leading to an explosive mixture is approximately once every ten years.

The consequence of the explosion has been determined to be a vessel rupture causing death or serious injury to 1 person

The occupancy in the exposed area is less than 10% of the time and is not related to the condition of the process.

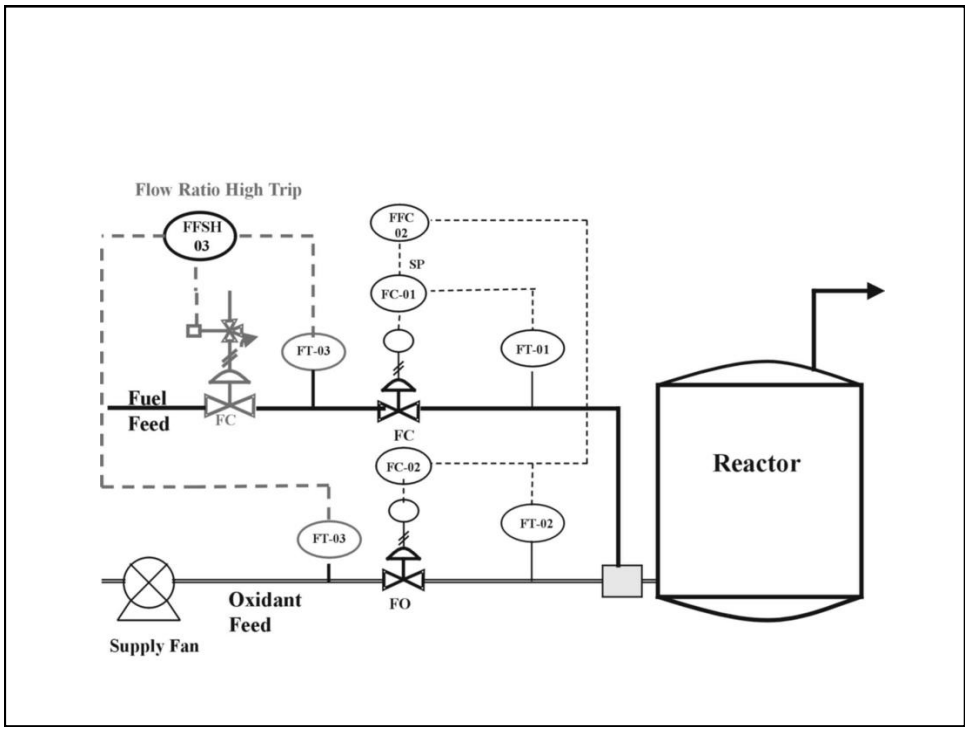
The onset of the event is likely to be to be fast with a worst-case time of 10 minutes between loss of oxidant and the possible explosion.

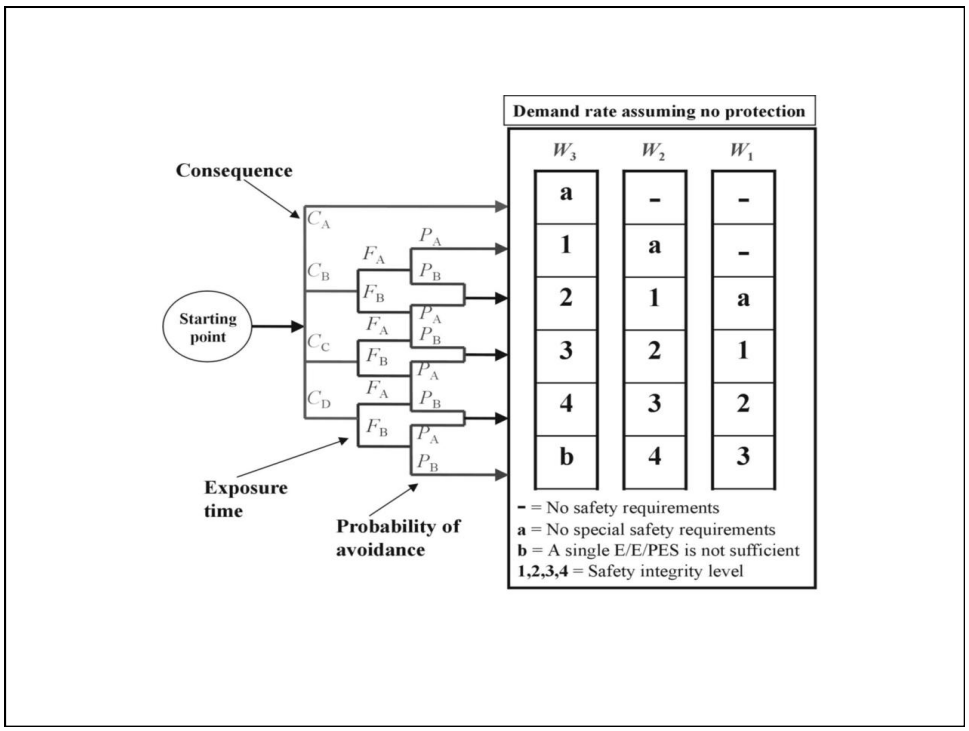
The material released from an explosion is not harmful to the environment.

The reactor will cost in excess of £250, 000 to replace.

Determine the target SIL, EIL and AIL

Determine the overall target integrity for the SIF





IEC 61511 Risk parameters chart (part 3 Annex D)

EIL = a / AIL = a

Risk Parameters:

***C* – Consequence**

C_A:
C_B:

C_C: the chance of death is 1 per event (Range >0.1 to 1.0) = Cc
C_D:

***F* –Occupancy**

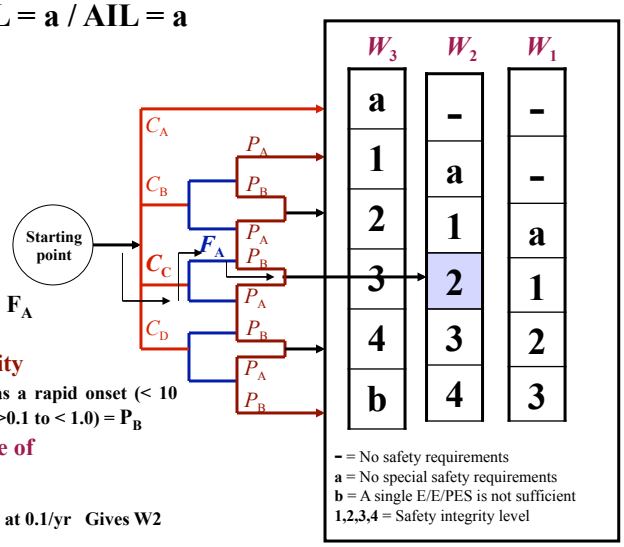
F_A: occupancy is less than 0.1 = F_A
F_B:

***P* – Hazard avoidance probability**

P_A: the explosion has a rapid onset (< 10 minutes) (Range >0.1 to < 1.0) = P_B
P_B:

***W* – Demand rate in the absence of the SIF under consideration**

W_1:
W_2: demand rate is estimated at 0.1/yr Gives W2
W_3:



Exercise No: 4 - Determination of SIL by LOPA

This practical exercise requires participants to determine the required SIL of a proposed SIS using the basic principles and LOPA parameters described in this module

Liquid is transferred manually to a holding tank before delivery to the plant, the operator must stop the pump at 75% Tank Level.

A Tank Over pressurisation hazard has been identified by the HAZOP team, two causes have been identified:

- Operator fails to stop pump : 0.1 per year
- Level Control Failure: 0.1 per year

Determine the required target SIL for personnel safety of the High Pressure Vent SIF to Flare

ProSalus Limited

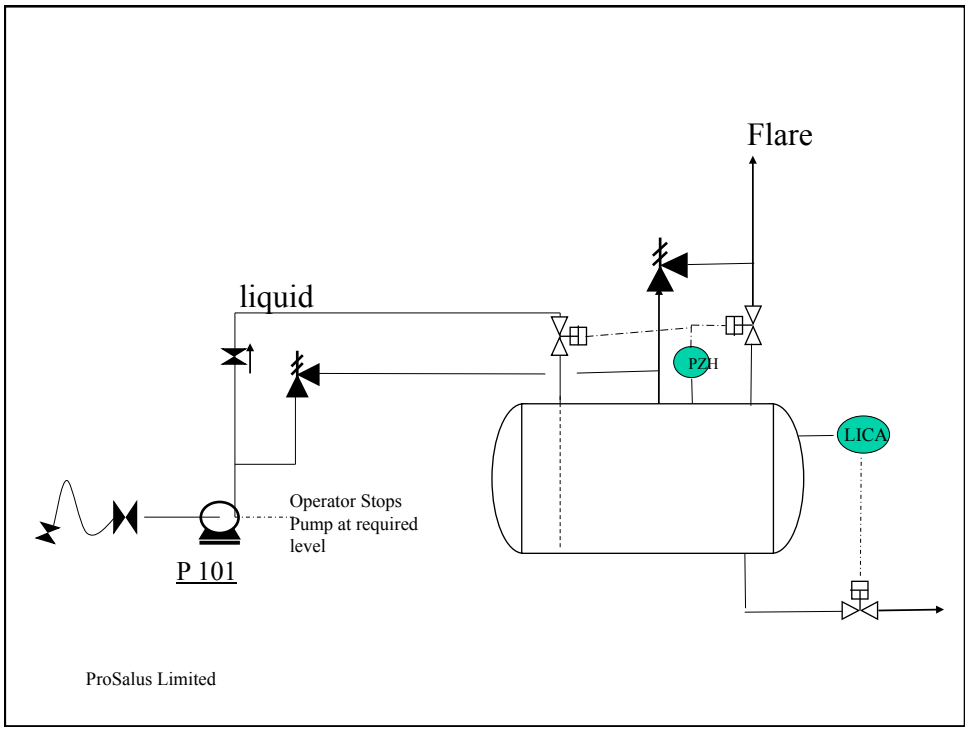
Exercise No: 4 - Determination of SIL by LOPA

The tolerable risk for the hazard is 1.0E-05

The Holding tank has a relief valve installed which is sized for full flow and vented to Flare

The process design is not considered to be fit for purpose

ProSalus Limited



LOPA Worksheet