Safety Instrumented Systems – Overview and Awareness

Workbook and Study Guide

V 1.0

Copyright Notice and Disclaimer

3366 Riverside Drive
Columbus, OH 43221
e-mail: info@kenexis.com
http://www.kenexis.com
Phone: +1 (614) 451-7031

In preparing this work Kenexis Consulting Corporation did not research or consider patents which may apply to the subject matter contained in this book. It is the responsibility of the readers and users of the material in this book to protect themselves against liability for the infringement of patents. The information and recommendations contained in this book are not intended for any specific application, or applications, and are of a general informative nature. As a result, Kenexis Consulting Corporation assumes no liability of any kind, however arising, as a result of using the information contained in this book. Any equipment that might be referenced in this work gas been selected by the authors as examples of technology. Kenexis makes no endorsement of any product, either expressed or implied. In all instances, an equipment manufacturer's guidance and procedures should prevail regarding the use of specific equipment. No representation, either expressed or implied, is made with respect to the availability of any equipment, process, formula, or other procedures contained in this book.

Introduction

This workbook and study guide is an integral part of the Safety Instrumented Systems – Overview and Awareness training module. The Safety Instrumented Systems – Overview and Awareness training modules provides a high-level discussion of what safety instrumented systems are and how they are employed in the process industries to reduce risk. The training course presents a discussion of what safety instrumented systems are and how they are different from basic process controls systems, provides an overview of why safety instrumented systems are employed – including a discussion of the associated legal and regulatory environment, and the presents the lifecycle for implementation of safety instrumented systems as presented in the IEC 61511 standard.

About Kenexis

Kenexis is an independent engineering consulting firm. We ensure the integrity of instrumented safeguards and industrial networks. Using skills in risk analysis, reliability engineering, and process engineering, we help establish the design and maintenance specification of instrumented safeguards, such as safety instrumented systems (SIS), alarm systems, fire and gas systems. We use the same skills for industrial control systems (ICS) network design, cyber security assessments, and industrial network performance analysis.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Section 0 – Scope and Roadmap

Safety instrumented systems (SIS) are one of the most flexible and common safeguards used in the process industries to reduce risk to a tolerable level. This training course will provide an overview and awareness level discussion of the topic, and is the starting point for further learning on the topic.

Course Objectives

The overall objective of this training course is to introduce the participant to the topic of performance based design of safety instrumented systems as defined in the international standard IEC 61511-2017: Functional Safety: Safety Instrumented Systems for the Process Industry Sector. This is accomplished by addressing the following points:

- Identify causes of accidents with SIS implications
- Understand philosophy of Layers of Protection
- Know steps in the Safety Lifecycle
- Understand Safety Integrity Levels (SIL) impact SIS Design
- Know what's needed in a Safety Requirements Specification (SRS)
- Understand SIS Operation, Maintenance & Testing Requirements

Course Roadmap

The training course is divided into the following sections:

- Section 1 Introduction / Overview
- Section 2 Selected Industry Incidents with SIS Implications
- Section 3 The Safety Lifecycle

Section 1 - Introduction

Section 1 - Introduction

What is an SIS?

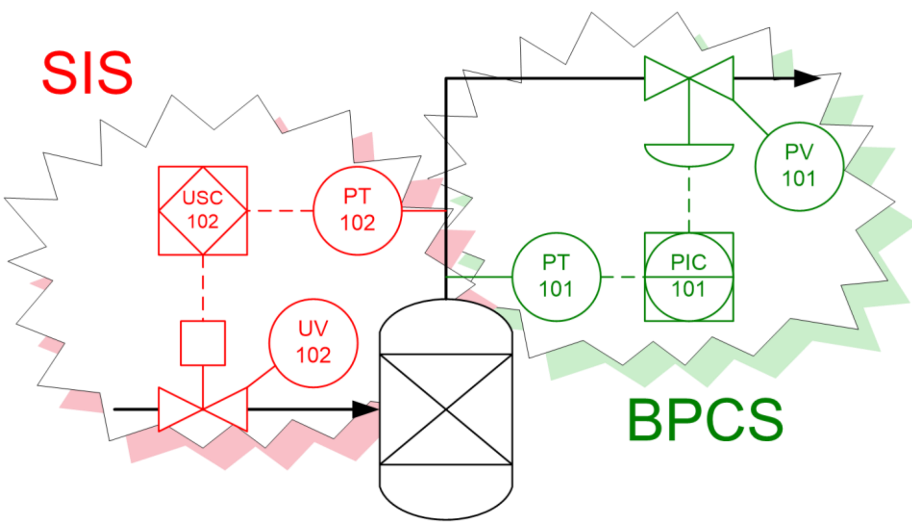
Informal Definition:

- Instrumented Control System that detects “out of control” conditions and automatically returns the process to a safe state

“Last Line of Defense”

- Not basic process control system (BPCS)

How are SIS Different from BPCS?



Technical Definition of a BPCS

Basic Process Control System (BPCS) is defined as,

> “system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to <u>operate in the desired manner</u> but which does not perform any SIF”
>
> – IEC 61511 (2016)

Practical Alternative:

> “an automation system that provides control functions that are normal, routine, and are not intended to be <u>protective</u> in nature”

Section 1 - Introduction

Technical Definition of SIS

Safety Instrumented System (SIS) is defined as,

- “Instrumented system used to implement one or more SIFs."

Safety Instrumented Function (SIF) is defined as,

- "Safety function to be implemented by a safety instrumented system (SIS)"

Safety Function is defined as,

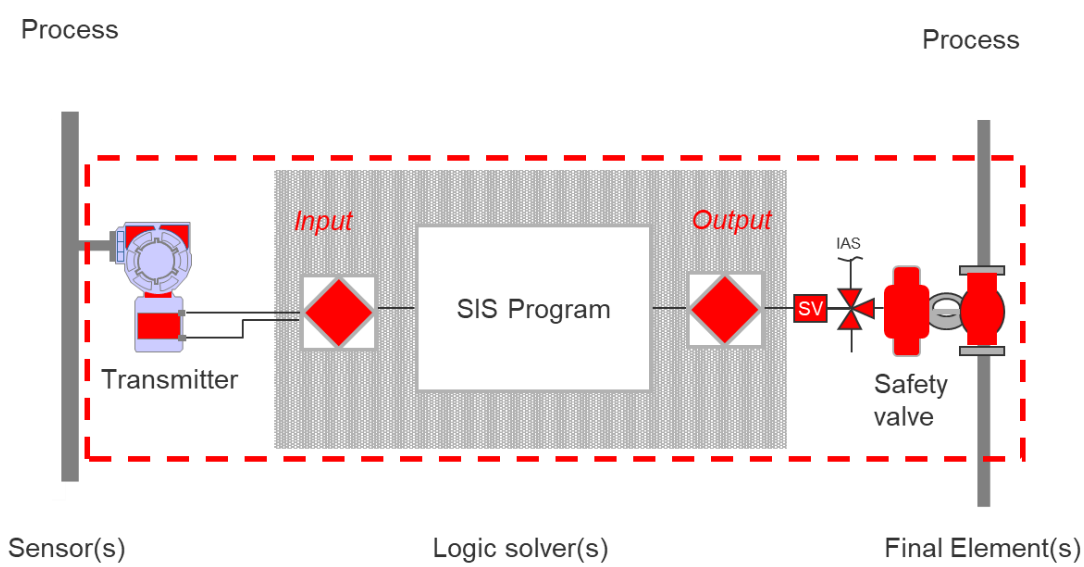
- “Function to be implemented by one or more protection layers which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event." IEC 61511-1 (2016)

Practical Alternative: “Control System composed of sensors, logic solvers and final control elements designed for the purpose of:

Automatically moving a process to a safe state when pre-defined safe operating limits have been violated; *“Preventative”*

Permit a process to operate only when permissive safe operating conditions have been proven; *“Permissive”*

Scope of the SIS

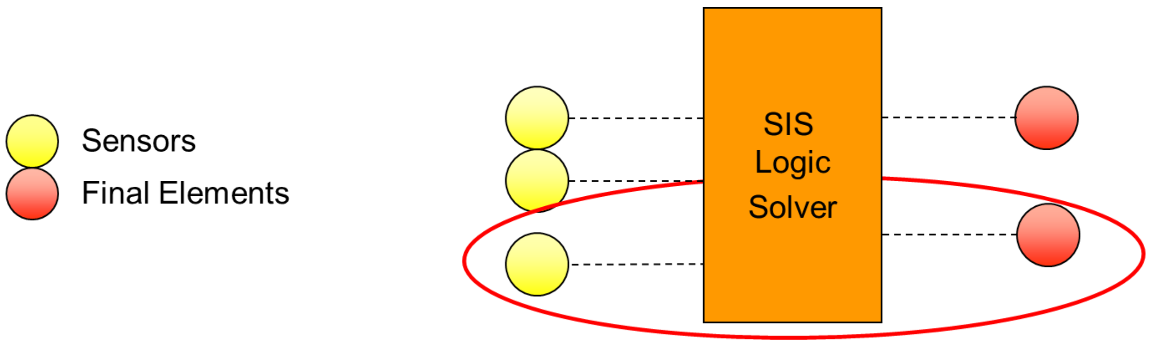


Section 1 - Introduction

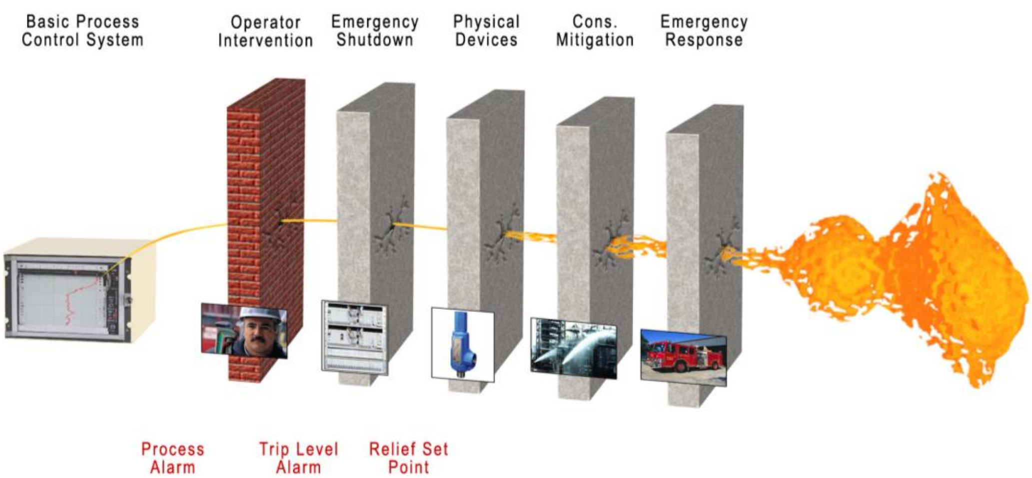
Safety Instrumented Function - Definition

"Safety function to be implemented by a Safety Instrumented System (SIS)"
IEC 61511-1 (2016)

- Alternative. A function be implemented by a SIS which is intended to achieve or maintain a safe state for a process with respect to a specific hazardous event.



SIF Prevents a Specific Hazard

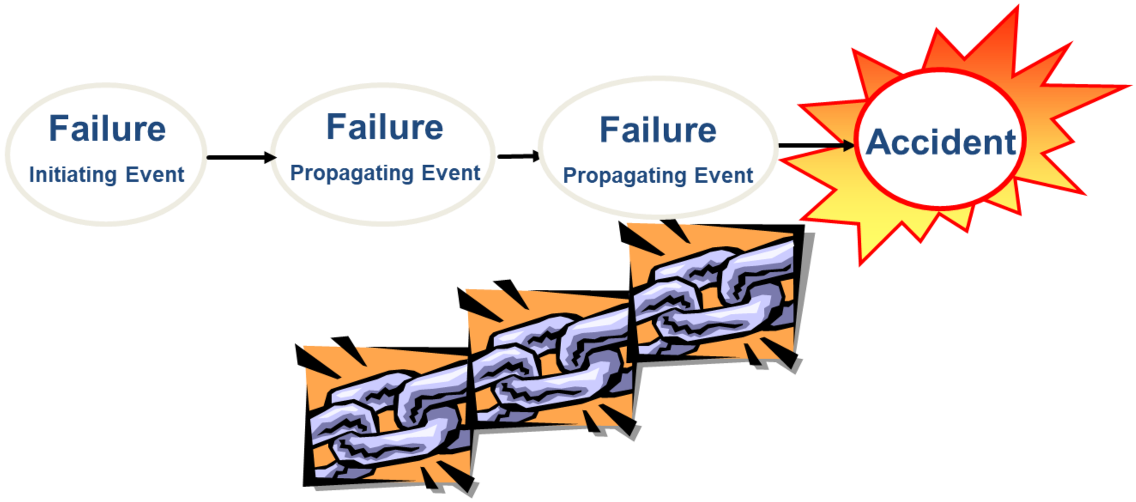


SIS is Protective in Nature

Hypothesis: Most major accidents happen because a multiple failures occur; starting with an initiating event

A well-engineered SIS stops the chain of events, but it is not intended to prevent an initiating event from occurring.

Section 1 - Introduction



Hazards Protected by SIS

Many common hazards are protected using safety instrumented systems. Some common examples include:

- Hydrotreater Runaway Reaction (Refining)
- High Pressure Feed Pump Anti-Backflow
- Fired Heater Burner Management
- Coker Interlocks
- Tank Overfill Systems

Concern for SIS Design, Maintenance, and Operation

Process Accidents are a reality and many are due to the lack of well-engineered safeguards. Process Design increasingly relies on *Automation Systems* to ensure Safety

There is a potential for SIS failures that are:

- "hidden" (not self-revealing),
- "dangerous" (inhibiting)

In order to address this there are Industry Standards for SIS Design, Operation, Maintenance, including:

- ANSI/ISA 84.01 - 1996
- IEC 61508, Published 1998
- IEC 61511, Published 2003

Section 1 - Introduction

Regulation and Standards

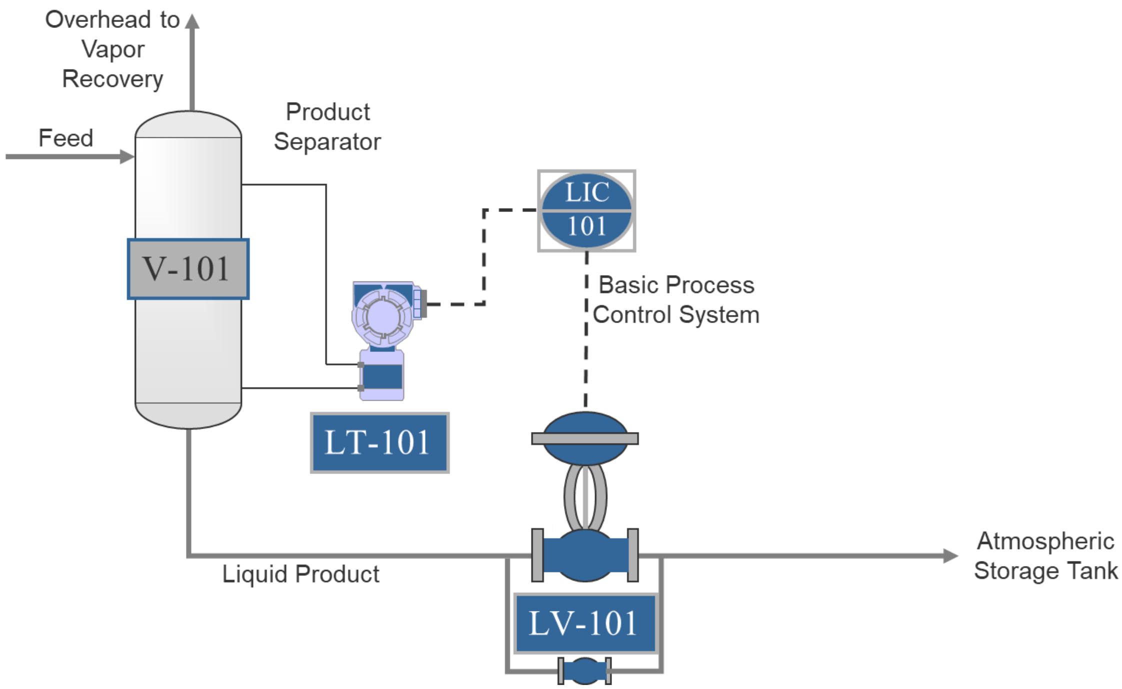
- During Late 1980's, industry safety performance deemed inadequate by regulators worldwide
- Many national regulations were enacted which required implementation of process safety programs (such as OSHA Process Safety Management rule in the US)
- Regulations require RAGAGEP as design basis for safety-critical equipment
- "Recognized and Generally Accepted Good Engineering Practice"
- International Standards bodies such as IEC develop standards to clarify RAGAGEP

Section 1 - Introduction

Application Exercise #1

An accident investigation reveals the need for a SIS to prevent overpressurization of a downstream atmospheric storage tank against the hazard of gas blowby that would result from loss of a liquid level seal.

- What type of “Standard” SIS design should be used?
- What factors (related to safety) should be considered in determining the “correct” design?
- Take 10 minutes to prepare a design. Use the space below and simplified piping and instrumentation diagram to sketch out the design.
- Answers are presented in Section 5



Section 1 - Introduction

What is a Standard SIS Design?

In most cases, the prescriptive approach to SIS design is not optimal from the standpoint of cost or safety…

Many design decisions depend on the specific application and the required level of safety performance

- Equipment type
- Vendor
- Voting arrangement
- Test Intervals

Section 2 – Lessons Learned

LESSONS LEARNED

Section 2 – Lessons Learned

Section 2 presents a series of case studies where instrumentation and control failures were key aspects of the accident scenarios and explains how the IEC 61511 standard was written to address these root causes. Then, provides a worked practical example of how the SIS safety lifecycle is implemented.

Case History 1: Automatic vs. Manual Action

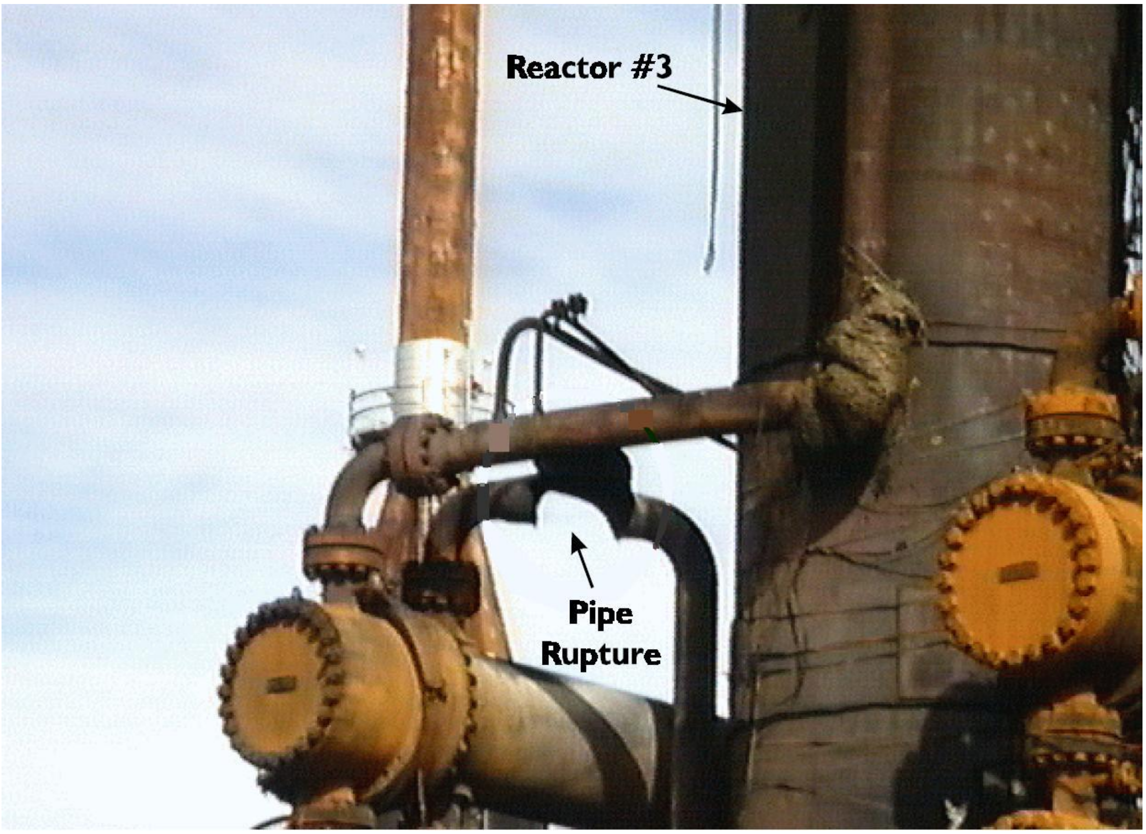
- Hydrocracker runaway reaction USA 1998
- Temperature excursion due to runaway reaction
- Operators failed to manually bring the process to a safe state (no manual de-pressure)
- Temperature in the effluent pipe reached in excess of 1400 F
- 1 worker fatality; 46 injured
- Current design, automated shutdown

Section 2 – Lessons Learned

LESSONS LEARNED

Case History 1: Failure and Loss of Containment Point

Section 2 – Lessons Learned



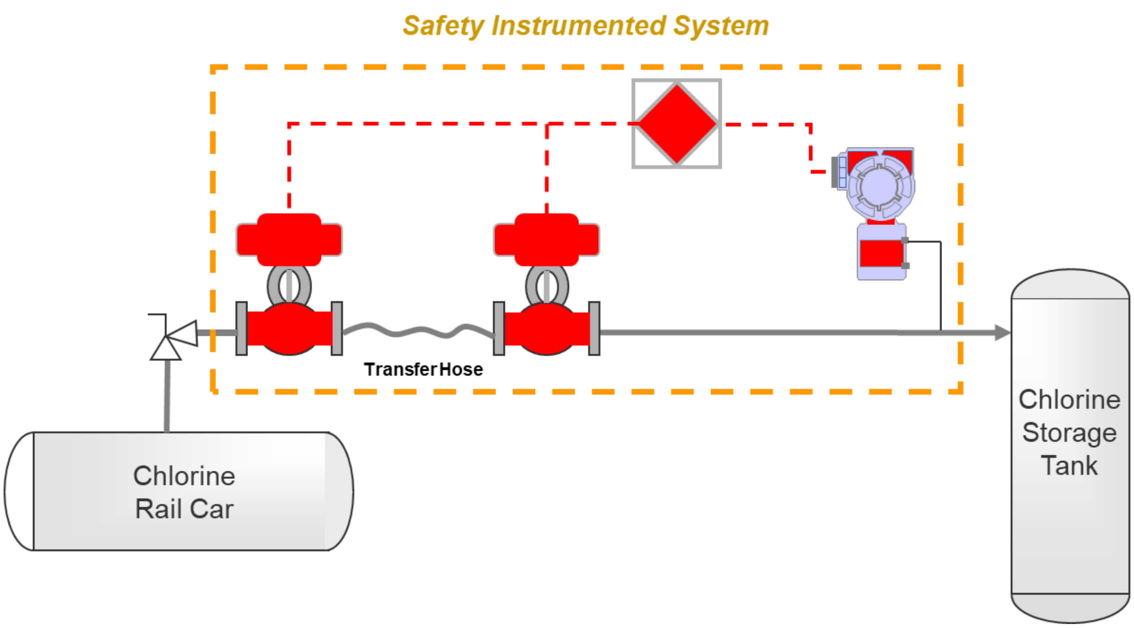
LESSONS LEARNED

Section 2 – Lessons Learned

LESSONS LEARNED

Case History 2: Improper Testing

- August 2002, USA
- Transfer hose failed during the unloading of a chlorine rail car.
- Automatic shutdown system malfunctioned
- Leak continued unabated for several hours
- 48,000 pounds chlorine gas released
- 63 people sought hospital treatment.



Case History 3: Equipment Selection

- Difficult Measurement
- 1994, North America
- Overcharge of Reactor
- Runaway Reaction
- Vent System Unable to Relieve
- Protection Layers?

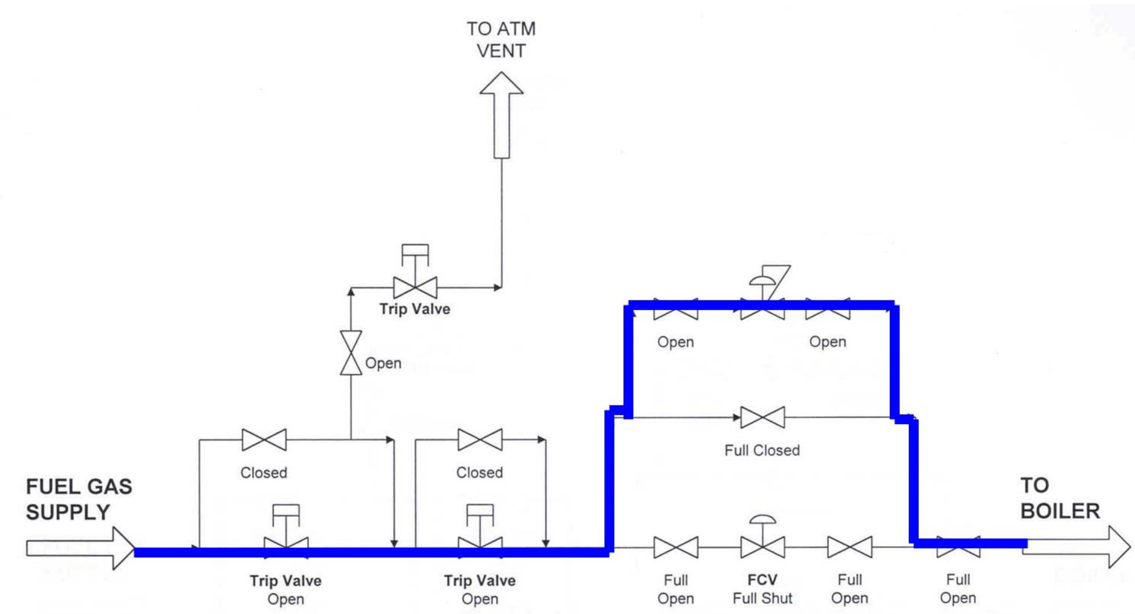
Section 2 – Lessons Learned

LESSONS LEARNED

Case History 4: Bypassing

Safety functionality is frequently bypassed

- Difficulty in startup (Boiler Explosion, Asia 1990's)
- Problematic instruments
- Confusing or complex operation



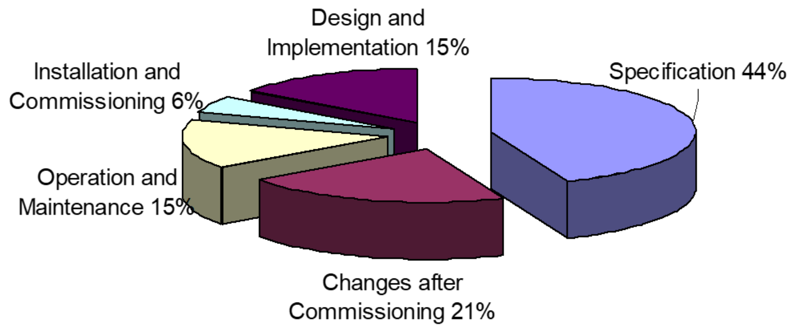
Accident Causal Factors

- No SIS installed
- Poor basis for when safety should be automated
- Questionable equipment selection
- Redundancy and Diagnostics
- Testing methods poor
- Poor basis for testing frequency
- Improper bypassing equipment and techniques

Section 2 – Lessons Learned

LESSONS LEARNED

HSE Study of Accident Causes



"Out of Control: Why Control Systems go Wrong and How to Prevent Failure," UK Heath and Safety Executive, 1995

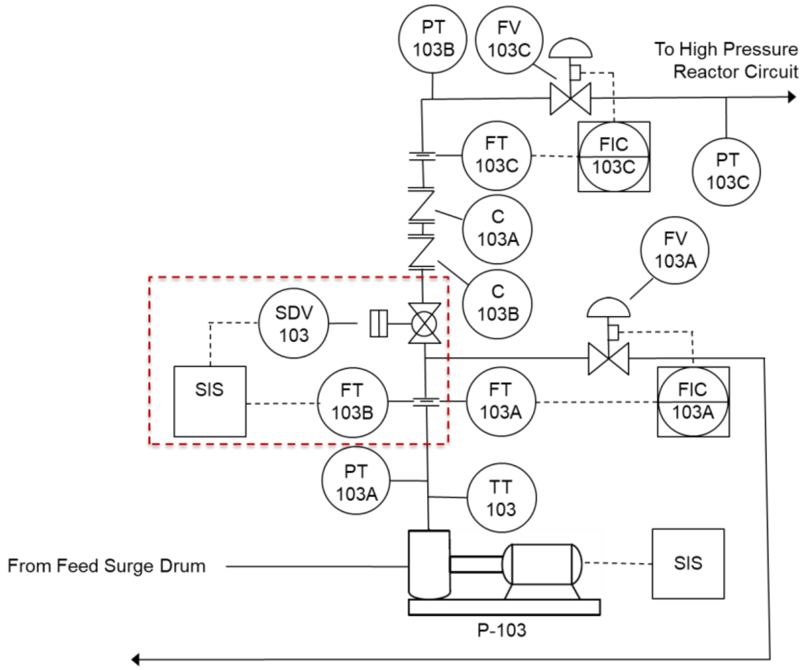
Implications of Accident Data on SIS

- Criteria for when to use alarms / operator judgment versus shutdown with SIS
- Defense in Depth Strategy
  - Separation of Protection Layers
- Design Specification(s) for SIS
  - Components
  - Architecture
  - Diagnostics
  - Testing
- Bypass and Defeat of Critical Safety Systems
  - Change Management
- Comprehensive Lifecycle Approach Necessary

Section 2 – Lessons Learned

LESSONS LEARNED

Practical Example: High-Pressure Anti-Backflow



Layer of Protection Analysis

KENEXIS OPEN PHA

Signed In As Edward Marszal of Kenexis

Study Data | Nodes | Deviations | PHA Worksheets | LOPA Worksheets | Recommendations | Safeguards | Parking Lot | Risk Criteria | Back

LOPA Worksheets

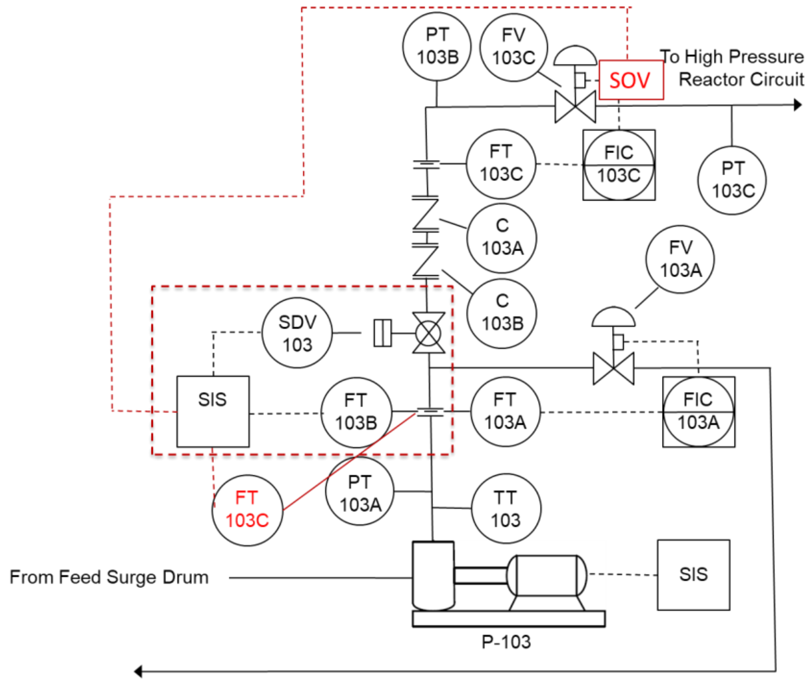
1. Reactor Feed Circuit

Deviation	Consequence	S	TMEL	Cause	Frequency	IPL	IPL Tag	PFD	MEL Safety	RRF Safety
Low Low Flow	Low-Low flow could be indicative of reverse flow, which could result in piping/vessels on pump suction side being exposed to high pressures. High pressures could result in mechanical failure of piping/vessel, which could result in loss of containment. Loss of containment could result in fire/explosion if source of ignition were contacted. Significant fire/explosion that could result in personnel injury. Size and severity of fire could cause life-threatening injury (fatal) to personnel in area.	H	1E-4	Failure of Export Pump (P-103) from all causes	0.1	Dual Check Valves	C-103A/B	0.1	1.00E-2	100

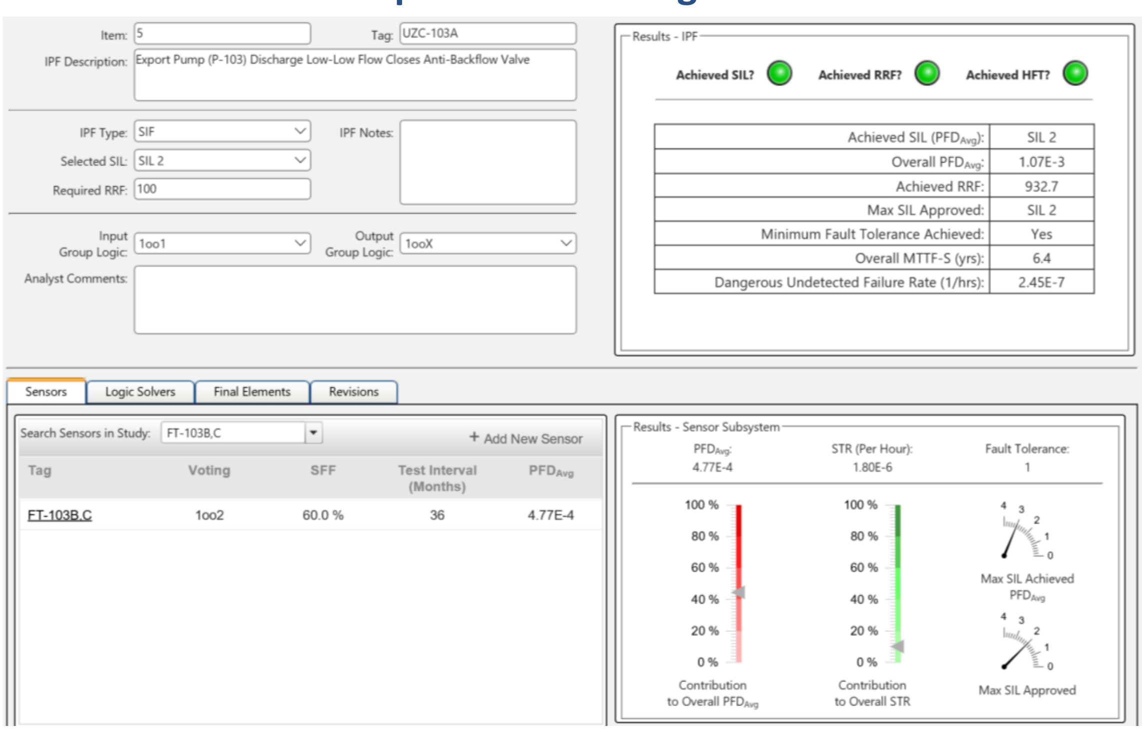
Section 2 – Lessons Learned

LESSONS LEARNED

Anti-Backflow SIF: Proposed SIL 2 Design



Anti-Backflow SIF: Proposed SIL 2 Design Verification



Section 3 – Safety Lifecycle

Section 3 – Safety Lifecycle

This section discusses the SIS Safety Lifecycle as defined in the IEC 61511 standard. This section also provides an overview of the SIS functional safety standard and the regulations underpin their use and requirement. The section also includes a discussion of the safety lifecycle phases and practical steps in their implementation.

Industry Standard for Safety Instrumented Systems (SIS)

International Electrotechnical Commission (IEC), IEC 61511-2017, Functional Safety: Safety Instrumented Systems for the Process Sector

Localized Versions:

- US - Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA S84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, 2004.

IEC 61511 Standard Safety Lifecycle

Provide a complete safety lifecycle to address all root causes of failure

- Identification of systems
- Design
- Testing
- Maintenance
- Management of Change

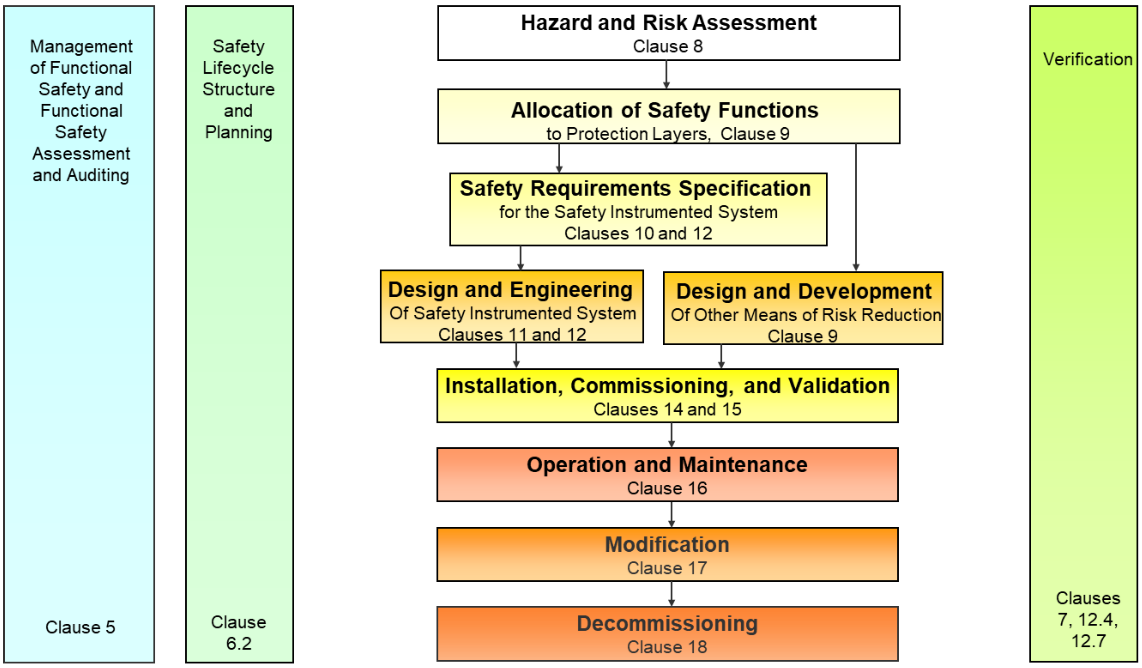
What does IEC 61511 require?

- Performance based
- Defines a “safety lifecycle”
- Requires selection of performance target for each SIF
- Requires the design each SIF to that target and quantitative verification of target achievement

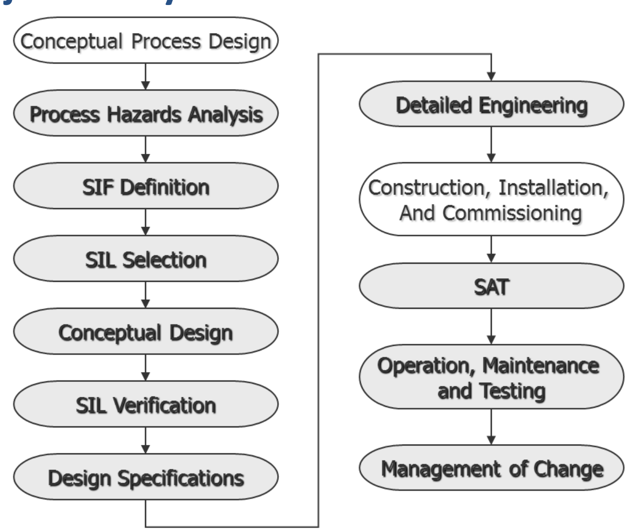
Section 3 – Safety Lifecycle

SAFETY LIFECYCLE

Safety Lifecycle IEC 61511

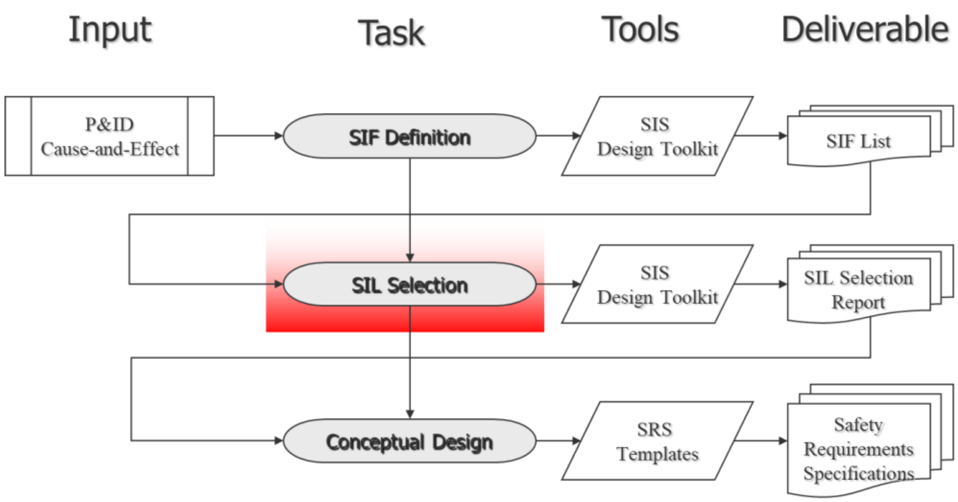


Typical SIS Project Lifecycle



Section 3 – Safety Lifecycle

SIL Selection

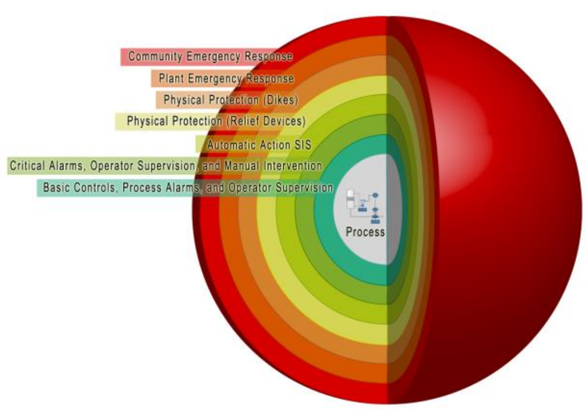


What is Safety Integrity Level?

A measure of the amount of risk reduction provided by a SIF.

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> 99.99%	0.001% to 0.01%	100,000 to 10,000
SIL 3	99.9% to 99.99%	0.01% to 0.1%	10,000 to 1,000
SIL 2	99% to 99.9%	0.1% to 1%	1,000 to 100
SIL 1	90% to 99%	1% to 10%	100 to 10

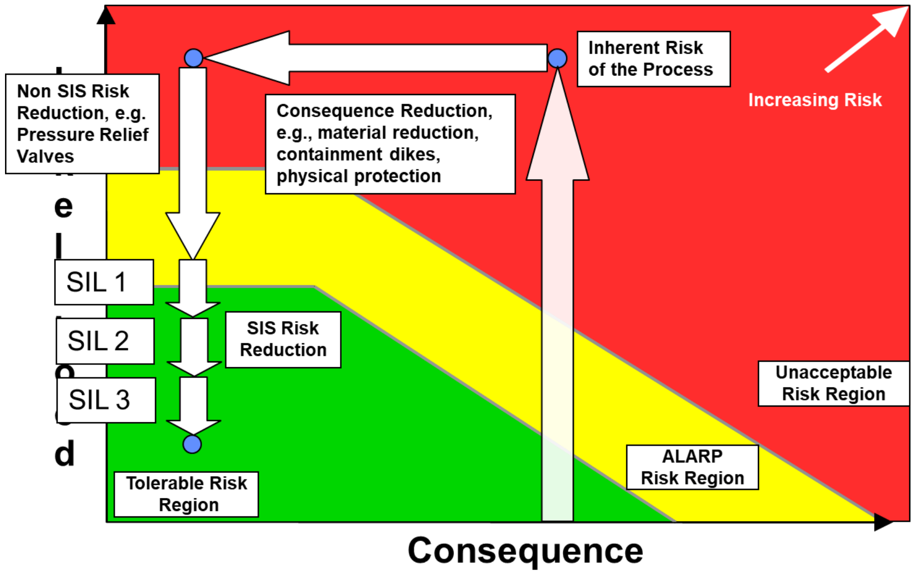
Philosophy of Layers of Protection



SAFETY LIFECYCLE

Section 3 – Safety Lifecycle

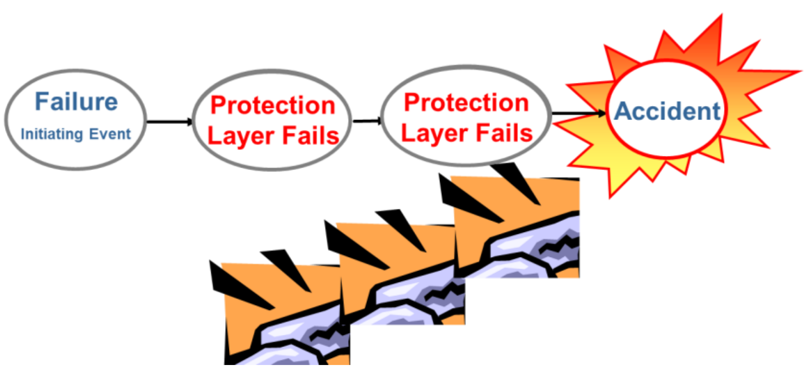
SIS Risk Reduction



Model of Accident Causation

Hypothesis #1: Most major accidents happen because a multiple failures occur; starting with an initiating event

Hypothesis #2: If an Independent Protection Layer (IPL) Functions as intended when an initiating event occurs, no accident will result. All IPLs must fail for the accident to occur.



Section 3 – Safety Lifecycle

Initiating Event Frequency

Initiating Event	Typical Frequency (F)	
Loss of cooling (standard controls)	1 / year	10^{0}
Loss of power (standard controls)	1 / year	10^{0}
Human error (routine, once-per-day opportunity)	1 / year	10^{0}
Loss of cooling (redundant/diverse controls)	1/10 years	10^{-1}
Loss of power (redundant supplies)	1/10 years	10^{-1}
Human error (routine, once-per-month opportunity)	1/10 years	10^{-1}
Human error (non-routine / low stress)	1/10 years	10^{-1}
Basic Process control Loop Failure (continuous use)	1/10 years	10^{-1}

Other frequency values may be selected based on an analysis of actual operating data, including that includes service factors.

CAUTION

IEC 61511 limits assumed frequency of BPCS failure to 10^{-5}/hr (about 1 / 11 years)

Requirements of an Independent Protection Layer

Independent Protection Layers (IPL) are limited to safeguards having the following characteristics

- Specificity
    - Specifically designed to prevent the Hazard Identified
- Independence
    - From cause and other IPL
- Dependability
    - One order of magnitude risk reduction
- Auditability
    - Can be tracked / measured

What is not an IPL?

- PPE / Procedures / Preventive Maintenance / Inspection

Section 3 – Safety Lifecycle

SAFETY LIFECYCLE

Credit for Layers of Protection

IPL Type	Qualitative IPL Credit	Quantitative IPL Credit
BPCS		
Automatic BPCS Control Loop	1	10^{-1}
Operator Intervention		
Manual response with > 10 minutes available	1	10^{-1}
Manual response with > 40 minutes available	2	10^{-2}
Manual response to abnormal readings collected regularly	1	10^{-1}
Emergency Pressure Relief		
Spring-loaded relief valve or rupture disk in clean service	1 to 2	10^{-1} to 10^{-2}
Safety Instrumented Functions		
SIL 3 (Safety Integrity Level)	3	10^{-3}
SIL 2	2	10^{-2}
SIL 1	1	10^{-1}

Risk Tolerance Criteria – Target Selection

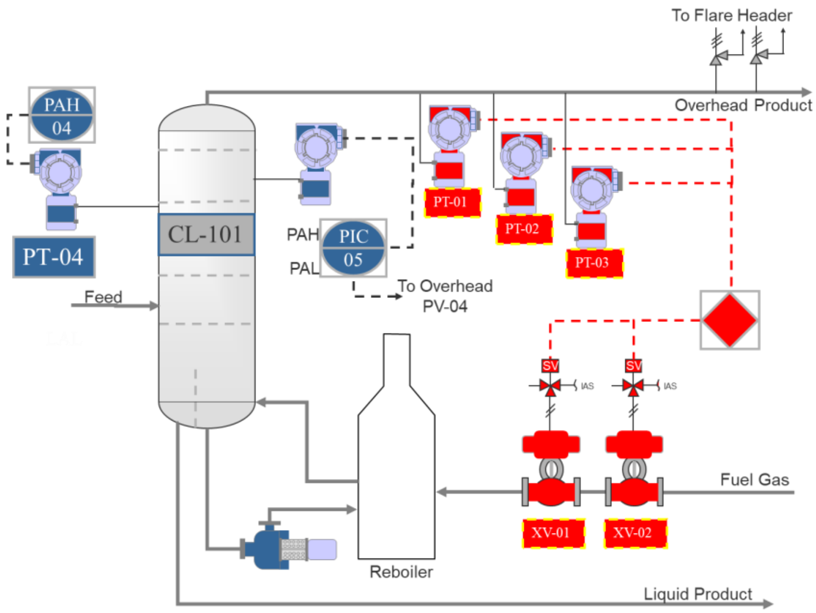
- Select Tolerable Mitigated Event Likelihood based on consequence severity
- Calculate required risk reduction factor (RRF)
- Assign SIL based on RRF and other IPLs

Category	Consequence Severity	TMEL
Minor	Minor injury or reversible health effects	**10^{-2} per year**
Serious	Serious injuries - hospitalization	**10^{-3} per year**
Extensive	One or more fatalities	**10^{-4} per year**

$$PFD_{Required} = \frac{TMEL}{f_{Unmitigated}}$$

Section 3 – Safety Lifecycle

LOPA Example – Distillation Column



ID	Description	Inputs	Outputs	Req. SIL	Notes
SIF -01	High-High Pressure in Column CL-101 causes shutoff of reboiler H-100 to remove heat input to column	PT-01 PT-02 PT-03 (2oo3)	XV-01 Close XV-02 Close (1oo2)		

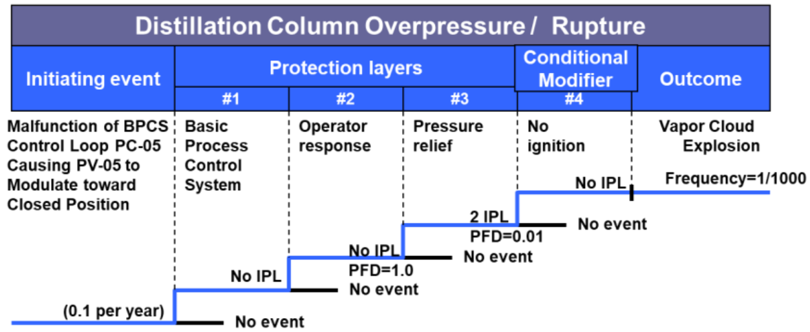
Risk Tolerance – Distillation Column

Overpressure could result in mechanical damage to column, release of flammable hydrocarbon to atmosphere, potential fire/explosion hazard and potential fatality.

Category	Consequence Severity	TMEL
Minor	Minor injury or reversible health effects	**10^{-2} per year**
Serious	Serious injuries - hospitalization	**10^{-3} per year**
Extensive	One or more fatalities	**10^{-4} per year**

Section 3 – Safety Lifecycle

LOPA Event Tree for Distillation Column



$$F_{unmitigated} = 10^{-3} \text{ per year}$$

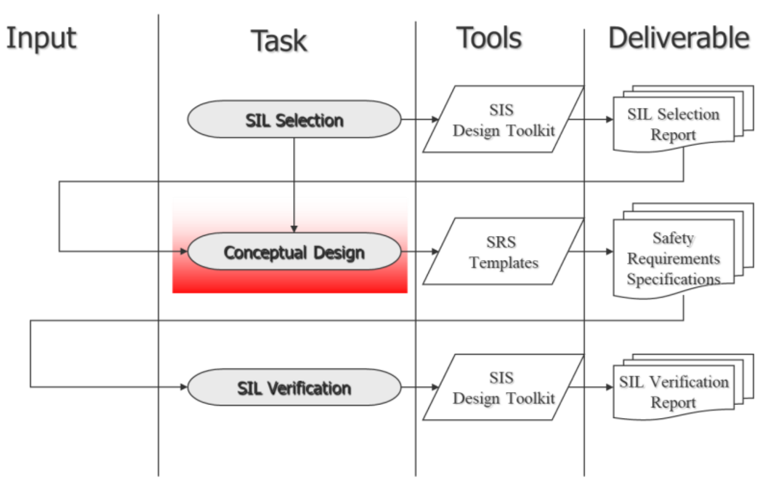
Required SIF Risk Reduction Calculation

$$RRF = \frac{F_{Unmitiged}}{TMEL}$$

$$RRF = \frac{10^{-3} \text{ per year}}{10^{-4} \text{ per year}}$$

$$RRF = 10 \quad \Rightarrow \textbf{SIL 1}$$

Conceptual Design



Section 3 – Safety Lifecycle

Conceptual Design Attributes

Select Technology

- SIL Certifications or Prior Use / Device-Specific Failure Rates

Select Architecture / Voting

- Select degree of Fault Tolerance / “Necessary and Sufficient” Actions

Design for Functional Testing

- Frequency / Online or during Shutdown / Full Functional Test or Partial Test

Diagnostic Testing

- Frequency / Response to detected fault

Safety Requirements Specifications

Definition

- IEC61511: “specification that contains all the requirements of the safety instrumented functions in a safety instrumented system”

SRS Contents

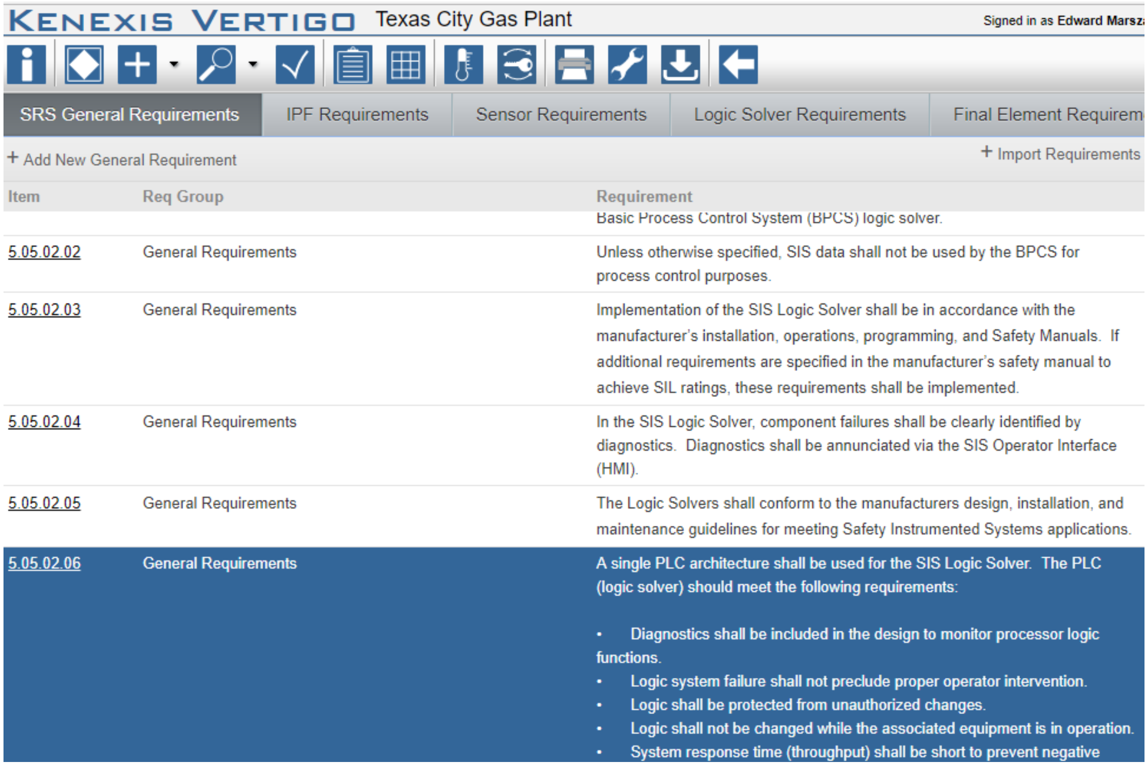
- General Requirements (Applies to Entire SIS)
- SIF Requirements
- Instrument Requirements
- Logic Description

SRS General Requirements

- Separation Philosophy
- Logic Solver Architecture
- Operator Interface Requirements
- Response to Detected Failures
- Environmental Conditions
- Manual De-energization
- Bypass Process
- Reset Process

Section 3 – Safety Lifecycle

- Voting Degradation



KENEXIS VERTIGO Texas City Gas Plant — Signed in as Edward Marsz

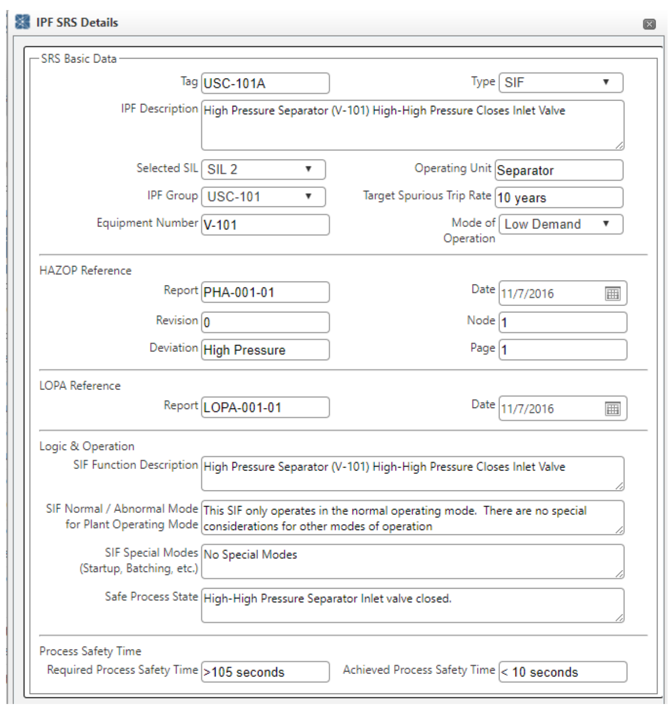
SRS General Requirements | IPF Requirements | Sensor Requirements | Logic Solver Requirements | Final Element Requirem

+ Add New General Requirement — + Import Requirements

Item	Req Group	Requirement
		Basic Process Control System (BPCS) logic solver.
5.05.02.02	General Requirements	Unless otherwise specified, SIS data shall not be used by the BPCS for process control purposes.
5.05.02.03	General Requirements	Implementation of the SIS Logic Solver shall be in accordance with the manufacturer's installation, operations, programming, and Safety Manuals. If additional requirements are specified in the manufacturer's safety manual to achieve SIL ratings, these requirements shall be implemented.
5.05.02.04	General Requirements	In the SIS Logic Solver, component failures shall be clearly identified by diagnostics. Diagnostics shall be annunciated via the SIS Operator Interface (HMI).
5.05.02.05	General Requirements	The Logic Solvers shall conform to the manufacturers design, installation, and maintenance guidelines for meeting Safety Instrumented Systems applications.
5.05.02.06	General Requirements	A single PLC architecture shall be used for the SIS Logic Solver. The PLC (logic solver) should meet the following requirements: • Diagnostics shall be included in the design to monitor processor logic functions. • Logic system failure shall not preclude proper operator intervention. • Logic shall be protected from unauthorized changes. • Logic shall not be changed while the associated equipment is in operation. • System response time (throughput) shall be short to prevent negative

SRS SIF Requirements

- Demand Mode
- PHA/LOPA Reference
- Operating Modes
- Process Safety Time
- Achieved SIF Response Time



IPF SRS Details

SRS Basic Data

Tag: USC-101A — Type: SIF

IPF Description: High Pressure Separator (V-101) High-High Pressure Closes Inlet Valve

Selected SIL: SIL 2 — Operating Unit: Separator

IPF Group: USC-101 — Target Spurious Trip Rate: 10 years

Equipment Number: V-101 — Mode of Operation: Low Demand

HAZOP Reference

Report: PHA-001-01 — Date: 11/7/2016

Revision: 0 — Node: 1

Deviation: High Pressure — Page: 1

LOPA Reference

Report: LOPA-001-01 — Date: 11/7/2016

Logic & Operation

SIF Function Description: High Pressure Separator (V-101) High-High Pressure Closes Inlet Valve

SIF Normal / Abnormal Mode for Plant Operating Mode: This SIF only operates in the normal operating mode. There are no special considerations for other modes of operation

SIF Special Modes (Startup, Batching, etc.): No Special Modes

Safe Process State: High-High Pressure Separator Inlet valve closed.

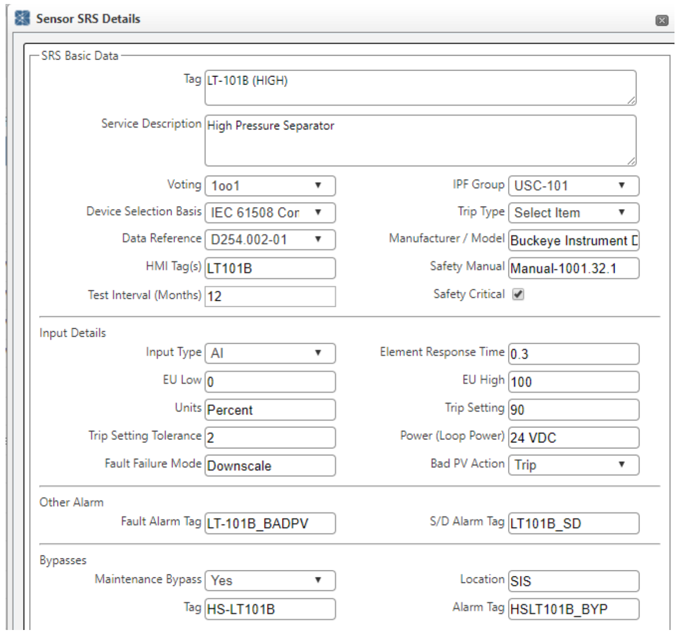
Process Safety Time

Required Process Safety Time: >105 seconds — Achieved Process Safety Time: < 10 seconds

Section 3 – Safety Lifecycle

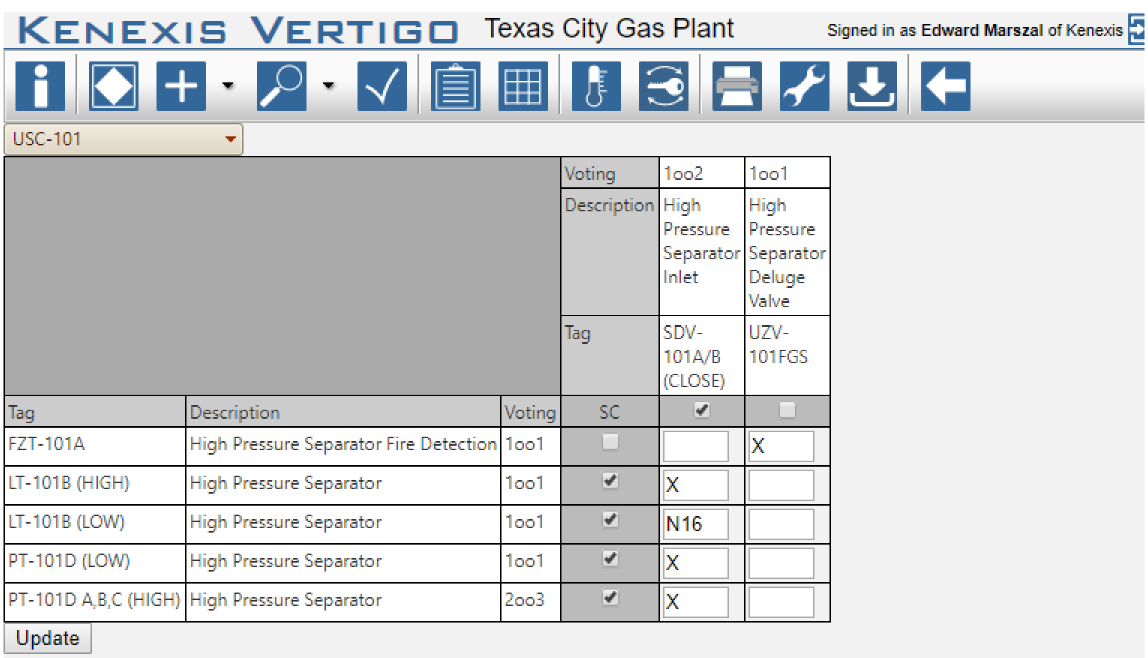
SRS Instrument Requirements

- Voting Arrangement
- Selection Basis
- Trip Settings
- Failure Responses
- Alarm Details
- Bypass Details



SRS Logic Description

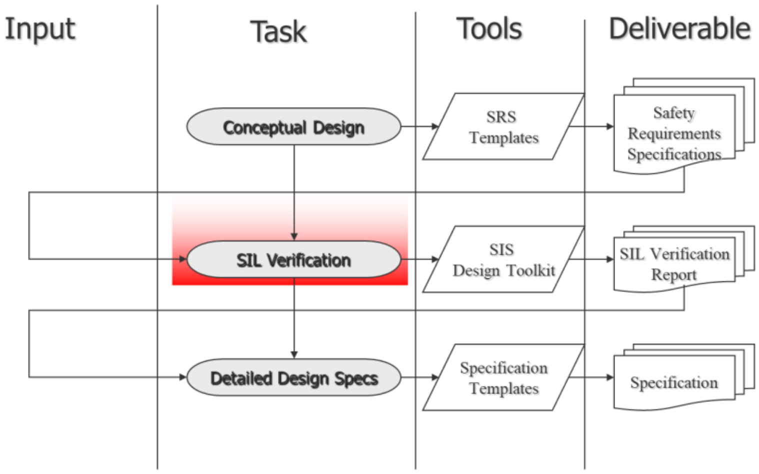
- Cause and Effect Diagram
- Inputs / Outputs
- Special Notes



			Voting	1oo2	1oo1
			Description	High Pressure Separator Inlet	High Pressure Separator Deluge Valve
			Tag	SDV-101A/B (CLOSE)	UZV-101FGS
Tag	Description	Voting	SC	✓	
FZT-101A	High Pressure Separator Fire Detection	1oo1			X
LT-101B (HIGH)	High Pressure Separator	1oo1	✓	X	
LT-101B (LOW)	High Pressure Separator	1oo1	✓	N16	
PT-101D (LOW)	High Pressure Separator	1oo1	✓	X	
PT-101D A,B,C (HIGH)	High Pressure Separator	2oo3	✓	X	

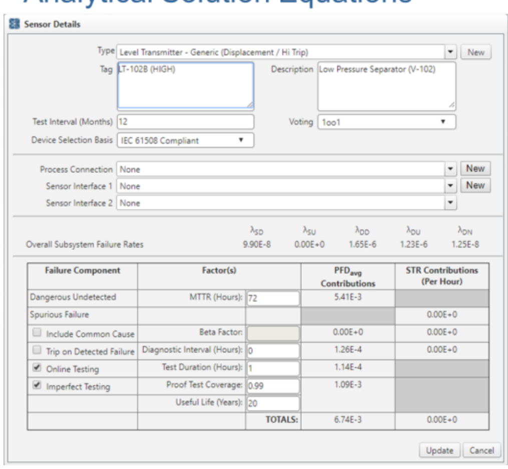
Section 3 – Safety Lifecycle

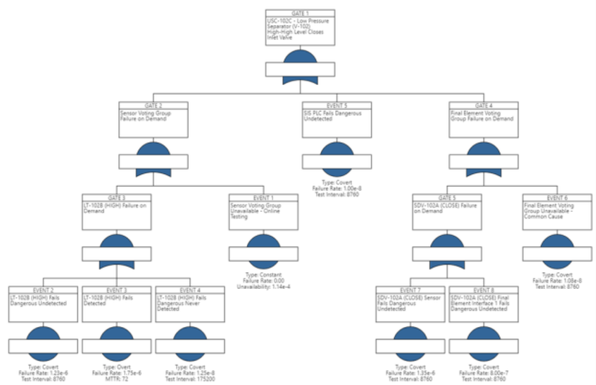
SIL Verification



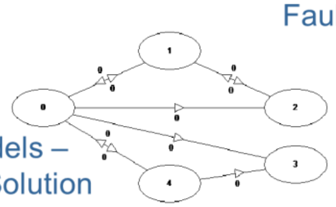
Reliability Models

Analytical Solution Equations





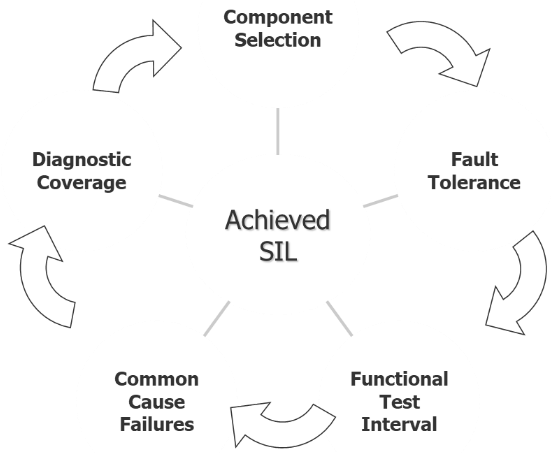
Fault Tree Analysis



Markov Models – Numerical Solution

Section 3 – Safety Lifecycle

Parameters Impacting SIL / Risk Reduction



Component Selection

Components and sub-systems selected for use as part of a Safety Instrumented System (SIS) for SIL 1 to SIL 3 applications shall either be

- In accordance with IEC-61508 Parts 2 and 3 (e.g., certified)
- Selected based on “prior use”

Fault Tolerance

Use of multiple devices

Voting “architecture” changes

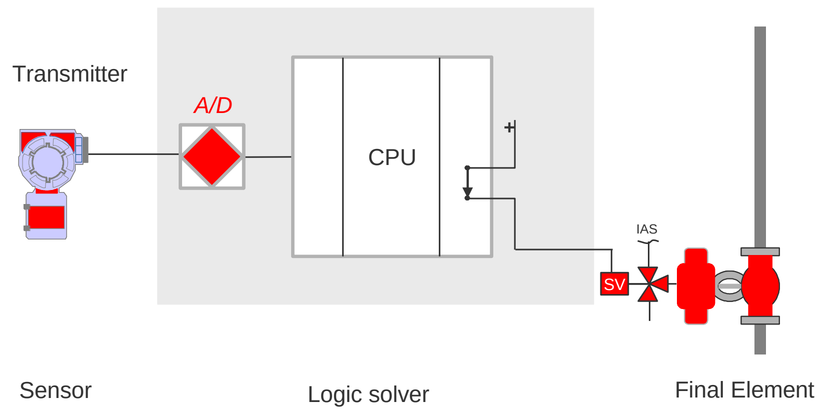
- Probability of Failure on Demand (PFD)
- Probability of Fail Safe (PFS)

Vote	PFD	PFS
1oo1	0.10	0.2
1oo2	0.01	0.4
2oo2	0.20	0.04
2oo3	0.03	0.12

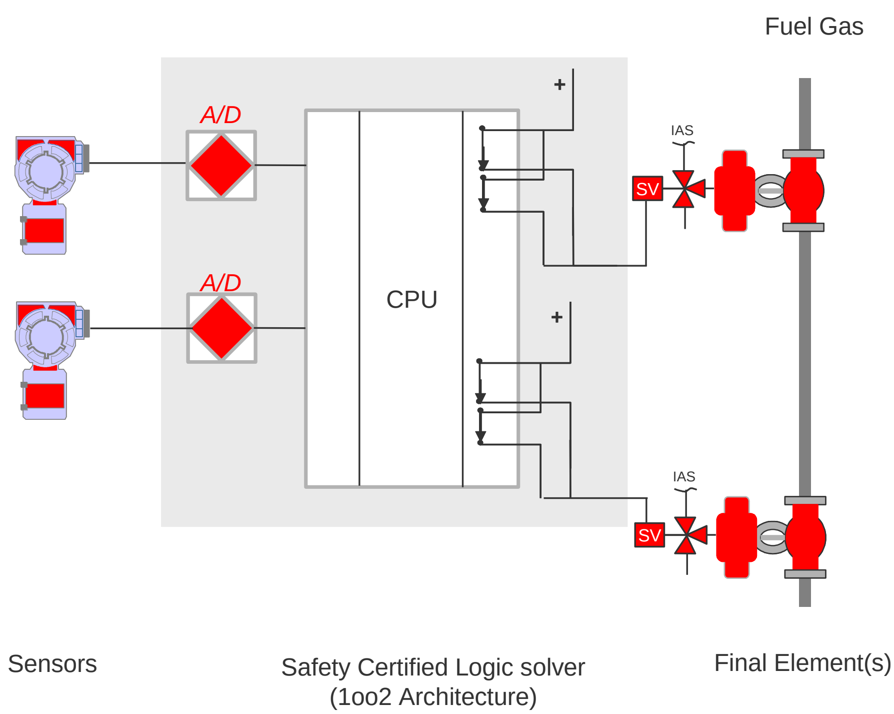
Achieving higher levels of Safety Availability may require fault tolerance

Section 3 – Safety Lifecycle

Typical SIL 1 Architecture



Fault Tolerant Architecture – SIL 2/3



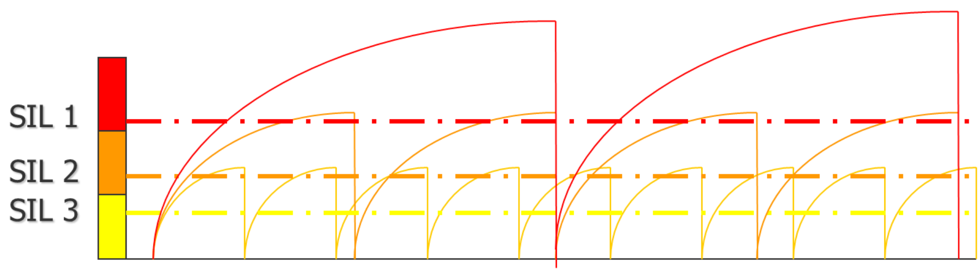
Section 3 – Safety Lifecycle

Functional Test Interval

Increased testing frequency leads to decreased probability of failure

- Average amount of time in failed state is decreased
- Tests return failed equipment to operational

Typically, the turnaround interval of the plant



Architectures – 1oo1 (one-out-of-one)

Dangerous Fault Tolerance	$= 0$
Safe Fault Tolerance	$= 0$

One vote to trip out of one device causes the FGS action

Analytical Solution Equations

$$PFD_{AVG} = \frac{\lambda^{DU} TI}{2}$$

$$STR = \lambda^{S} + \lambda^{DD}$$

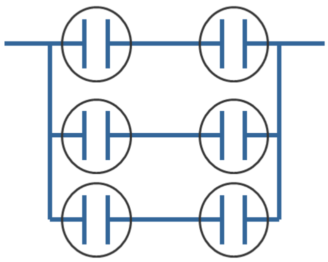
	PFD	STR
1oo1	3.29E-2	4.50E-6
1oo2		
2oo2		
2oo3		

PFD – Probability of Failure on Demand   STR – Spurious Trip Rate

Section 3 – Safety Lifecycle

Architectures – 2oo3 (two-out-of-three)

Dangerous Fault Tolerance	= 1
Safe Fault Tolerance	= 1



Analytical Solution Equations

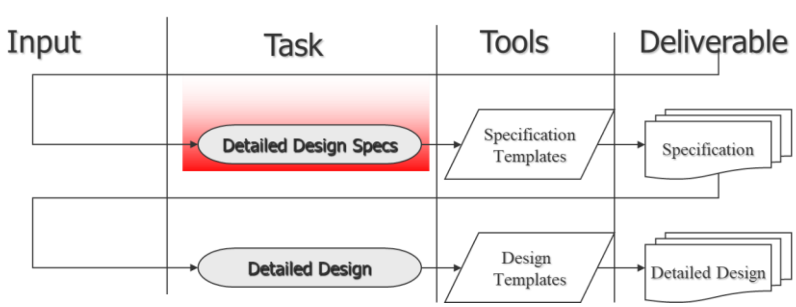
$$PFD_{AVG} = \left(\lambda^{DU}\right)^2 \times TI^2$$

$$STR = 2\left(\lambda^{S} + \lambda^{DD}\right)^2 \times MTTR$$

	PFD	STR
1oo1	0.0329	4.50E-6
1oo2	0.00144	9.00E-6
2oo2	0.0657	2.920E-6
2oo3	0.00432	8.750E-6

Detailed Design

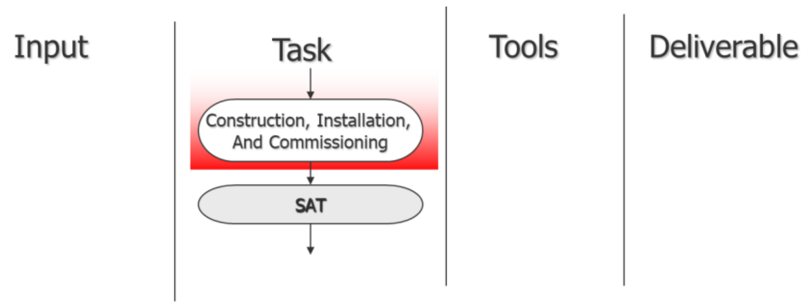
- Loop Sheets
- Wiring Diagrams
- Cable Schedules
- PLC Programs
- System Integration
- SIS Operating Procedures (startup, reset, bypass, response to fault)
- SIS Maintenance and Testing Procedures
- Factory Acceptance Test (FAT)



Section 3 – Safety Lifecycle

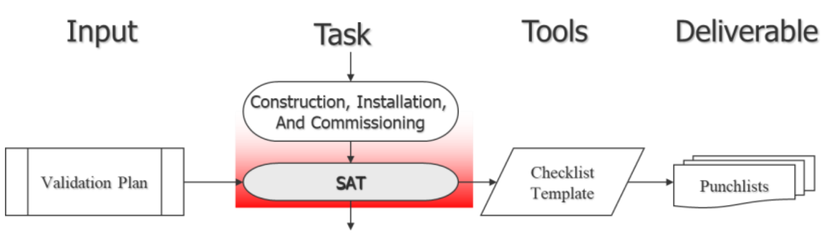
Construction, Installation, and Commissioning

- Install Control Equipment
- Load software
- Install field wiring, Junction Boxes
- Install Instrumentation
- Instrument Calibration and Loop Checks



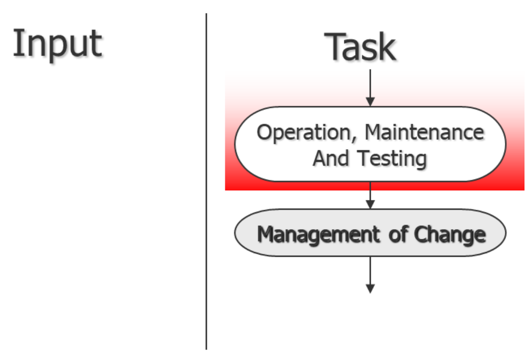
Site Acceptance Testing

- Verify that installed equipment and software conform to safety requirements specifications
- Review software and hardware
- Full Function Testing of Equipment
- Generate deviation record (punch list)



Operation and Maintenance

- Respond to overt faults
- Manage bypass for SIS maintenance
- Periodic function testing



SAFETY LIFECYCLE

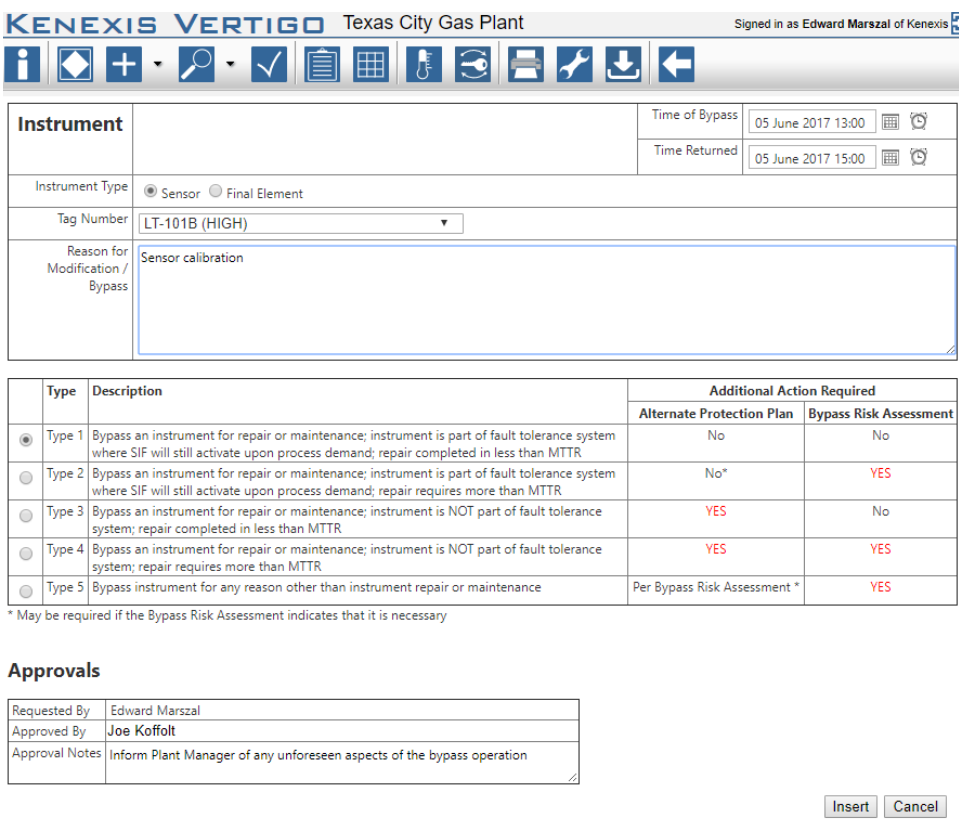
Section 3 – Safety Lifecycle

Management of Bypasses

Activation of any bypass should only be performed using a formal program

The formal program should include

- A procedure for authorizing and executing bypasses
  - Development of Alternate Protection Plan, if required
  - Bypass Risk Assessment, if required
- Mechanism for requiring appropriate approvals
- Auditing of bypass activations
- Restore to Operational within Assumed MTTR



KENEXIS VERTIGO Texas City Gas Plant

Signed in as Edward Marszal of Kenexis

Instrument

Time of Bypass: 05 June 2017 13:00

Time Returned: 05 June 2017 15:00

Instrument Type: Sensor / Final Element

Tag Number: LT-101B (HIGH)

Reason for Modification / Bypass: Sensor calibration

	Type	Description	Additional Action Required	
			Alternate Protection Plan	Bypass Risk Assessment
◉	Type 1	Bypass an instrument for repair or maintenance; instrument is part of fault tolerance system where SIF will still activate upon process demand; repair completed in less than MTTR	No	No
○	Type 2	Bypass an instrument for repair or maintenance; instrument is part of fault tolerance system where SIF will still activate upon process demand; repair requires more than MTTR	No*	YES
○	Type 3	Bypass an instrument for repair or maintenance; instrument is NOT part of fault tolerance system; repair completed in less than MTTR	YES	No
○	Type 4	Bypass an instrument for repair or maintenance; instrument is NOT part of fault tolerance system; repair requires more than MTTR	YES	YES
○	Type 5	Bypass instrument for any reason other than instrument repair or maintenance	Per Bypass Risk Assessment *	YES

* May be required if the Bypass Risk Assessment indicates that it is necessary

Approvals

Requested By	Edward Marszal
Approved By	Joe Koffolt
Approval Notes	Inform Plant Manager of any unforeseen aspects of the bypass operation

Insert Cancel

Alternate Protection Plan

- What process variables should be monitored?
- What are the manual trigger points?
- What personnel will perform the monitoring and manual shut down actions?
- What degree of independence from normal operation staff is required for alternate protection plan staff?

Section 3 – Safety Lifecycle

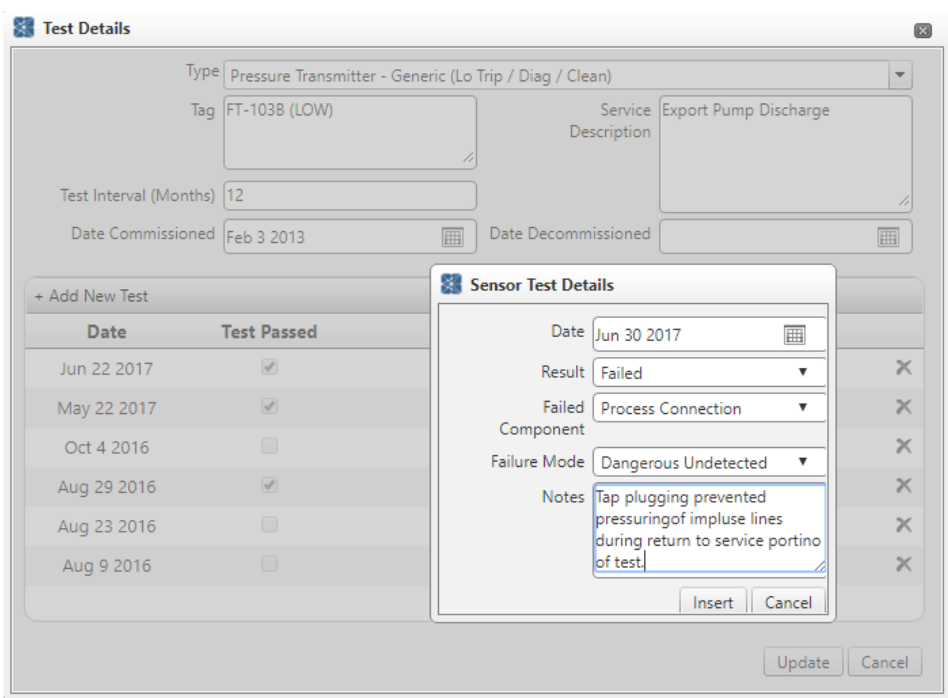
- What specific actions must be taken to manually shut down?
- Can a manual shutdown be performed within the process safety time?

Bypass Risk Assessment

- Identify hazard prevented by bypassed SIF
- Identify consequence associated with the hazard
- Identify cumulative impact of addition of this bypass to any other existing bypasses
- Identify initiating events during bypass that could result in the consequence and ensure APP are capable of preventing the consequence
- Risk assessment performed by team including operations, engineering, HSE, and equipment specialist

SIS Maintenance and Testing

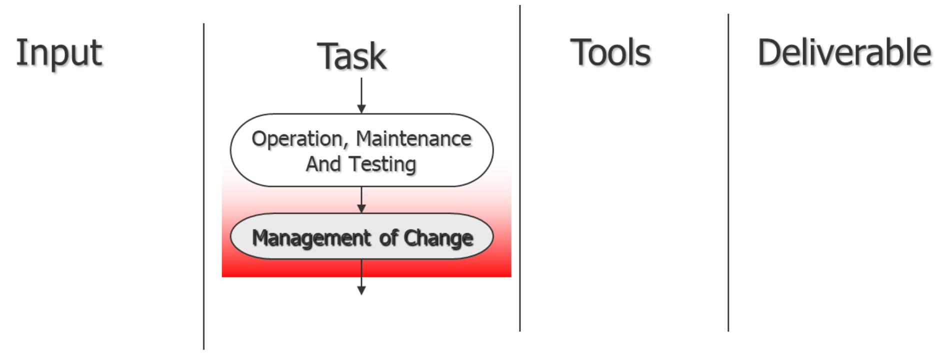
- Key objective: Ensure the integrity of each SIF is maintained and the required SIL achieved
- Maintenance Testing Procedures & Controls
- Proof Test procedures shall be developed to reveal all covert, dangerous failures.
- Documentation of Proof Tests and Inspection



Section 3 – Safety Lifecycle

Management of Change

Follow site Management of Change procedures…



Section 4 – Quiz

QUIZ

Post Instructional Quiz

1. Which of the following is the best definition of a Safety Instrumented System?
    a. A control loop whose failure may result in the initiating of a chain of events that could result in a hazardous outcome
    b. Any instrumentation function that is related to process safety, such as a critical alarm or a manually activated shutoff switch
    c. A programmable logic controller that is dedicated to safety functionality
    d. An instrumented control system that detects "out of control" conditions and automatically returns the process to a safe state
2. Which of the following is the best definition of a safety instrumented function?
    a. All the safety functionality contained in a safety instrumented system
    b. A function that is implemented by an SIS that is intended to achieve or maintain a safe state for a process with respect to a specific hazardous event
    c. A safety certified instrument
    d. All basic process control loops whose failure could result in a safety consequence
3. Most national regulations for process safety require which of the following as a means to achieve functional safety of SIS?
    a. Adherence to Recognized and Generally Accepted Good Engineering Practice
    b. Use of third party certified equipment and engineering resources
    c. Development of prescriptive procedures by each individual operating company with submittal of the procedures for licensure
    d. Most regulations for process safety do not consider functional safety of SIS
4. Which of the following is a causal factor where poor SIS design resulted in, or contributed to a process safety incident?
    a. Improper isolation procedures were used to isolate pipe segments prior to welding
    b. Poor permitting procedures resulted in sources of ignition in an area where flammable materials were stored
    c. Poor basis for when safety should be automated as opposed to allowing operator actions as the sole means of safeguarding
    d. Failure to measure oxygen concentration before entry into a confined space.
5. In accordance to IEC 61511, how must verification that a safety integrity level has been achieved by performed?
    a. Qualitatively
    b. Quantitatively

QUIZ

   c. Using third party certifications
   d. Using standard design guidebooks
6. Which of the following activities, as defined in the IEC 61511 safety lifecycle, occurs throughout the entire lifecycle of a SIS?
   a. Hazard and Risk Assessment
   b. Safety Requirements Specification
   c. Operation and Maintenance
   d. Management of Functional Safety and Functional Safety Assessment and Auditing
7. Which range of average probability of failure on demand corresponds to SIL 1?
   a. 1% to 10%
   b. 0.1% to 1%
   c. 0.01% to 0.1%
   d. 0.001% to 0.01%
8. Which of the following is not an independent protection layer?
   a. Preventive Maintenance
   b. Operator Intervention Based on Alarms
   c. Relief Valves
   d. Check Valves
9. Which of the following is the best description of Target Maximum Event Likelihood?
   a. The maximum frequency at which an SIS should be activated
   b. The maximum frequency of failure on non-SIS safeguards
   c. The maximum frequency at which a control system failure can occur
   d. The maximum frequency at which an event of a given consequence magnitude is tolerable
10. Which of the following items can most appropriately be described in a safety requirements specifications general note?
   a. Process safety time for a SIF
   b. Sensor measurement set point
   c. Philosophy for separation of basic process control and safety control
   d. Valves that are closed when a process switch indicates an out of control condition
11. Which is the most common form of logic description in safety requirements specifications?
   a. Text Narrative
   b. Cause-and-Effect Diagrams
   c. Sequential Function Charts
   d. Binary Logic Diagrams

Section 4 – Quiz

12. Achievement of higher SIL levels (2 and 3) often require some degree of tolerance to dangerous failures which is provided by more advanced voting schemes like 1oo2 or 2oo3 voting.
    a. True
    b. False
    c. Not discussed in the IEC 61511 standard
    d. Not application to safety instrumented systems
13. More frequent testing results in lower average probability of failure on demand and higher achieved SIL because?
    a. Better maintained instruments fail less frequently
    b. The average amount of time that a device is in the failed state decreases
    c. Improved auditing results in less scrutiny from regulatory agencies
    d. When a device is bypassed in order to allow a test to occur it is not capable of causing a spurious shutdown
14. If a SIS instrument is bypassed for any reason, and that device is the sole means of bringing the process to a safe state if the SIF were to be activated by a process loss-of-control (i.e., no redundancy), what documentation needs to be prepared in order to allow the process to operate safely while the device is bypassed?
    a. Bypass Risk Assessment
    b. Management of Change
    c. Alternate Protection Plan
    d. Bypass Authorization Form
15. What is the most critical attribute of a proof test of an SIS component?
    a. Any known dangerous failure mode that is undetectable by automatic diagnostics would be detected
    b. The test is executed in the presence of the equipment vendor
    c. The test procedure is provided by a SIL certified equipment vendor
    d. The test uses automated tools that are connected to a computerized maintenance management system (CMMS)

QUIZ

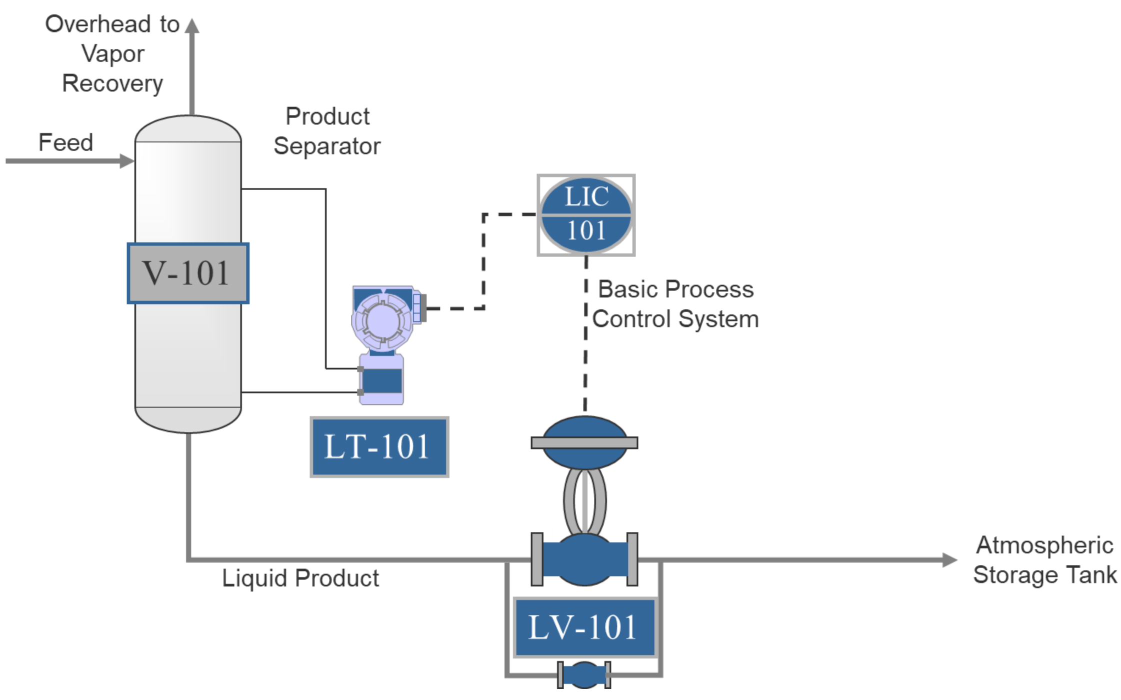
Section 5 – Application Exercise and Quiz Solutions

Application Exercise #1 - Solution

Application exercise #1 asks for the development of a "standard" SIS design for a low-level shutdown to be employed on a separate to prevent a gas blow-by hazard in downstream equipment that is not rated for the higher pressures. The problem is particularly difficult because there is no such thing as a standard design, and as a result there are an unlimited number of designs that could provide some degree of safeguarding against this hazard. Selection of the most appropriate design requires risk analysis and reliability engineering to determine what performance for an SIS is required, and what performance can any particular design achieve. Some of the potential options are shown below.

Option #1 – Do Nothing

A very valid option is to do nothing because the risk associated with the hazard may not warrant any additional safeguarding. The figure below could also represent the simple addition of a DCS alarm on the existing control loop.

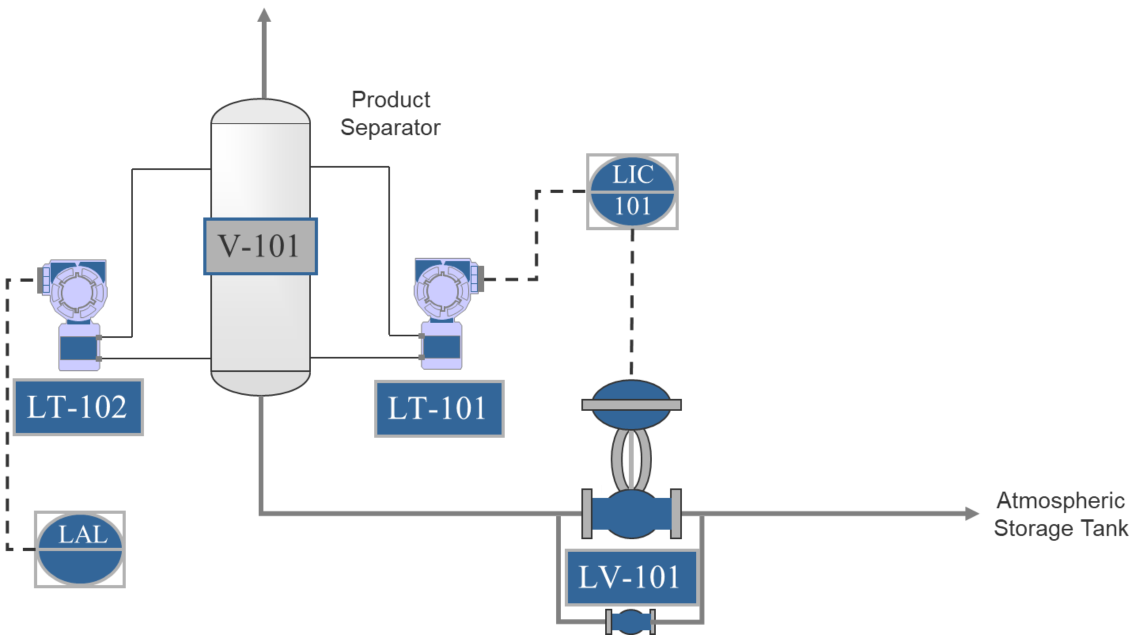


EXERCISE/QUIZ SOLUTIONS

Section 5 – Application Exercise and Quiz Solutions

Option #2 – Independent Alarm

The second option provides the hardware that allow for an operator intervention protection layer because the alarm will be physically and functionally separate from the DCS.

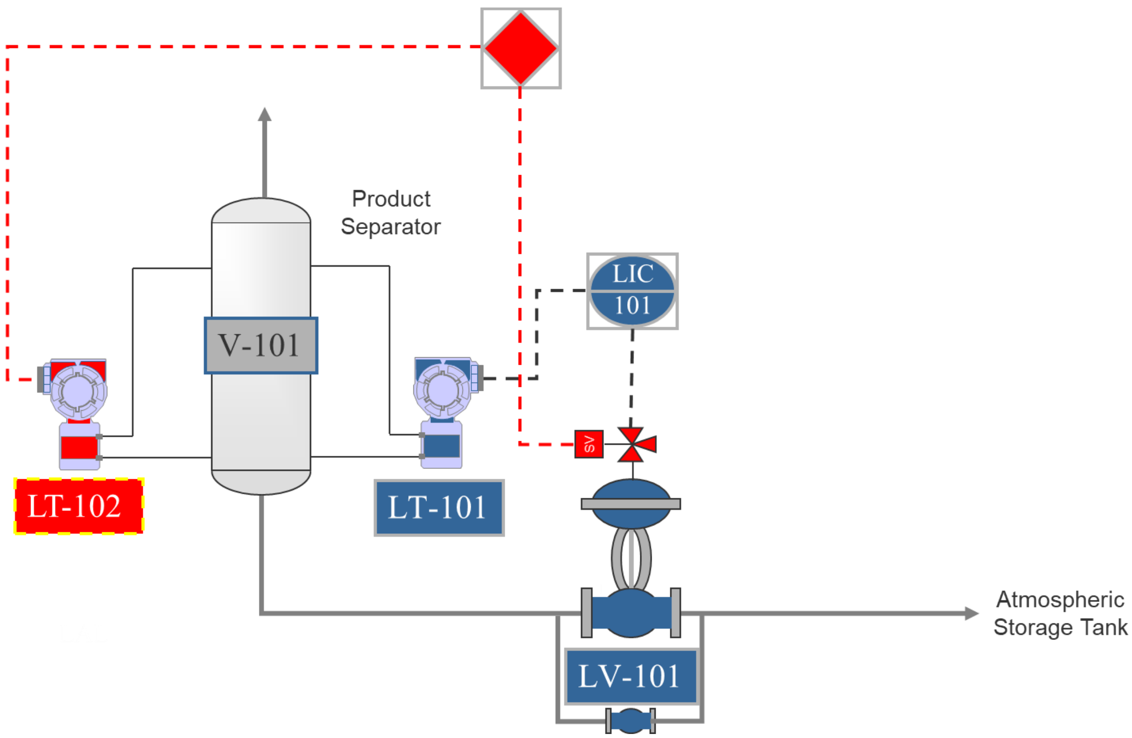


EXERCISE/QUIZ SOLUTIONS

Section 5 – Application Exercise and Quiz Solutions

Option #3 – SIF with Shared Final Element

The third option is the first option that provides an automatic action, a complete SIF. In this case, in order to minimize costs, the same valve that is used for the basic process control loop is used for the SIF.

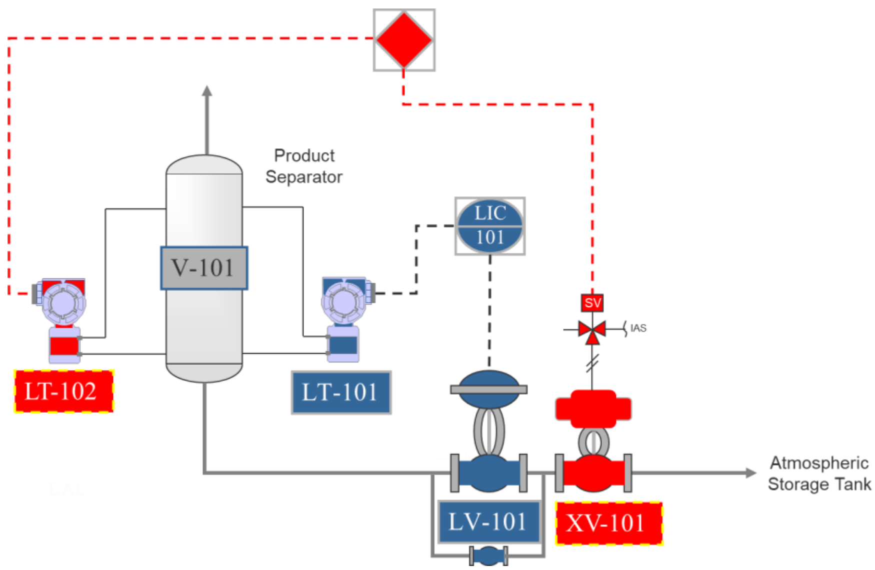


Section 5 – Application Exercise and Quiz Solutions

EXERCISE/QUIZ SOLUTIONS

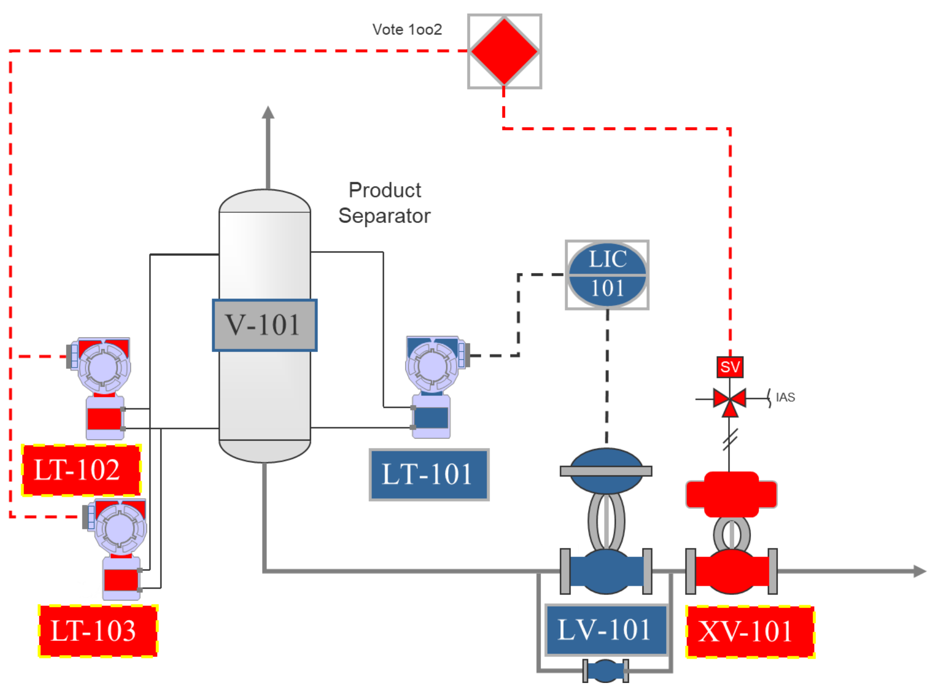
Option #4 – Complete Independent SIF – No Redundancy

Option #4 presents a complete SIF, but this SIF design includes no redundancy.



Option #5 – Complete Independent SIF – Sensor Redundancy

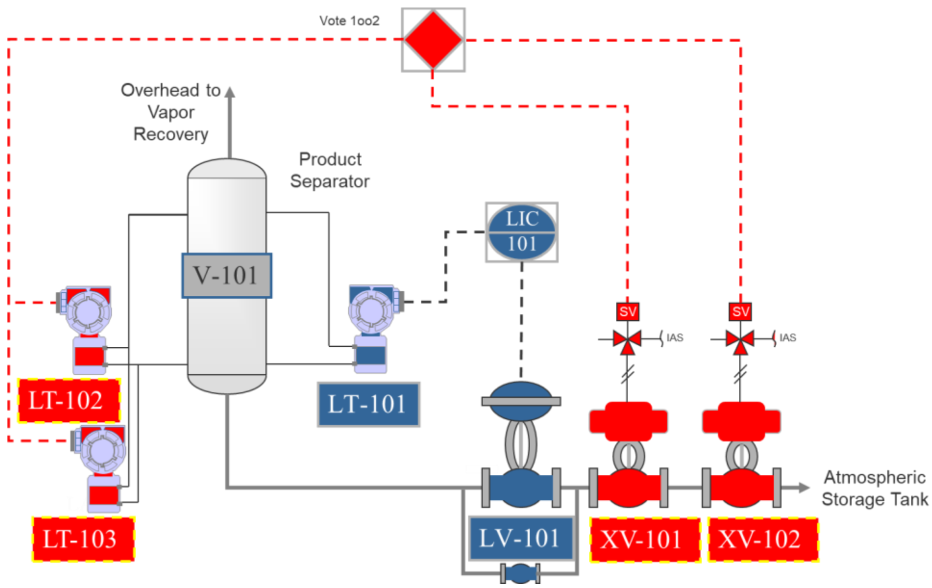
Option #5 is a complete SIF that provides sensor redundancy to improve safety.



Section 5 – Application Exercise and Quiz Solutions

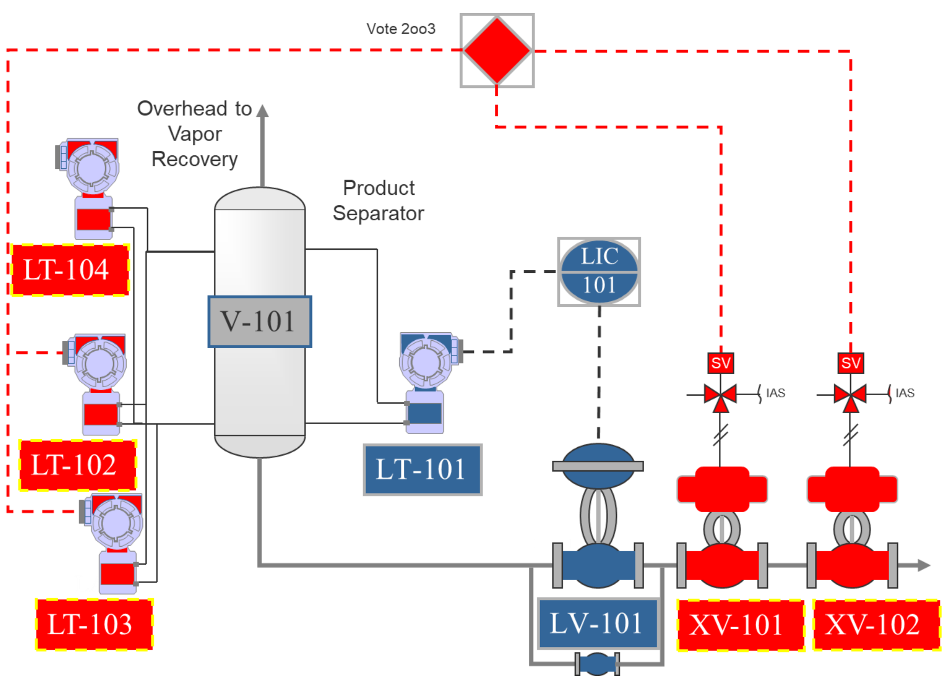
Option #6 – Complete SIF – Sensor and Valve Redundancy

Option #6 is a complete SIF that provides sensor and final element redundancy to improve safety.



Option #7 –Redundancy for Safety and Nuisance Trip Avoidance

Option #7 is a SIF that includes sensor redundancy to improve safety and avoid spurious trips.

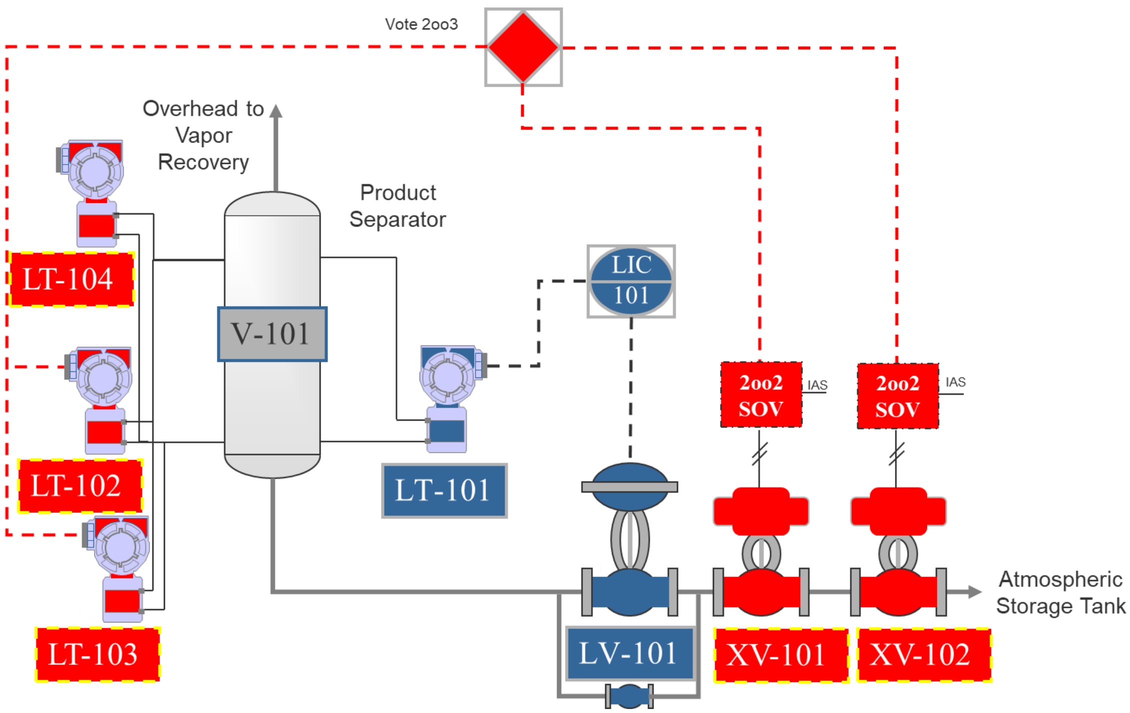


EXERCISE/QUIZ SOLUTIONS

Section 5 – Application Exercise and Quiz Solutions

Option #8 –Solenoid Valve Redundancy for Spurious Trip Avoidance

Option #8 extends Option #7 to include additional redundancy for the avoidance of nuisance shutdowns of the final element subsystem.



All of the design presented above, and many more, could meet the objective of reducing the risk posed by a low-level scenario. The most appropriate design, however, is not standard, and can only be determined using performance based methods such as the ones presented in the IEC 61511 standard.

Post Instructional Quiz Solution

1. Which of the following is the best definition of a Safety Instrumented System?

   <u>(d)</u> An instrumented control system that detects "out of control" conditions and automatically returns the process to a safe state

2. Which of the following is the best definition of a safety instrumented function?

   <u>(b)</u> A function that is implemented by an SIS that is intended to achieve or maintain a safe state for a process with respect to a specific hazardous event

Section 5 – Application Exercise and Quiz Solutions

EXERCISE/QUIZ SOLUTIONS

3. Most national regulations for process safety require which of the following as a means to achieve functional safety of SIS?

   (a) Adherence to Recognized and Generally Accepted Good Engineering Practice

4. Which of the following is a causal factor where poor SIS design resulted in, or contributed to a process safety incident?

   (c) Poor basis for when safety should be automated as opposed to allowing operator actions as the sole means of safeguarding

5. In accordance to IEC 61511, how must verification that a safety integrity level has been achieved by performed?

   (b) Quantitatively

6. Which of the following activities, as defined in the IEC 61511 safety lifecycle, occurs throughout the entire lifecycle of a SIS?

   (d) Management of Functional Safety and Functional Safety Assessment and Auditing

7. Which range of average probability of failure on demand corresponds to SIL 1?

   (a) 1% to 10%

8. Which of the following is not an independent protection layer?

   (a) Preventive Maintenance

9. Which of the following is the best description of Target Maximum Event Likelihood?

   (d) The maximum frequency at which an event of a given consequence magnitude is tolerable

10. Which of the following items can most appropriately be described in a safety requirements specifications general note?

    (c) Philosophy for separation of basic process control and safety control

Section 5 – Application Exercise and Quiz Solutions

EXERCISE/QUIZ SOLUTIONS

11. Which is the most common form of logic description in safety requirements specifications?

    (b) Cause-and-Effect Diagrams

12. Achievement of higher SIL levels (2 and 3) often require some degree of tolerance to dangerous failures which is provided by more advanced voting schemes like 1oo2 or 2oo3 voting.

    (a) True

13. More frequent testing results in lower average probability of failure on demand and higher achieved SIL because?

    (b) The average amount of time that a device is in the failed state decreases

14. If a SIS instrument is bypassed for any reason, and that device is the sole means of bringing the process to a safe state if the SIF were to be activated by a process loss-of-control (i.e., no redundancy), what documentation needs to be prepared to allow the process to operate safely while the device is bypassed?

    (c) Alternate Protection Plan

15. What is the most critical attribute of a proof test of an SIS component?

    (a) Any known dangerous failure mode that is undetectable by automatic diagnostics would be detected