Hints, Tips & Pitfalls

SIF Design & Compliance Evaluation

Dave Ransome - BA, CEng, FInstMC

Registered Functional Safety Engineer

About me

Chairman of P & I Design Ltd

BA, CEng, Fellow of the InstMC and InstMC Registered Functional Safety Engineer

Involved in Process & Instrumentation for over 50 years

Involved with Safety Instrumented Systems for over 45 years

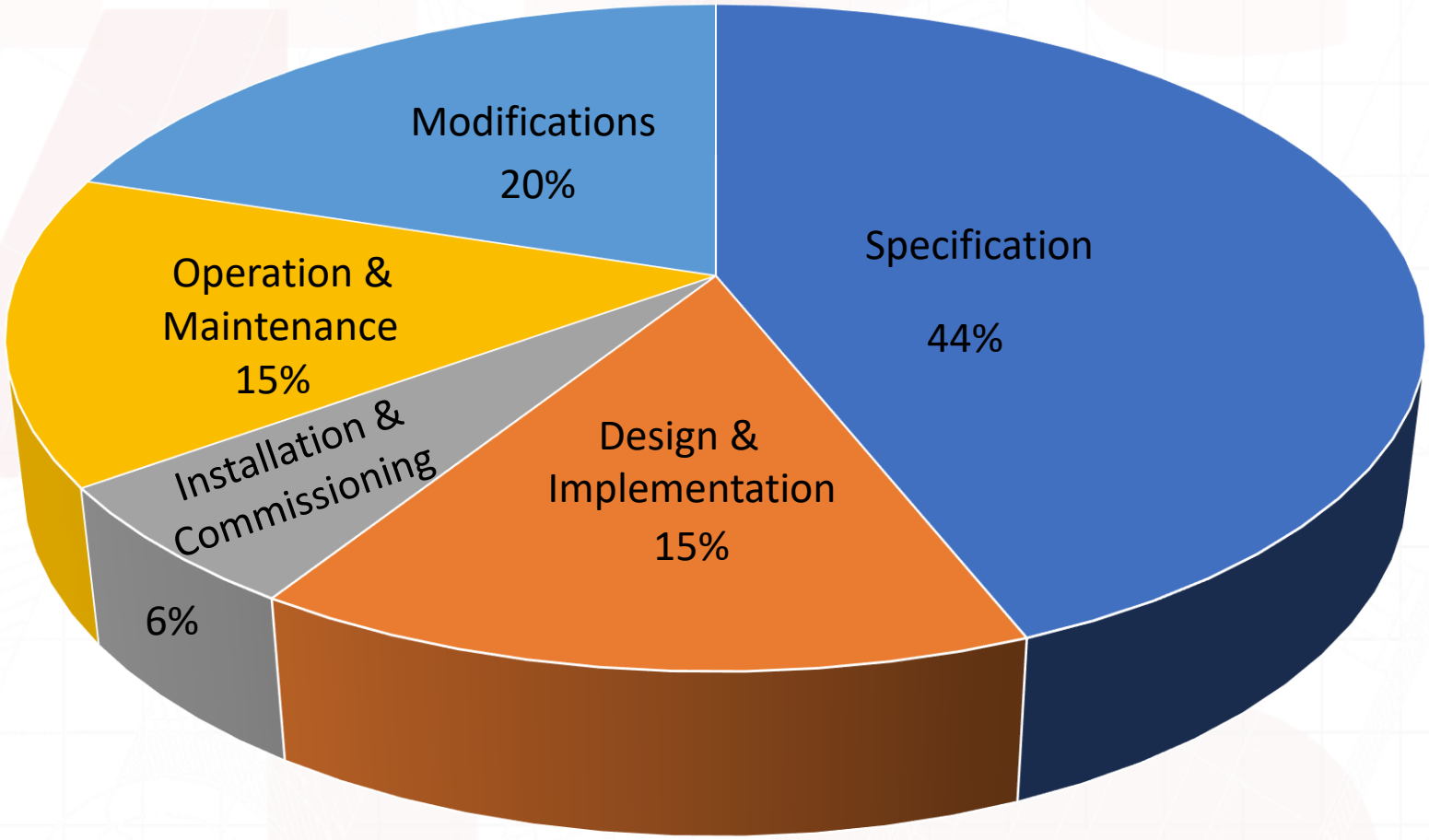
SIS prior to IEC 61511

- HIPS – Relief Valve Discharge System
- Tenor Drum – Plant Safety Checks
- Dreloba Logic – Ethylene Oxide Storage and Road Loading

Contributing member on:

- BSTG
- PSLG
- CDOIF
- InstMC – Safety Panel and FS-SIG
- 61508 Association

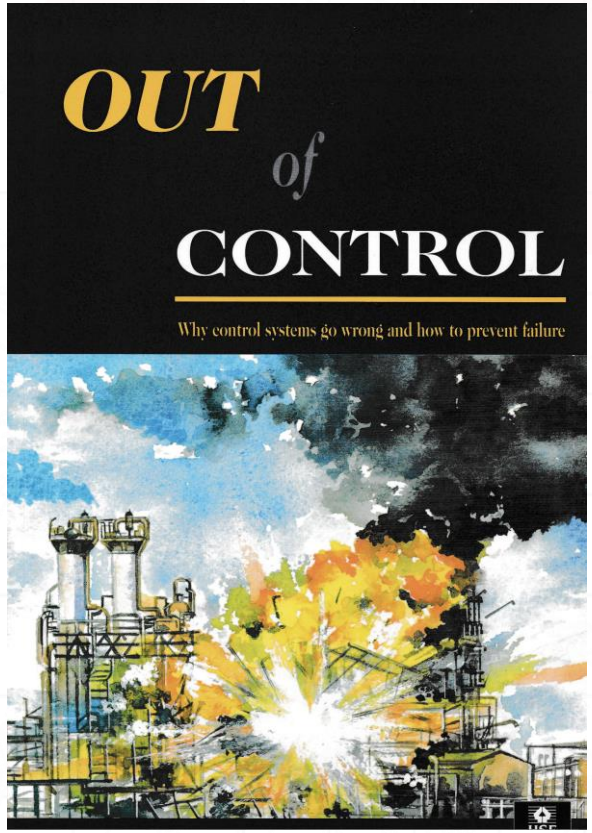
Primary Cause of incidents by life-cycle phase



Source: HSE – Out of Control – Why control systems go wrong and how to prevent failures

The previous slide - analysis of the failures contained in “Out of Control” was produced in the 1990’s

Would it be the same today?



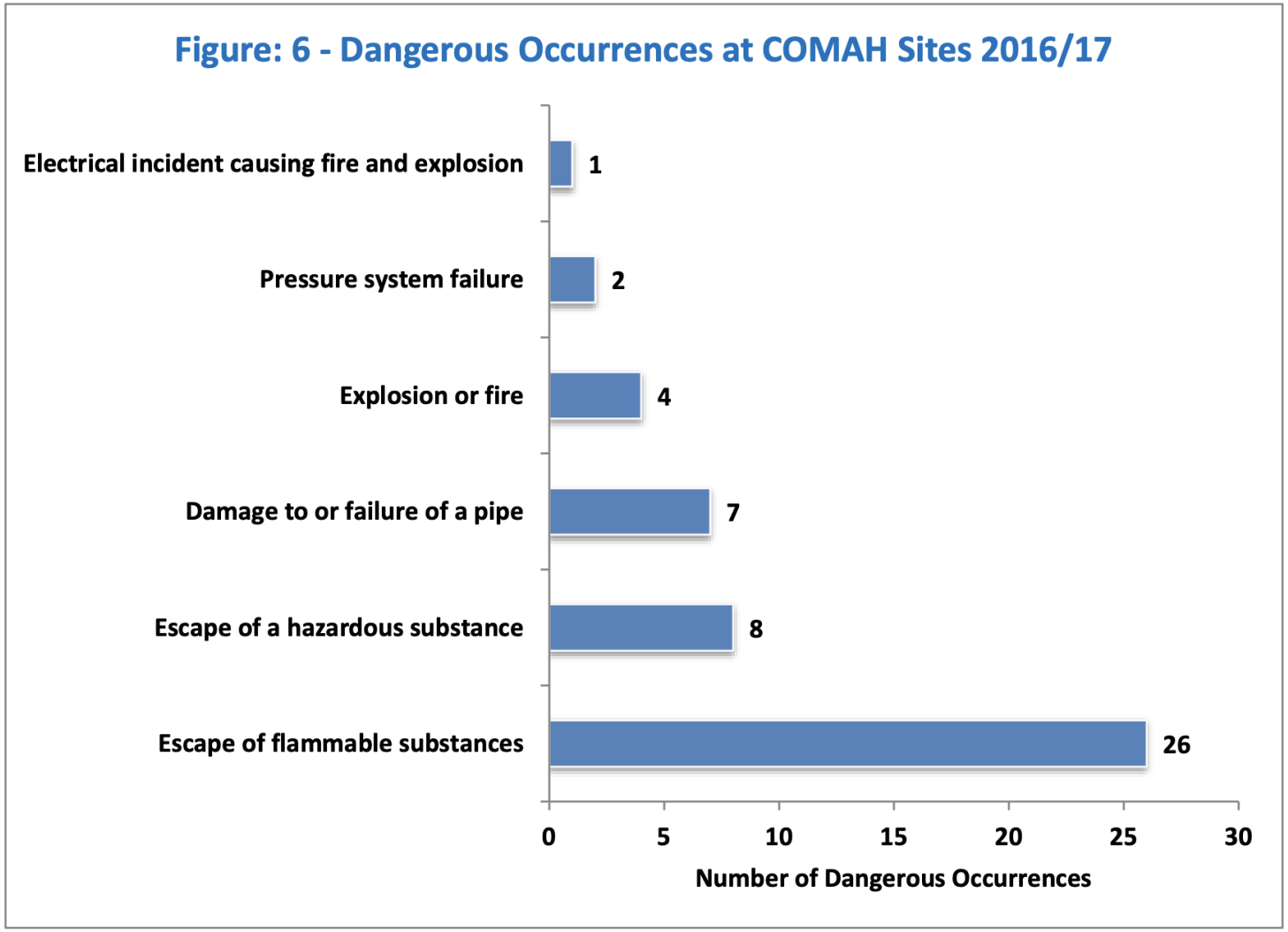
The COMAH Strategic Forum have recently published the following performance report:

COMAH Strategic Forum

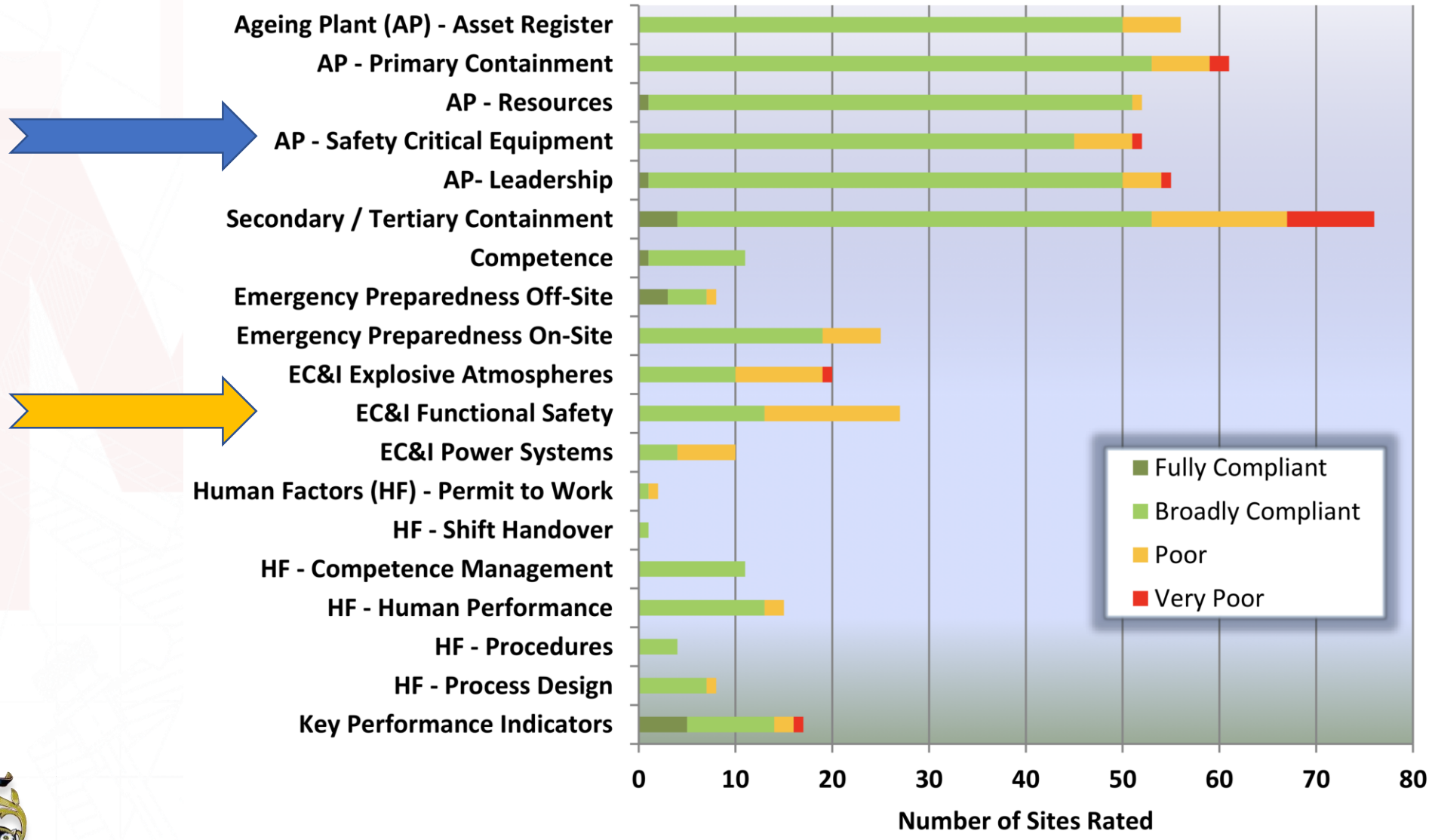
Control of Major Accident Hazards Regulations 2015 (COMAH)

PERFORMANCE REPORT 2016/17

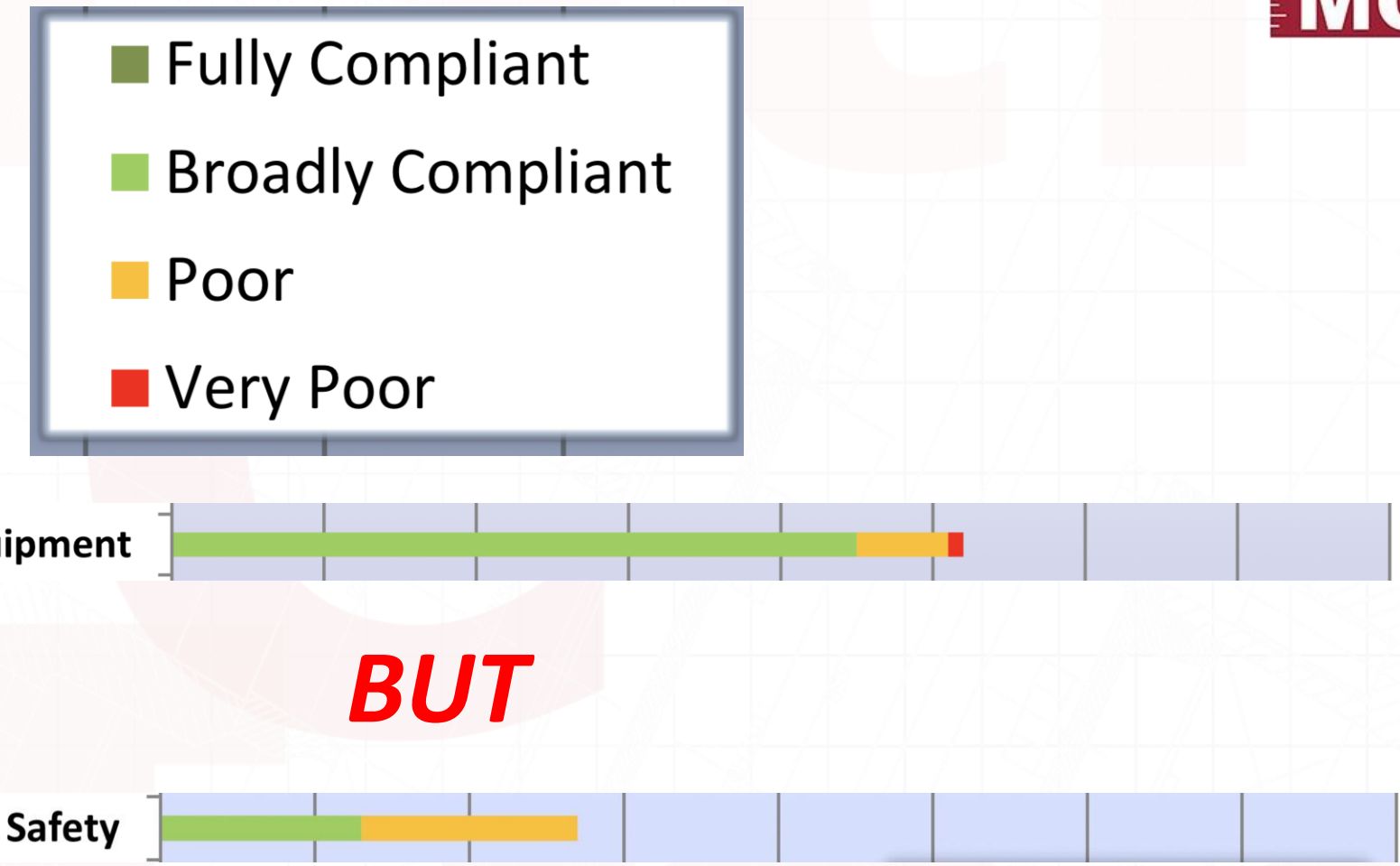
A dangerous occurrence is an incident with a high potential to cause death or serious injury, but which happens relatively infrequently. All businesses are required to report such incidents to the enforcing authorities.



What the inspections revealed



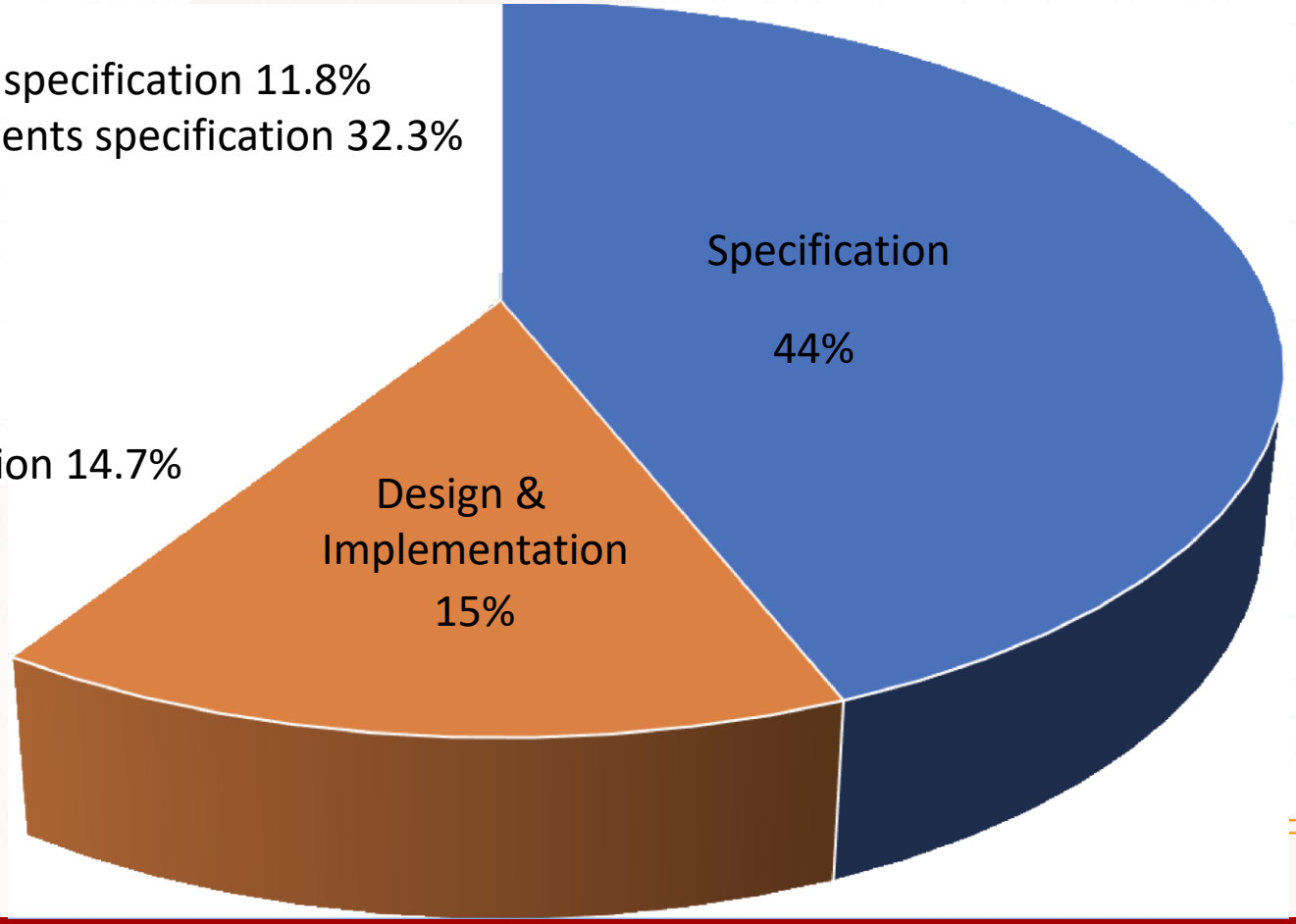
What the inspections revealed



Incidents due to causes in Realisation Phase

Specification:
Inadequate functional requirements specification 11.8%
Inadequate safety integrity requirements specification 32.3%

Design:
Inadequate design and implementation 14.7%



Hint !

Develop realisation life-cycle phase safety plan

evaluate SRS and conceptual design

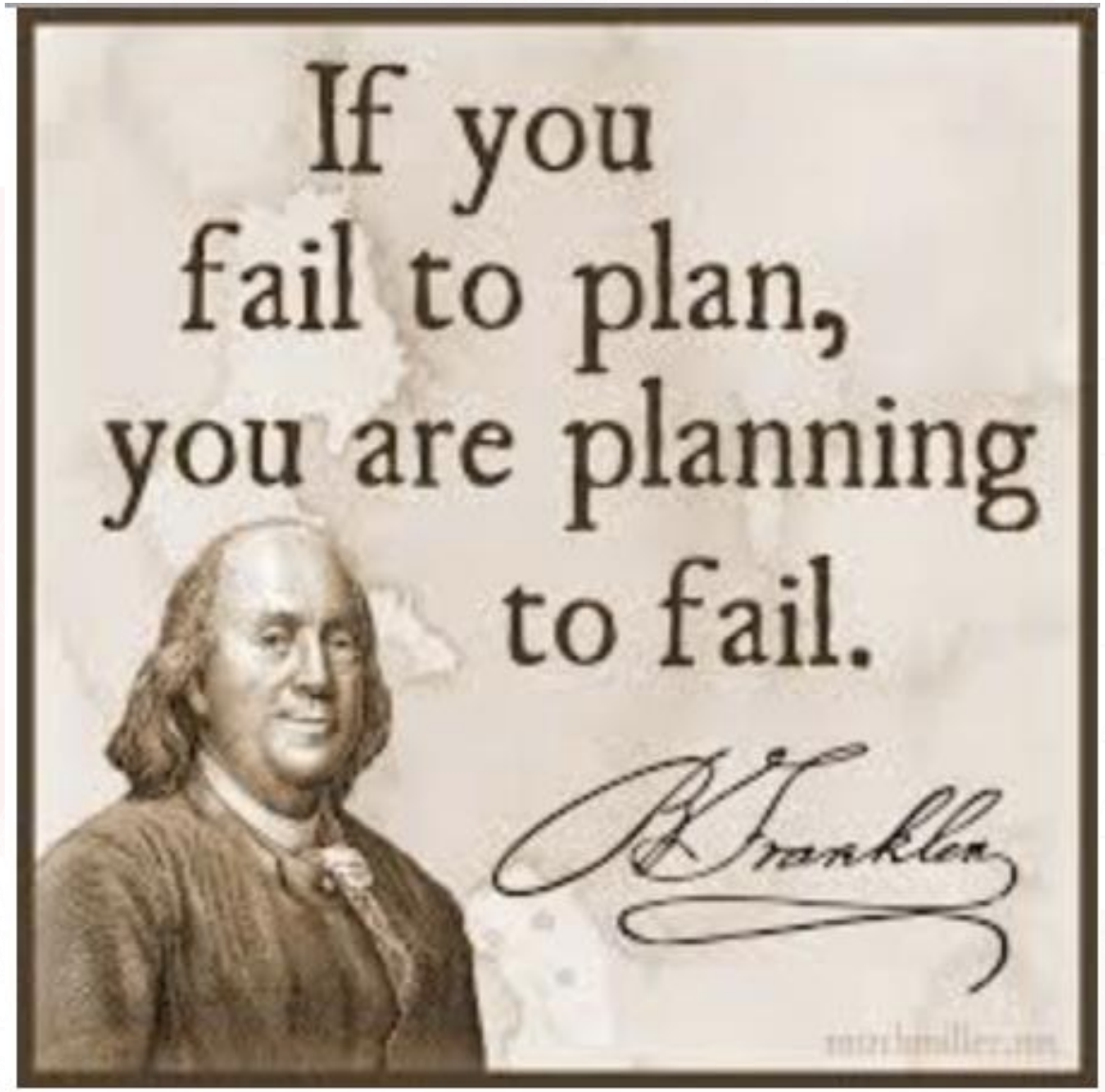
Specify the SIS components

integrate the SIS design

generate SIL verification, design and testing documentation

notify FSA team in preparation for FSA 2

Develop realisation life-cycle phase safety plan



Develop realisation life-cycle phase safety plan

Hint !

Is there a high level life-cycle plan already in place to cover all life-cycle phases?
If not the Designer should raise this omission with the end user (system owner).

The designer should create specific detailed plans for the elements of the life-cycle they are involved in.

Elements of the life-cycle plan:

- activity list
- objectives, inputs and outputs for the life-cycle phase
- verification methodologies and techniques
- roles, responsibilities and competency
- specific plans for Software, FAT or other elements of the realisation phase.

Develop realisation life-cycle phase safety plan

SIS life-cycle planning is an iterative process:

From the cradle to the grave

HRA → SRS → Design → Install & Commission → Operation & Maintenance → Modification → De-commission

With different Stakeholders throughout the SIS life-cycle interactions and interfaces can be overlooked.

All activities in the safety life-cycle are impacted by upstream and downstream activities.

An interesting formula.

Where there are many companies/interfaces within the life-cycle phase, then complexity will increase.

C = Complexity
N = Number of interfaces

Then:

$$C = 2^N$$

Source: Safety instrumented Systems – A life-cycle Approach – Paul Gruhn and Simon Lucchini

Evaluate SRS and conceptual design

proceeding with the design without a complete or with an inadequate Safety Requirement Specification.

A complete SRS covers:-

all functional, safety and performance aspects as well as testing and diagnostics requirements.

it includes bypass philosophy, testing philosophy, approved device criteria, process and response SIF time, providing the crucial inputs for efficient SIS design.

it is a specification requirement document, not a detailed design document.

it is a living document which is to be updated if any modification to the SIS arise.

Inst MC

Read the FSA 1 report and verify all actions have been resolved.

An open action may lead to a change in the SRS, SIL or SIF's functionality.

=Method Functional Safety

Specify the SIS components

Specifications

Many component specifications produced are incomplete, inadequate, or don't exist.

A good specification will cover the following:

Functional specification – what the system should do!

Integrity specification – how well it should do it!

Incidents due to causes in Realisation Phase

Specification:
Inadequate functional requirements specification 11.8%
Inadequate safety integrity requirements specification 32.3%

The following incident illustrates how a SIF specified correctly for functionality, but with an inadequate integrity specification led to a **Systematic Failure** with a dangerous outcome.

What Happened

A driver was loading 3700L Super Unleaded Fuel at Hemel Hempstead Terminal.

Flow failed to stop, causing an overfill from the top of vehicle.

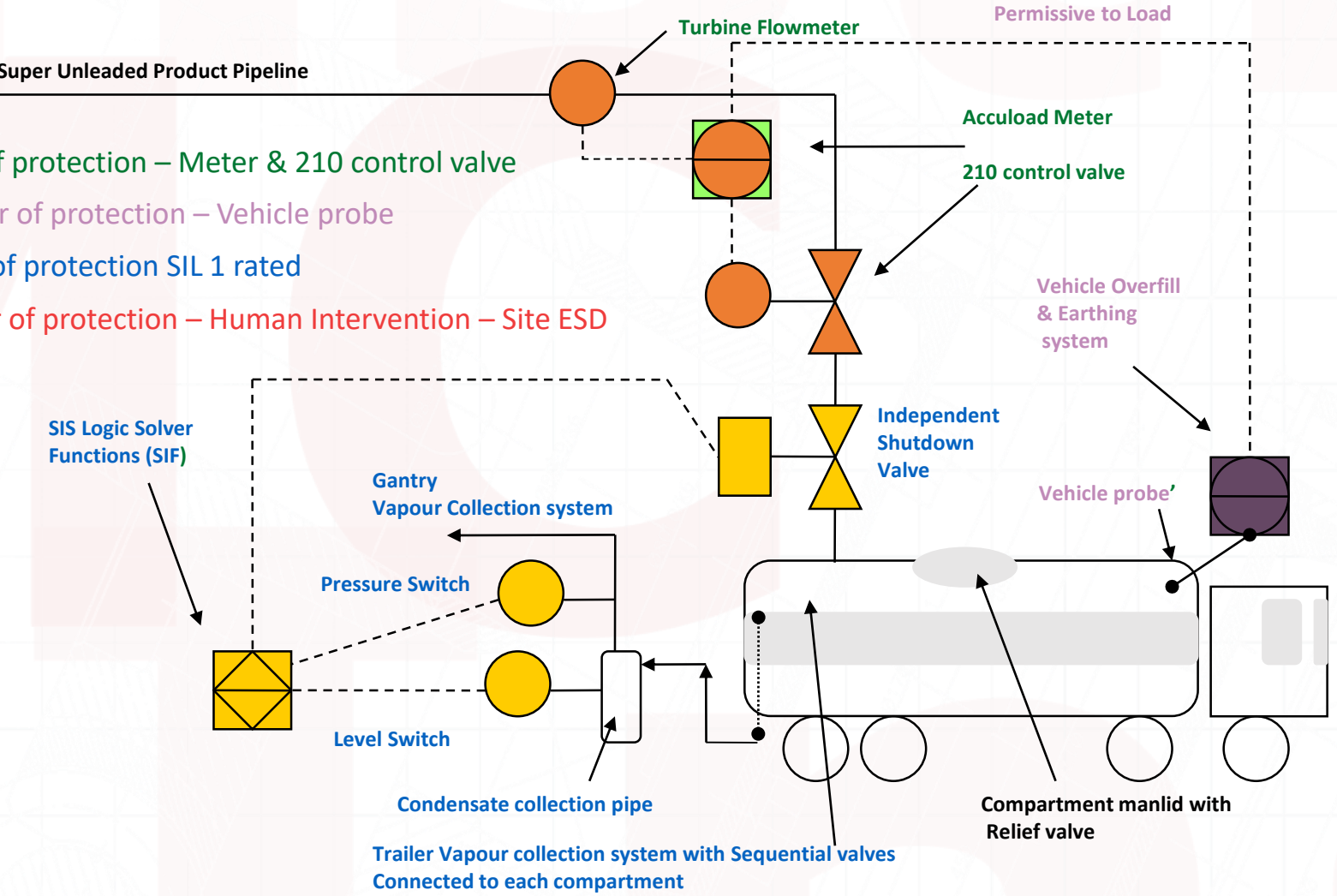
The driver hit the ESD causing a site wide shutdown, stopping the flow of fuel.

The Investigation reconciled the spilt quantity as 528 litres.

Specification – Failure Example

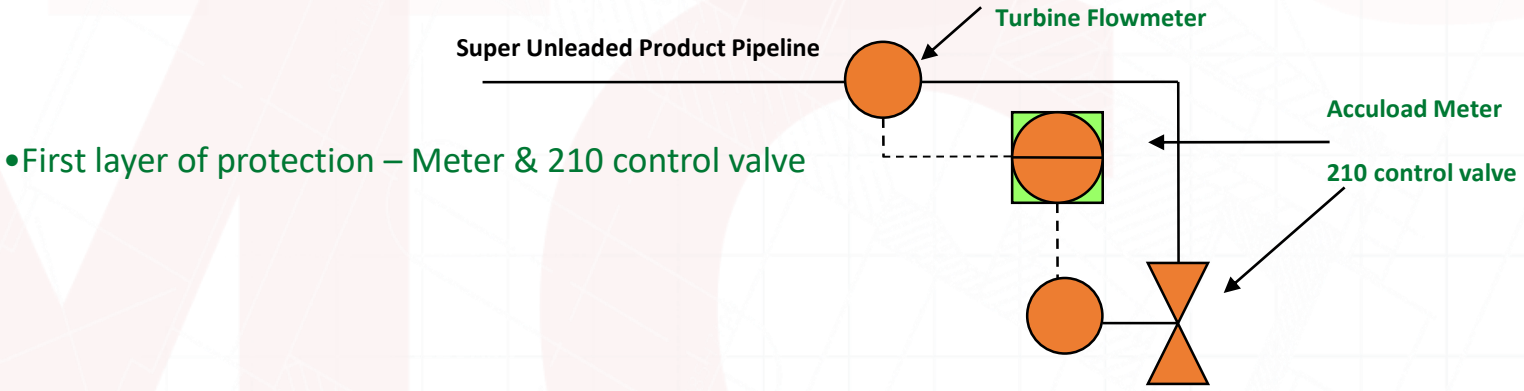
Road Tanker Overfill prevention. Layers of Protection

- First layer of protection – Meter & 210 control valve
- Second layer of protection – Vehicle probe
- Third layer of protection SIL 1 rated
- Fourth layer of protection – Human Intervention – Site ESD



What Happened

First Layer of Protection:
Basic Process Control System

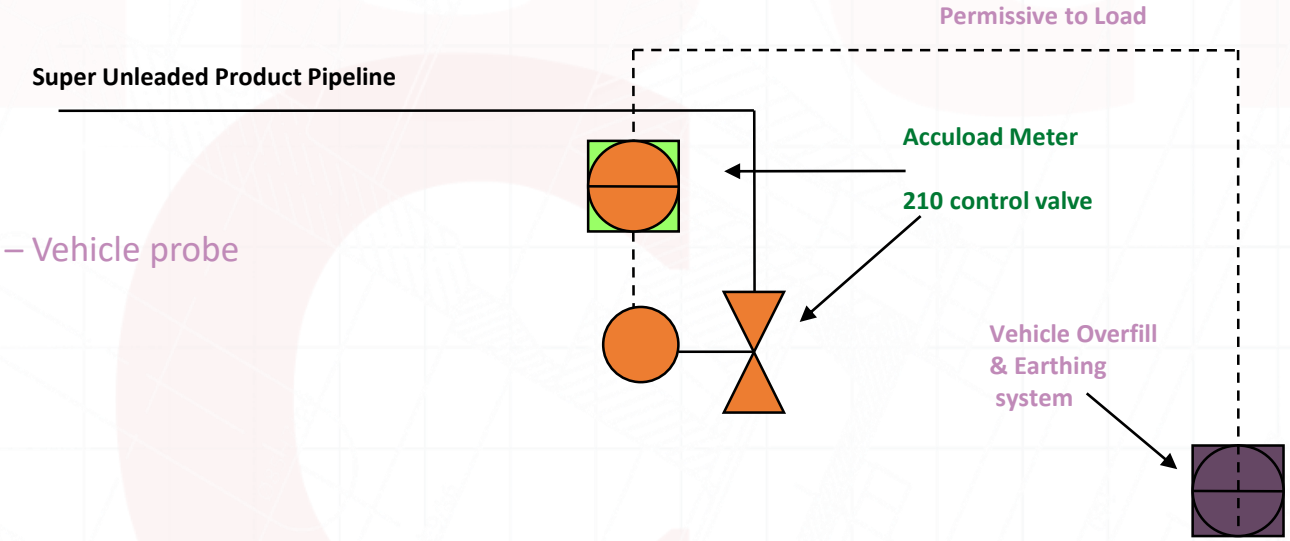


The product flow is regulated via a “210” control valve. This valve is controlled via the “Accuload” intelligent meter connected to the Terminal automation system.
Post incident the 210 valve was tested and an intermittent fault discovered.
The valve sticking in the open position was determined to be the immediate cause of the incident.

Specification – Failure Example

What Happened

Second Layer of protection:



- Second layer of protection – Vehicle probe

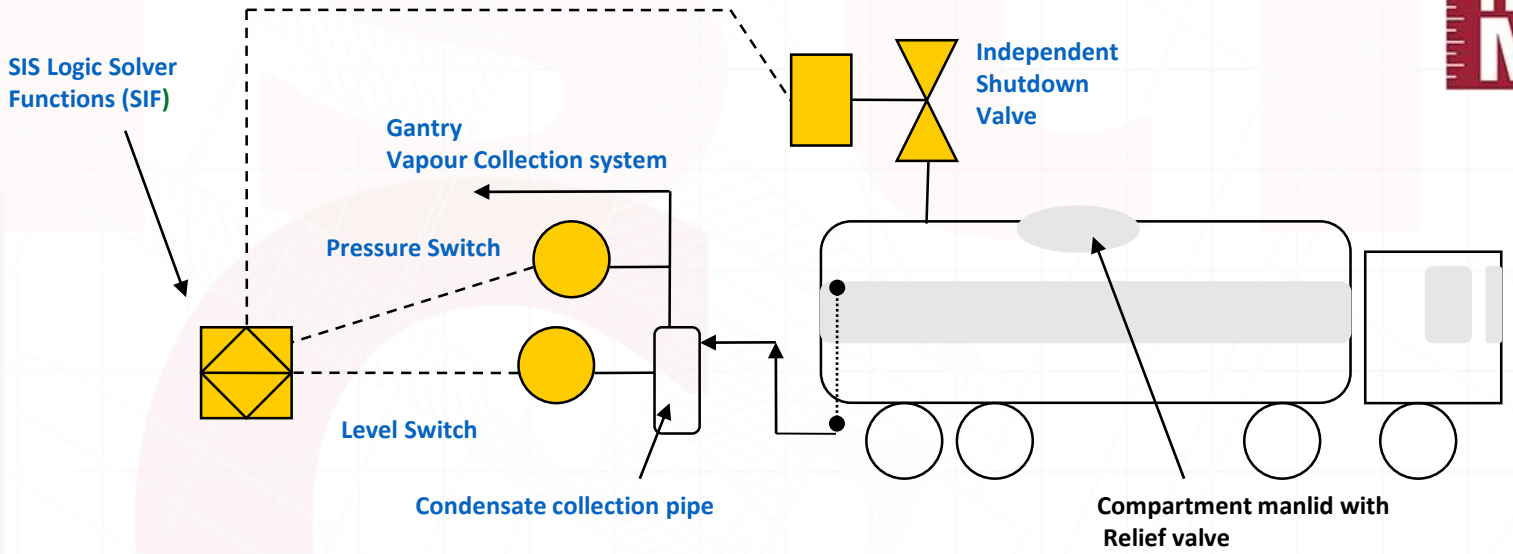
Each vehicle compartment is fitted with a high level optical probe which, when covered by the product, removes the “permissive to load” from the Accuload device and closes the 210 control valve.

This layer of protection failed due to the 210 control valve being stuck in the open position.

PROTECTION LAYER WAS NOT INDEPENDENT TO PL 1.

Specification – Failure Example

Third Layer of Protection: SIL 1



The design of the 3rd layer of protection is based upon product overfilling the vehicle compartment into the vapour recovery system and triggering a high level switch installed in a liquid collection pipe on the loading gantry. In addition a pressure switch detects a high pressure in the same vapour line.
Both the high level and pressure switch are connected to an independent Logic Solver and this, when triggered, removes the air supply to an independent valve on the loading arm.

Third Layer of Protection: SIL 1

The SIL 1 rated system failed to operate due to:

1. A fundamental flaw in the specification and design
2. The design flaw was overlooked by an Independent Functional Safety Assessment (FSA)
3. The flaw was not discovered due to inadequate “proof” testing during system commissioning

SIS Specification and Design Functionality

SIS functionality was tested and was found to operate when the level of liquid in the vapour knock-out pot reached 6 Litres or the pressure in the vapour line reached 46mbar.

SIS Specification and Design Integrity

After the incident the pot was drained and 5 Litres was found to be present hence not enough liquid had entered the vapour system quickly enough to activate the SIS system prior to the vehicle overtopping form the vehicles man-lid with relief valve.

Fourth Layer of Protection:

There was an ultimate fourth layer of protection, reliant on human intervention which is the gantry Emergency Shutdown Button.

In this incident the driver hit the button in line with the standing instructions, which limited the spill to 528l.

Integrate the SIS design

Design

Structured design process:

- consideration of interfaces, manual shutdown, bypasses
- de-energise or energise to trip – or mix?
- software

Modular Design
Function Blocks
Approved Software Module Testing

Consider the end user

Hardware components:

- well-tried / well-known
- complex or unique?

Where possible keep it simple, don't over complicate

Auditability and Design reviews:

all design documentation must be auditable and under revision/change control review and approvals.

Verification versus Validation

Verification – Checking that each "output" of that life-cycle phase is adequately and suitably completed , provide the associated documentation to move forward to the next life-cycle process or phase.

One of the main purposes of Verification is to identify and eliminate Systematic Failures through checking and review.

It is difficult to catch your own mistakes.

Design Reviews are required throughout the design, the FSA 2 is an Independent Review – Project Design Reviews are still required.

Verification versus Validation

Validation – Checking through inspection and testing that the "output" achieves the specified requirements.

Functionality and Integrity!

Late design changes often increase the risk of introducing faults.

They also lead to increased costs.

Generate SIL verification, design and testing documentation

SIS Product Selection Presentation (Next)

- Using certificated components and their pfd/SIL without reading the safety manual
- Not considering process and environmental conditions
- 100% belief in certificated failure data based upon FMEDA, MTBF assessment

Who produces the proof testing procedures?

I believe – the designer with the end user!
Why!

The **designer** integrated the components into a system. He/she:

- is aware of any constraints with the component selection
- understands the interaction relevant to redundant hierarchy
- understands the requirements of BS EN 61511
- may be aware of possible systematic and/or dangerous undetected failures

Who produces the proof testing procedures?

The **end user** knows his plant and process. They:

- are aware of any constraints in what and when can be tested
- understands the impact on the process during testing
- are responsible for the testing of the SIS
- are responsible for the safe operation of their facility

Proof testing procedures

Should be:

- useable and logical
- should identify critical tasks which may need independent checking
- structured to identify dangerous undetected failures
- if end to end testing is not possible, they should be structured to cater for modular testing
- the results must be recorded and be auditable
- the end user must be informed of any failures or shortfalls as a result of the test
- allow for efficient testing where redundant systems are employed

$C = 2^N$ - Therefore you could consider a 1oo2 sub-system as $C = 2^2$ and therefore efficient proof test procedures can be complicated.

Notify FSA team in preparation for FSA 2

Stage 2 – After the SIS has been designed.

The membership of the FSA 2 team shall include at least one senior competent person not involved in the project design team.

FSA team members should have the relevant experience covering the required disciplines, together with the end user.

TIP!

Ensure all actions which could have an affect on future life-cycle phases are resolved before proceeding with the procurement, build and installation phases of the life-cycle.

The End

Functional Safety 2018