# 8th Chemical Process Safety Sharing (CPSS)

## Safeguard Audit and Improvement


**Sittichai Poolsawad**
**OS&IH Manager-South Asia**
**Solvay Industrial Function HSE Asia Pacific**



**Nitad Suphattharasakda**
**Maintenance Supervisor**
**Solvay(Bangpoo)Specialty Chemicals Ltd.**


# Contents

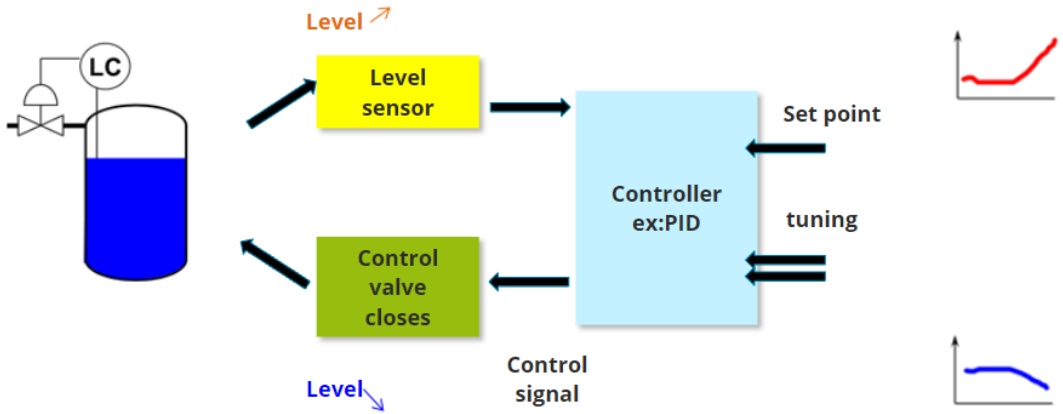


# Layers of protection

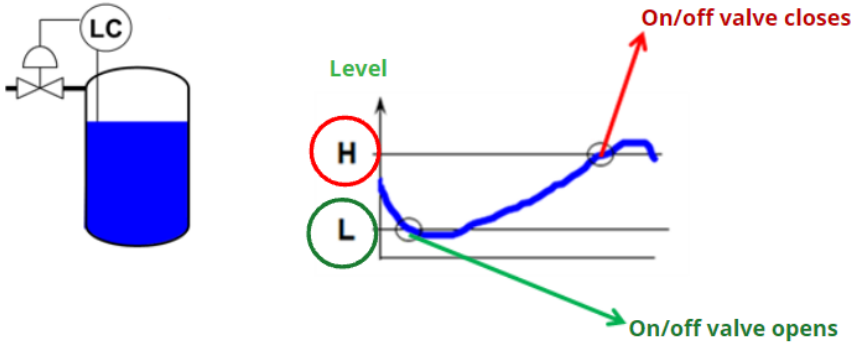
**1. Process Control**

Automatic functions are used in process control.

This process control can be continuous as shown in the following diagram for a level control LC.




The process control can also be an on-off control (LX):




The purpose of the **control system, process alarms and operator supervision** is to maintain the process in its **normal operating range**.

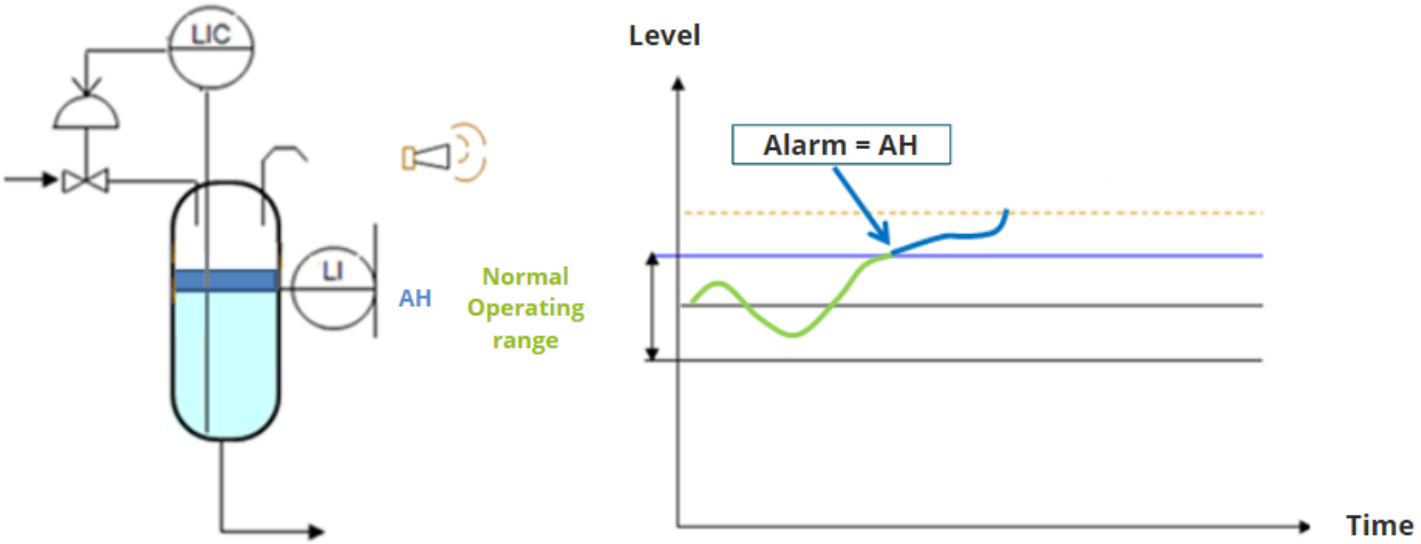


# Layers of protection

## 2. Safety functions

If something unusual happens, an action has to be done to stop the drift out of the normal operating range:

- this action can be a human action (following an alarm: A)





# Layers of protection

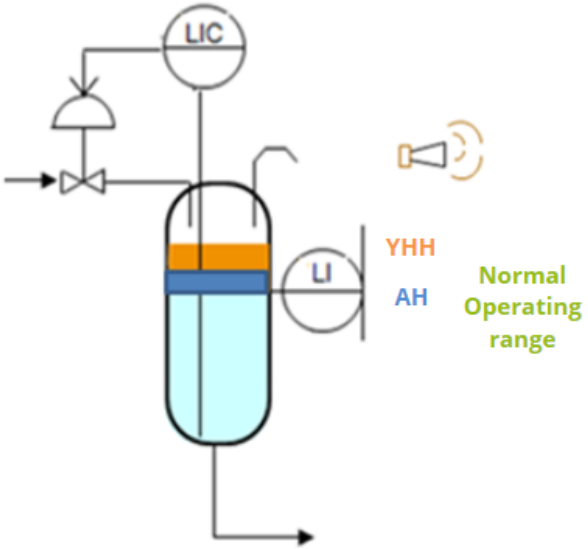
## 2. Safety functions

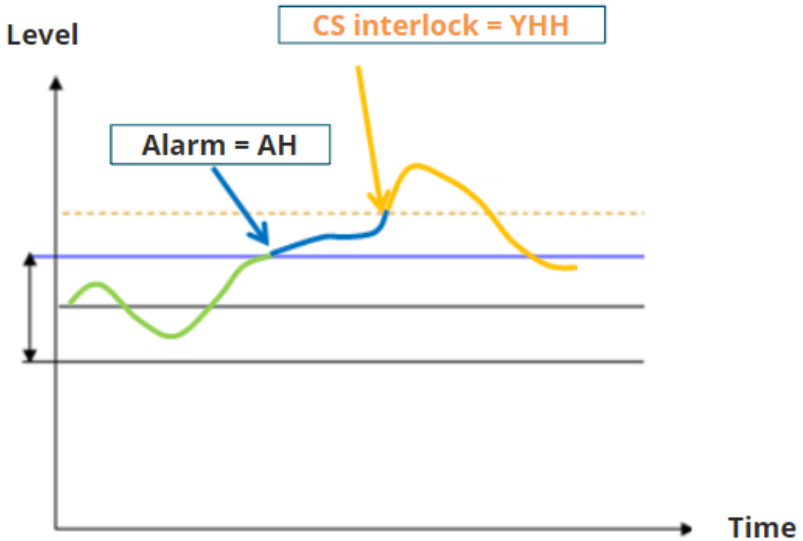
If something unusual happens, an action has to be done to stop the drift out of the normal operating range:

- this action can be a human action (following an alarm: A)

  or an automatic action done by the control system (Control System Interlock: Y).

Both are **instrumented safeguards**.



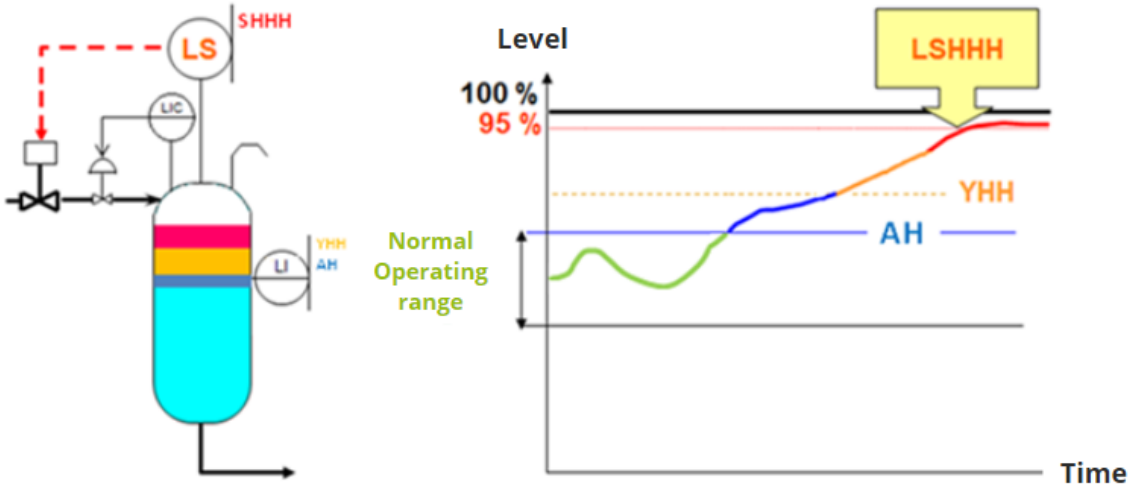


# Layers of protection

## 2. Safety functions (continued)

To control a potential risk, a safety action (S) **independent** of the control system is activated (in this case of high level to **prevent** the overflowing through the vent pipe).

It is an **instrumented safeguard**.





# Layers of protection

## II – Fundamentals of instrumented safeguards

### 2. Instrumented safeguards and Layers of protection (continued)


a **S**afety **I**nstrumented **F**unction, or **SIF**, is in the "Safety Instrumented Functions" layer of protection.

a **B**asic **P**rocess **C**ontrol **S**ystem **I**nstrumented **F**unction, or **BPCSIF**, is in the "Control System Interlocks" layer of protection.

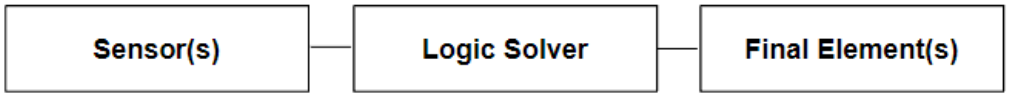
a **H**uman **I**nstrumented **F**unction, or **HIF**, is in the "Human Safeguards, Alarms with operator action, Operator safety interlocks" layer of protection

Normal operating range

# Layers of protection

## 1. General Structure

An **instrumented safeguard** is made of **three subsystems**: (i) **Sensor(s)**, (ii) **Logic Solver** and (iii) **Final Element(s)**.




i. The **"Sensor(s)" subsystem** corresponds to the measurement subsystem: sensor(s) and **transmitter(s)**.

ii. The **"Logic Solver" subsystem** corresponds to the logic treatment section:
threshold detection, logic treatment and sending of an order to the final element(s) subsystem.
The Logic Solver is called a Safety Logic Solver (**SLS**) for the safeguards of the layer of protection "safety instrumented functions".

iii. The **"Final Element(s)" subsystem**, also called **"actuator(s)"** subsystem actsdirectly on the process with mechanical or instrumented devices.

Their implementation is based on international references, as follows:

- IEC (EN) 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems,
- **IEC (EN) 61511**: Functional safety - Safety Instrumented Systems **for the Process Industry Sector,**
- **ANSI / ISA 84.00.01- Parts 1-3**: "Application of Safety Instrumented Systems **for the Process Industries**".



## III - Structure of an instrumented safeguard

### 2. Contents of the subsystems

The sensor(s) and the final element(s) subsystems are made up of one or more components in order **to achieve the desired levels of effectiveness and reliability.**

Any subsystem is MooN type, i.e. "**M"out of "N"** system (M and N are numbers).

That means that this system is made up of **N** independent components so that **M amongst these N** components need to be activated in order to perform the function of the subsystem.

**The most common MooN subsystems are:**

- **1oo1**
- **1oo2**
- **2oo3**

They are presented further.

A safeguard with a MooN subsystem where N is higher than 1 and different from M is more reliable than a safeguard with a 1oo1 subsystem.

Note: a MooN system is also termed "MooN voting" system.



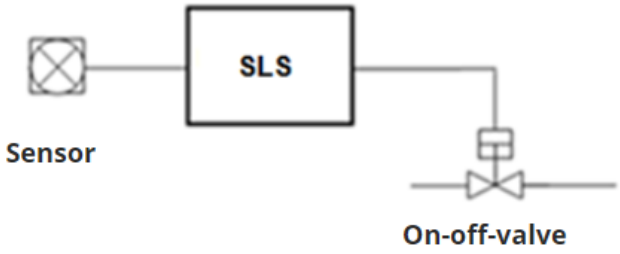
## III - Structure of an instrumented safeguard

### 3. Redundancy

➢ **Instrumented safeguard without redundancy:**

- An **instrumented safeguard** without redundancy (also called simple safeguard) is **made up of only one sensor** and **one final element**.
- The sensor and the final element subsystems are both **1oo1** subsystems.
- The logic solver subsystem is always a 1oo1 subsystem.

➢ **Example:**

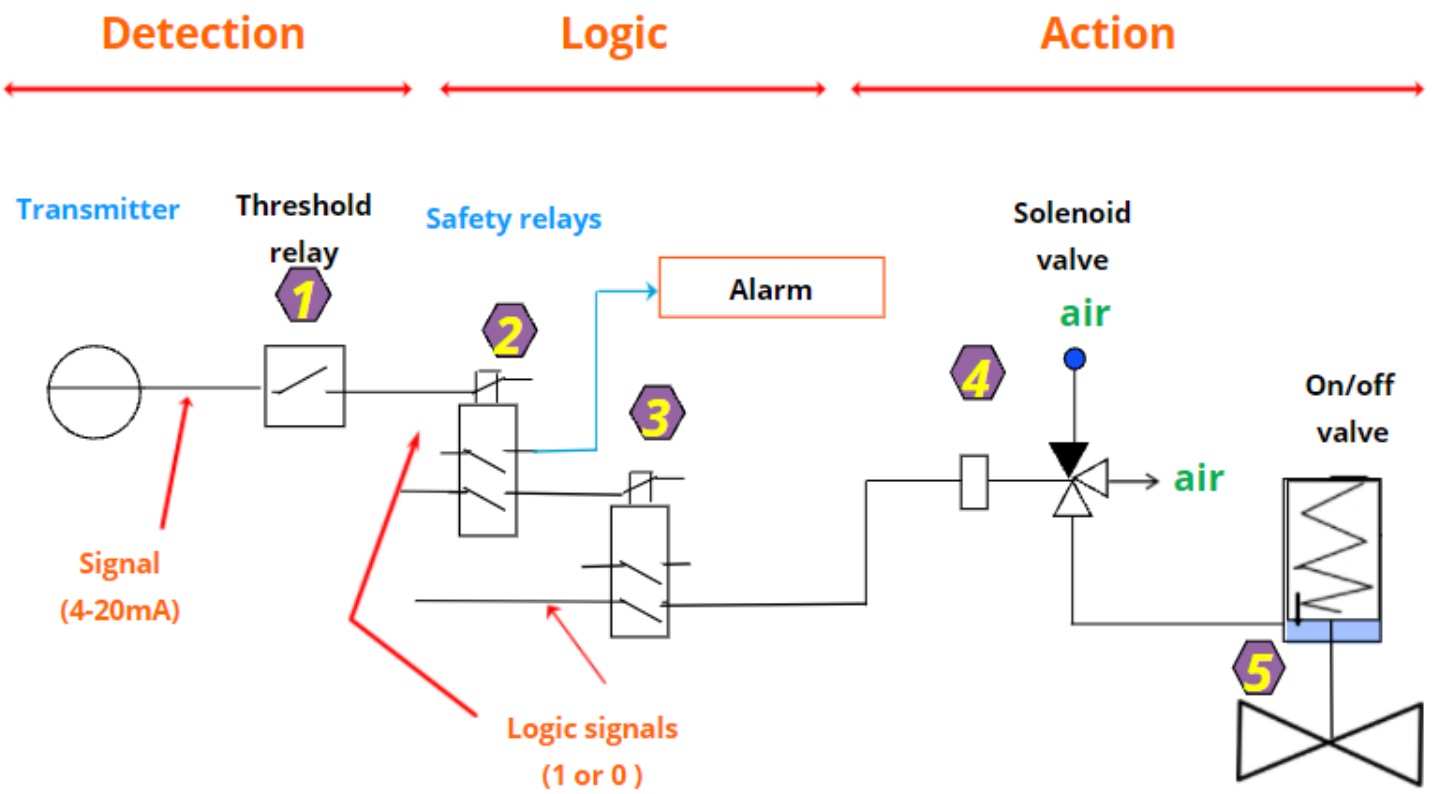



**SLS: Safety Logic Solver**



# IV - Characteristics of instrumented safeguards

## 3. Standard design







*Monthly process safety bulletin – May 2020*

# Overfilling a storage tank

## *Description*

7 m³ of hydrogen peroxide (70 %) overflowed from a storage tank into a retention dike. The spillage was dealt with according to the Standard Operating Procedure, in order to prevent uncontrolled decomposition from occurring. No one was hurt and there was no damage to the environment.

## *The facts*

70 % hydrogen peroxide has the following hazard classifications under the Global Harmonized System:

- H271: May cause fire or explosion; strong oxidizer.
- H302: Harmful if swallowed.
- H314: Causes severe skin burns and eye damage.
- H318: Causes serious eye damage.
- H335: May cause respiratory irritation.

The stock tank was designed with two level instruments:

- analogic level sensor with a high level DCS alarm,
- on/off high high level sensor with DCS interlock which stops the feed of hydrogen peroxide (pump + automatic valve).

On the day of the incident, the stock tank was being filled with 70 % hydrogen peroxide. A shift leader saw that hydrogen peroxide was spilling from the overflow line of the stock tank into the retention dike. He immediately stopped the flow of hydrogen peroxide to this storage tank. He diluted the hydrogen peroxide in the retention dike with water to reduce its concentration below 10%. Diluting the material in this way keeps it below its boiling point and avoids the emission of fumes of hydrogen peroxide. The operating team then added caustic soda slowly to decompose the hydrogen peroxide in a controlled way, following the Standard Operating Procedure.



# Lessons Learned

## *Explanation*

The scenarios of overfilling the stock tank were examined during the risk analysis. The working group concluded that the potential Severity of such a scenario was Low, given the retention dike, which is a passive safeguard, and that the potential Risk was level 3 (acceptable). Therefore, no active safeguard was required and the on/off high high level sensor was never tested.

The analog level sensor failed due to ageing of its membrane. The level reading got stuck at 80.6% during the filling operation so the high level alarm was not triggered.

At the same time the on/off level sensor failed because its magnet was blocked (Mobrey type), so the DCS interlock, which should have stopped the filling pump and closed the automatic valve, was not triggered either.

| Hydrogen Peroxide Storage Tank | On-off (Mobrey) level sensor |
|---|---|
|  |  |

# Lessons Learned

***Lessons learnt***

## Mechanical Integrity- Element 9 of the Process safety management system (PSM)

It is widely believed that safety instrumentation is fail-safe and utterly reliable. Some go so far as to question the need to test it on a regular basis. This incident shows that safety instruments can and do fail.

In this case, the Risk Analysis showed that the second level instrument was not necessary to have an acceptable risk for the scenario and the decision not to test it was justified.

But, when the risk analysis shows that an active safeguard, such as a Safety Instrumented Function or an interlock in the process control system (a BPCSIF) is required, then it must be tested on a regular basis. If it is not tested then no credit should be given to it in terms of risk reduction.

This is covered by element 9 of Process Safety Management: Mechanical Integrity (see procedure IND-HSE-43 “Mechanical Integrity and Preventive Inspection”).

Of course, the same thing is true for all active safeguards, including not just Safety Instrumented Functions but also pressure relief valves.



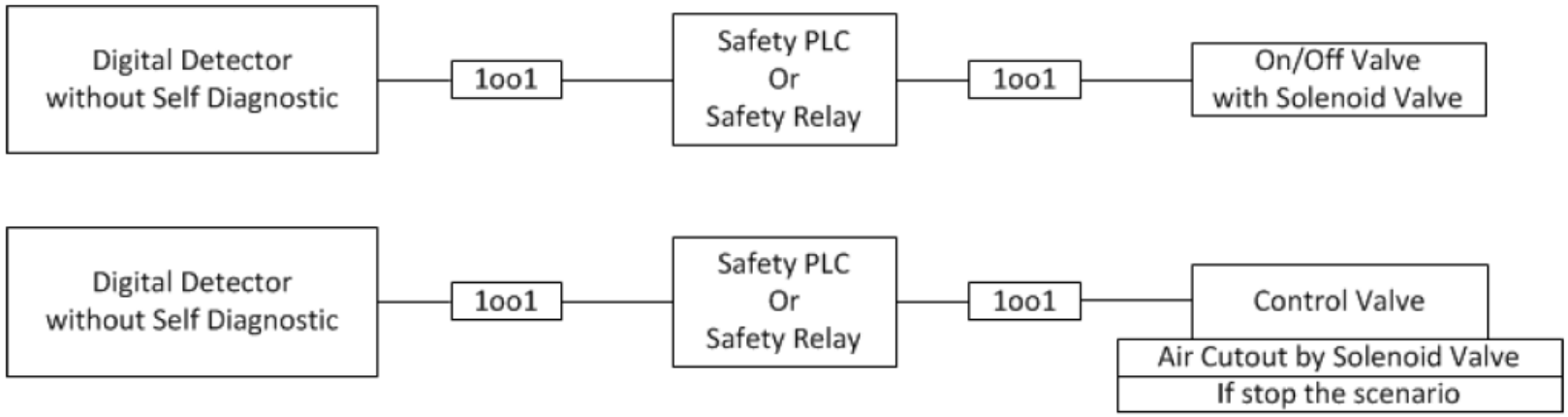
# Independent Protection Layer Audit Requirements

- **Control System Interlocks / Safety Instrument Functions**
  - Physically Exist
  - Sensors and actuators used ‘proven in use’
  - Threshold value set same as in risk analysis report
  - Access to the threshold is protected
  - Periodically tested & Test frequency complies with functional specification requirement
- **Pressure Relief Devices**
  - Physically Exist
  - Installed w’out any shut-off valve (in case of valve, complies with good practice)
  - Inspected at regular intervals
  - Opening pressure same as in risk analysis report
  - Sized for the scenario
- **Passive Safeguards**
  - Physically Exist
  - Inspected regularly & Inspection frequency complies with plant inspection plan
  - Sized for scenario
- **Safeguard (IPL) Management**
  - Cause & Effect matrix is up-to-date
  - Categorized as ‘Safety Critical’ for purchasing & service provider
  - By-passing of Safeguard is recorded



# Independent Protection Layer Audit Requirements

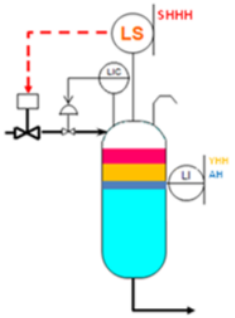
## SIL 1 – Typical Architectures – PTi up to 2 years




- Periodic Tests
  - To prove that SIS still works after period of time, as normally it is not activate until they are needed for protection
  - To maintain the SIL rating required for each SIF, as devices could fail covertly and never show that they are, in fact, no longer providing the protection required
  - Allow to detect the Dangerous Failure normally Undetected
  - Test frequency is set in $PFD_{avg}$ calculation and named Periodic Test interval (**PTi**)
  - Timetable & Follow-up with SIF list, last three tests date, PTi, next test date, derogation status (YES/NO) & maximum postpone delay



# A proof test challenge




## Sensors

Testing of sensors shall be carried out using the maintenance overrides (see “overriding” in the SIF functional specifications above) in order to avoid the trip of the related SIF.

The tests shall consist in a signal simulation which is as close as possible to the actual process, in which the variable measured by the sensor crosses the safety threshold.

When this happens, correct operation of the safety function must be checked as far down the line as possible: ideally at the Logic Solver, and at least up to the input.

## Final elements

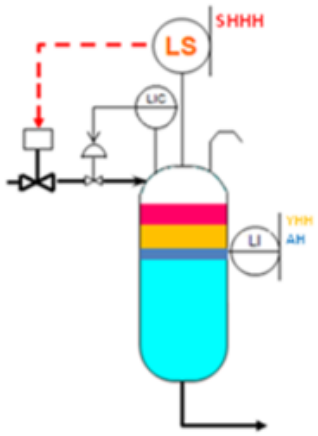
Final elements are the most critical components of the safety function:

- They represent at least 50 % of the SIS failures
- The failure rate of the automatic valves is mainly related to a dangerous failure (dormant failure).
- They usually do not have a self-diagnostic system.
- It is difficult or impossible to test them in operation.



# A proof test challenge

## Testing a Vessel High Level Sensing Instrument in Hazardous Service




In order to assure a high level interlock is functioning properly, the sensing device must be physically tested. Normally, the sensing device itself must be removed from the vessel and tested in a bucket of water or some other liquid.

However, for the removal of a device from a vessel that contains a hazardous material, a procedure that assures safety and no personnel exposure must be developed.

**Summary descriptions of level device testing for six sites are listed below.**

**Site A – Dual level indication floats are in the propylene oxide tanks and are only tested when the tanks are empty.**

**Site B – Testing of a knockout drum of sulfuric acid level switch. Operations personnel will empty the drum and wash it. Maintenance personnel preform a line break wearing chemical specific PPE then remove the switch and test it in a bucket of water.**

# A proof test challenge

**Summary descriptions of level device testing for six sites are listed below.**

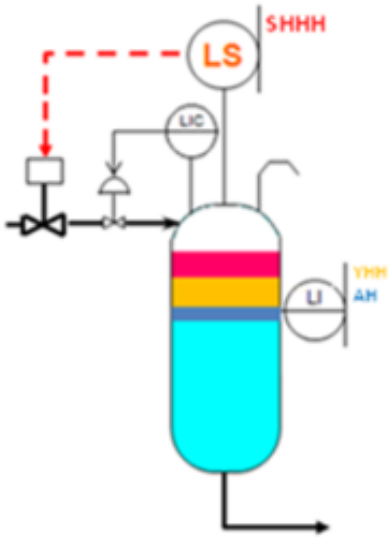
**Site C – They do remove high level probes and bench test the functionality in a bucket of water. Depending on the situation an MOC is required to temporarily disable the interlock. Operations would then put the equipment in a safe condition. Some isolation or blinding might be required by maintenance. In the nitrogen blanket case, the mechanic or tech would wear a full face respirator connected to breathing air to protect against an oxygen deficient atmosphere. The mechanic or technician will also wear the PPE to protect against possible exposure to the chemical stored in the tank. It can require a total chemical splash suit and hood and respirator. Then they would remove the device with normal or non-sparking tools, and install a temporary blind flange until the interlock and device can be tested, calibrated, and repaired or replaced, and re-installed.**

**Site D – Testing of high level sensing instruments is avoided since they can schedule their work during a shutdown.**

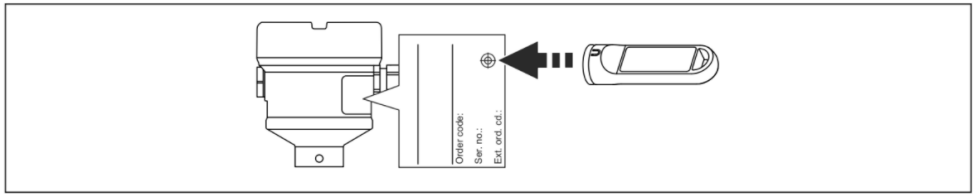
**Site E – The valves are set up so that pressure sensing instruments can be properly isolated and taken out of service. It is still a line break and requires the full PPE for the given chemical, but once the line is broken and conditions have been determined to be safe, PPE can be downgraded. Level indicating floats are not tested.**

**Site F - In the case of a vessel that is operated at very low pressure (DMAPA), the vessel is locked out so that nothing can flow into or out of the vessel. They suit up in the proper PPE, pull the switch and install a temporary blind to keep vapors from coming out any more than needed. In vessels that are maintained at a bit higher pressure (Epichlorohydrin and Monochloroacetic Acid), the pressure is bleed off, first, by venting through a scrubbing tote. In both cases, once the venting is complete and the vessel is locked out, the line break procedure is followed including wearing the proper PPE and the level switch is pulled. Again, a blind flange is installed. The level switch is then tested in a bucket of water before it is re-installed in the vessel.**

# Improvement








42 *Functional test with test magnet*

## 7.1.3 Functional test of the electronic switch with a test magnet

Perform functional test of the electronic switch without opening the device:

- Hold the test magnet against the marking on the nameplate on the outside.
  - Simulation is possible in the case of the FEL62, FEL64, FEL64DC, FEL68 electronic inserts.

The functional test with the test magnet acts in the same way as the functional test using the test button on the electronic insert.

Chemical Process Safety Sharing

# Thank you for your attention