Safety Instrumented Systems Appreciation Training

A series of presentations for managers, operators and maintainers of Installed Safety Instrumented Systems. Intended to provide awareness of the requirements of and compliance to IEC 61511.

David Ransome BA, CEng, FInstMC

Registered Functional Safety Engineer, RFSE

P & I Design Ltd - Chairman

P & I Design Ltd

2 Reed Street

Thornaby

TS17 7AF

01642 617444

http://www.pidesign.co.uk/

Safety Instrumented Systems Appreciation Training Part 1 – Why do we need SIS

David Ransome BA, CEng, FInstMC

Registered Functional Safety Engineer, RFSE

P & I Design Ltd - Chairman

Purpose!

This presentation is for managers, operators and maintainers.
It is intended to provide awareness of the requirements of installed Safety Instrumented Systems complying to IEC 61511.

Purpose!

This presentation gives an introduction to, and why we need **Safety Instrumented Systems** referred to as

SIS

Background!

11th December 2005
Buncefield, UK
Hertfordshire Oil Storage Depot

Vapour Formation

Background!

The Explosion!

Vapour Cloud Explosion

The Explosion!

Aftermath!

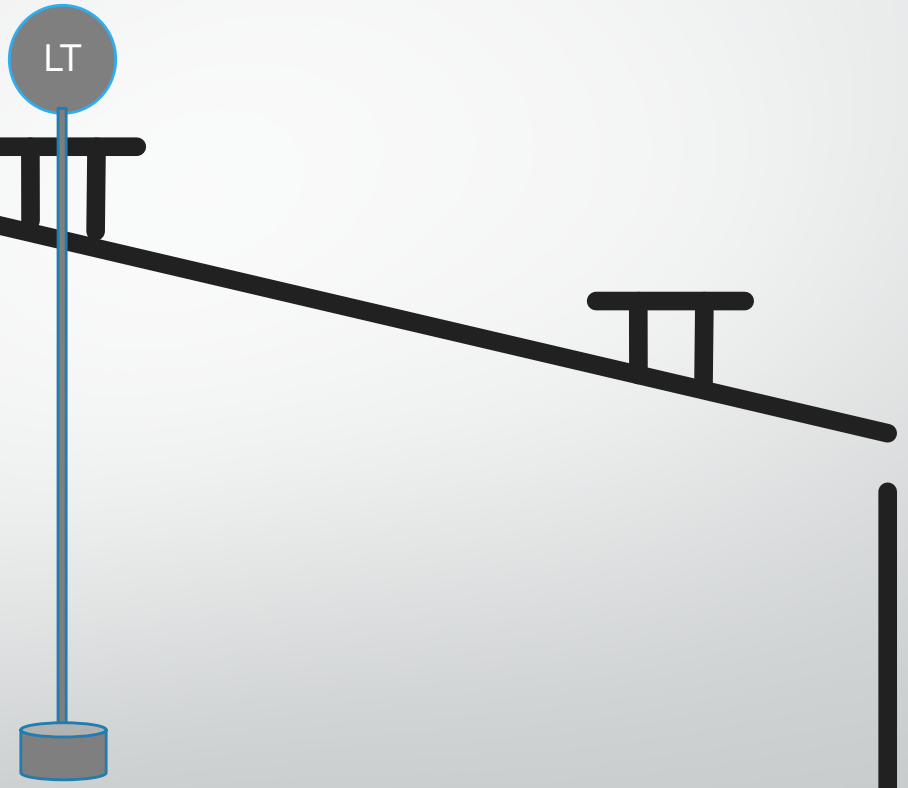
The Remains of HOSL and surrounding buildings

The Aftermath!

A closer look at what happened!

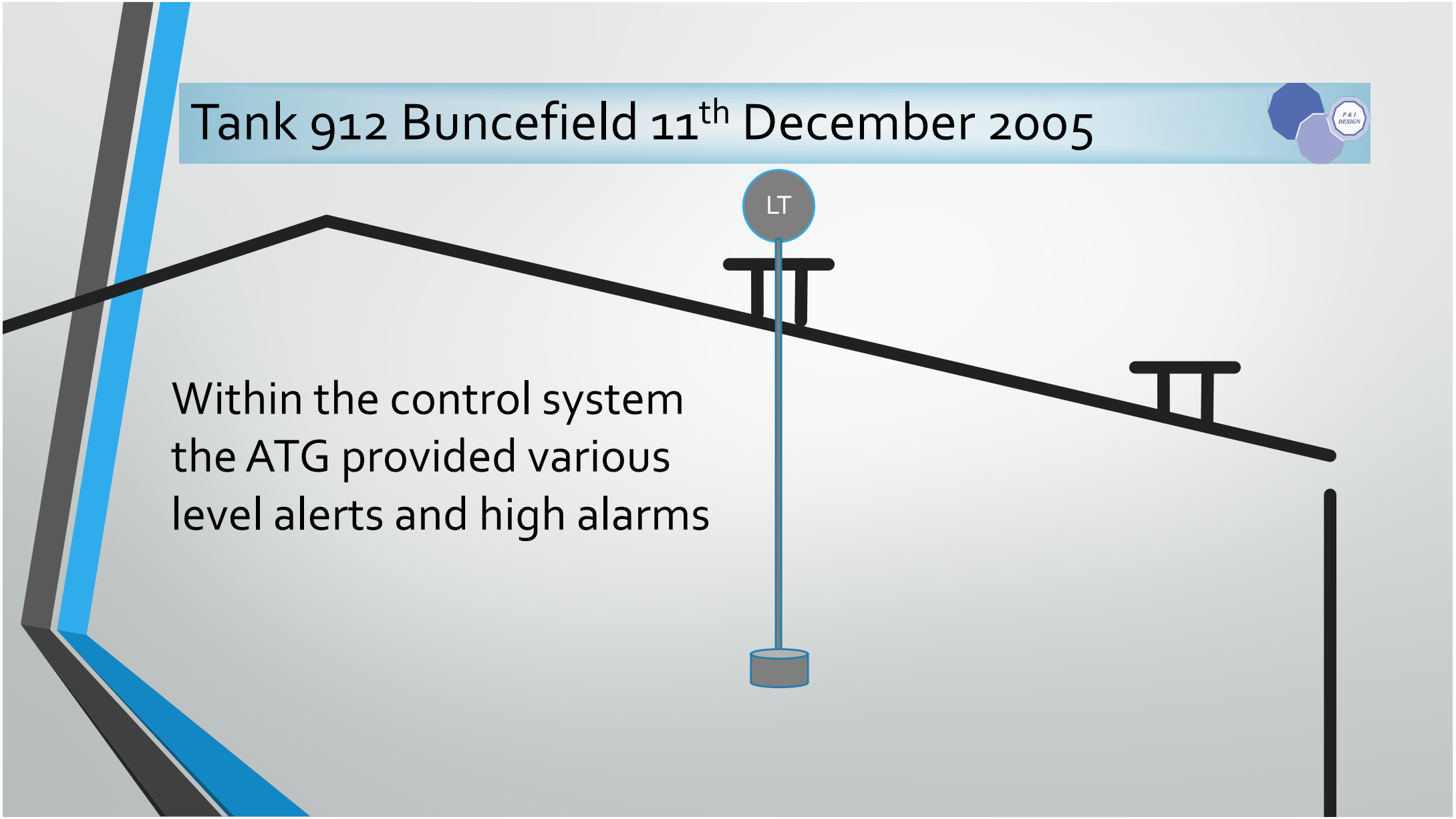
The following slides analyse how Tank 912 was overfilled leading to a massive explosion.

Tank 912 Buncefield 11th December 2005



The tank was fitted with a servo/displacer, automatic tank gauge (ATG) for measuring continuous movement of the level within the tank

Tank 912 Buncefield 11th December 2005

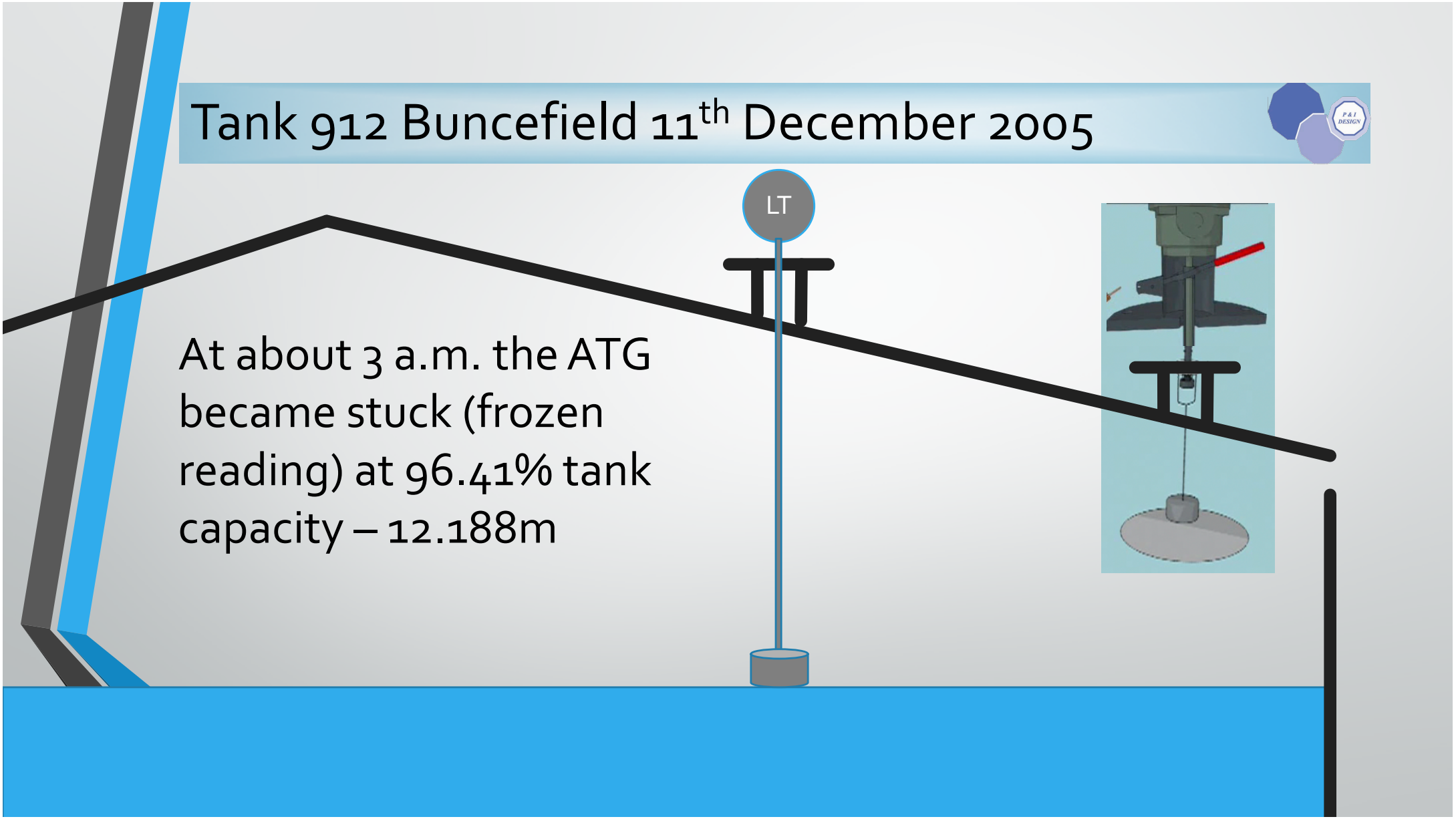


Within the control system the ATG provided various level alerts and high alarms

Tank 912 Buncefield 11th December 2005

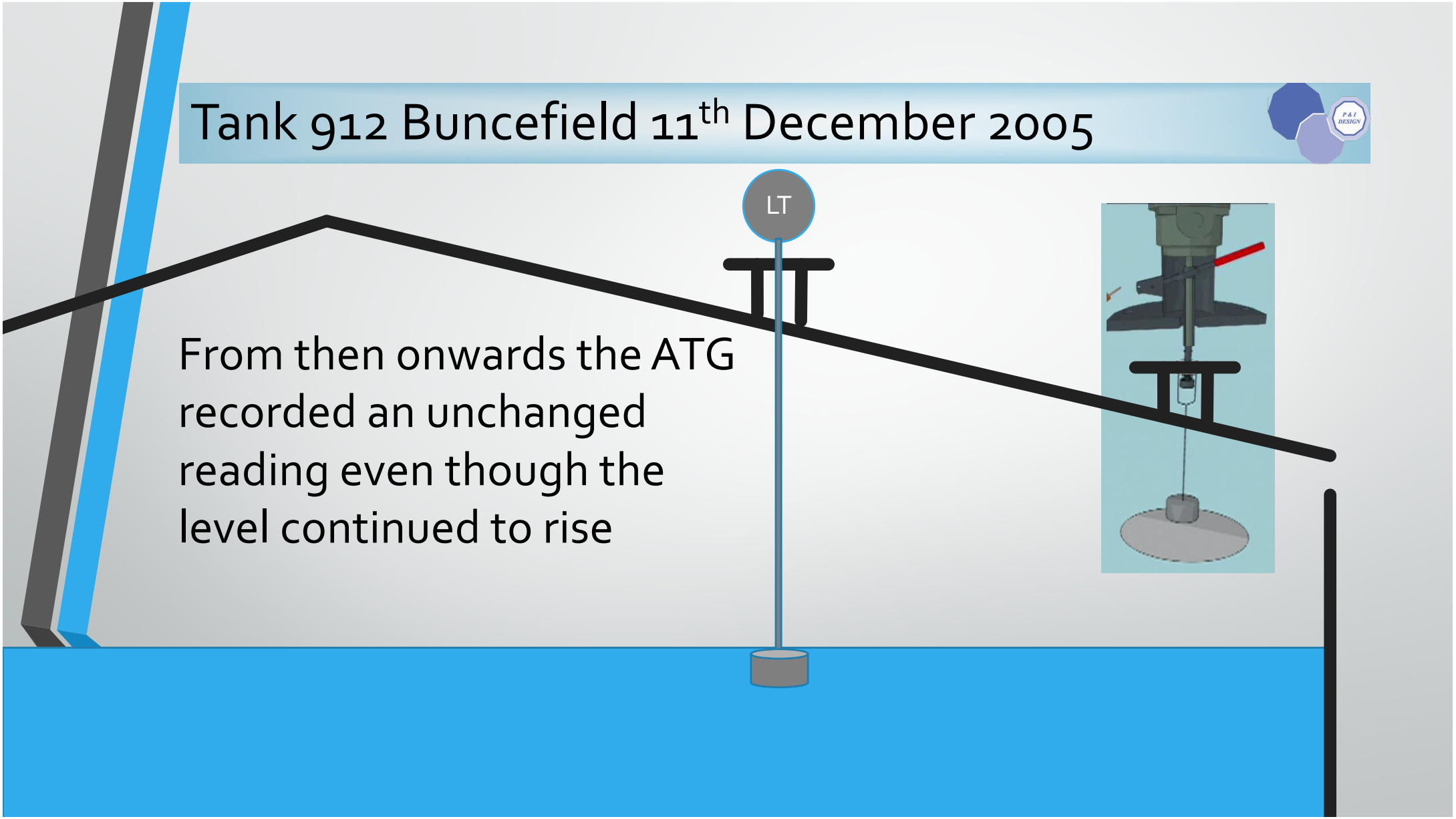
The tank was also fitted with an independent high level alarm (IHLA), which when operated would stop gasoline flow into the tank by closing the import valve.

Tank 912 Buncefield 11th December 2005



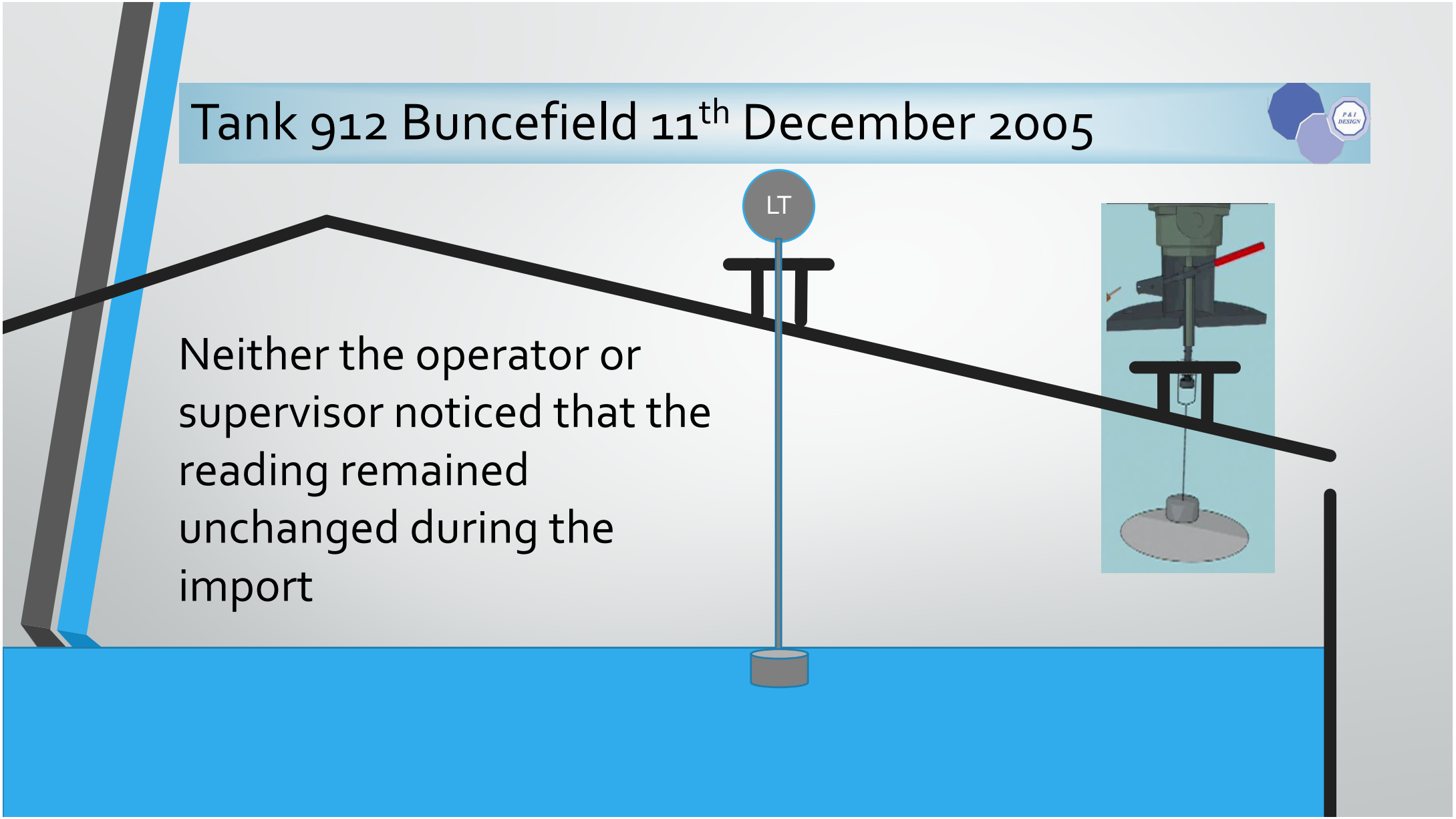
At about 3 a.m. the ATG became stuck (frozen reading) at 96.41% tank capacity – 12.188m

Tank 912 Buncefield 11th December 2005



From then onwards the ATG recorded an unchanged reading even though the level continued to rise

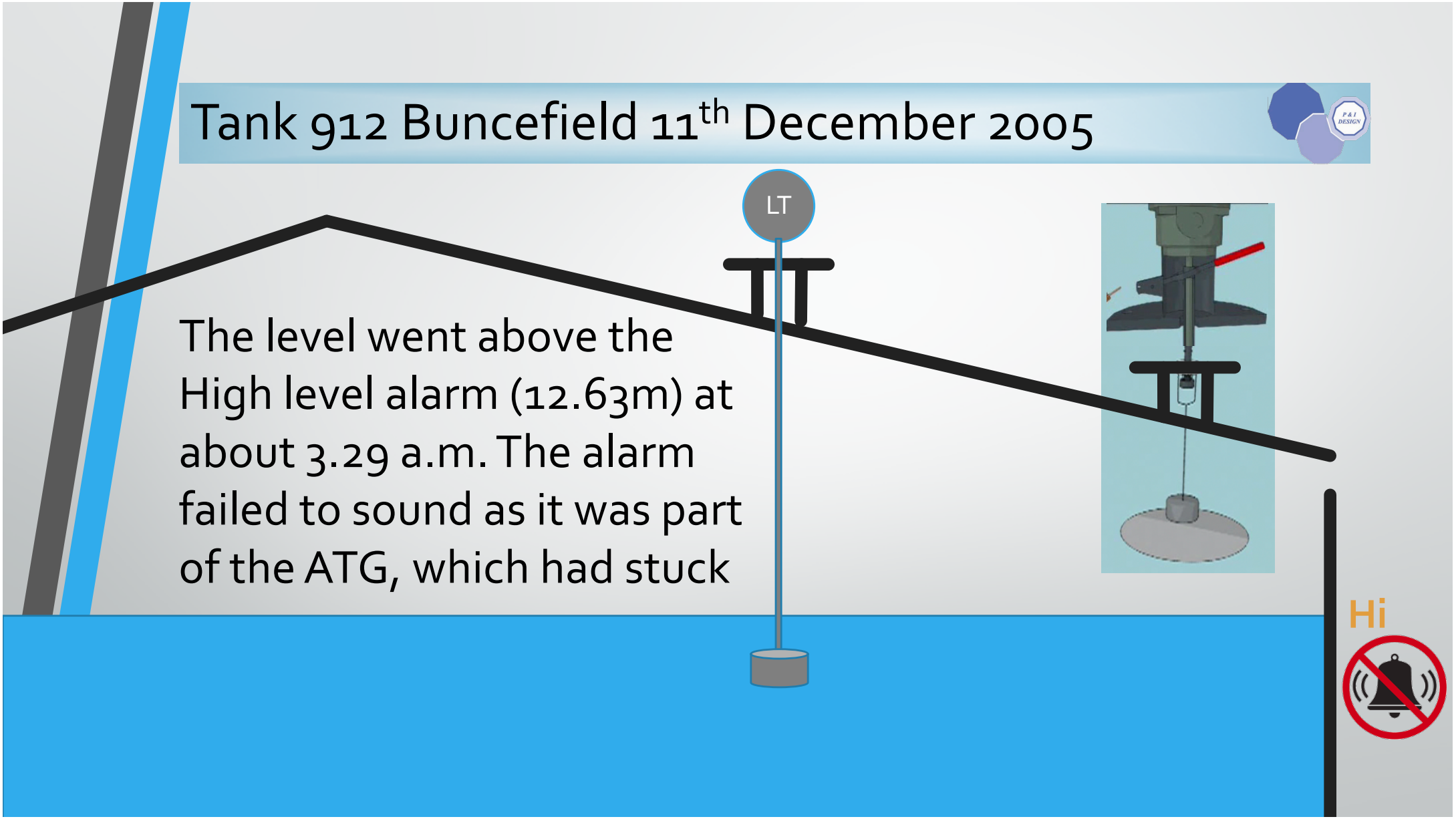
Tank 912 Buncefield 11th December 2005



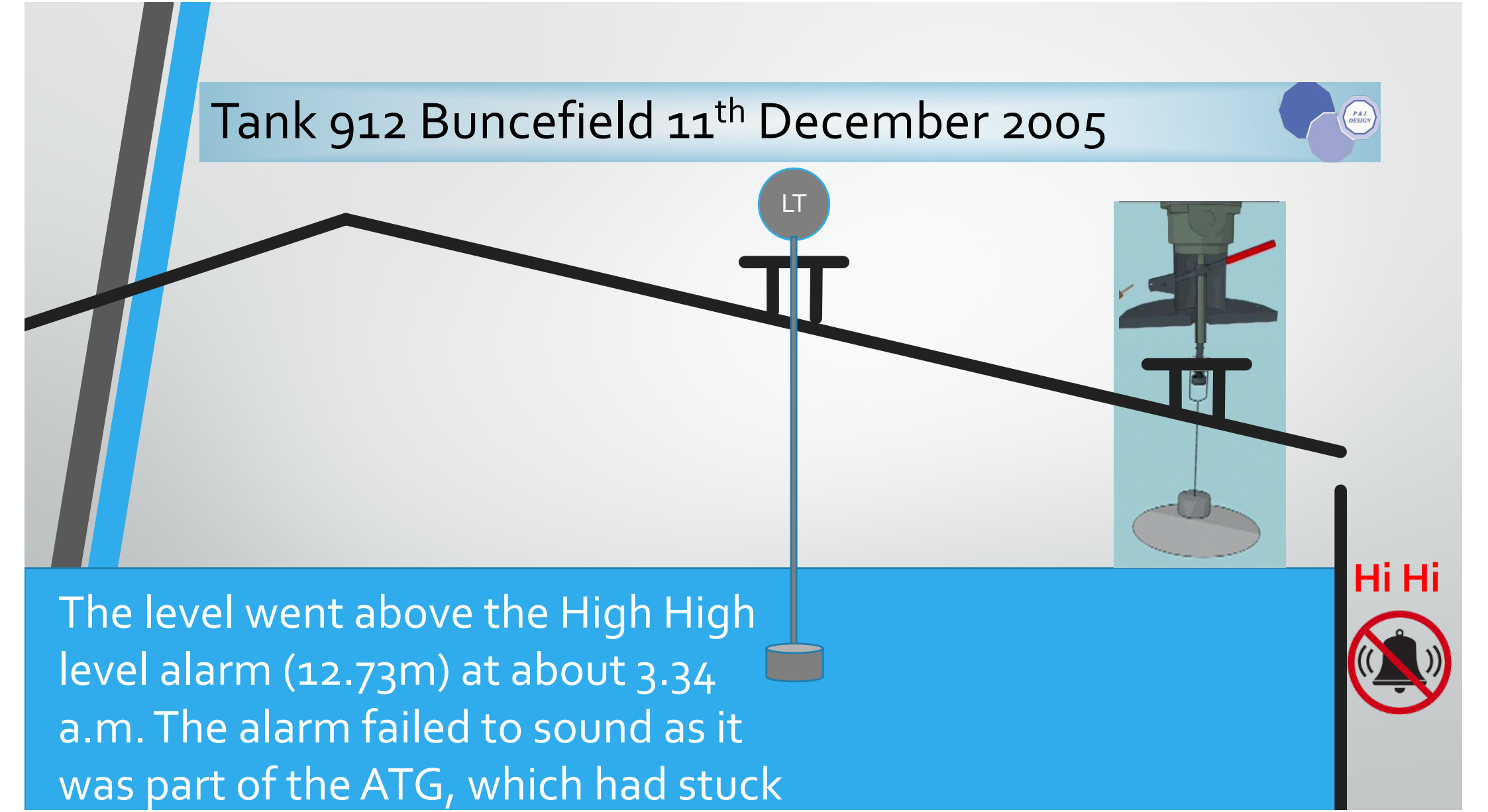
Neither the operator or supervisor noticed that the reading remained unchanged during the import

Tank 912 Buncefield 11th December 2005

The level went above the High level alarm (12.63m) at about 3.29 a.m. The alarm failed to sound as it was part of the ATG, which had stuck

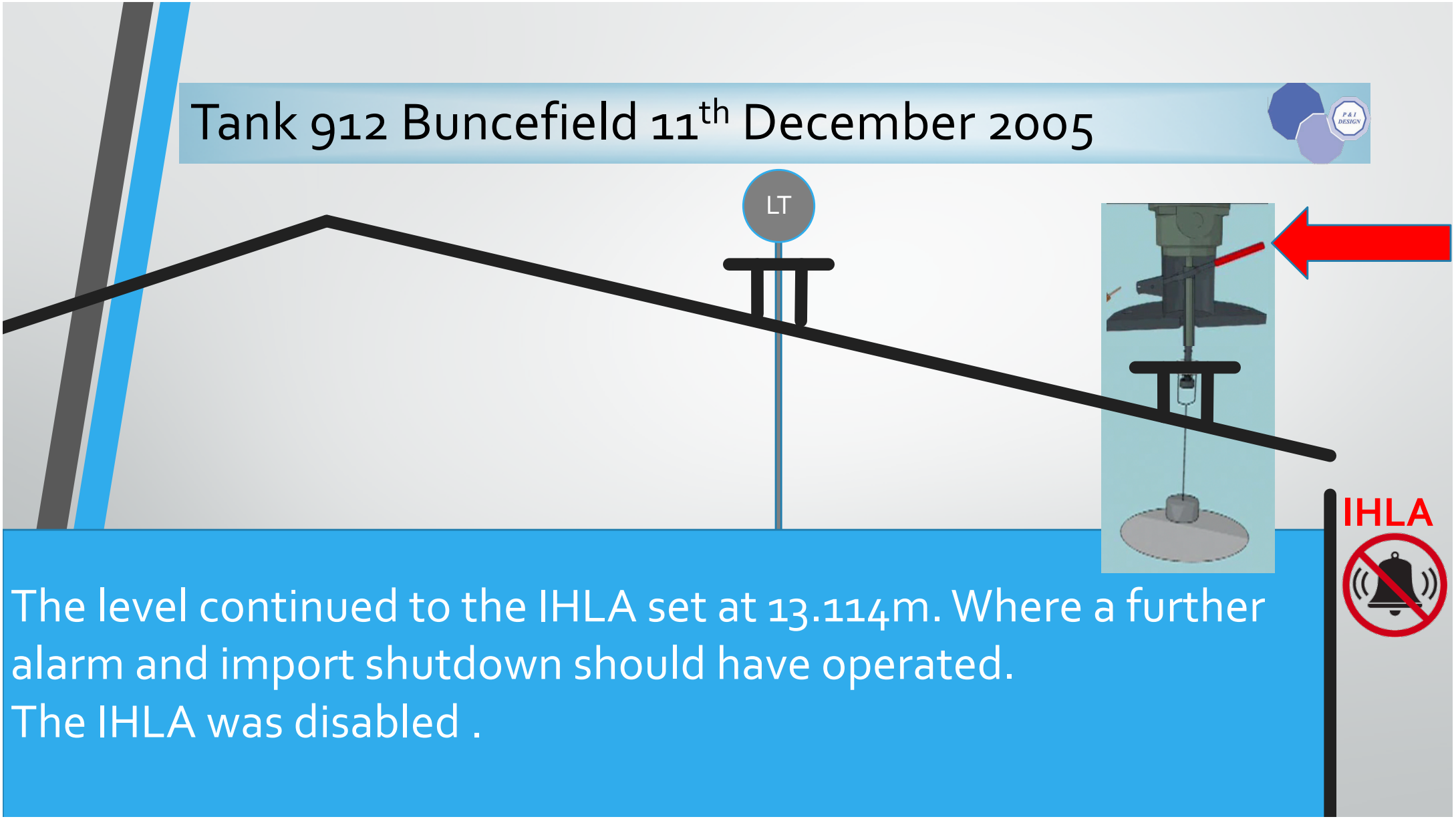


Tank 912 Buncefield 11th December 2005



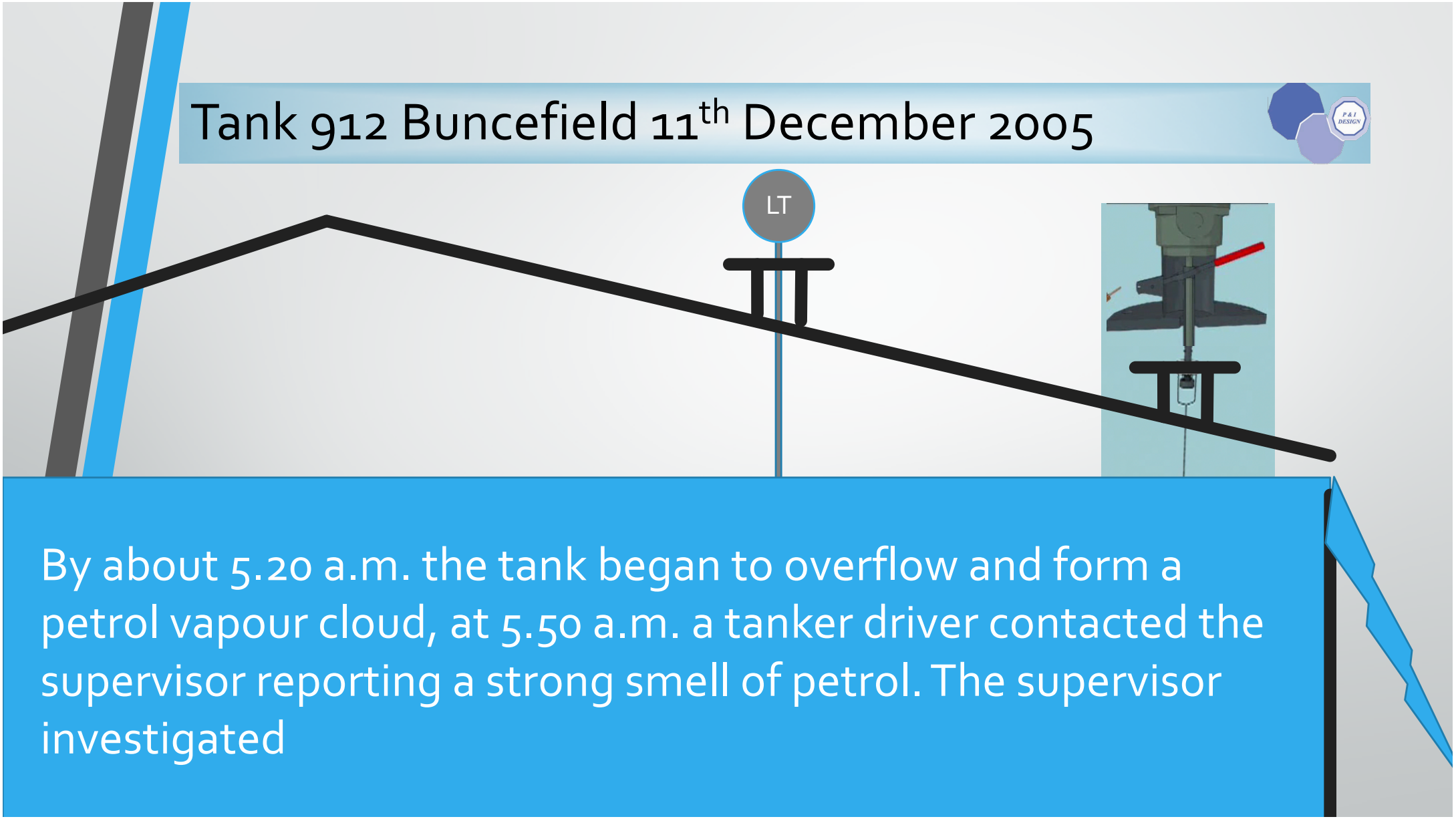
The level went above the High High level alarm (12.73m) at about 3.34 a.m. The alarm failed to sound as it was part of the ATG, which had stuck

Tank 912 Buncefield 11th December 2005



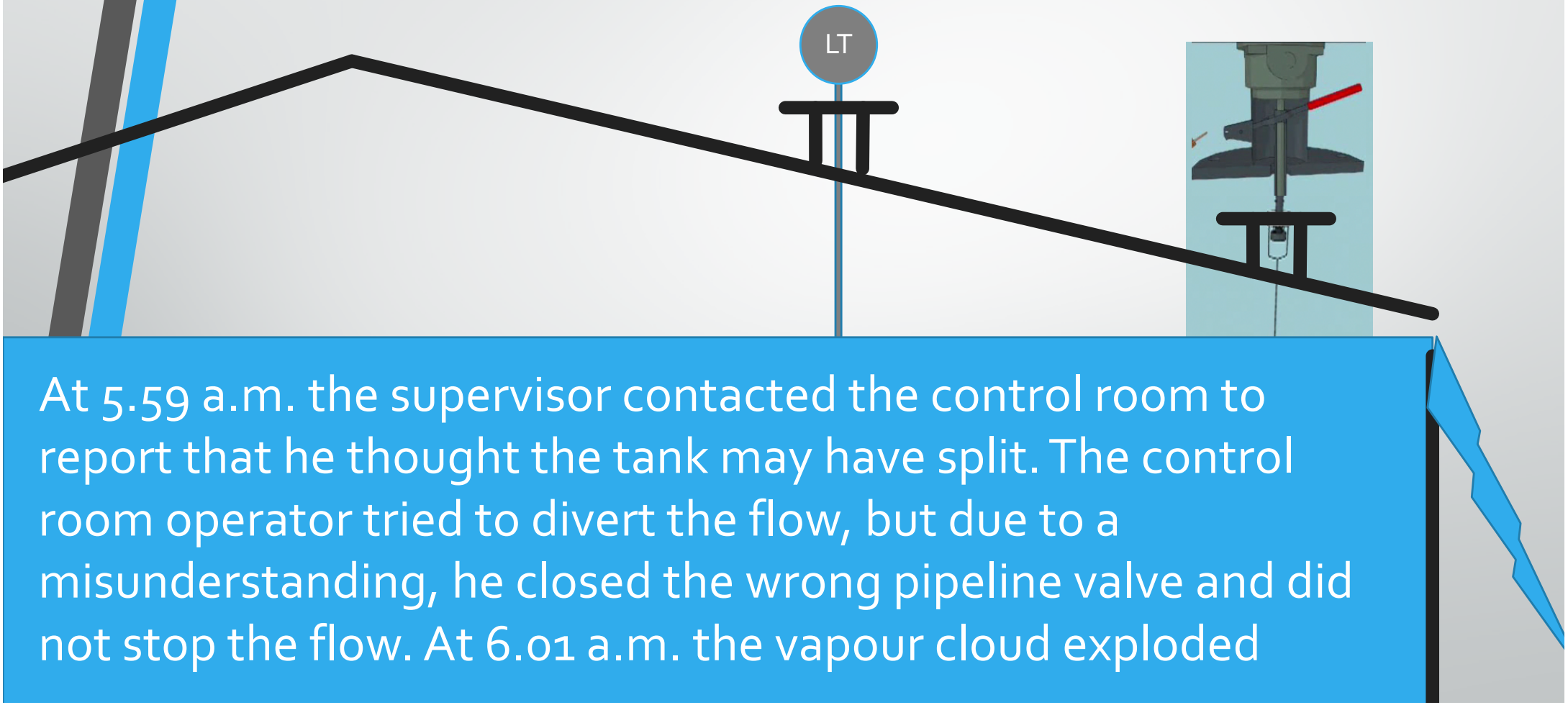
The level continued to the IHLA set at 13.114m. Where a further alarm and import shutdown should have operated.
The IHLA was disabled .

Tank 912 Buncefield 11th December 2005



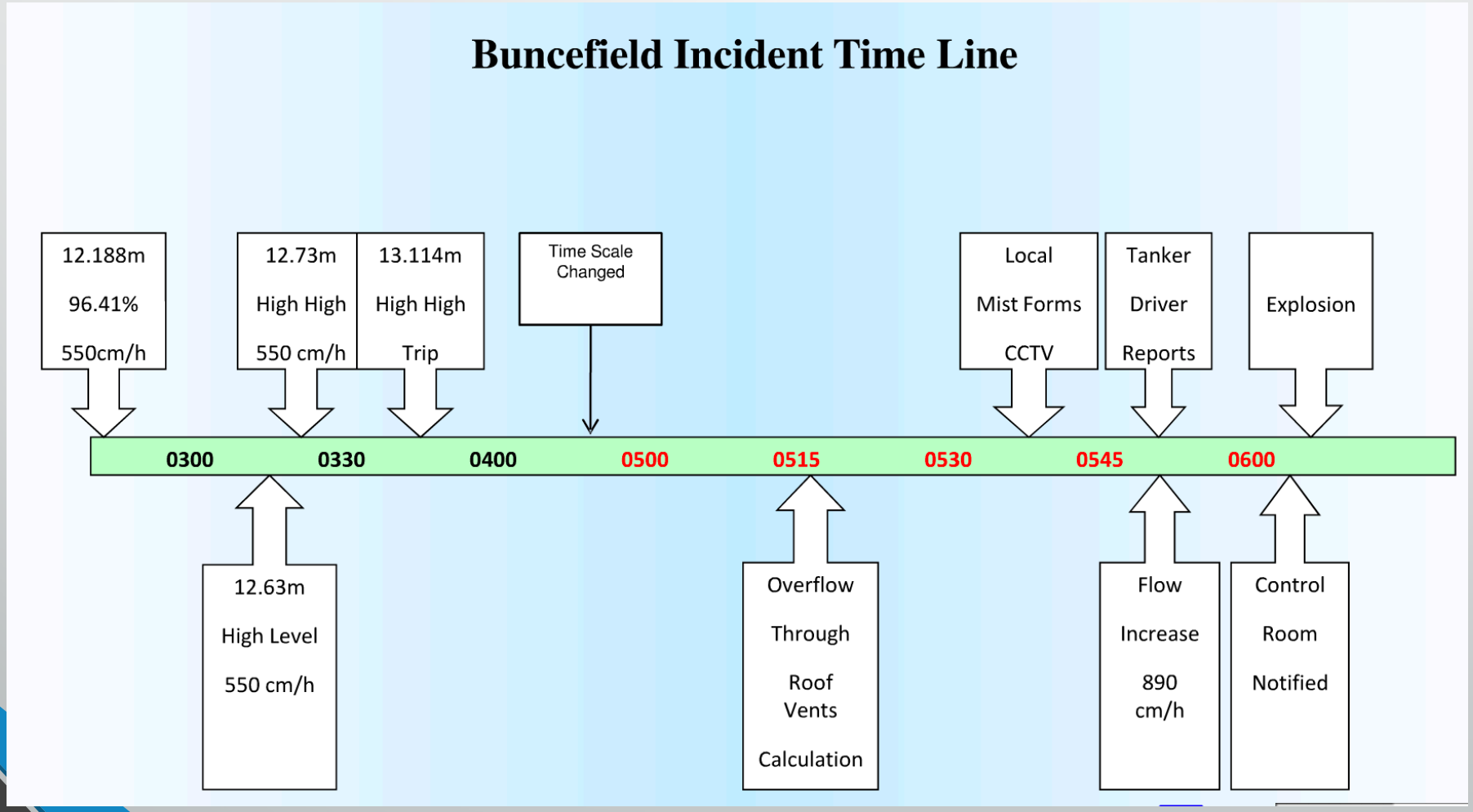
By about 5.20 a.m. the tank began to overflow and form a petrol vapour cloud, at 5.50 a.m. a tanker driver contacted the supervisor reporting a strong smell of petrol. The supervisor investigated

Tank 912 Buncefield 11th December 2005



At 5.59 a.m. the supervisor contacted the control room to report that he thought the tank may have split. The control room operator tried to divert the flow, but due to a misunderstanding, he closed the wrong pipeline valve and did not stop the flow. At 6.01 a.m. the vapour cloud exploded

A closer look at what happened!



Why did the IHLA TAV Switch fail?

After Buncefield!

Following the Buncefield Incident the Major Incident Investigation Board (MIIB) made recommendations for terminals which store gasoline products

After Buncefield!

The HSE together with the industry sector agreed to work together to develop guidelines to improve process safety in the UK

After Buncefield!

Industry trade associations including the Tank Storage Industry (TSA) and the UKPIA agreed amongst other safety measures, to install automatic tank overfill protection systems with a defined Safety Integrity Level (SIL)

MIIB Recommendation 3

Operators of Buncefield-type sites should protect against loss of containment of petrol and other highly flammable liquids by fitting a high integrity, automatic operating overfill prevention system(or a number of such systems, as appropriate) that is physically and electrically separate and independent from the tank gauging system. Such systems should meet the requirements of Part 1 of BS EN 61511 for the required safety integrity level, as determined by the agreed methodology (see Recommendation 1). Where independent automatic overfill prevention systems are already provided, their efficacy and reliability should be reappraised in line with the principles of Part 1 of BS EN 61511 and for the required safety integrity level, as determined by the agreed methodology

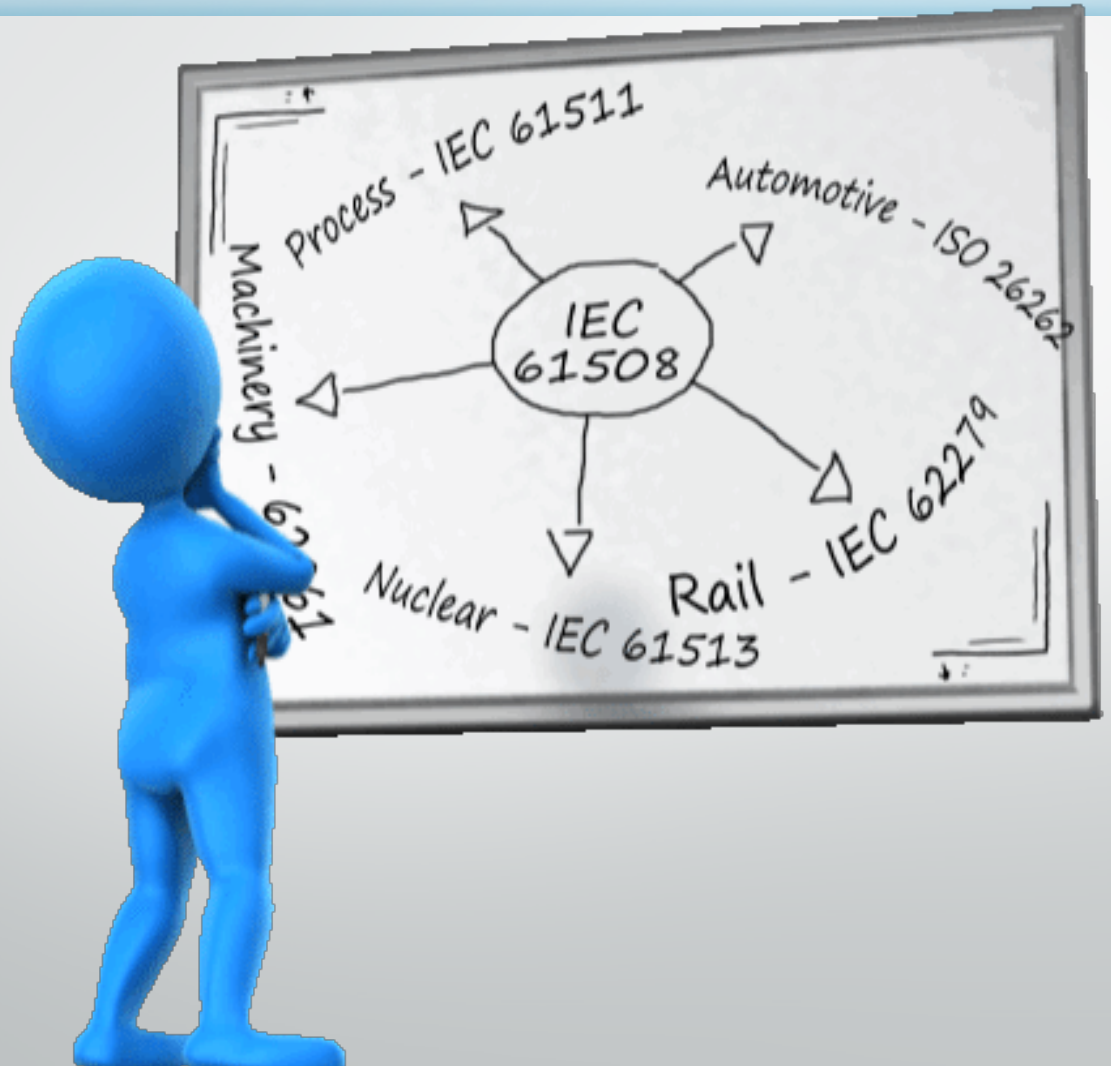
High Integrity?

Q. What is high integrity and why should it meet EN61511?

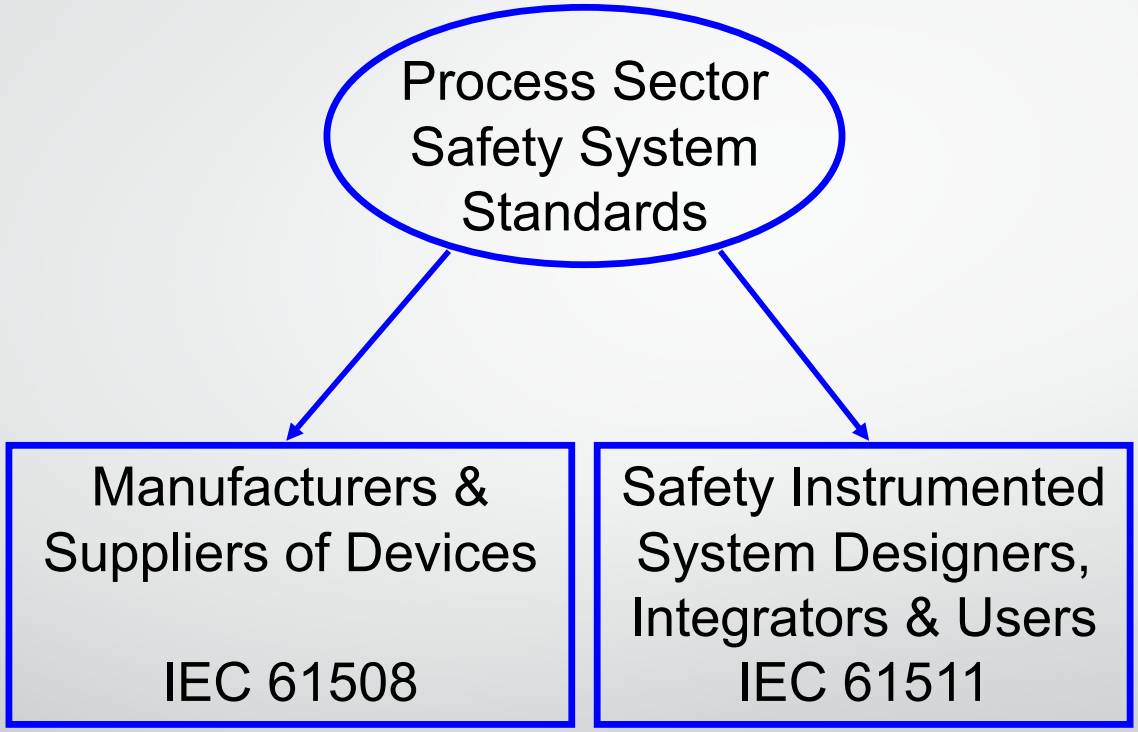
A. High Integrity, in this reference means that the automatic shutdown system should be designed, installed and maintained to ensure a specified reliability. i.e. SIL rated - Safety Integrity Level
The International Standard EN61511 provides a life cycle approach to the:

Risk Assessment
Specification
Design
Installation
Maintenance
Proof Testing
Modification
De-commissioning of the Safety Instrumented Systems

SIS Standards!



SIS Standards!



IEC 61511

IEC 61511 is accepted by the UK regulator as good practice for the implementation of Safety Instrumented Systems in the process industries

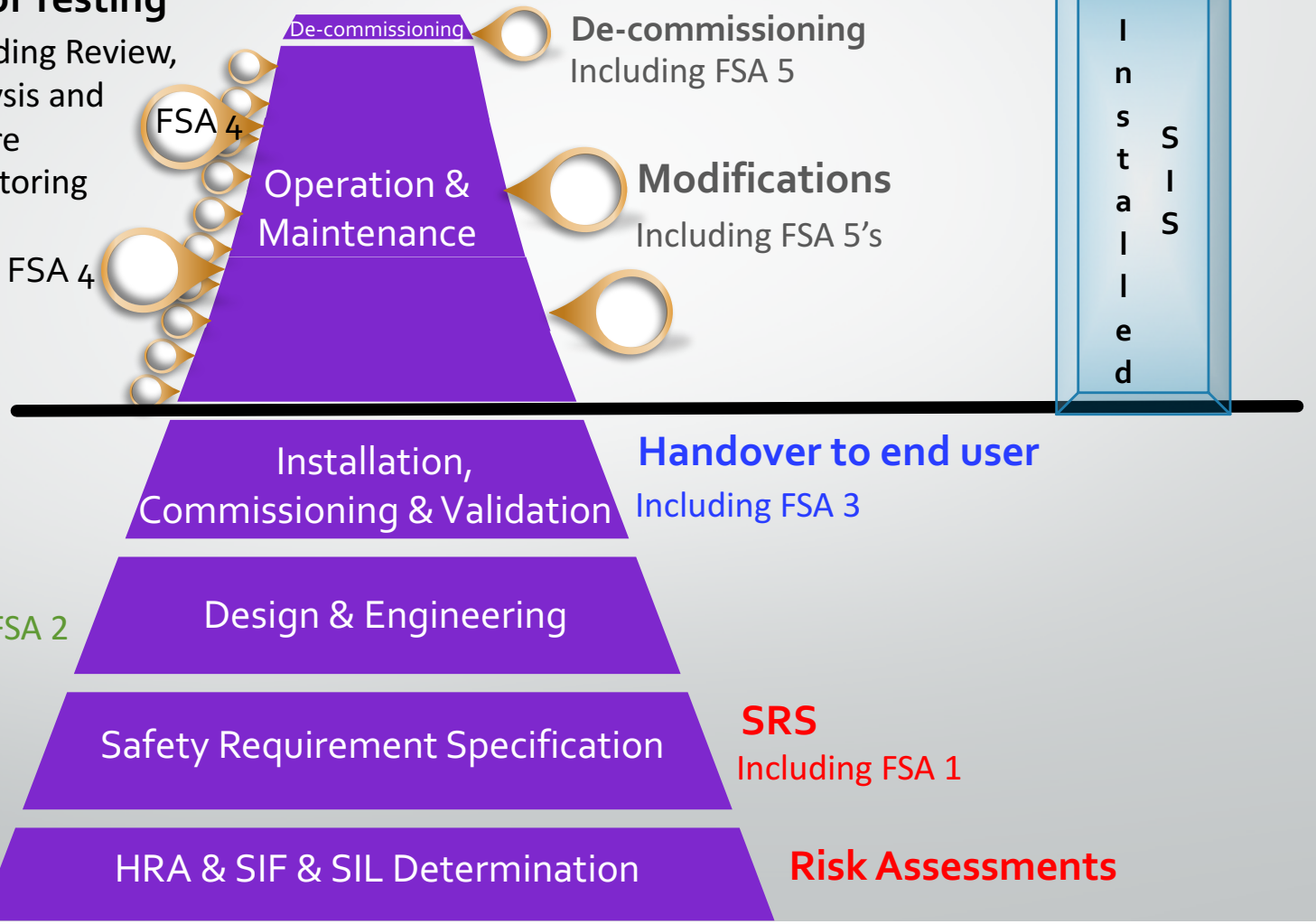
IEC 61511

IEC 61511 defines a system for all phases of the SIS life.
It is referred to as the Safety Life-Cycle

The SIS Lifecycle

Operation & Maintenance Phase Typically 10 to 30 times longer than all other phases

Proof Testing
Including Review, Analysis and Failure Monitoring



De-commissioning
Including FSA 5

Modifications
Including FSA 5's

Handover to end user
Including FSA 3

Design
Including FSA 2

SRS
Including FSA 1

Risk Assessments

Following Buncefield!

It is over 10 years since Buncefield.

So where are we now?

Following Buncefield!

- The UK has adopted IEC 61511 as the recognised good practice for SIS, and the Competent Authority use it as a bench mark to assess operators
- End users are now starting to address Functional Safety Management for the SIS

Following Buncefield!

But in 2009

CAPECO

End of Part 1!

Safety Instrumented Systems Appreciation Training Part 2 – HRA, SIL and SRS

David Ransome BA, CEng, FInstMC

Registered Functional Safety Engineer, RFSE

P & I Design Ltd - Chairman

Purpose!

This presentation is for managers, operators and maintainers.
It is intended to provide awareness of the requirements of installed Safety Instrumented Systems complying to IEC 61511.

Agenda!

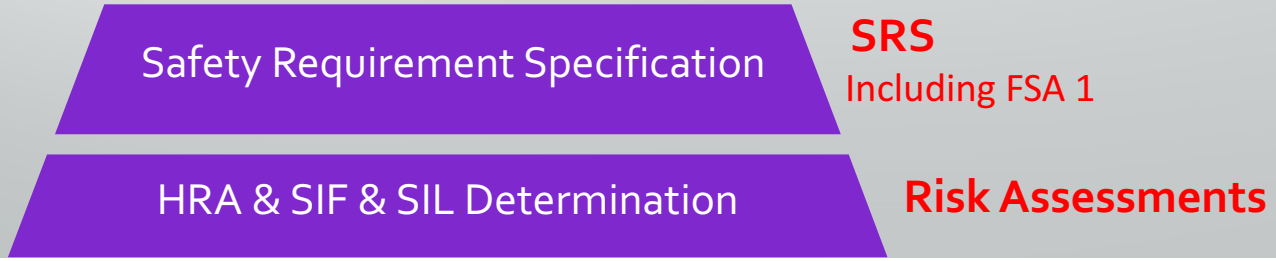
To provide an appreciation of:

- Hazard & Risk Assessment Techniques;
- Safety Integrity Levels & SIL Determination;
- Safety Requirement Specification.

Related to IEC 61511 Life-cycle

SIS Lifecycle – Up to FSA 1

This phase is often referred to as the Early Life-cycle Phase



SRS
Including FSA 1

Risk Assessments

Hazard & Risk Assessment

In order to establish the risks and hazards that a particular process presents, an assessment or assessments need to be conducted.

Common assessment methods are:

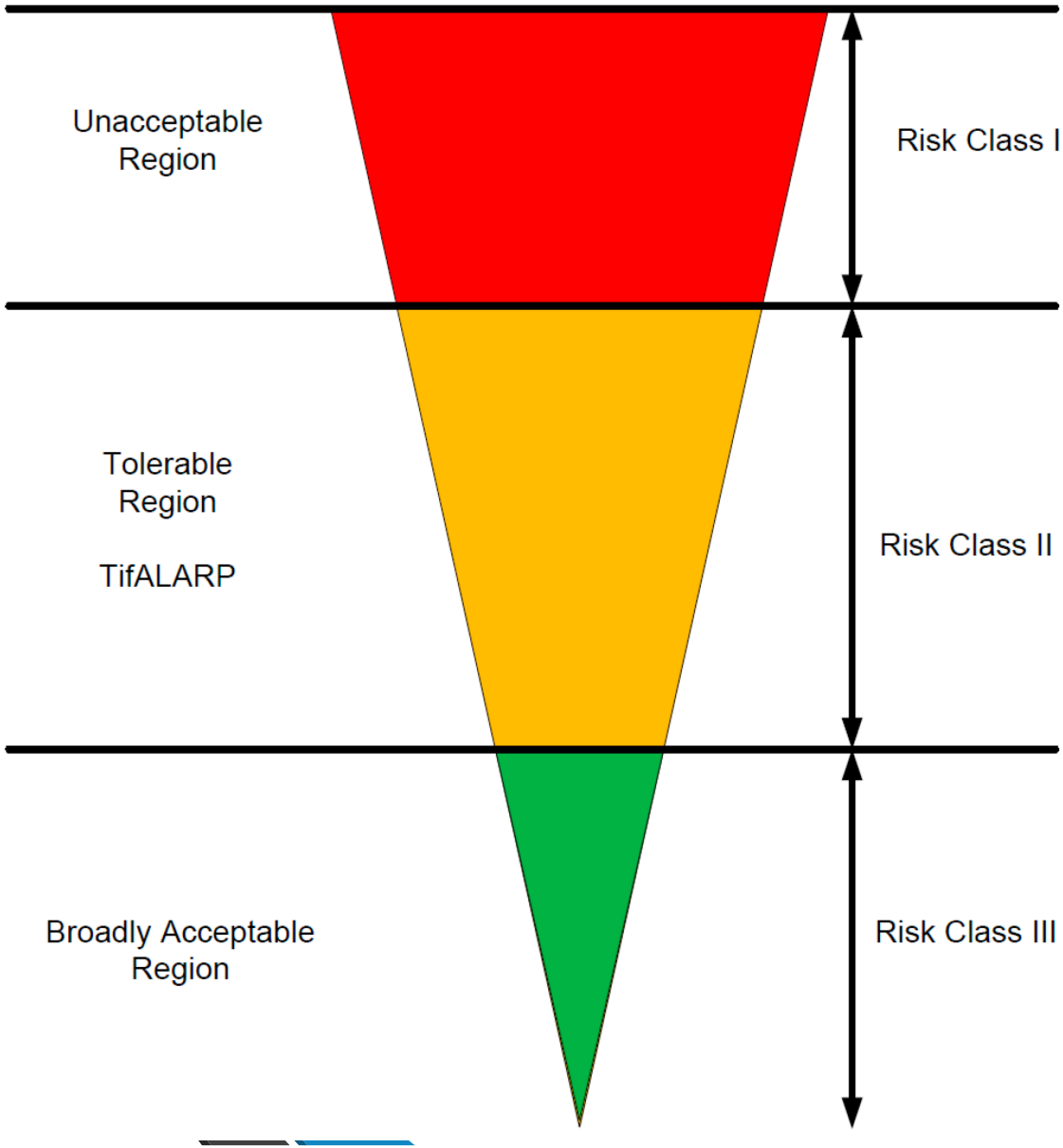
- Hazard Identification - HAZID;
- Hazard & Operability Study - HAZOP;
- Process Hazard Analysis – PHA;
- Risk Graphs;
- Layer of Protection Analysis - LOPA;
- Fault Tree Analysis - FTA;
- Quantitative Risk Assessment – QRA.

Hazard & Risk Assessment

The previous techniques are used to establish hazards and protections necessary to reduce the risk.

It is necessary to reduce the risk to an acceptable level.

In order to equate the risk, we use what is called the ALARP triangle.



Risk cannot be justified except in extraordinary circumstances

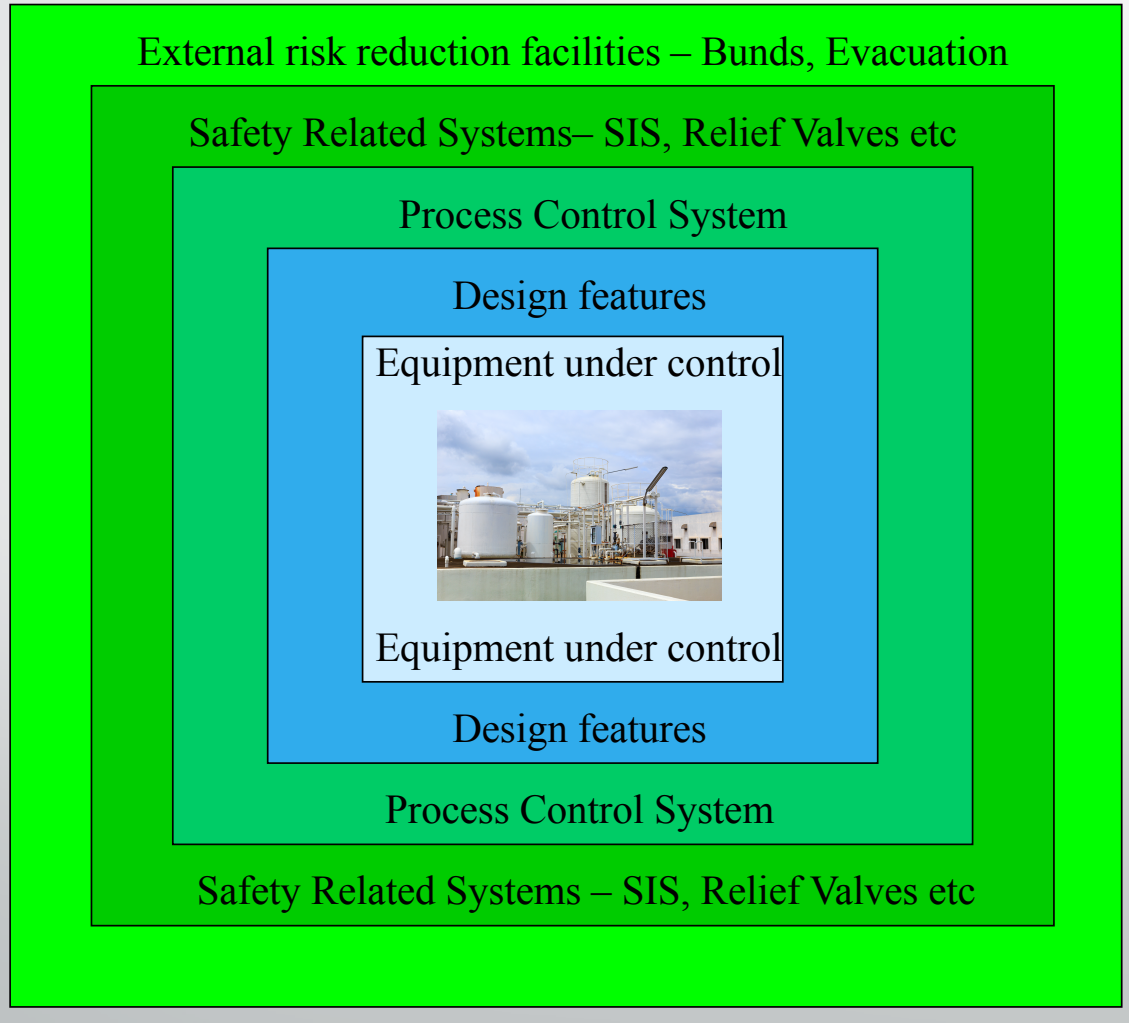
Risk is tolerable only if:

a) further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained and

b) society desires the benefit of the activity given the associated risk

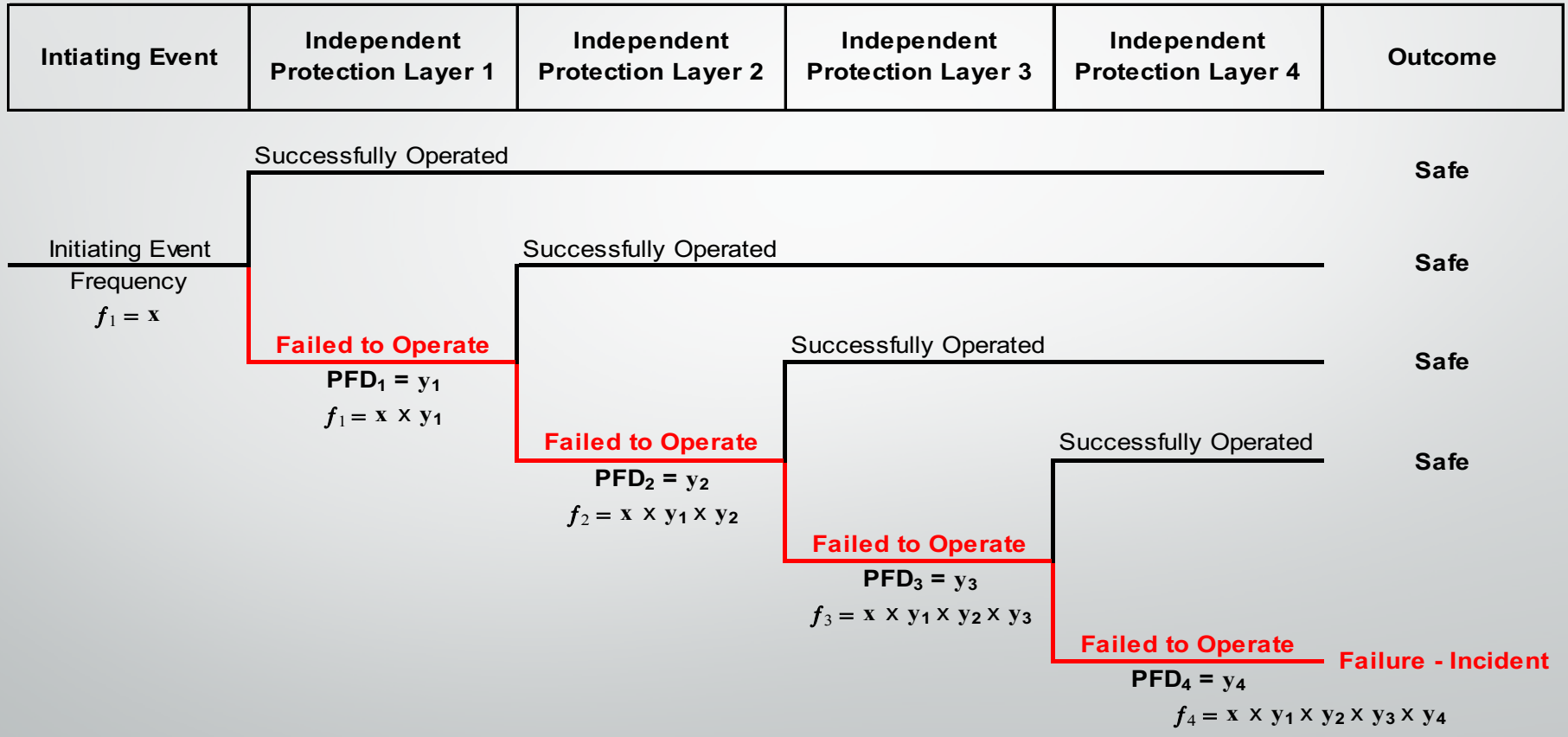
Level of residual risk regarded as negligible and further measures to reduce risk not usually required. No need of detailed working to demonstrate ALARP.

Principles of Layers of Protection



LOPA Model

LOPA Model



Consideration for Protection Layers

- Each Layer of Protection must operate totally independent from other layers;
- The Layer of Protection must be effective in providing the risk reduction claimed;
- All claimed Layers of Protection must be auditable;
- There must be sufficient Layers of Protection to provide the required level of protection;
- There must be sufficient Layers of Protection to mitigate the initiating event being a failure of a Protection Layer.

Prevention Protection Layers

The primary purpose of a Protection Layer is to prevent the initiating event resulting in an un-safe outcome.

These Layers are called Prevention Systems:

- Process Control Systems;
- Alarm Systems;
- Human Intervention;
- Safety Instrumented Systems.

Mitigation Protection Layers

It may be necessary to provide additional Protection Layers to reduce the consequence of the event due to failure of the prevention protection layers.

These Layers are called Mitigation Systems:

- Containment;
- Fire and Gas Detection;
- Evacuation Procedures.


Mitigate
Plant and Emergency Response
Dike
Relief valve, Rupture disk
Prevent
Safety Instrumented System
Operator Intervention
Basic Process Control System
Emergency response layer
Passive protection layer
Active protection layer
Emergency Shut Down
Safety layer
Trip level alarm
Process Shutdown
Process control layer
Process alarm
Process Value
Normal behaviour
Process control layer

SIF & SIS

SIF – Safety Instrumented Function

A safety function to be implemented by a safety instrumented system.

SIS – Safety Instrumented System

System used to implement one or more SIF's.

The SIS includes all devices necessary to carry out each SIF from sensor(s) to final element(s).

Safety Integrity Levels - SIL

Safety Integrity Level	Probability of failure on demand	Availability %	Non Availability Continuous Demand	Risk Reduction Factor
SIL 1	0.1 to 0.01	90 to 99%	876 to 87.6 hours/year	10 – 100
SIL 2	0.01 to 0.001	99 to 99.9%	87.6 to 8.76 hours/year	100 - 1000
SIL 3	0.001 to 0.0001	99.9 to 99.99%	8.76 to 0.876 hours/year	1000 - 10000
SIL 4	0.0001 to 0.00001	99.99 to 99.999%	52 to 5.2 minutes/year	>10000

How does LOPA work?

- LOPA stands for Layer of Protection Analysis;
- LOPA is a scenario based risk assessment technique;
- It can be used for Safety, Environmental and Financial Assessments.

LOPA - Scenario

Establish the Scenario to be assessed:

Example:

1. A Tank overfill during a pipeline import;
2. A Tank overfill whilst importing from a ship;
3. A Tank overfill whilst transferring from another tank.

What is the difference

LOPA - Consequences

What could happen?

Example:

1. A Tank overfill leading to an explosion and possible fatalities;
2. A Tank overfill leading to a flash fire;
3. A Tank overfill leading to harm to the environment.

Likelihood of 'n' fatalities from a single scenario	Risk Tolerability		
10^{-4}/yr – 10^{-5}/yr	Tolerable if ALARP	Tolerable if ALARP	Tolerable if ALARP
10^{-5}/yr – 10^{-6}/yr	Broadly acceptable	Tolerable if ALARP	Tolerable if ALARP
10^{-6}/yr – 10^{-7}/yr	Broadly acceptable	Broadly acceptable	Tolerable if ALARP
10^{-7}/yr – 10^{-8}/yr	Broadly acceptable	Broadly acceptable	Broadly acceptable
Fatalities (n)	**1**	**2 - 10**	**11 - 50**

LOPA – Initiating Events

What could lead to this happening?

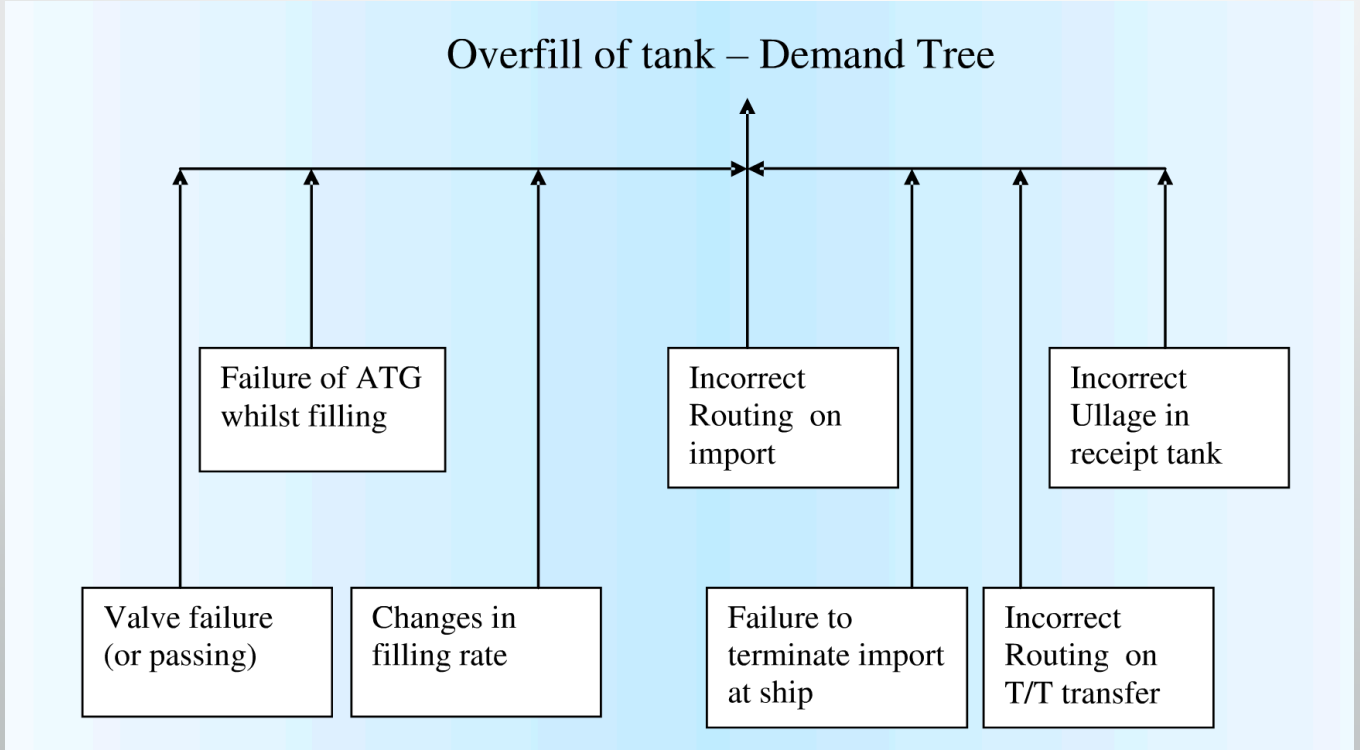
Example:

1. Failure of ATG;
2. Incorrect Routing;
3. Incorrect ullage in tank;
4. Failure to terminate import.

LOPA – Initiating Events

What could lead to this happening?

A demand tree is often used to establish all initiating events.



LOPA – Initiating Event Frequency

How often will it happen?

LOPA is a quantitative assessment so it is necessary to establish the frequency of events.

These calculations can be conducted in the LOPA itself or provided to the LOPA from a fault tree analysis.

The calculation considers enabling events, which must be present, this ensures a realistic frequency is used.

LOPA – Initiating Event Frequency

Scenario		Initiating Event Frequency IEF
Description	Major Release of Gasoline from any single on-site tank leading to open flammable cloud explosion and 2 to 5 on-site fatalities	
	Description	
IE No.	Initiating events	Events/year
1	Incorrect line up	3.25E-03
2	Incorrect Ullage in receipt tank.	6.50E-03
3	ATG Failure (Sticks or reads low) and operator does not pick this up.	3.81E-02
	Total of Initiating Events = IEF1 + IEF2 + IEF3 + IEF4 + IEF5 + IEF6 + IEF7 + IEF8 + IEF9 + IEF10 + IEF11	4.78E-02

LOPA – Protection Layers

How will the risk be reduced?

It is necessary to provide a risk reduction figure for each of the protection layers.

Protection Layer 1	Protection Layer 2	Protection Layer 3	Protection Layer 4	Mitigation Layer 1
ATG and Operator Action	High High Alarm and independent shutdown of tank import (SIL2)	Cross Check: Quantities transferred from ship is compared to quantity to be exported.		Failure to detect and stop overfill
1.00E-01	5.00E-03			1.00E-01
1.00E-01	5.00E-03			1.00E-01
	5.00E-03	1.00E-01		1.00E-01

LOPA – Conditional Modifiers

How will the risk be reduced?

The consequence may only occur when certain conditions are present, these conditions are calculated within the LOPA as conditional modifiers.

Conditional Modifier 1	Conditional Modifier 2	Conditional Modifier 3	Conditional Modifier 4
Required Meteorological Conditions	Probability of ignition	Probability of personnel in affected area	Probability of fatal injury
0.03	0.6	1.0	1.0

LOPA – Perform the LOPA calculations

Results!

The results of the initiating event frequencies, protection layers and conditional modifiers are calculated to provide a frequency of the consequence with all protection measures in place. This is then compared to the Risk Tolerance Criteria to ensure it has been met.

LOPA Summary	
Risk Tolerance Criteria	1.0E-07
Frequency of Consequence mitigated by conditional modifiers but not by protection layers	8.61E-04
Frequency of Mitigated Consequence	4.31E-08
Risk Tolerance Criteria Met	Yes

LOPA – Sensitivity Analysis

Results!

In order to ensure that uncertainty within the calculations do not provide a false answer, it is necessary to conduct a sensitivity analysis.

This tests the assumptions made by modifying various assumptions made in the LOPA.

LOPA – Output and Deliverables

The Risk Assessment will have provided the protection layers required for the processing activities under review.

If any of these layers are Safety Instrumented Systems then these must comply with IEC 61511 during all life-cycle phases.

In order to ensure that the requirements of what the SIS is to provide then the next life-cycle phase is the creation of the:

Safety Requirement Specification

The Safety Requirement Specification - SRS

Why is it required?

The SRS is a mandatory document for the SIS, as defined in IEC 61511.

The Safety Requirement Specification - SRS

What does it do?

Firstly – It defines the Safety Instrumented Function (SIF) and the Safety Integrity Level (SIL) of the Safety Instrumented System (SIS)

The Safety Requirement Specification - SRS

What does it do?

Secondly – It provides information on all aspects of the functional safety required from it :

- The Safe State;
- The time of response of the SIF and the process safety time (PST);
- Process and Environmental conditions it is to work in;
- Methods of manually shutting down in a safe manner;
- Method of rest and the requirement of any overrides;
- The proof test requirements in order to discover undetected dangerous failures if the SIS .....

The Safety Requirement Specification - SRS

What does it do?

Thirdly – It provides the Designer, Installer and End User with the requirements of the system.

It is essential that the SRS is maintained and updated as required, throughout all life-cycle phases. This should be conducted as part of the Functional Safety Management System (FSMS).

End of Part 2!

Safety Instrumented Systems Appreciation Training Part 3 – Design, Installation and Commissioning

David Ransome BA, CEng, FInstMC

Registered Functional Safety Engineer, RFSE

P & I Design Ltd - Chairman

Purpose!

This presentation is for managers, operators and maintainers.
It is intended to provide awareness of the requirements of installed Safety Instrumented Systems complying to IEC 61511.

Agenda!

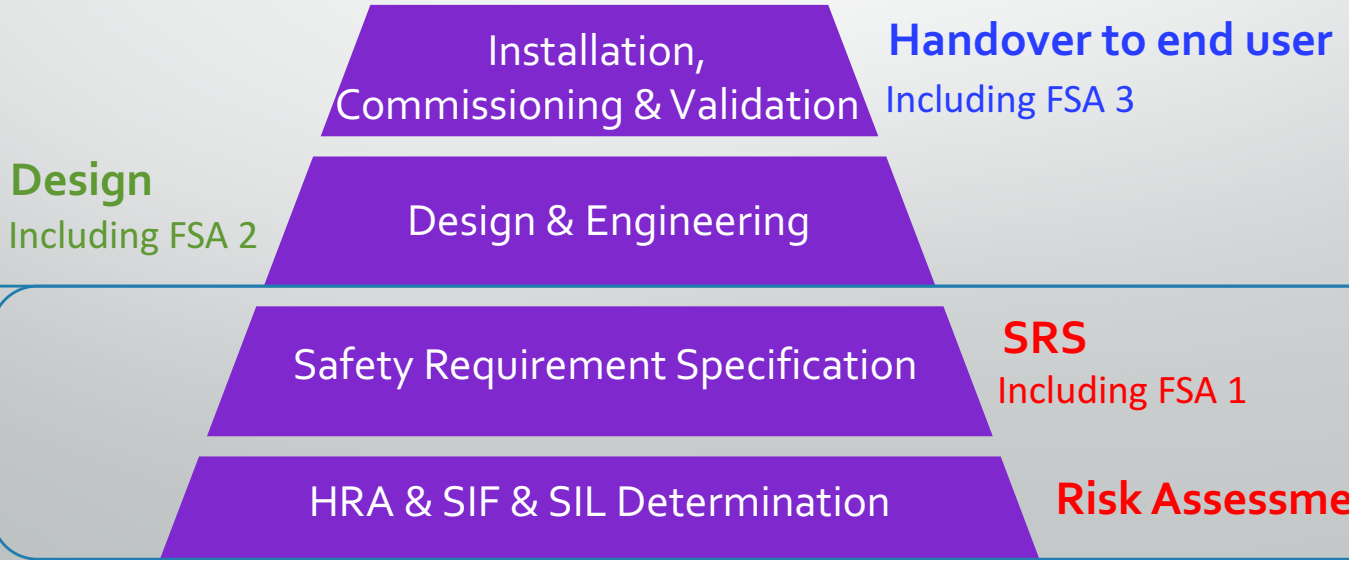
To provide an appreciation of:

- The Realisation life-cycle phase;
- System Architecture,
- SIL & PFD

Related to IEC 61511 Life-cycle

Reminder of the SIS Lifecycle

This phase is often referred to as the Realisation Phase



SIS Design

This phase of the SIS life-cycle is where the outputs from the SRS and LOPA are transposed into an actual system.

Throughout the design phase all necessary drawings, calculations and other associated documentation are produced.

There are many constraints on the design life-cycle phase in order to comply with IEC 61511, including redundancy, operability and testing.

SIS Design

The design will provide a calculated Safety Integrity Level SIL for the system, derived from component reliability data.

The SIL, PFD (Probability of Failing on Demand) and spurious trip calculations are all mathematical calculations based on certain assumptions.

It is very important that once in service, reliability data is recordered to confirm these assumptions.

Safety Instrumented Function

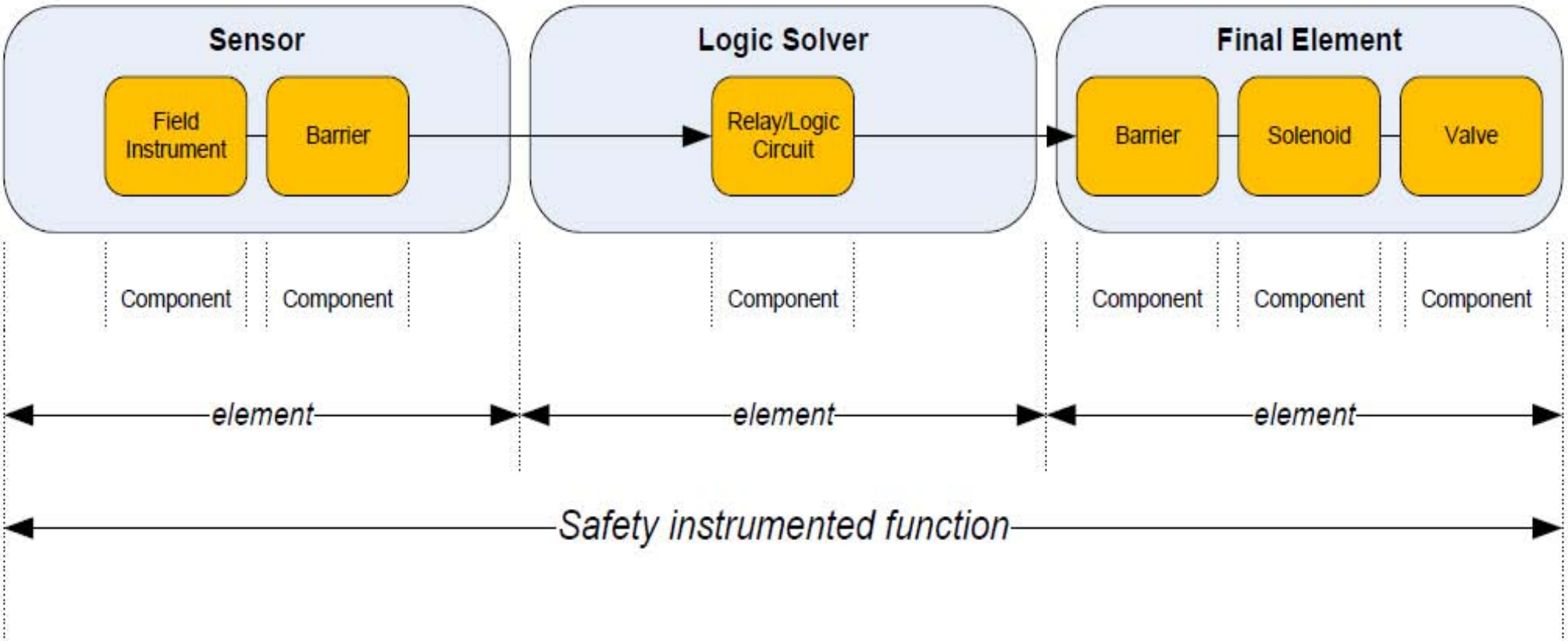


Figure 1 – Elements and Components of a Safety Instrumented Function

Architecture

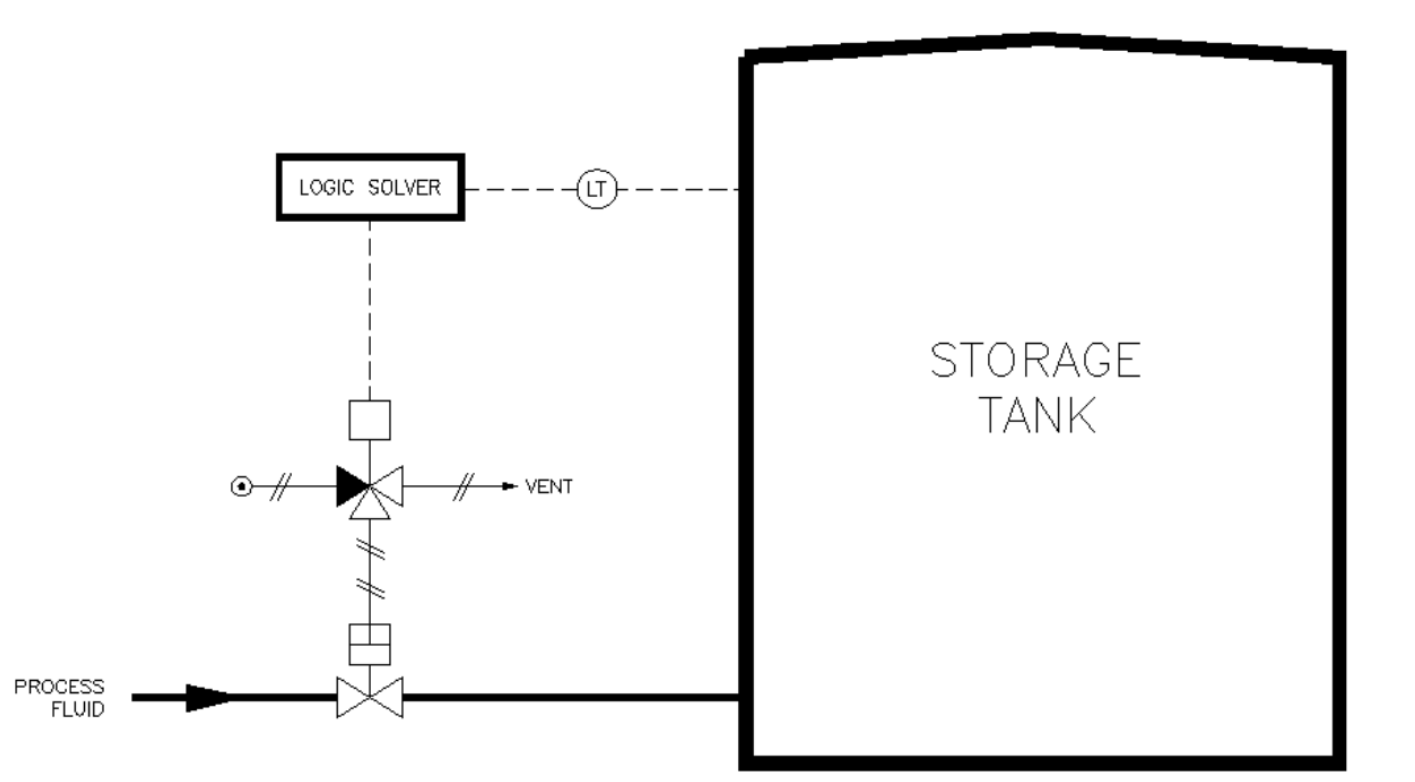
Any of the sub-groups can have additional components added to decrease the probability of failing on demand value.

This is referred to as Hardware Fault Tolerance – That is the system can tolerate a failure and still function.

Architecture

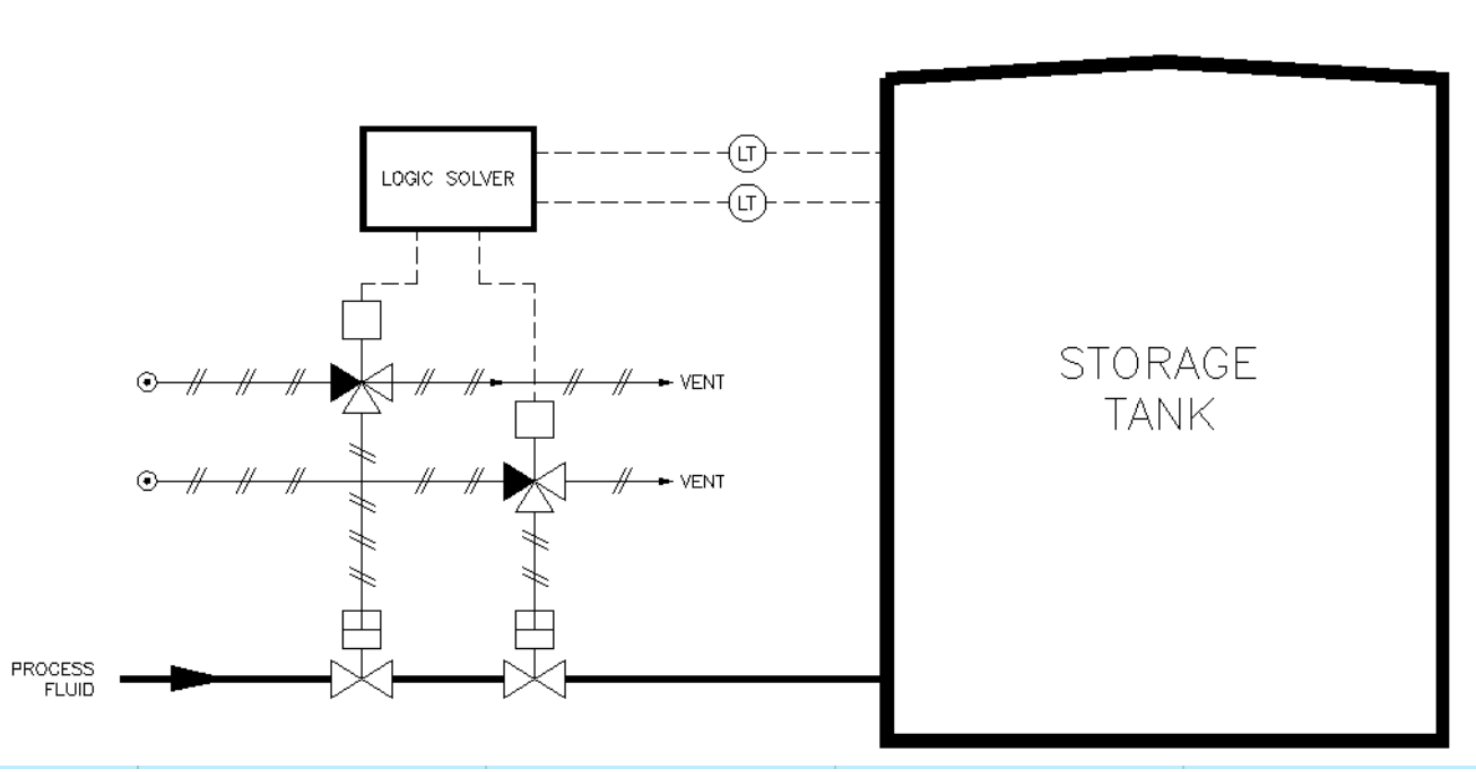
The terminology used to indicate this is:

1oo1 – One out of One



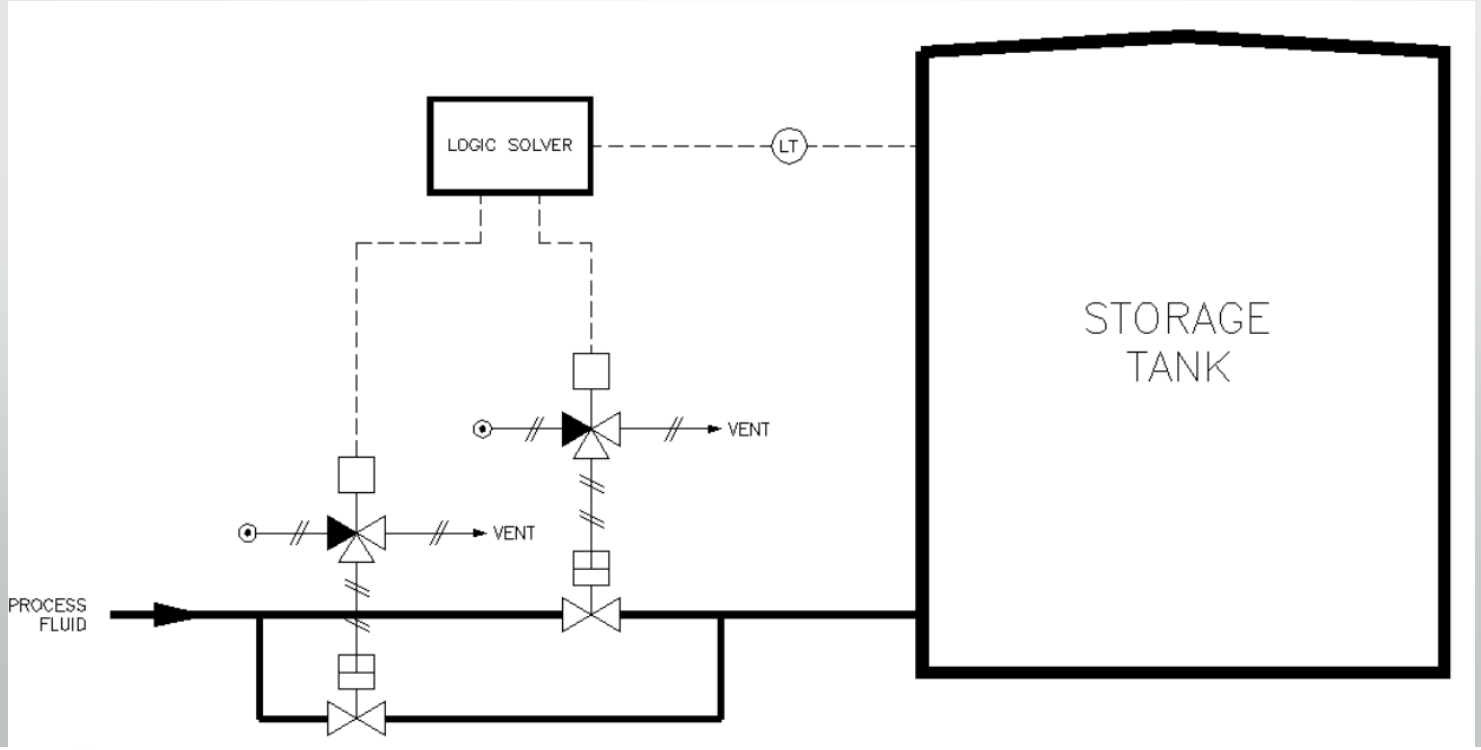
Architecture

1oo2 – One out of Two



Architecture

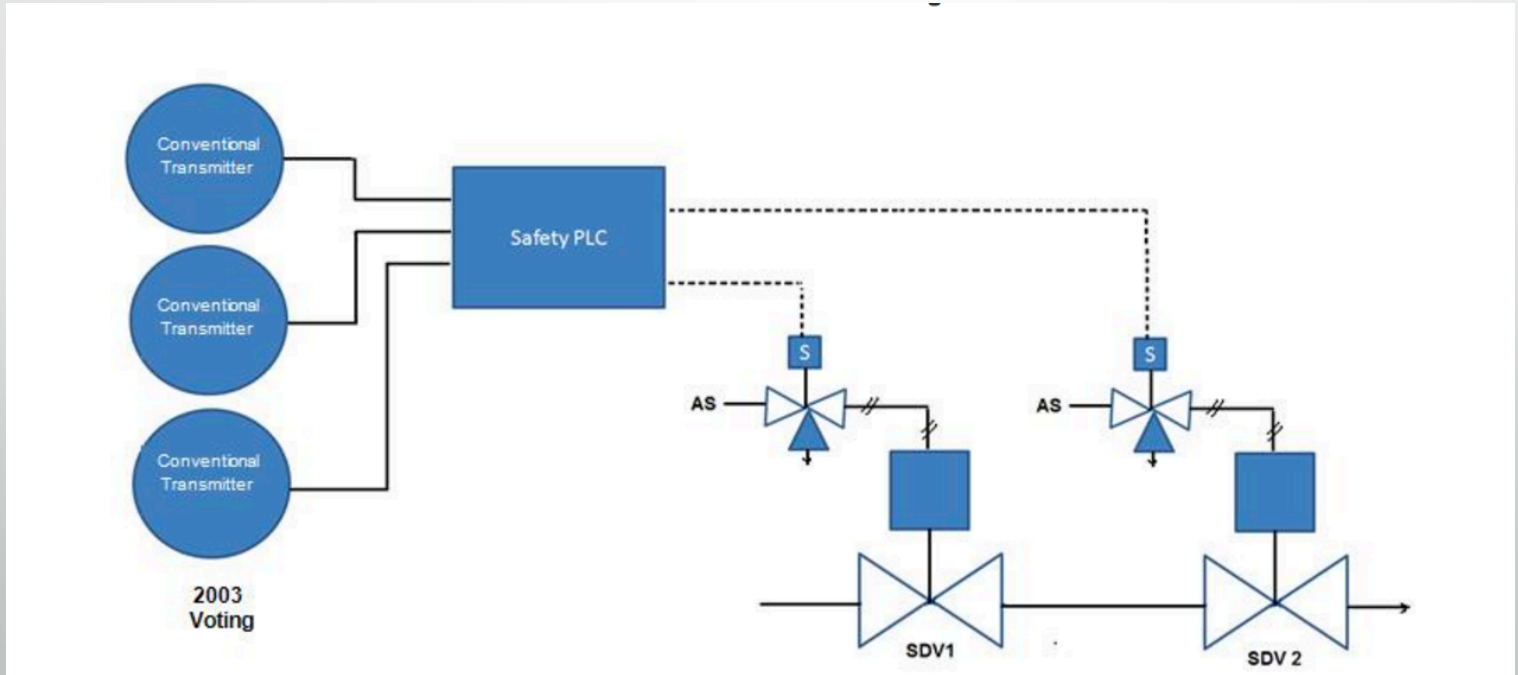
2oo2 – Two out of Two



Architecture

2oo3 – Two out of Three

1oo2 – One out of Two



Hardware Fault Tolerance

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode or continuous mode)	1
4 (any mode)	2

SIL Determination and PFD values of SIF

The Sensor element – $PFD_{(S)}$, i.e $PFD_{(S1)} + PFD_{(S2)}$
Logic Solver element – $PFD_{(L)}$
and Final element $PFD_{(FE)}$
values are all calculated to provide an overall PFD & SIL.

$$PFD_{(SYS)} = PFD_{(S)} + PFD_{(L)} + PFD_{(FE)}$$

SAFETY INTEGRITY LEVEL REQUIRED

SIL 2

SAFETY INTEGRITY LEVEL ACHIEVED

Valid

CALCULATION SUMMARY

$PFD_{(SYS)}$	=	$PFD_{(S)}$		$PFD_{(L)}$		$PFD_{(FE)}$	
4.92E-03	=	1.50E-03	Valid	5.55E-04	Valid	1.00E-06	Valid
		0.00E+00	n/a	3.07E-05	Valid	2.75E-03	Valid
		0.00E+00	n/a	3.78E-05	Valid	4.58E-05	Valid
Valid		1.50E-03	Valid	6.24E-04	Valid	2.79E-03	Valid

SPURIOUS TRIP SUMMARY

$S.Trip_{(SYS)}$	=	$S.Trip_{(S)}$		$S.Trip_{(L)}$		$S.Trip_{(FE)}$	
29.3	=	74	Years	200	Years	10101.0	Years
Years		n/a	Years	3619	Years	69.2	Years
		n/a	Years	2939	Years	2426.0	Years

PFD v SIL

Table 4 – Safety integrity requirements: PFD_{avg}

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**PFD_{avg}**	**Required risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

Design & Engineering

During the Design & Engineering phase of the lifecycle. Equipment will be specified and procured, installation documentation will be produced.

It is essential that all equipment selected for inclusion in the SIS is specified correctly and the safety manual consulted to ensure the equipment's suitability.

During the detail design phase, the Safety Instrumented System Manual is developed.

Design & Engineering

Also all necessary information is produced to allow the system to be installed in accordance with the design.

Together with the all testing plans and procedures.

During the detail design phase, the Safety Instrumented System Manual is developed.

The Stage 2 FSA is performed on completion of the design phase.

Pre-Testing & Factory Acceptance Test

Prior to the installation of the Safety Instrumented System. All components, where possible, are tested and verified.

The Logic Solver (SIS Panel) will be tested at the manufacturers by simulating inputs and outputs. This is known as a Factory Acceptance Test (FAT). The testing procedure is produced prior to the test and all results of the test are recorded.

Installation

It is a requirement of the Standard that everyone working on Safety Instrumented Systems is competent to do so and aware of their responsibilities.

In order to ensure the installation is completed satisfactorily it is essential that the installer is aware of his responsibilities and has available all documentation to install the system.

On completion of the Installation, all testing documentation (including DSEAR) is provided by the installation contractor. The installation is then inspected before pre-commissioning.

Site Acceptance Testing – Functional Testing

To ensure the SIS performs correctly, a series of functionality tests are required.

A testing plan will be produced. This not only includes Site Acceptance Tests (SAT) but also those required throughout the operational phase of the SIS lifecycle.

On completion of installation and pre-commission testing, a Functional Safety Assessment 3 is conducted before the SIS is subjected to live process conditions.

End of Part 3!

Safety Instrumented Systems Appreciation Training Part 4 – Operational Phase

David Ransome BA, CEng, FInstMC

Registered Functional Safety Engineer, RFSE

P & I Design Ltd - Chairman

Purpose!

This presentation is for managers, operators and maintainers.
It is intended to provide awareness of the requirements of installed Safety Instrumented Systems complying to IEC 61511.

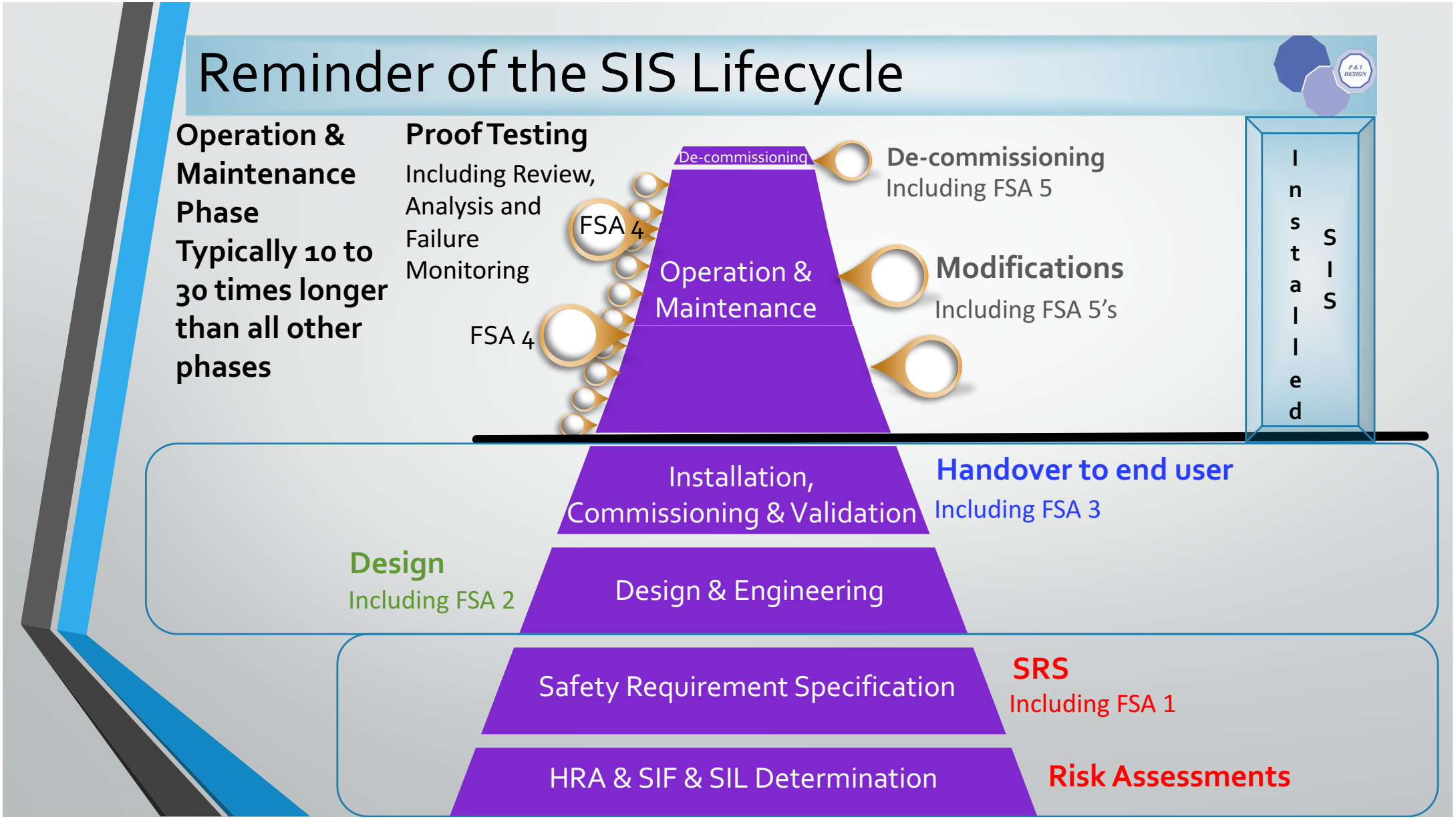
Agenda!

To provide an appreciation of:

- The Operational Phase of the SIS life-cycle;
  - Operation
  - Maintenance and Testing
  - Modification
  - Decommissioning

Related to IEC 61511 Life-cycle

Reminder of the SIS Lifecycle



Operation

The Safety Instrumented System has now been installed and Commissioned, it is essential that all those who come into contact with the SIS are aware of their roles and responsibilities together with the knowledge of what to do if the system activates or fails.

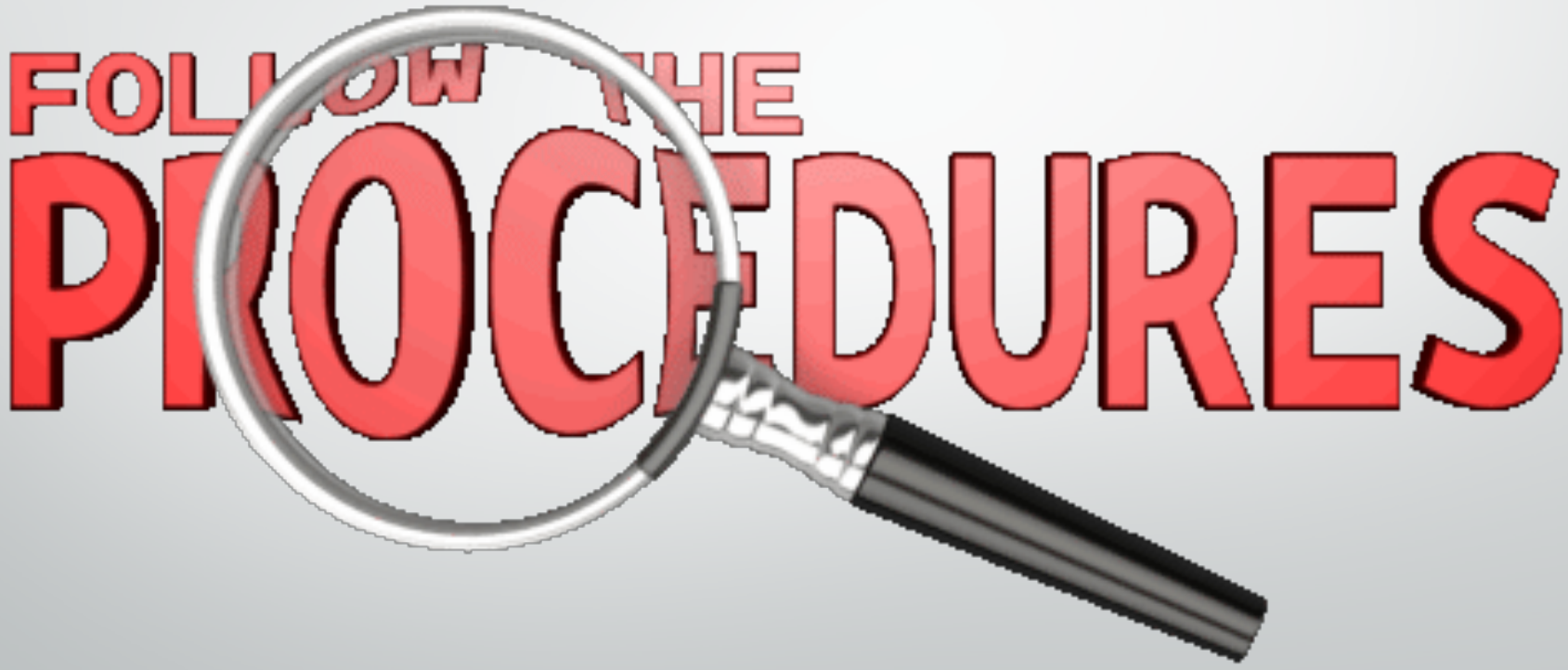
Operation

Operators need to know how the system operates and what to do. It is quite possible that throughout an operators working life he may never see the system work due to a true high high level.

Operation

Operational Procedures have been developed to ensure safe operation. It is probable, that following these procedures are part of a protection layer, as defined in the LOPA.

Operation



What to do if unsure!

Record Keeping

It is essential that full records are kept on all activity associated with the SIS.

Maintenance

Purpose!

To maintain the SIS so that the designed functional safety is maintained.

Why!

- To ensure that employees, public and the environment remain protected from harm.
- To prevent damage to business assets and reputation.
- Ensure the demand rate does not change with time (due to deterioration of other layers of protection).
- Protection of the investment in the SIS itself.
- Lastly – to comply with the standard.

Maintenance

When!

Throughout the operational phase of the lifecycle in accordance with defined maintenance schedules.

Maintenance consists of two types:

- Preventative – Planned refurbishment of Sensors and Final Elements .
- Reactive – Repair, or like for like replacement.

Maintenance

Who!

Technicians who are competent to work on the Safety Instrumented System and are aware that the system is high integrity and as such all work and testing must be recorded.

Proof Testing

Purpose!

To test the SIS so that the designed functional safety is maintained and to detect dangerous un-detected faults.

Why!

- To ensure that employees, public and the environment remain protected from harm
- To prevent damage to business assets and reputation
- To discover hidden faults
- Lastly – to comply with the standard.

Proof Testing

When!

- After commissioning as part of a validation test;
- Part of schedule periodic testing;
- Prior to planned preventative maintenance;
- After any maintenance or modification.

Activities of Maintenance & Proof Testing

Maintenance

- Hazardous Area (ATEX) inspections;
- Visual inspection;
- Calibration of Sensors;
- Service of valves;
- Don’t forget the logic solver.

Proof Testing

- Complete system Functional testing;
- Partial testing;
- End to End testing;
- Calibration check of Sensors.

SIS Failures

SIS Failures

Random Hardware Failures:

A failure of a hardware component.

- Typically caused by component wear, corrosion, thermal stress, physical manufacturing defects;
- Most SIS component failures result in a safe failure causing a spurious activation of the SIS;
- The failure rates of components can be mathematically predicted, providing:
  - Average probability of failure data;
  - Typical failure modes for the failure.

SIS Failures

Random Hardware Failures:

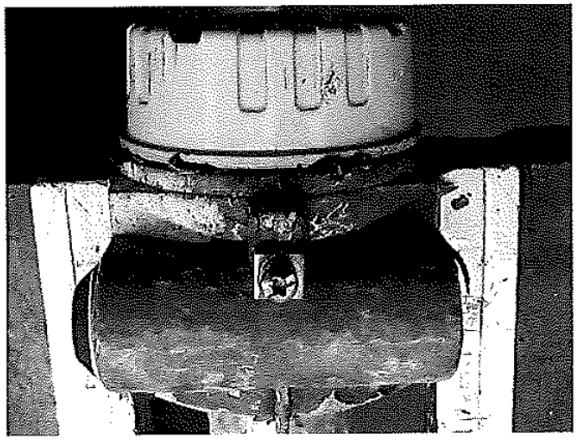


Fig. 5: Cover gasket

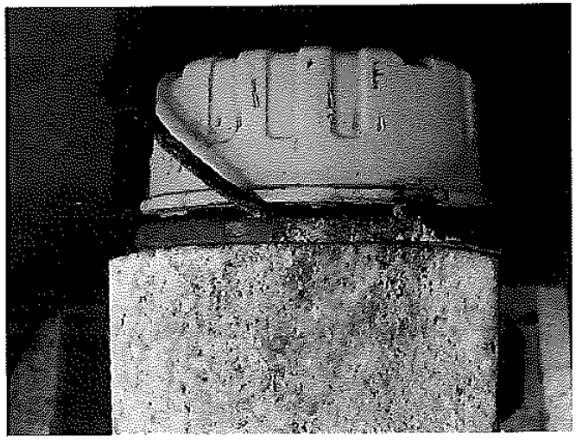


Fig. 6: Cover gasket

SIS Failures

Random Hardware Failures:

After dismantling from the electronic insert it was found that the connector is corroded.
During the function test on the open circuit board it was observed a defective component in the area of the signal processing. (Fig. 10) + (Fig. 11)

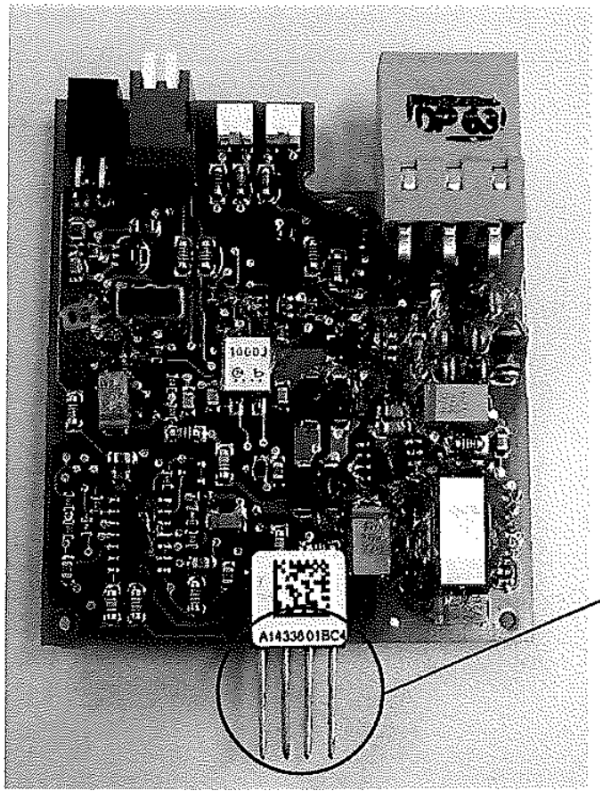


Fig. 10: Electronic circuit board

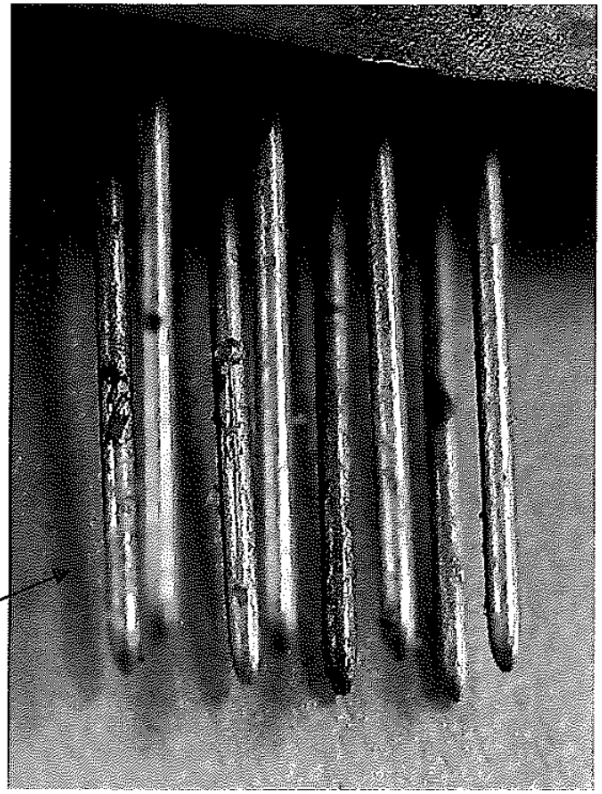
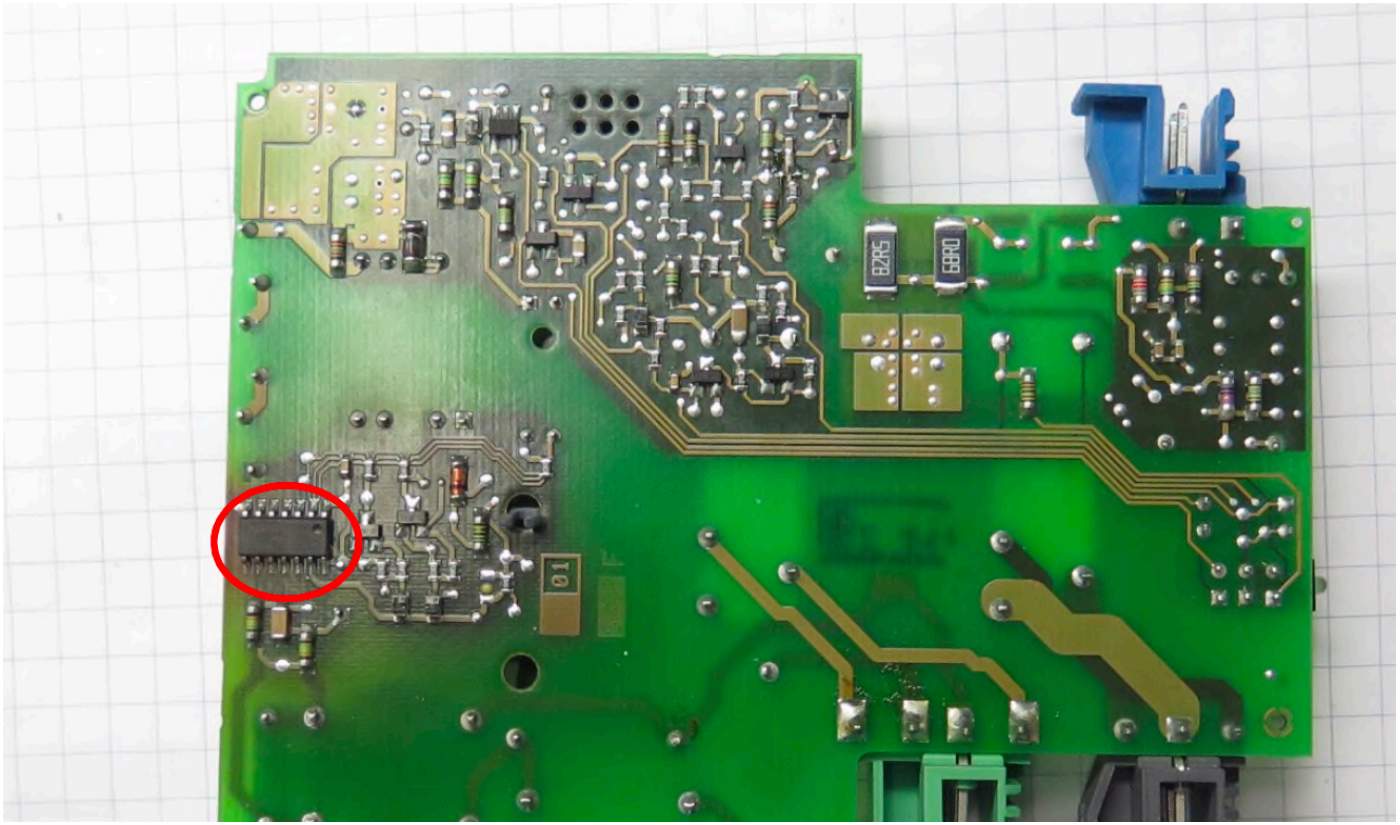


Fig. 11: Corroded connector

SIS Failures

Random Hardware Failures:

The reason for the fault was traced down to a blown fuse which in turn was caused by a defective switch mode power supply (SMPS) controller(see figure 2).

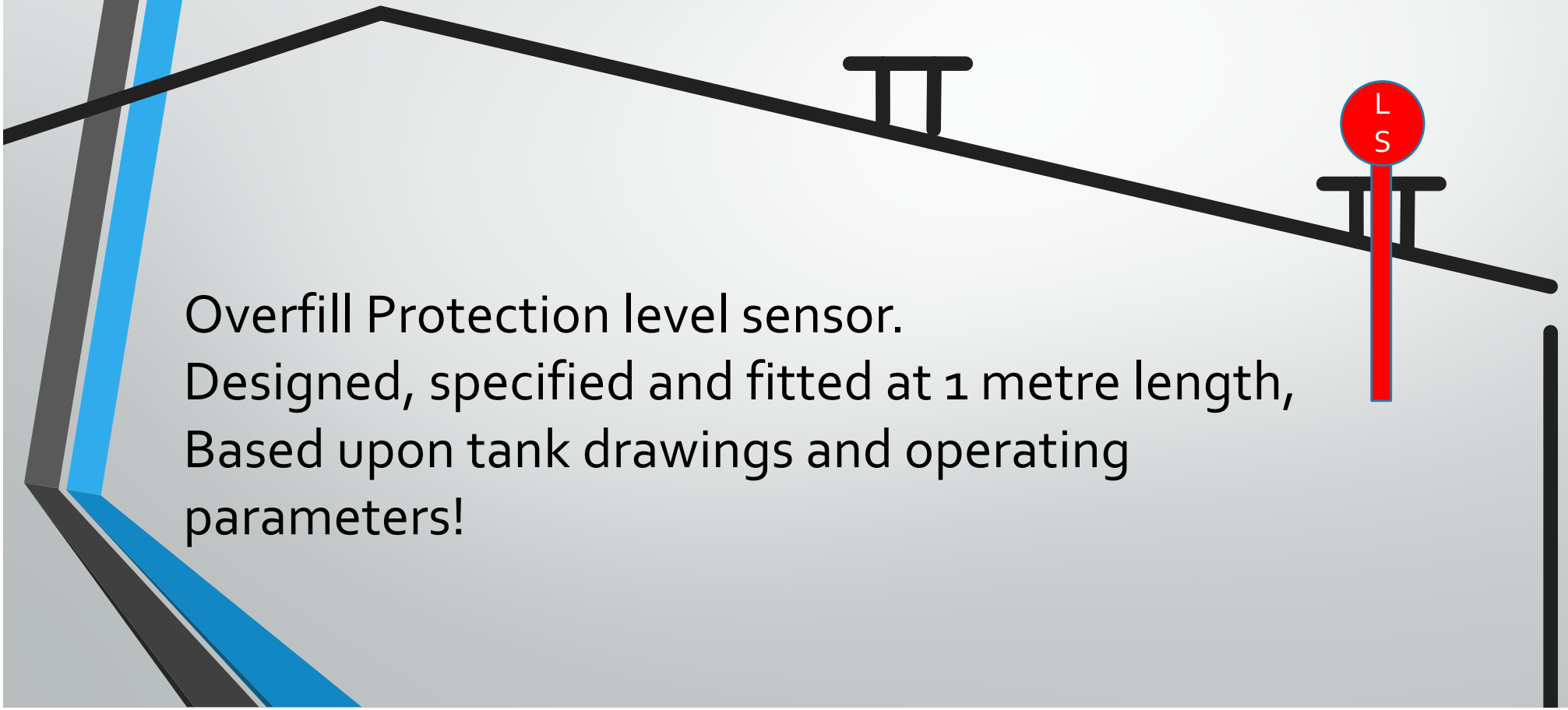


SIS Failures Systematic Failures

Systematic Failures:
Produced by Human error.

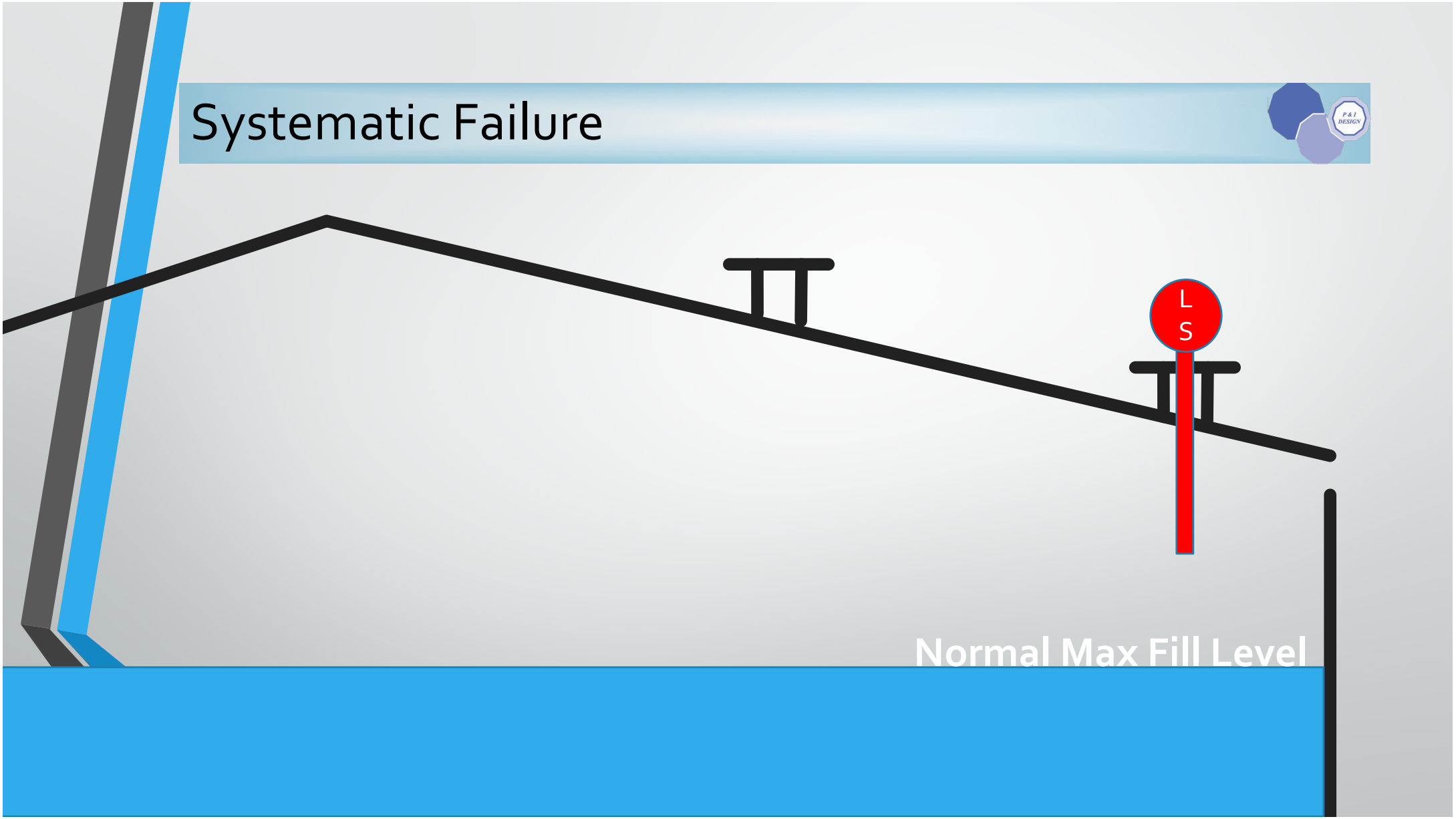
- Not easily detected and may only occur in specific scenarios;
- Can be created at any stage of the SIS lifecycle
  - Specification – Design – Manufacture – Installation – Operation – Maintenance – Modification;
- Very difficult to predict when and how they will occur;
- Can only be removed by a modification to the SIS or SIS procedures.

Systematic Failure

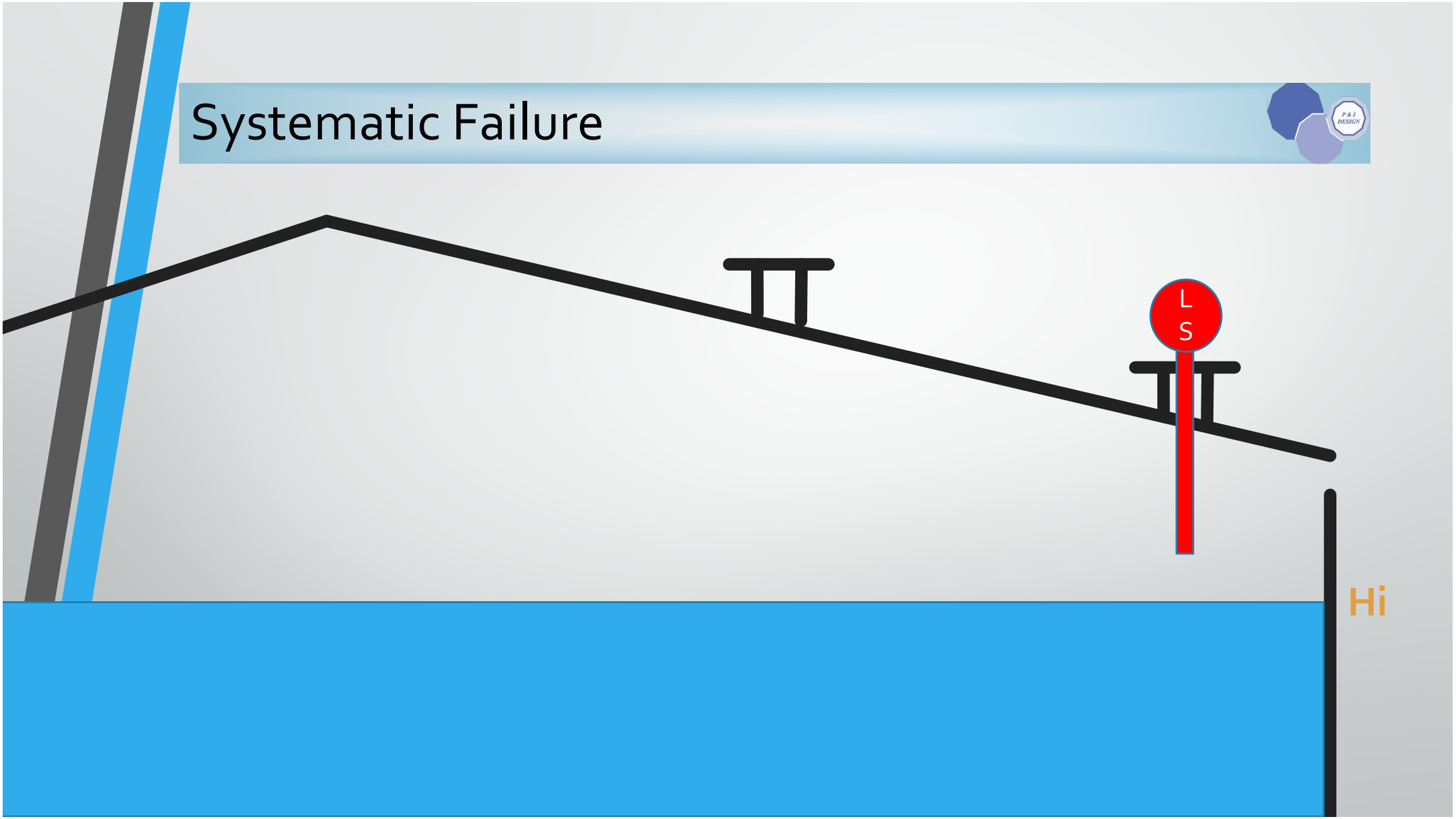


Overfill Protection level sensor.
Designed, specified and fitted at 1 metre length,
Based upon tank drawings and operating parameters!

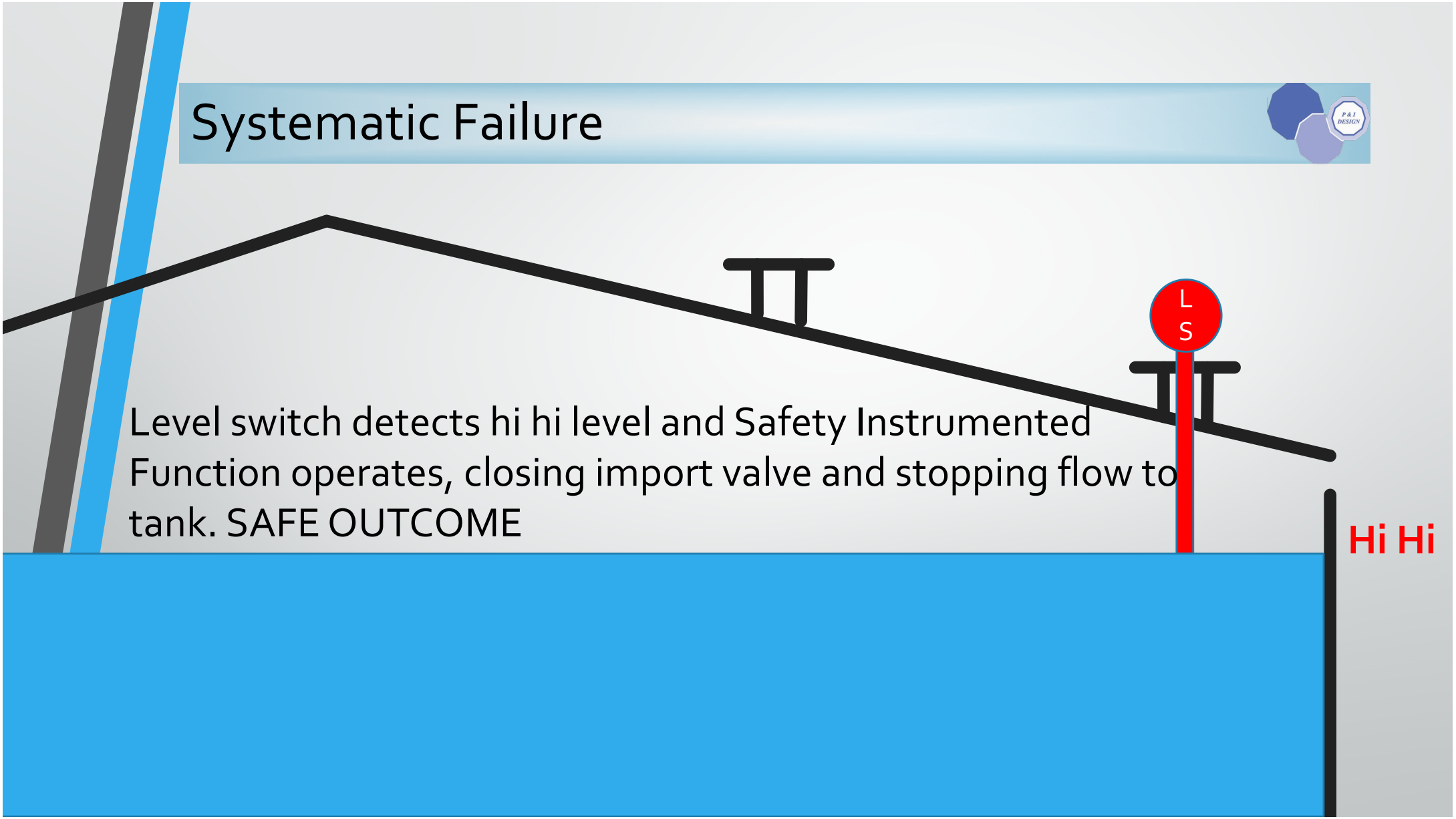
Systematic Failure



Systematic Failure

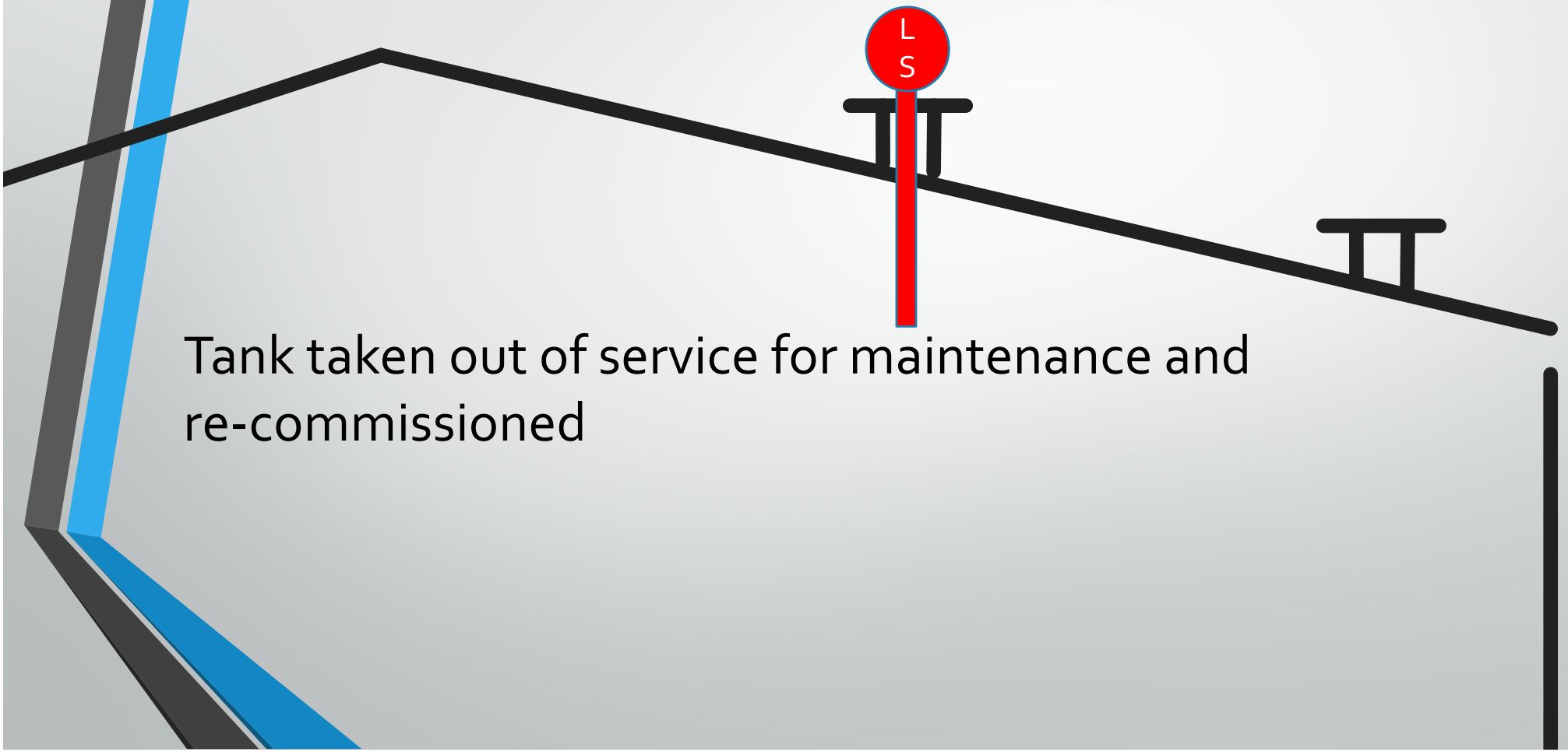


Systematic Failure



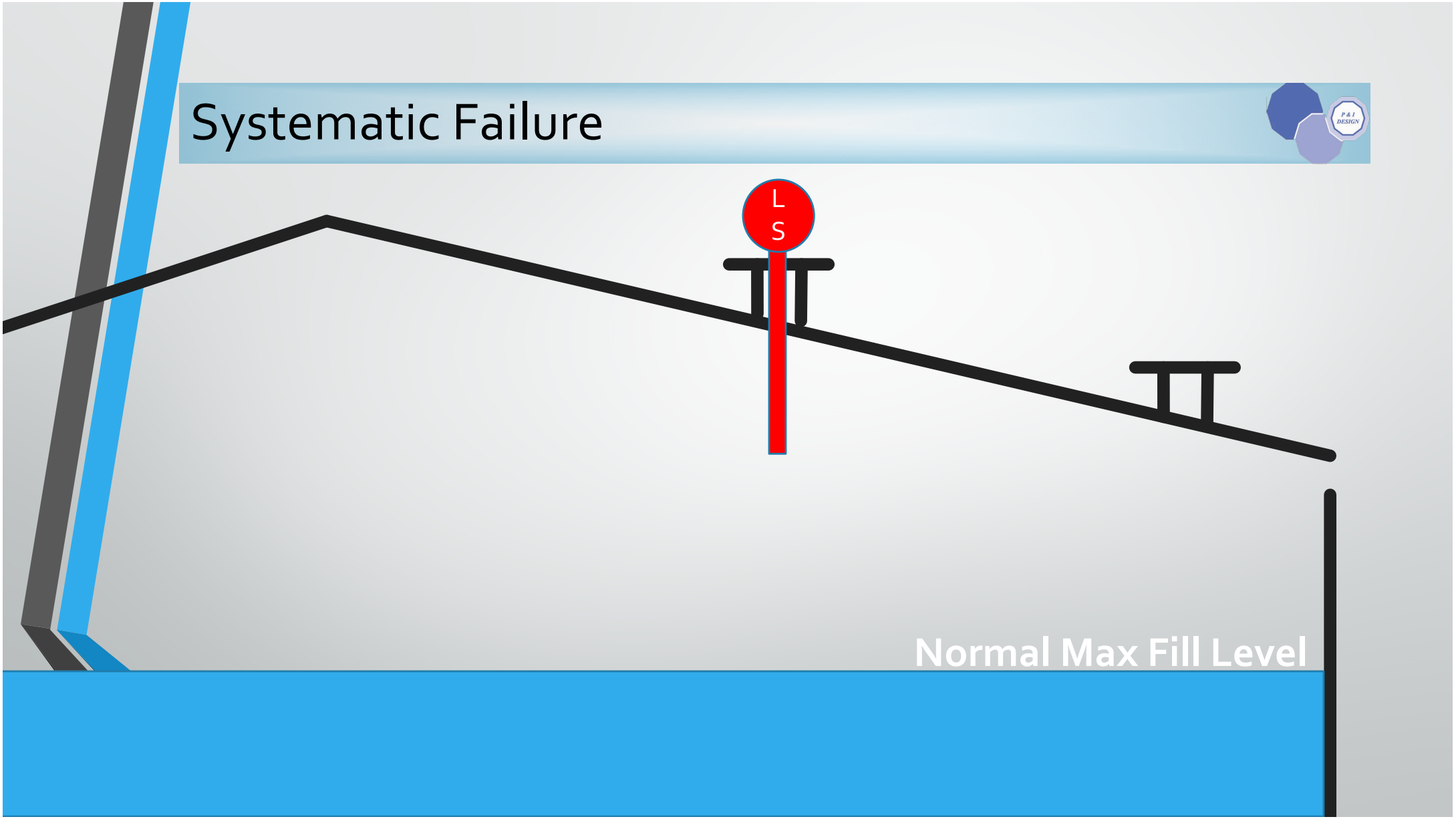
Level switch detects hi hi level and Safety Instrumented Function operates, closing import valve and stopping flow to tank. SAFE OUTCOME

Systematic Failure

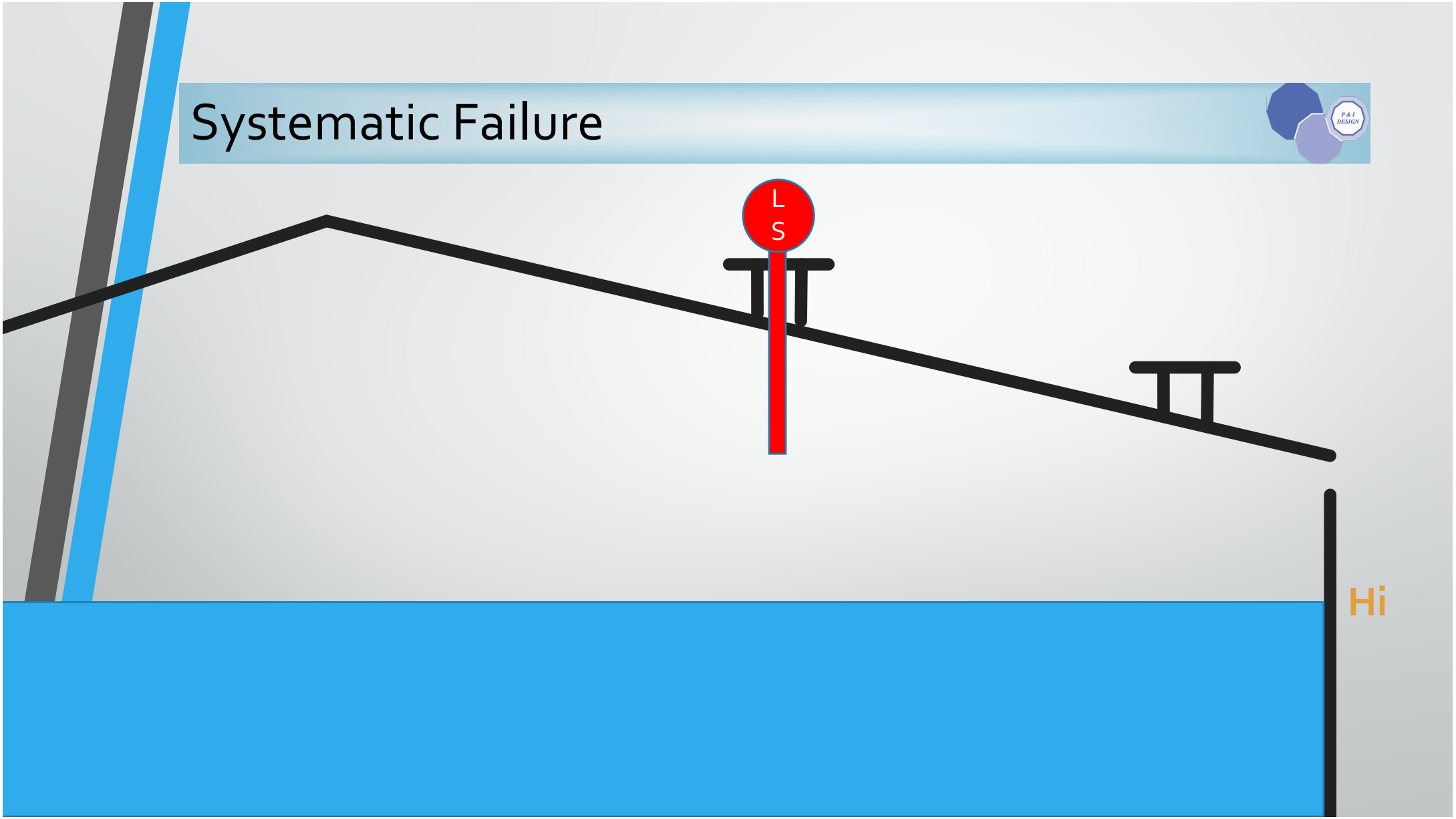


Tank taken out of service for maintenance and re-commissioned

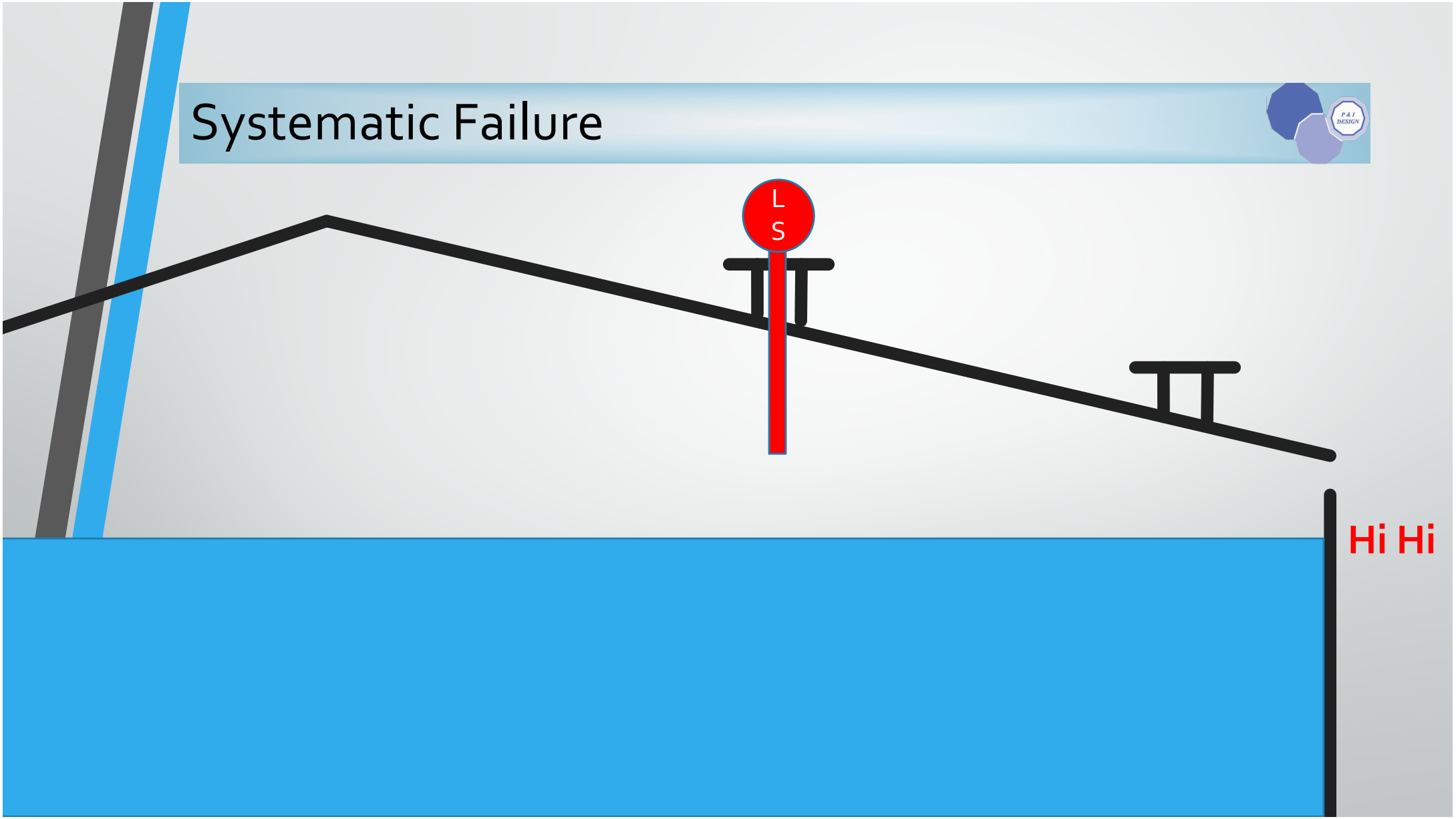
Systematic Failure



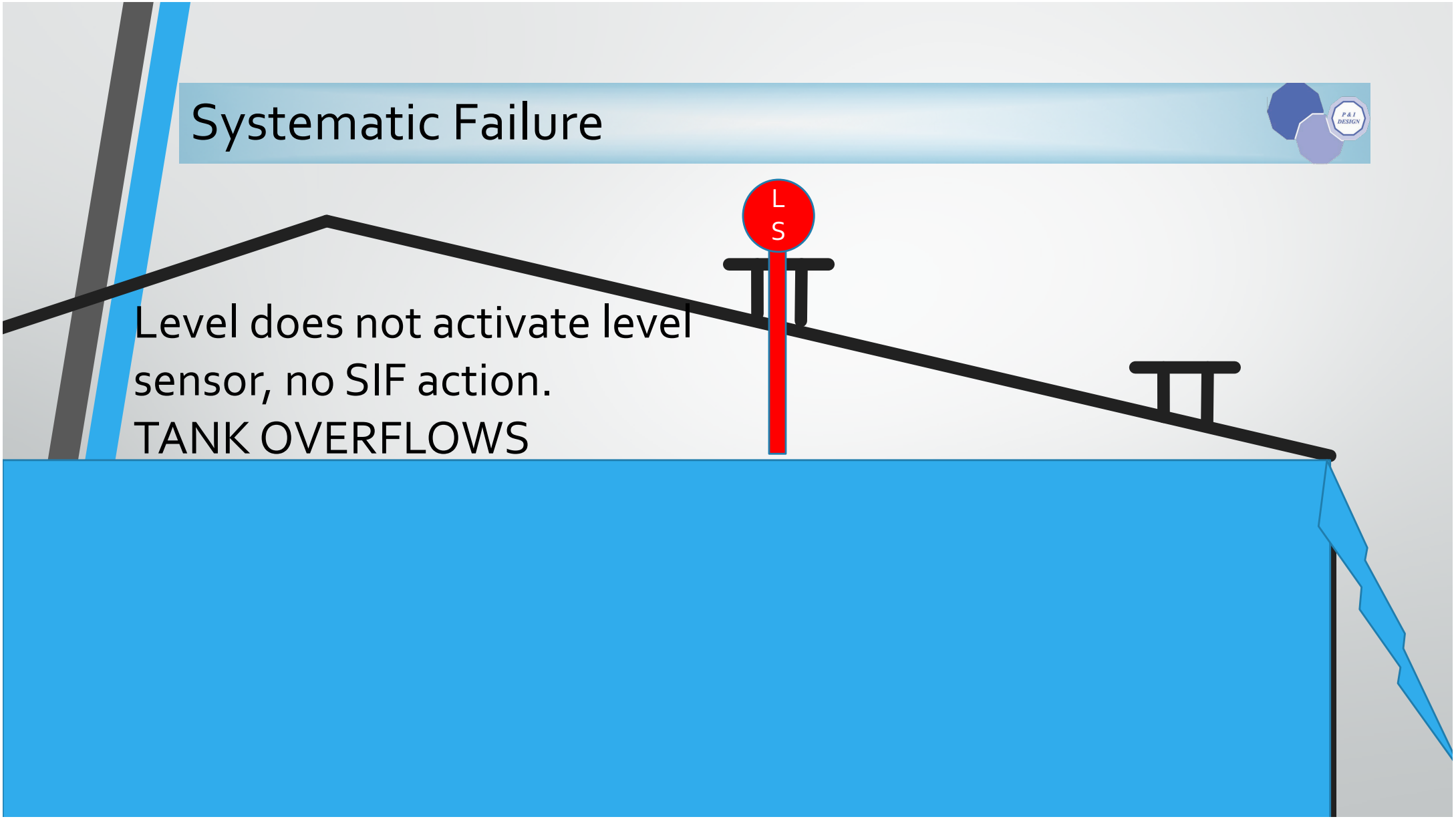
Systematic Failure



Systematic Failure



Systematic Failure



Level does not activate level sensor, no SIF action.
TANK OVERFLOWS

SIS Failures - Preventing Systematic Failures

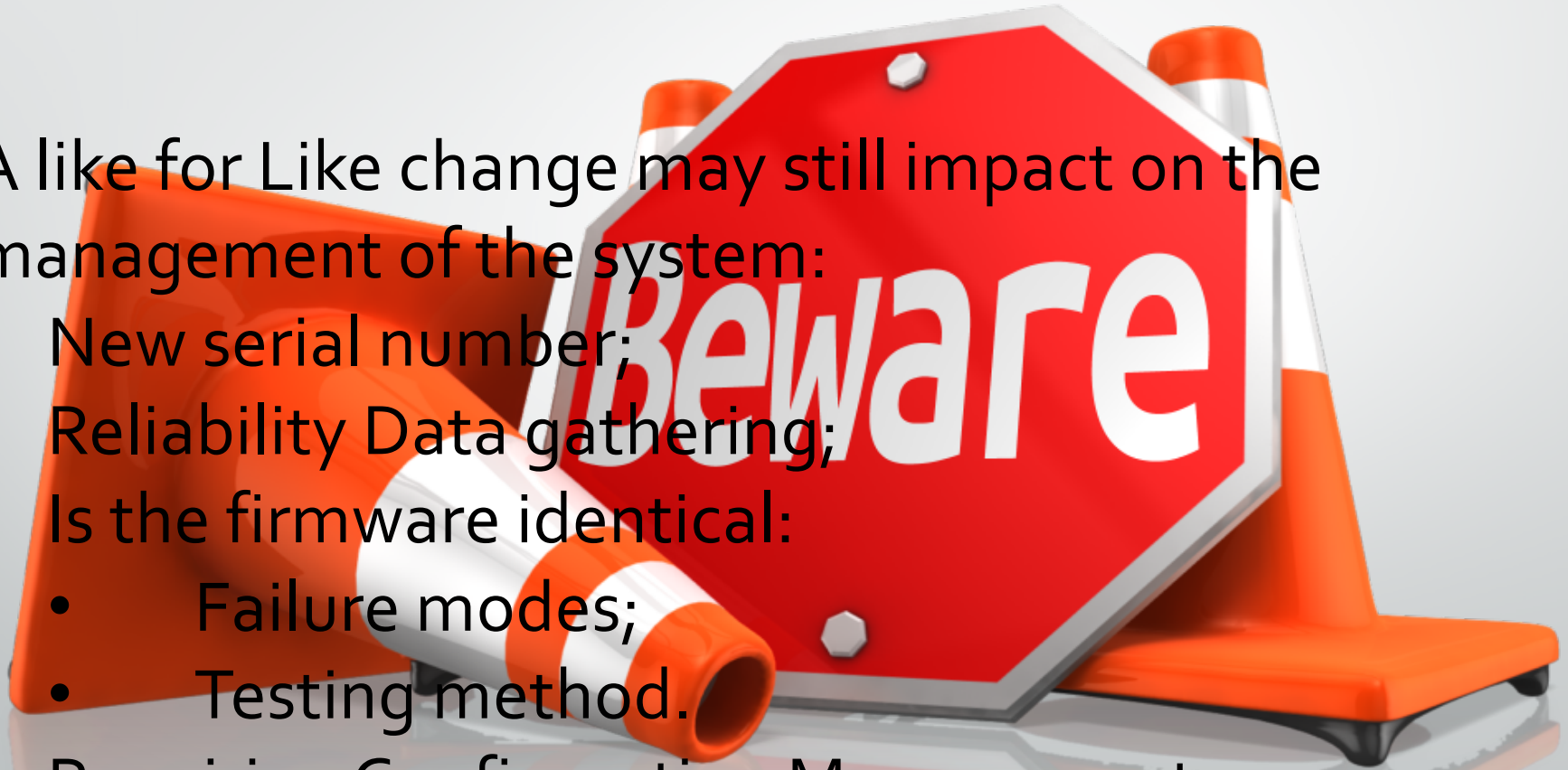
Employment of safety competent personnel
Controlled realisation including design reviews
Verification processes
Configuration management
Document control (including software)
Functional Safety Assessments
Validation processes – including FAT & SAT
Controlled operation, proof testing and maintenance
Controlled site modifications – including MoC & FSA's

Modification

What is a modification?

A modification, is any change to the SIS other than a like for like replacement of a component.

Modification



A like for Like change may still impact on the management of the system:

- New serial number;
- Reliability Data gathering;
- Is the firmware identical:
  - Failure modes;
  - Testing method.

Requiring Configuration Management

Modification

No modifications to the SIS should be carried out without following the SIS procedures for modification in order to ensure functional safety.

MoC

FSA 5

SIS Lifecycle - Modification

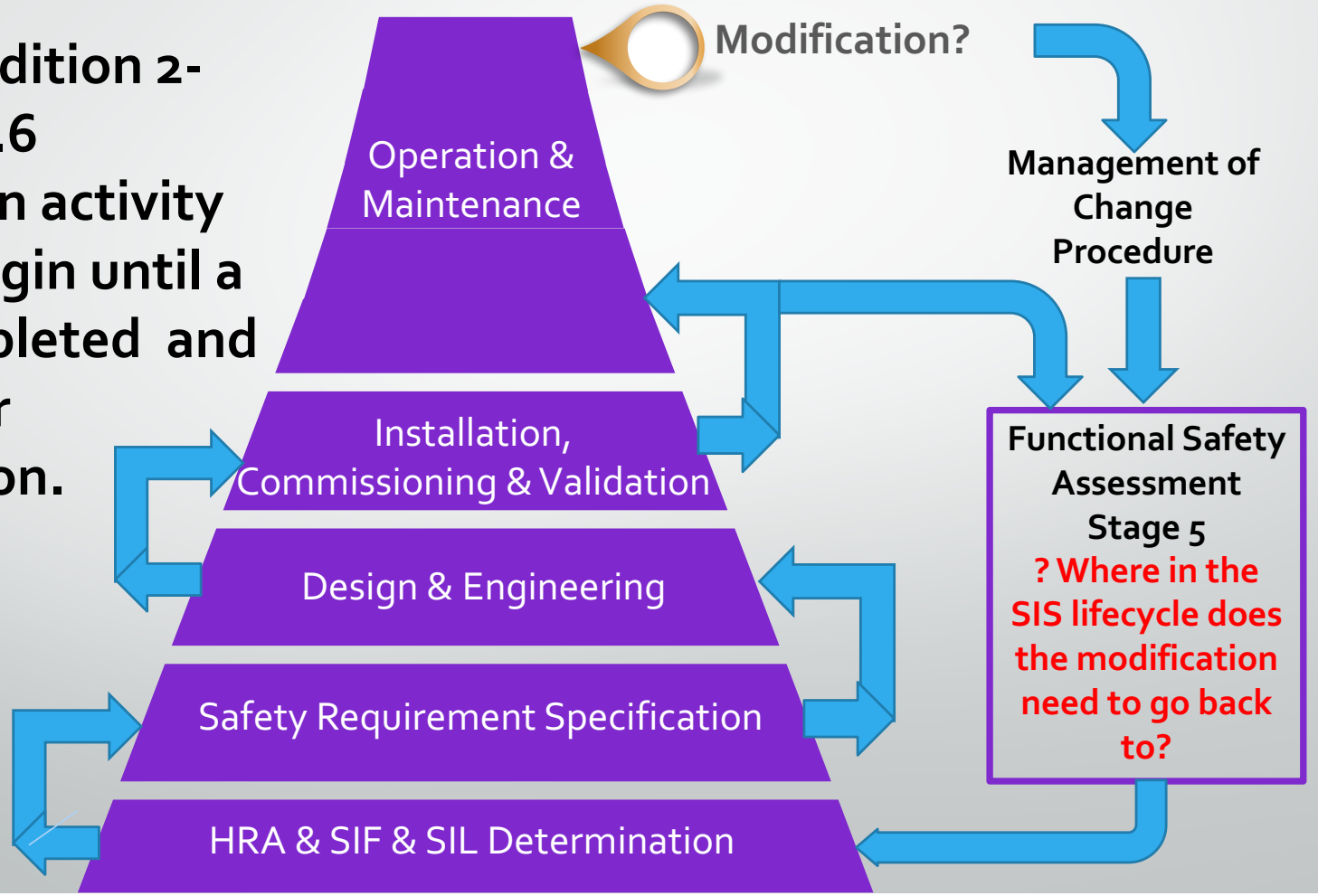
Modification?

Management of Change Procedure

Functional Safety Assessment Stage 5

SIS Lifecycle - Modification

IEC 61511 Edition 2- Clause 17.2.6 Modification activity shall not begin until a FSA is completed and after proper authorisation.



Decommissioning of the SIS

Decommissioning of the SIS should be treated the same as a modification.

It is essential that a FAS 5 is conducted to ensure that by removing the SIS or SIF that no extra demand is placed on other protection layers.

End of Part 4!

P & I Design Limited

P & I DESIGN

2 Reed Street,
Gladstone Industrial Estate,
Thornaby TS17 7AF
Tel: +44 (0) 1642 617444
Fax: +44 (0) 1642 616447
Email: sales@pidesign.co.uk
www.pidesign.co.uk

Produced by www.billinghampress.co.uk