ASEAN HSSE
LOSS PREVENTION &
PROFESSIONAL DEVELOPMENT
CONFERENCE & EXHIBITION
18-19 SEPTEMBER 2019
ISTANA HOTEL, KUALA LUMPUR
MALAYSIA

"Operational Excellence Through HSSE Innovation"

Principles and Practices of Proof Testing for SIS according to IEC 61511

Chen Zhenkang

Functional Safety Expert,

TÜV Rheinland Singapore Pte. Ltd.

Email: Zhenkang.Chen@tuv.com

Phone: +65-9815 4123

Web: https://insights.tuv.com/safety-case

MOGSC
MALAYSIAN OIL & GAS SERVICES COUNCIL

Agenda

- I: Context: Functional Safety, Process Industry and IEC 61511
- II: 3 key S-words: SIS, SIF & SIL
- III: The "SHALL" Requirement on Proof Testing for SIS
- IV: Proof Testing: Why?
  1. Why Safety (Function)?
  2. Why Safety (Function) Integrity?
  3. Why Proof Testing?
- V: Proof Testing: What?
- VI: Proof Testing: When and How?

I: Context: Functional Safety, Process Industry and IEC 61511

Safety

IEC 61508-4, 3.1

Safety :

Freedom from unacceptable risk of **physical injury** or of **damage** to the **health of people**, either directly, or indirectly as a result of damage to property or to the environment. [IEC 61508-4, 3.1; ISO / IEC Guide 51:1999, definition 3.1]

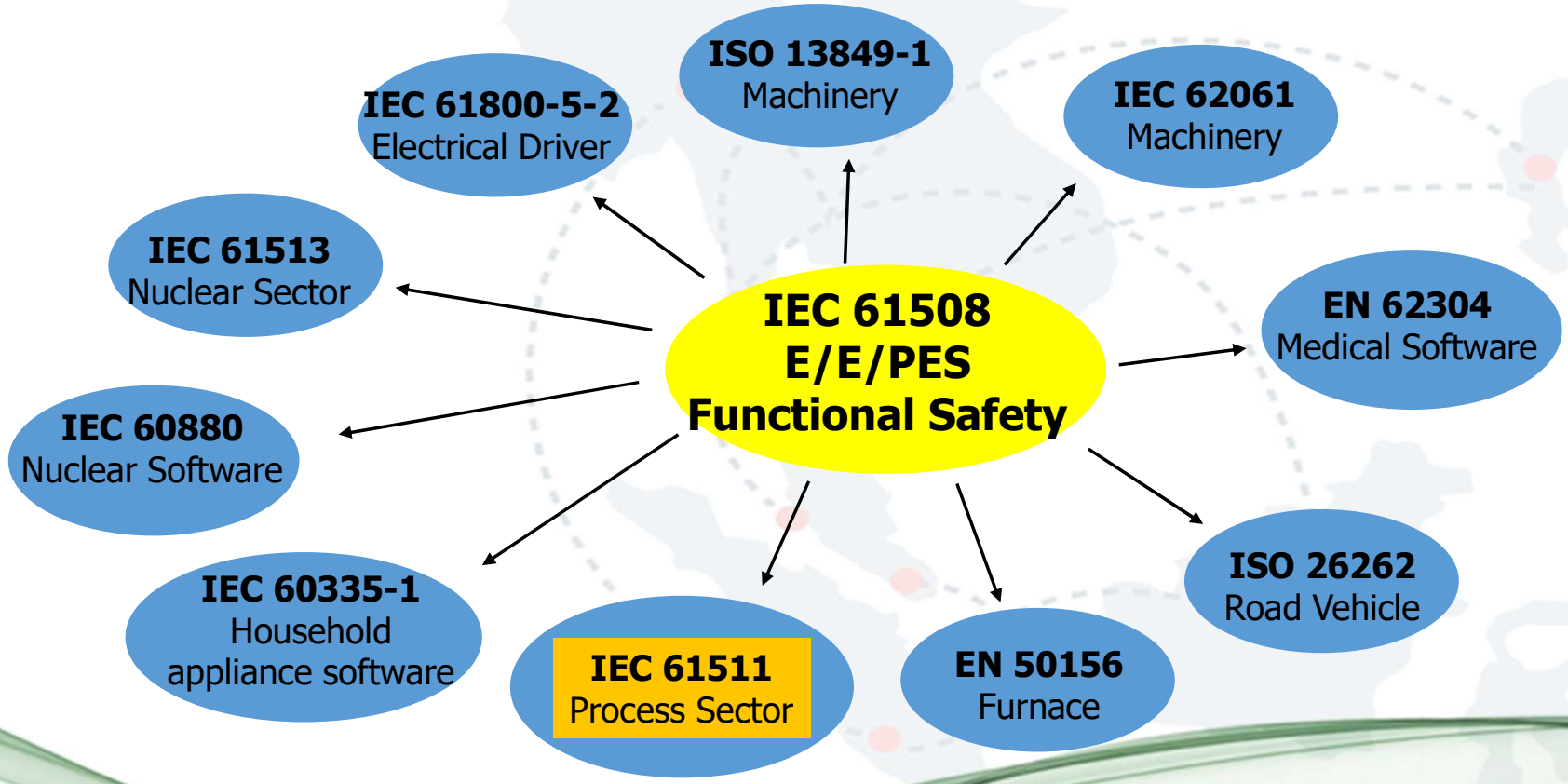
Functional Safety

IEC 61508-4, 3.1.12

Functional Safety:

…**part of** the **overall safety** relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.

Functional Safety Standards



IEC 61511 concerning Process Industry

Chemical Plants

Refineries

Power Plants

Semiconductor Fabs

Oil and Gas

Storage Terminals

FPSO

Pharmaceutical Plants

IEC 61511: Functional Safety Application (SIS) for Process Industry

IEC61511: Functional safety - Safety instrumented systems (**SIS**) for the **process industry** sector

Edition 2: Issued in Feb 2016

3 Parts:

- **Part 1**: Framework, definitions, system, hardware and application programming Requirements;
- **Part 2**: Guidelines for the application of IEC 61511-1:2016
- **Part 3**: Guidance for the determination of the required safety integrity levels

II: 3 key S-words: SIS, SIF & SIL

3 key S-words: SIS, SIF & SIL

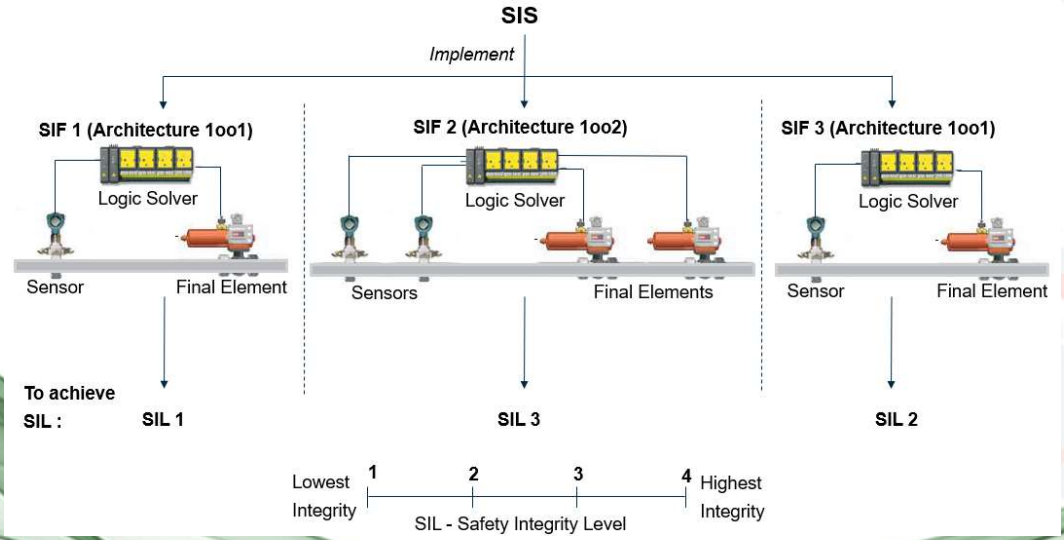
SIS: Safety Instrumented System

Hardware and software systems built to perform safety functions

E.g. Emergency Shutdown (ESD), High Integrity Pressure Protection System (HIPPS)

Reduce risks through SIFs

Each SIS has one or multiple SIF loops



Img Credit: Jasmine Wong & Adrian How of SIT

- **SIF:** Safety Instrumented Function
  - Made up of subsystems/components;
  - Each SIF designed to achieve a required SIL;
- **SIL:** Safety Integrity Level
  - Discrete Level (1, 2, 3, 4);
  - Allocated to each SIF for specifying the safety integrity requirements to be achieved by SIS;
- NOT a property of a system, sub-system, element or component.

Safety Integrity Requirement: Target Failure Measures

IEC61511-1:2016 Table 4/5

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

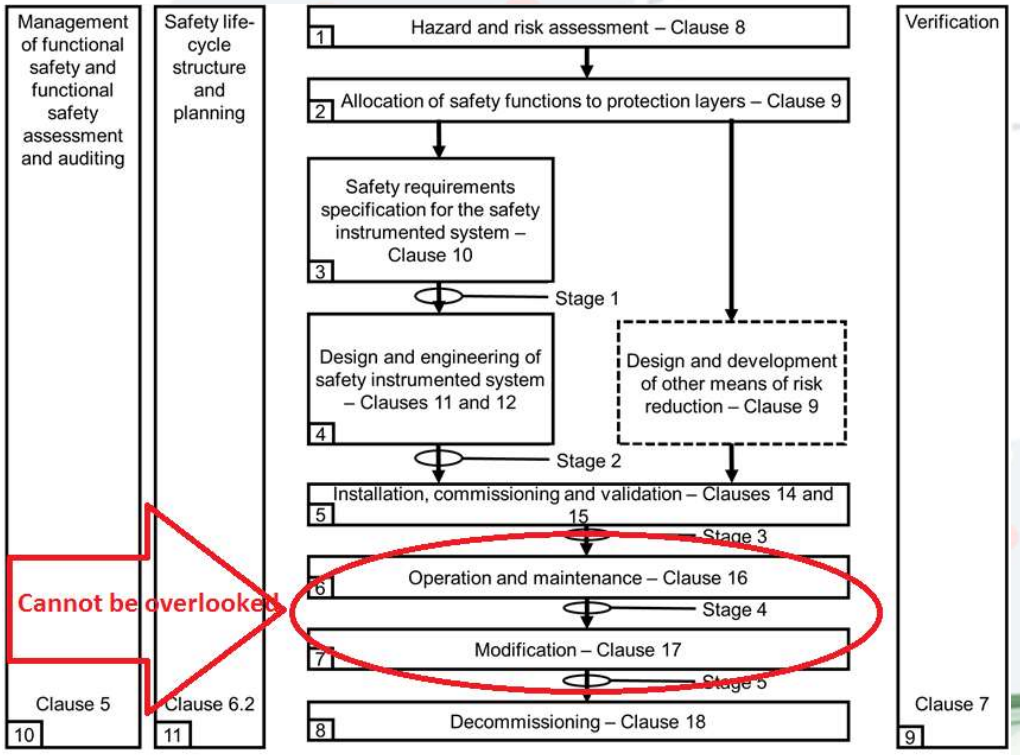
Table 5 – Safety integrity requirements: average frequency of dangerous failures of the SIF

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	Average frequency of dangerous failures (failures per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

III: The "SHALL" Requirement on Proof Testing for SIS

SIS Safety Life-cycle phases

IEC61511-1: 2016, Figure 7: SIS safety life-cycle phases and FSA stages



MOGSC
MALAYSIAN OIL & GAS SERVICES COUNCIL

The "SHALL" Requirement on Proof Testing for SIS

IEC 61511-1: 2016, 16.3.1 Proof Testing

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

NOTE 1 Particular attention can be made to identify failure causes that may lead to common cause failures.
NOTE 2 Functional test procedures can also emphasize the need to avoid introducing common cause failures.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors)

NOTE Testing of the SIS can be performed either end-to-end or in segments (see 11.8.1).

IV: Proof Testing: Why?

Why Safety (Function)?

There is Risk.

Why Safety (Function) Integrity?

All, including safety (functions), are associated with **failure(s)** / **fault(s).**

3.2.68
safety integrity
ability of the SIS to perform the required SIF as and when required

Note 1 to entry: This definition is equivalent to the dependability of the SIS with regard to the required SIF. Dependability, being often understood as an economical rather than a safety concept, has not been used to avoid confusion.

dependability
/dɪpɛndəˈbɪlɪti/

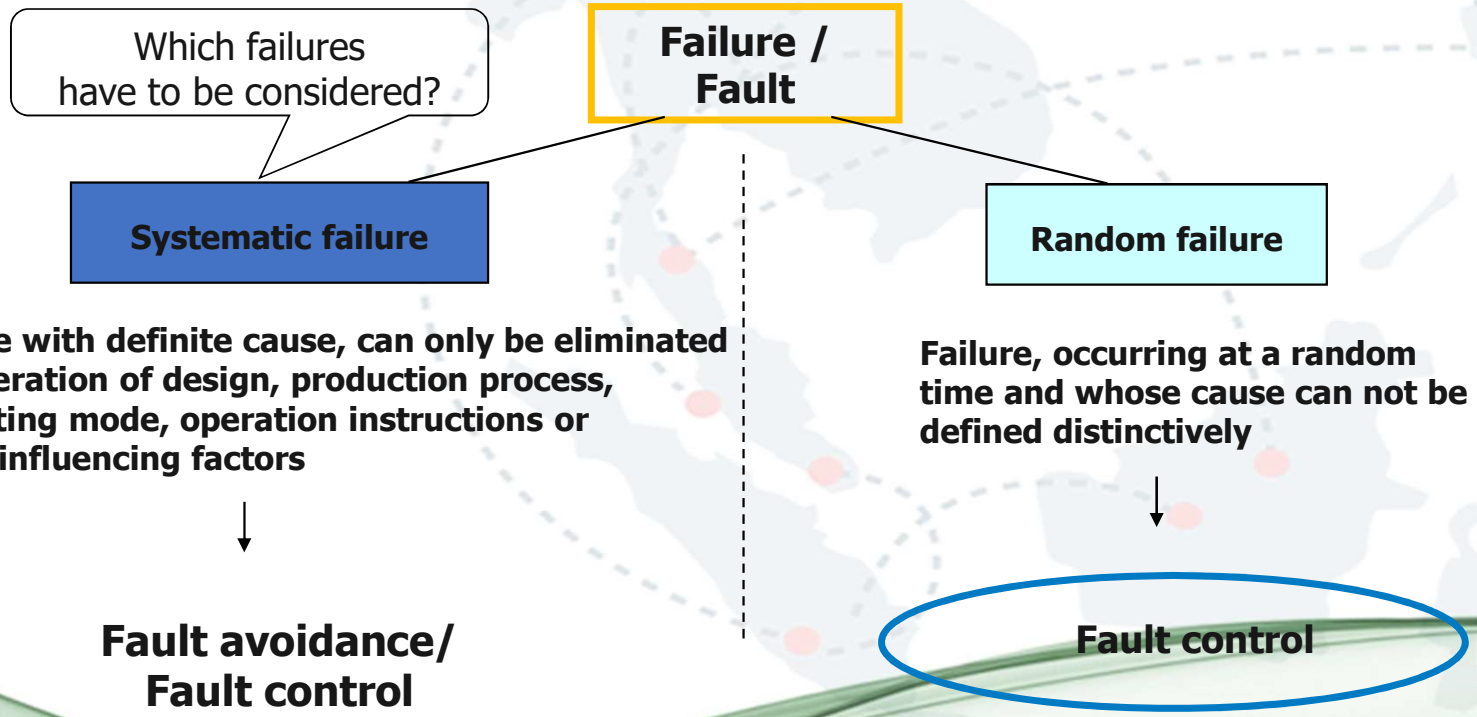
noun
noun: dependability

the quality of being trustworthy and reliable.
"the brand has built its reputation on rock-solid dependability"

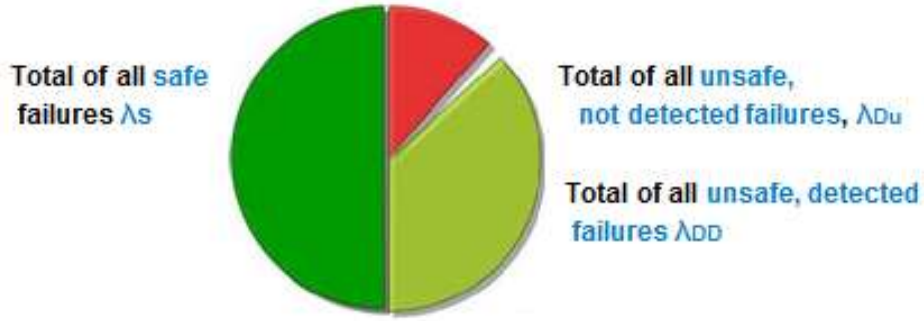
Source: IEC61511-1: 2016, 3.2.68;
https://www.google.com/search?rlz=1C1PQCZ_enSG808SG808&q=Dictionary#dobs=dependability

Types of Failures / Faults

Fault: abnormal condition, that may cause loss or at least a reduction of a functional unit (system or sub-system) to perform a required function



λDu (Dangerous un-detected failures): the trouble maker



λDu really bothers us: it will make that the safety system cannot perform the action. It's the only one that goes into the PFD_{AV} calculation.

Why Proof Testing?

In order to reveal the λDu (Dangerous Un-detected failure):

3.2.56
proof test
periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition

16.2.11 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include:

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

Source: IEC61511-1:2016, 3.2.56, 16.2.11

Is proof test the only way to reveal λDu?

No.

There is another way: **accidents** will help you reveal the λDu.

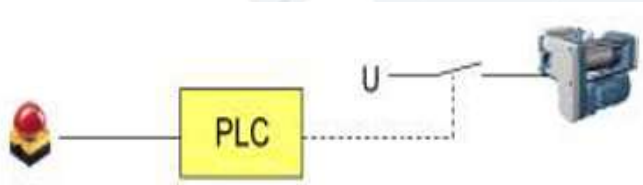
V: Proof Test: What?

Proof Test

3.2.56
proof test
periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition

Average Probability of Failure on Demand (PFDAV)

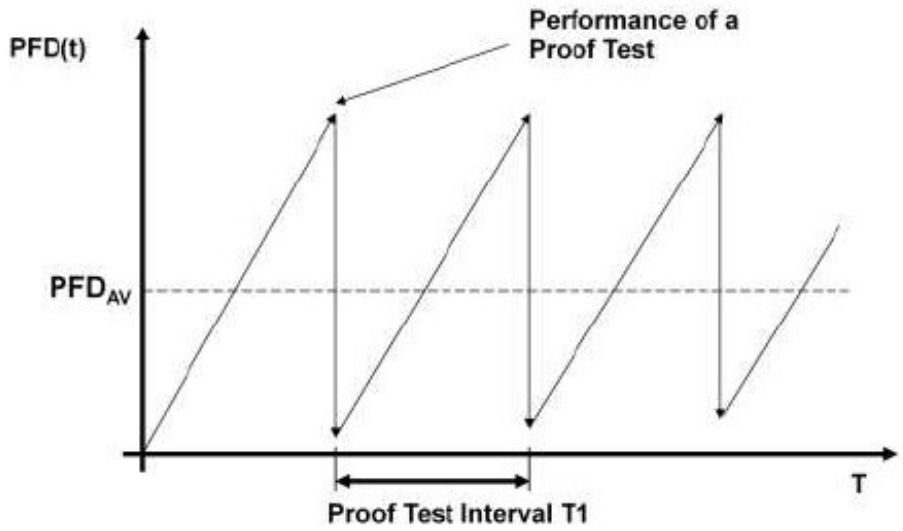
For a single channel system the PFD_{AV} can be determined as :



$$PFD_{Av} = \frac{1}{2}\lambda_{DU} \cdot T_1$$

T1 is the considered time interval (Proof Test Interval)

Relation of PFDAV and Proof Test Interval (PTI)



… for the detection of failures (λDU)…, so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition

Proof Test Interval (PTI)

… "as new" condition…

1) … in practice 100% is not achievable for other than low-complexity safety-related systems. But this should be the target.

2) As a minimum , all the safety function which are executed are checked according to the safety requirements specification.

Meaning:

Only for simple (not electronically) system the condition, "as new" can be achieved by a test of the safety function during the PTI.

For complex (electronically / programmable) systems the condition "as new" cannot only be achieved by a test of the safety function during the PTI.

Proof Test Interval (PTI): Complex Systems

Therefore:

In case of complex systems a PTI > 10 years should be aimed at, as the necessary high diagnosis detects many failures.

Otherwise the complex systems should be checked by the manufacturer during the proof test or should be replaced by a new system.

The product life cycle shall not exceed the proof-test interval

Target: product life cycle < proof-test interval (PTI)

VI: Proof Test: When and How?

When and How: Phase 3 - SIS SRS

Phase 3: SIS SRS:

10.3.2 These requirements shall be sufficient to design the SIS and shall include a description of the intent and approach applied during the development of the SIS safety requirements as applicable:

…;

requirements relating to proof test intervals;

requirements relating to proof test implementation;

functions enabling proof testing and automated diagnostics tests of external devices (e.g., sensors and final elements) performed in the application program;

When and How: Phase 4 - SIS Design and Engineering

1. When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation.

2. Where any dangerous fault in an SIS is brought to the attention of an operator by an alarm then the alarm shall be subject to appropriate proof testing and management of change.

3. The design shall allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.

4. When on-line proof testing is required, test facilities shall be an integral part of the SIS design.

When and How: Phase 5 - SIS Safety Validation

The validation of the SIS and its associated SIF(s) shall be carried out in accordance with the SIS validation planning. Validation activities shall include, but not be limited to, the following:

…;

the proof-test policy documented in the maintenance procedures.

When and How: Phase 6 - SIS Operation and Maintenance: Planning

Planning:

16.2.1 Operation and maintenance **planning** for the SIS shall be carried out. It shall provide the following:

…;

inspection, proof testing, preventive and breakdown maintenance activities;

When and How: Phase 6 - SIS Operation and Maintenance: Procedure

16.2.2 Operation and maintenance **procedures** shall be developed in accordance with the relevant safety planning and shall provide the following:

…;

the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;

16.2.11 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include:

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

When and How: Phase 6 - SIS Operation and Maintenance: Guideline part 1/2

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the SRS.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element(s) (e.g., shutdown valves and motors).

16.3.1.3 The schedule for the proof tests shall be according to the SRS. The frequency of proof tests for a SIF shall be determined through PFD_{avg} or PFH calculation in accordance with 11.9 for the SIS as installed in the operating environment.

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner. A proof test shall be repeated after the repair is completed.

When and How: Phase 6 - SIS Operation and Maintenance: Guideline part 2/2

16.3.1.5 At some periodic interv(determined al by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience and hardware degradation.

16.3.1.6 Any change to the application program requires full validation and a proof test of any SIF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.

16.3.1.7 Suitable management procedures shall be applied to review deferrals and prevent significant delay to proof testing.

When and How: Proof Testing Documentation

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

a) description of the tests and inspections performed including identification of the test procedure used;

b) dates of the tests and inspections;

c) name of the person(s) who performed the tests and inspections;

d) serial number or other unique identifier of the system tested (e.g., loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection including the "as-found" condition, all faults found (including the failure mode) and the "as-left" condition.

ASEAN HSSE LOSS PREVENTION & PROFESSIONAL DEVELOPMENT CONFERENCE & EXHIBITION
18-19 SEPTEMBER 2019
ISTANA HOTEL, KUALA LUMPUR
MALAYSIA

"Operational Excellence Through HSSE Innovation"

Contact Chen Zhenkang

Email: Zhenkang.Chen@tuv.com

Phone: +65-9815 4123

MOGSC
MALAYSIAN OIL & GAS SERVICES COUNCIL

Thanks and Questions

MOGSC
MALAYSIAN OIL & GAS SERVICES COUNCIL