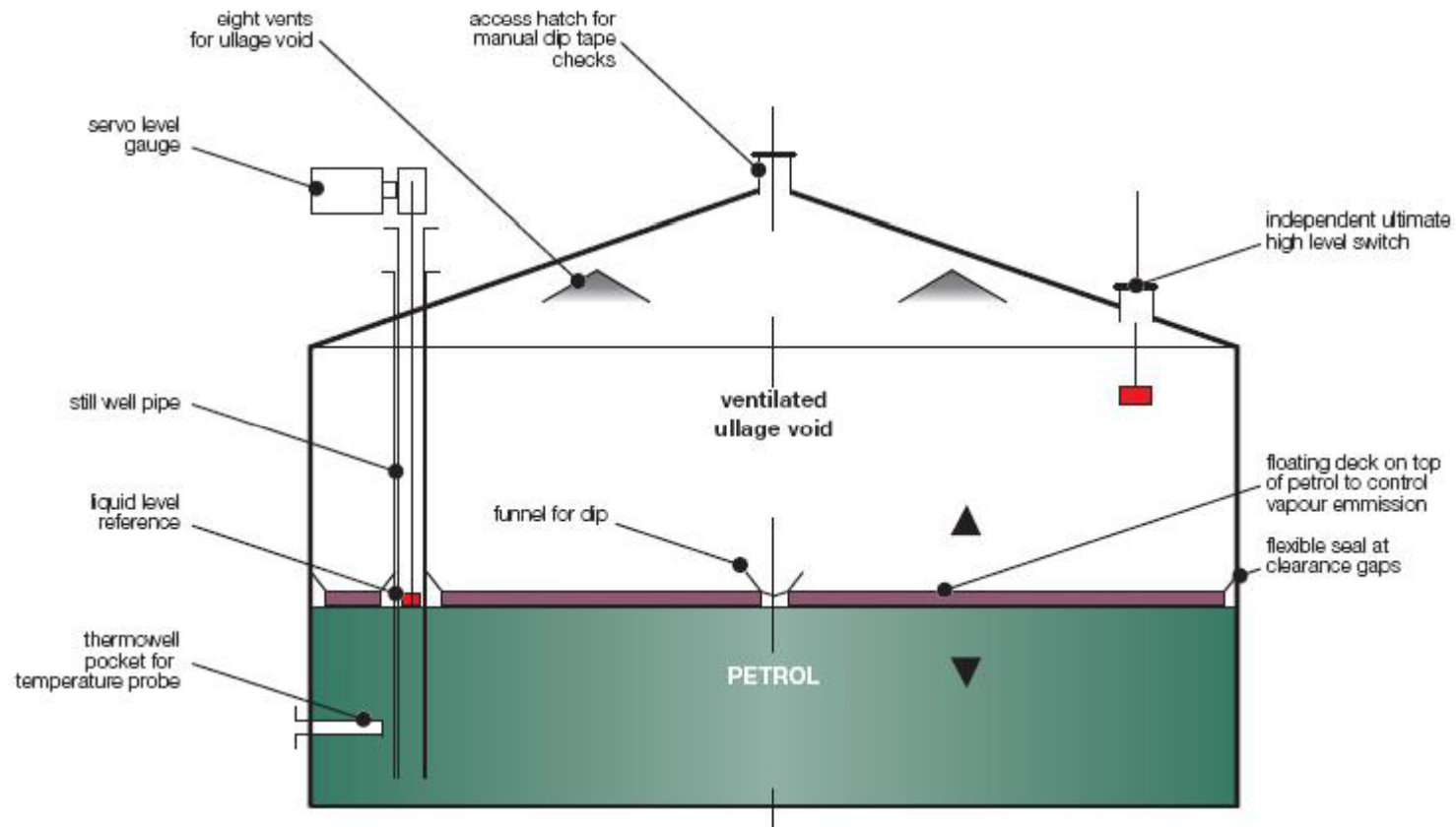


# SIS Design Basis Program For Tank Overfill Protection Systems



# Presenter Introduction

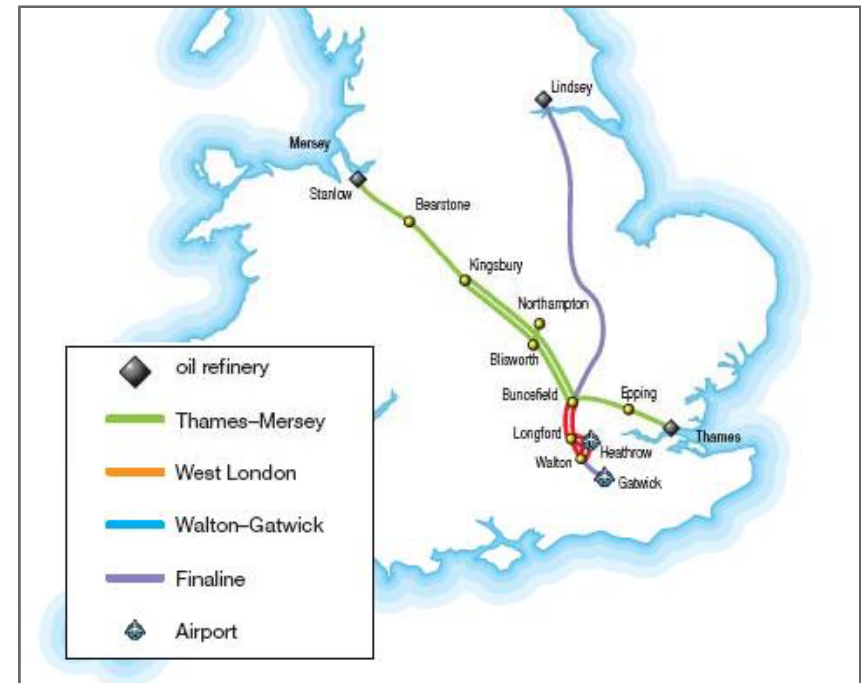


- Edward M. Marszal, PE, CFSE
- President, Kenexis
- 17 Years Experience
- ISA Author “SIL Selection”
- ISA Committees - S84, S91, S18
- ISA Safety Division Director
- ISA, AIChE, NFPA Member
- BSCHE, Ohio State University



# Buncefield Background

- Major pipeline transfer crossroad
- 5<sup>th</sup> largest fuel storage depot in UK
- 40km north of London



Source: Buncefield Final Report



# Local Incident Effects

- 43 injuries
- 2,000 evacuated
- Damage estimate:  
*£*1 billion



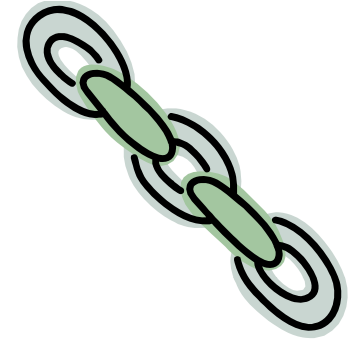
Source: Buncefield Final Report





# Timeline Overview

- Initiating event:
  - Misoperation during loading
- Propagating events/conditions:
  - Poor administrative controls
  - Failure of primary level & alarm
  - Failure of operations to recognize
  - Failure of safety system to act
  - Poor maintenance practices





# MIIB Board Recommendations

- Intended for “Buncefield-type” sites
- 78 Recommendations in 5 key areas
  - Off-site hazard mitigation
  - Emergency response preparedness
  - Land use planning
  - Regulation for inspection enforcement
  - Risk-based application of prevention measures



# IEC-61511 Application

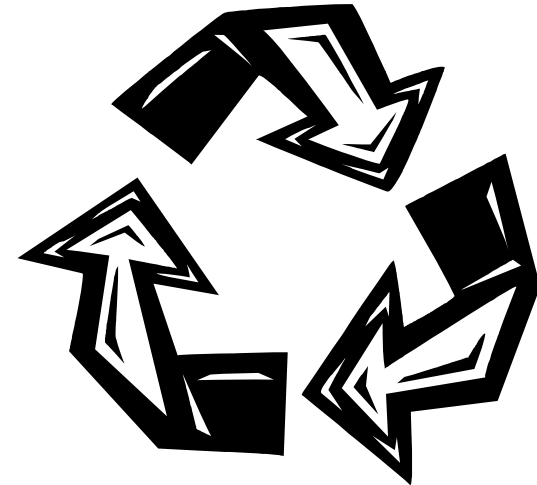
- Recommendations 1-5 directly or indirectly references IEC-61511
  - Select a SIL using its methodology
  - Verify OPS (new/existing) achieves SIL
  - Design OPS using its methodology
  - Proof test per its methodology
  - Procedures for maintenance and testing, keep test records





# 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





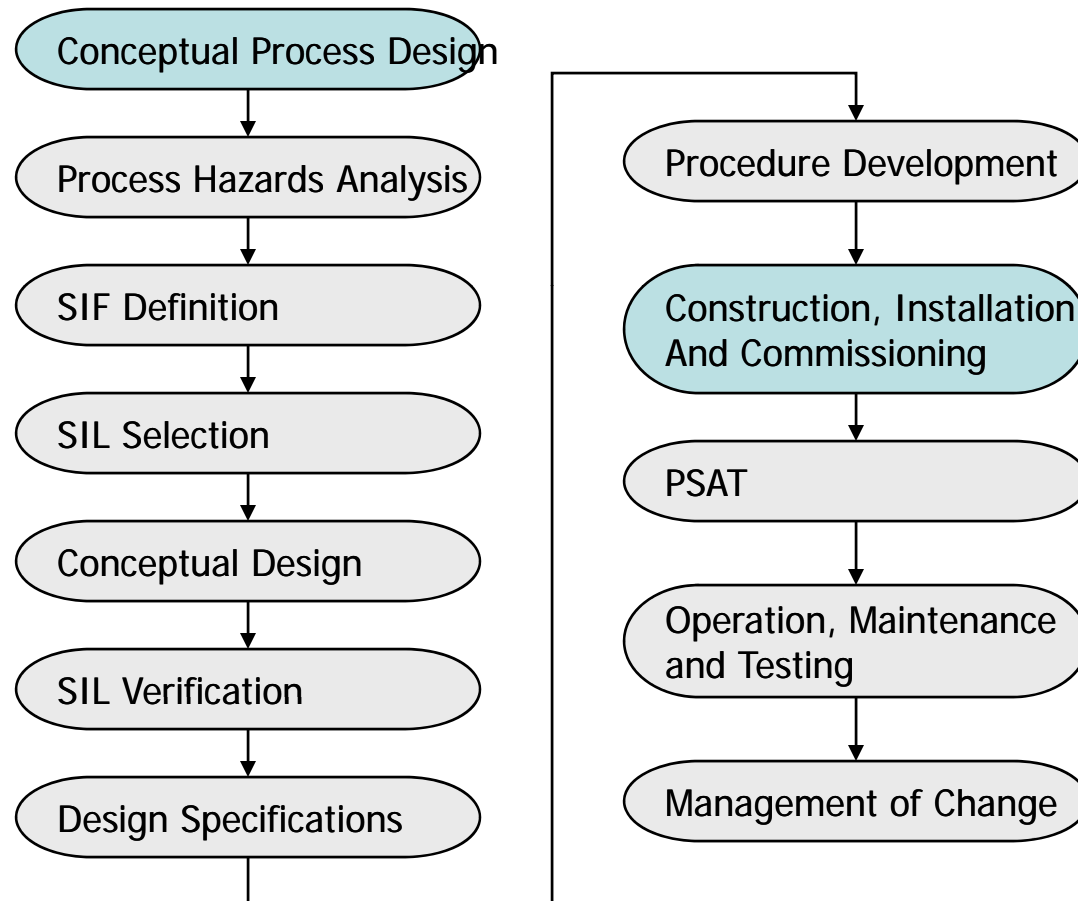
# What does IEC 61511 require?

- Performance based
- Defines a “safety lifecycle”
- Requires selection of performance target
- Requires confirmation of target achievement, quantitatively



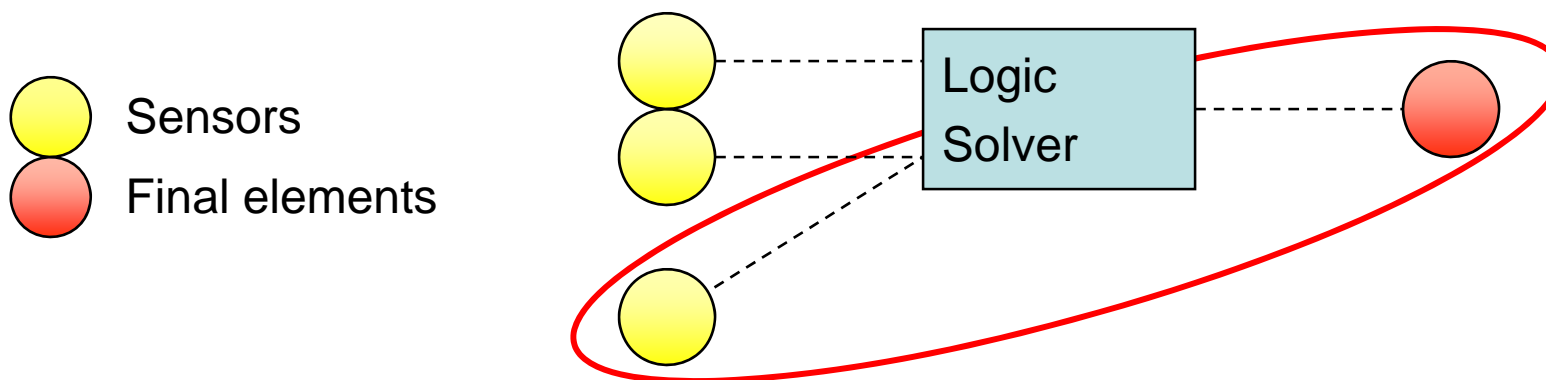


# Typical SIS design lifecycle



# Safety Instrumented Function – Practical Definition

- Safety Instrumented Function(SIF) is
  - Specific actions to be taken under specific circumstances, which will automatically move the process from a potentially unsafe state to a safe state



# What is a Safety Integrity Level (SIL)?

A measure of the amount of risk reduction provided by a Safety Instrumented Function (SIF)

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



# How do I assign SIL?



“What is the Safety Integrity Level for my Safety Function ?”



Assign SIL that reduces risk to tolerable level

- Numerous techniques
  - Layer of Protection Analysis
  - Risk Graph
  - Quantitative
  - Others
- Be consistent!





# LOPA Application - Qualitative

- Use *Risk Matrix* calibrated to company risk management guidelines
- Qualitative LOPA
  - Qualitative Consequence Analysis
  - Qualitative Likelihood Analysis
  - Determine Required Number of orders of Magnitude Risk Reduction (= number of IPLs)
  - Determine existing number of IPLs
  - SIL level covers remaining gap, if any





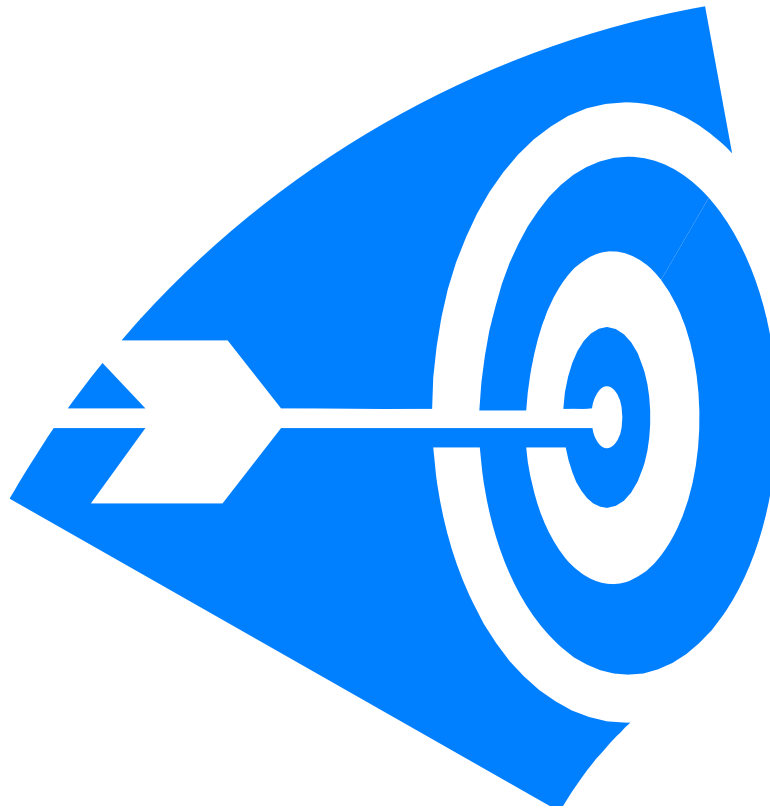
# LOPA Application - Quantitative

- Quantitative LOPA
  - Identify Risk Tolerance Level
  - Quantitative Analysis of Initiating Event Frequency
  - Determine Required Risk Reduction Factor
- Spreadsheet uses Quantitative LOPA for analysis
  - Can be adapted for Qualitative LOPA





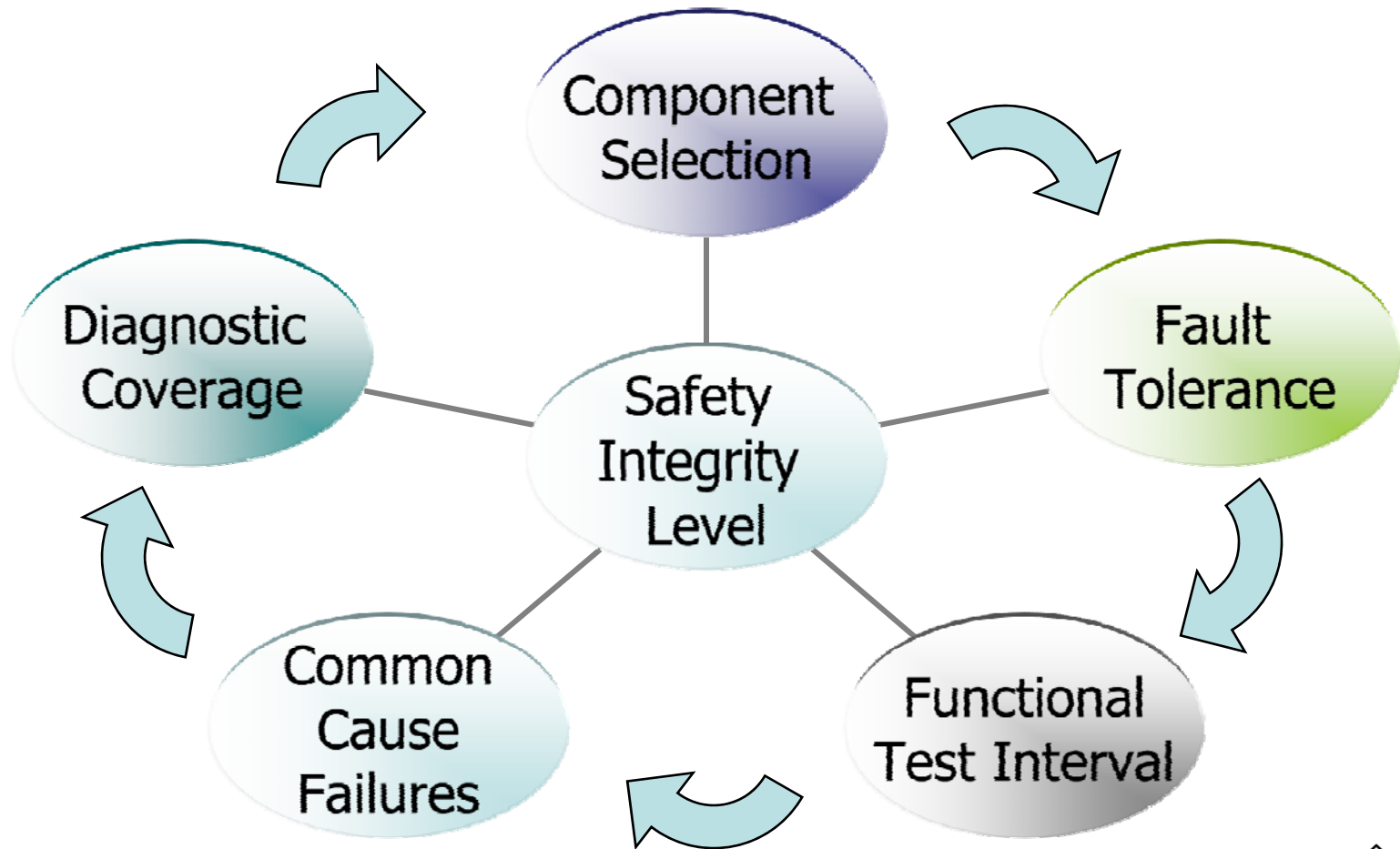
# SIL Verification



- Purpose is to quantitatively verify selected equipment and testing meets requirements
- Uses reliability engineering calculations



# Parameters impacting SIL



# Safety Requirements Specifications

- Purpose
  - Select equipment appropriate for SIL
  - Specify how the system operates
  - Basis for detailed design
  - Basis for Managing Change
- Result
  - Logic Solver Functional Specification (a.k.a, safety requirements specifications)



# Test Plans

- One for each SIF
- Describes each step taken
- Matches PFD calculations
- Takes into account startup resources
  - Personnel
  - Equipment
  - Time



# SIL Selection Spreadsheet

- Assists in SIL Selection
- Excel-based
- Contains some basic SIL calculations in IEC-61511 Technical Report
- Contains some common level sensors and their “generic” failure rate





# Responsibilities/Obligations

- User must select a proper team
  - Operations, I&E, Manager, Specialists
- User must read this presentation and the in-spreadsheet notes
- User **MUST** verify **ALL** failure rate data entered for SIL verification





# Uses of the Spreadsheet

- For facilities new to SIL selection
  - Supports Safety Lifecycle
- Training tool
- Simple storage tank shutdown systems
- Flexible: can add instrumentation





# Abuses of the Spreadsheet

- Does NOT handle complex SIFs (multiple interactions)
- Is NOT for complex initiating events with complex protection layers
- Does NOT take into account benefits of diagnostic coverage
- Higher than SIL 2 – consult specialist



# Spreadsheet Example



# SIL Selection Overview

1. Provide background, hazard and consequence description
2. Provide Initiating Events (IE) and Independent Protection Layers (IPL)
3. Check SIL Level



# Step 1: Background

- SIF Description
  - Only include “minimum necessary and sufficient” actions
- Hazard Prevented
  - From high level, follow hazard evolution. Don’t account for protection
- Consequence
  - Describe hazard impact to receptors



# Example Background

**STEP 1: Provide Safety Function background, Hazard Prevented, Consequence and TMEL:**

Service:	Tank #219, West Facility
Provide Safety Instrumented Function (SIF) Description:	High-High Storage Tank Level closes tank inlet valve
Hazard Prevented:	High-high tank level could result in overfilling of tank with petrol, which could result in loss of containment. Loss of containment with continued filling could result in large cloud of flammables, which if ignited could result in fire or explosion.
Consequence:	Fire or explosion could result in multiple injuries to on-site and possibly off-site personnel.
Consequence Rating:	<b>High (potential life-threatening injury)</b>



# Step 1: Background

- Provide TMEL Equivalent
  - TMEL = Target Max Event Likelihood
- TMEL for Unmitigated Event
- Consider corporate practices
- Consider industry practices
  - For single life-threatening injury events  
 $1 \times 10^{-5}$  to  $1 \times 10^{-6}$  annual likelihoods



# Example TMEL

TMEL Equivalent, per year:	0.00001
Event period ( $=1/\text{TMEL}$ ), years:	100,000





# Step 2: Initiating Events

- Enter up to 3 Initiating Events (IE)
- Assign a frequency for each IE
- IEC-61511:
  - BPCS malfunction 1/10 year freq
- Common industry practice:
  - Operator error rate once per 100 to 1,000 opportunities





# Example IE Frequency

- Operations loads a tank once every 3 days (100 times per year)
- 1/1000 chance of incorrectly executing procedure

IE Frequency =  $100 * 1/1000 = 1/10$  years

- Is this rate consistent with reality?



# Example Initiating Event

## STEP 2: Initiating Events and Protection Layers

### Initiating Event #1:

Description	Operator error during filling process (wrong setpoint)
Frequency	<b>Medium (once per ten years)</b>
Frequency, in years	0.1



# Step 2: Independent Protection Layers (IPLs)

- Enter IPLs for each IE
  - BPCS
  - Operator Intervention
  - Other
  - Occupancy
- Spreadsheet populates commonly used risk reduction factor (IPL RRF)



# Requirements of an IPL

- Independent Protection Layers (IPL) are limited to safeguards having the following characteristics
  - Specificity
    - Specifically designed to prevent the Hazard Identified
  - Independence
    - From cause (initiating event)
    - No shared equipment between IPLs
  - Dependability
    - Provides at least one order of magnitude risk reduction
  - Auditability
    - Can be tracked / measured



# Typical IPL “Rules of the Road”

- IPLs DON’T prevent initiating event from occurring
- IPLs DO function once the initiating event has already occurred
- IPLS MUST Completely Prevent Hazard
- DON’T use training or preventative maintenance as an IPL



# Typical IPL “Rules of the Road”

- If a BPCS control loop failure was the initiating event, don’t use equipment from a BPCS Loop that failed to justify credit for an IPL
- DON’T take credit for an operator more than once
- DON’T identify the SIS for more than one IPL



# Commonly used IPLs

- Operator Intervention
  - Annunciated alarm
  - Continuously manned location
  - Proper training for response
  - Adequate Response time



# Example IPL

## Independent Protection Layer (IPL) for Initiating Event #1:

Description	IPL RRF	NOTES
Operator Intervention	10	
BPCS (Control Loop)	10	
Occupancy (<10%)	10	
Other	1	
None	1	



# Step 3: Check SIL of SIF

- SIF RRF Required is the sum of all IEs divided by the TMEL
- SIL Rating:
  - RRF 10-99 is SIL 1
  - RRF 100+ is SIL 2



# Example SIL

## STEP 3: Check Safety Integrity Level (SIL) of SIF

SIF RRF Required: **110**

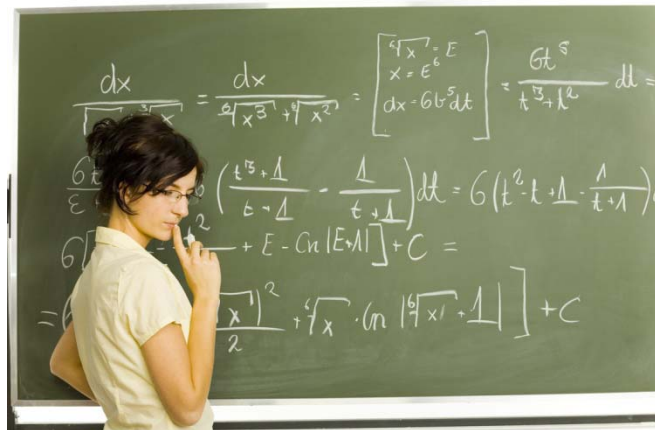
SIL Rating

**SIL 2**

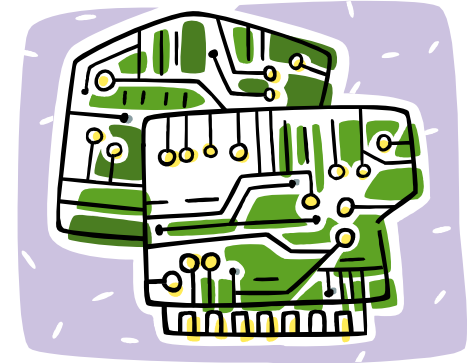


# SIL Verification Overview

1. Provide SIF info
  - Select Test Interval
2. Check RRF Required is satisfied



# Sensors



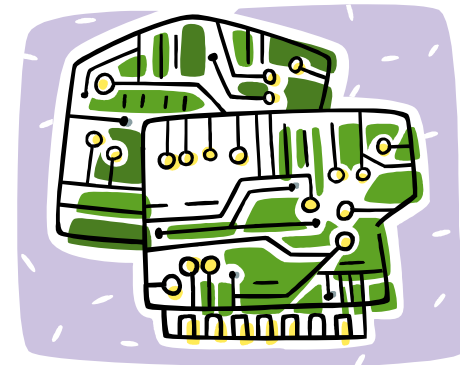
1. Float Switch
2. Mechanical Limit Switch
3. Generic Radar Transmitter
  - PLC Diagnostics Over/Under Range
4. Mechanical Servo Gauge
5. Custom





# Logic Solvers

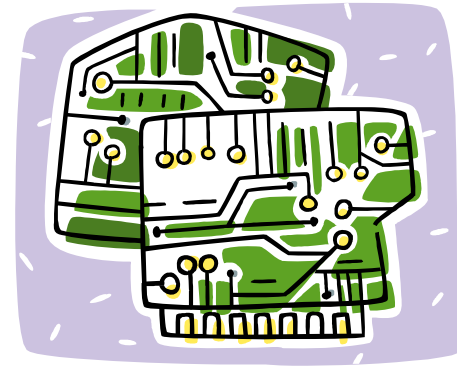
1. Non-SIS rated PLC (BPCS)
2. Relay
3. Relay with Trip Amp
4. SIL-3 PLC
5. Custom





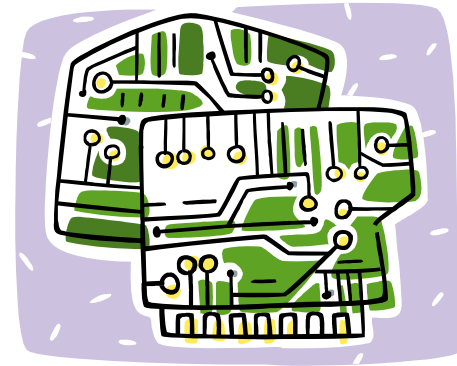
# Final Elements

1. Ball or Globe Valve
2. Control Valve
3. Motor Actuated Valve
4. Pump Motor Starter
5. Custom



# Final Element Interface


1. 3-way DTT solenoid valve
2. Interposing relay
3. Custom



# Do I Need New SIS Equipment?

- Designed/Manufactured per IEC-61508
- Proven in Use
  - ~5 yrs or more experience with components in similar service
  - Should provide maintenance data to support the PIU claim
  - Be prepared to replace-in-kind





# Other Parameters that affect SIL

- Architecture (Voting)
  - 1oo1, 2oo2, 1oo2, 2oo3
- Test Interval
  - Full functional test (sensor to final element)
  - No signal “forcing”



# Example Equipment Input

## STEP 1: SIF Hardware

	SENSOR	LOGIC SOLVER	FINAL ELEMENT (FE)	FE INTERFACE
Sensor tag	LAHH-69	Relay panel	XV-69	SV-69
Voting	1oo2	1oo1	1oo2	1oo2
Type	Generic Radar	Generic SIL-3 PLC	Generic Ball or Globe valve	Generic 3-way solenoid
Description	Generic radar, overrange and underrange PLC diagnostics, vote to trip on error	Generic SIL 3 Certified PLC, with diagnostics	Generic air actuated ball or globe valve, spring return, fail safe	Generic solenoid operated valve, 3- way, DTT
Failure Rate, dangerous undetected, per hr	5.00E-07	1.00E-08	1.35E-06	8.00E-07
Test Interval, years	1	1	1	1
Max SIL Approved	2	3	2	2
Probability of Failure on Demand (PFD):	0.0002	0.0000	0.0006	0.0004





# Step 2: Verify Function Achieves IEC Requirements

- Is RRF achieved  $>$  RRF target?
- Is Sensor & FE Fault Tolerance met?
  - SIL 2: 2oo3 or 1oo2 Voting
  - Logic Solvers treated differently



# Example Check Function

**STEP 2: Check function meets SIL target**

	Achieved	Target
SIF PFD	0.0013	0.009
SIF RRF	785	110

Does Function meet RRF Required?	YES
Is Fault Tolerance Achieved?	YES



# What's Next?

- Print Out Spreadsheet & Report
- Safety Requirements Specification
- Test Plans
- Review Results with an Expert





# Conclusions/Overview

- Recent events make IEC-61511 necessary for Storage Tank Operators
- Spreadsheet a simple tool for simple situations
- Useful demo to understand the safety lifecycle
- The user must verify the tool is utilized correctly and the calculations are accurate!





# Thank You for Attending!

Edward M. Marszal

Kenexis Consulting Corporation  
2929 Kenny Road, Suite 225  
Columbus, OH, 43221  
USA  
(614) 451-7031  
<http://www.kenexis.com>

