Safety Instrumented System

A Critical Barrier

Presented by:

Sujith Panikkar, CFSE

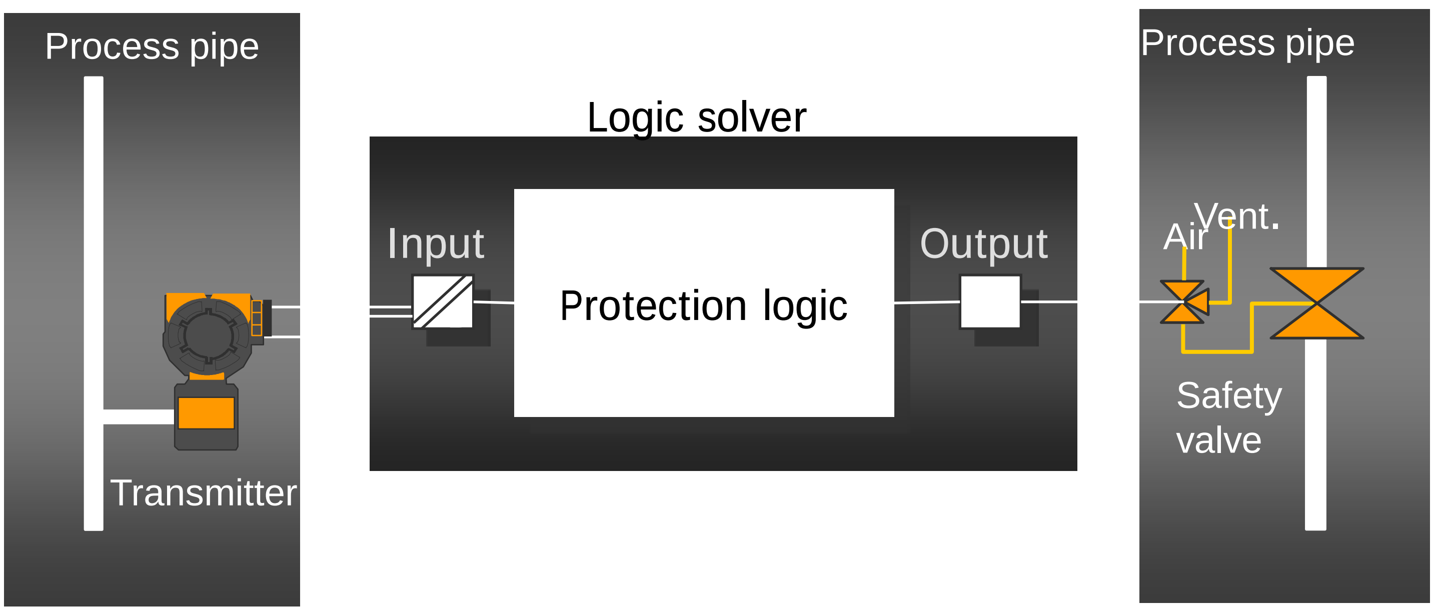
Contents

The Safety Instrumented System

What is a Safety Instrumented System ???

A Safety Instrumented System is a system that provides an independent and predetermined emergency shutdown path in case a process runs out of control

Safety System – “IPS”, “ESD”, “SGS” etc… = SIS



SIS: The need for Protection

EUC = Equipment Under Control

Industrial Process

Control

DCS

If something runs out of control a dangerous situation can arise ==> a demand for a protective action

Consequences

(how serious, how much money, how many injuries, how many fatalities)

Demand Rate

(frequency, how many times per how many year)

What has to be Protected ?

Chemical Industry Accidents - History

Some of the major ones...

- 1974: Flixborough
- 1976: Seveso
- 1984: Bhopal
- 1988: Piper Alpha

And many more...

- 2010: BP Gulf of Mexico

the Consequences...

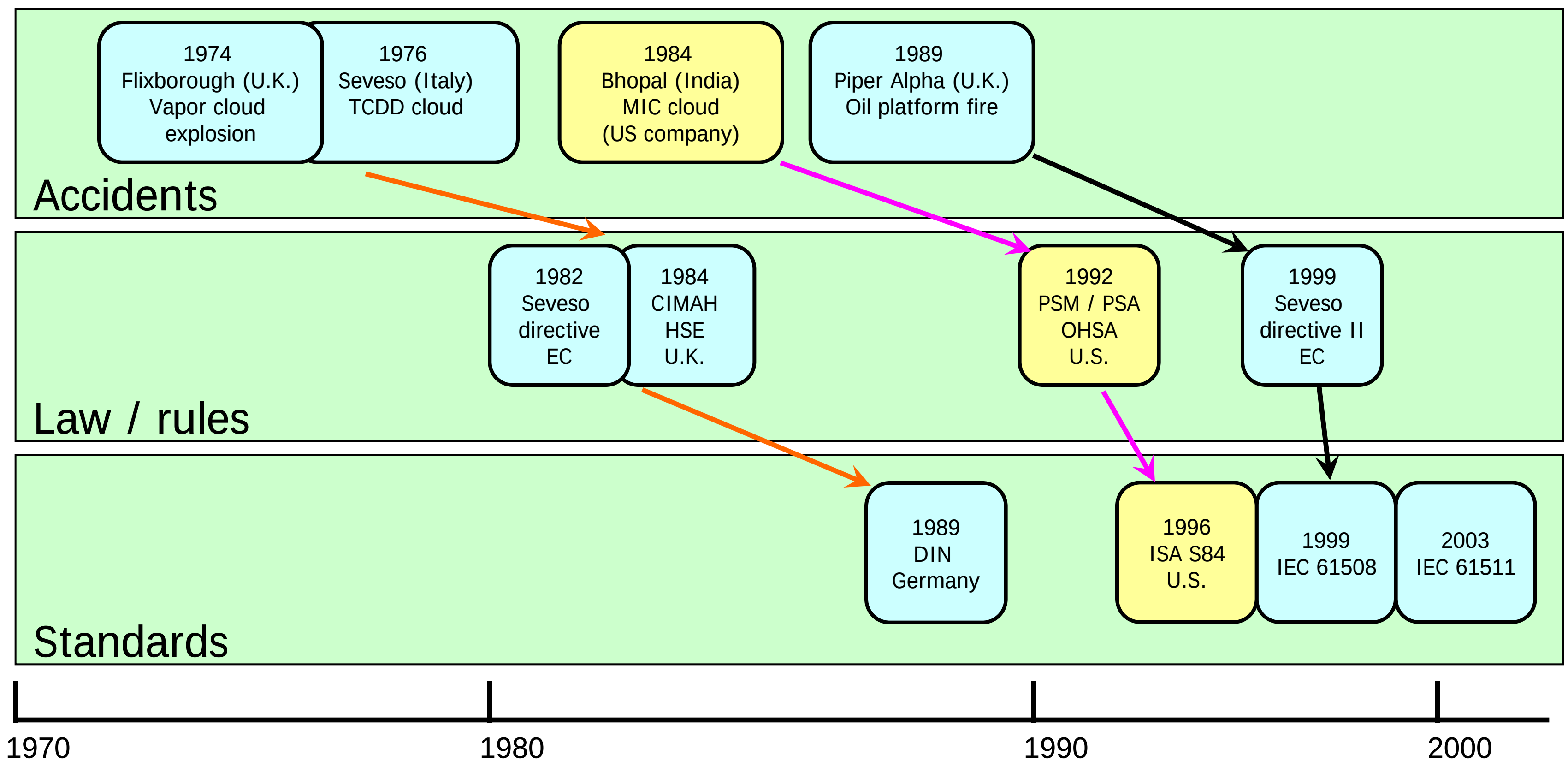
Piper Alpha platform, July 1988

Consequences: Piper Alpha platform, July 1988

- 61 survivors, but many badly burnt
- 167 fatalities
- Piper Alpha was producing about 125,000 bpd in 1988
- Insured losses of over US$ 3.4 Billion

Evolution of Regulations and Standards

History of Functional Safety Standards

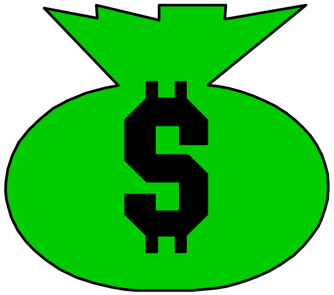


Preventing Accidents: Risk Reduction

Def. Risk

"Combination of the frequency of occurrence of harm and the severity of that harm"

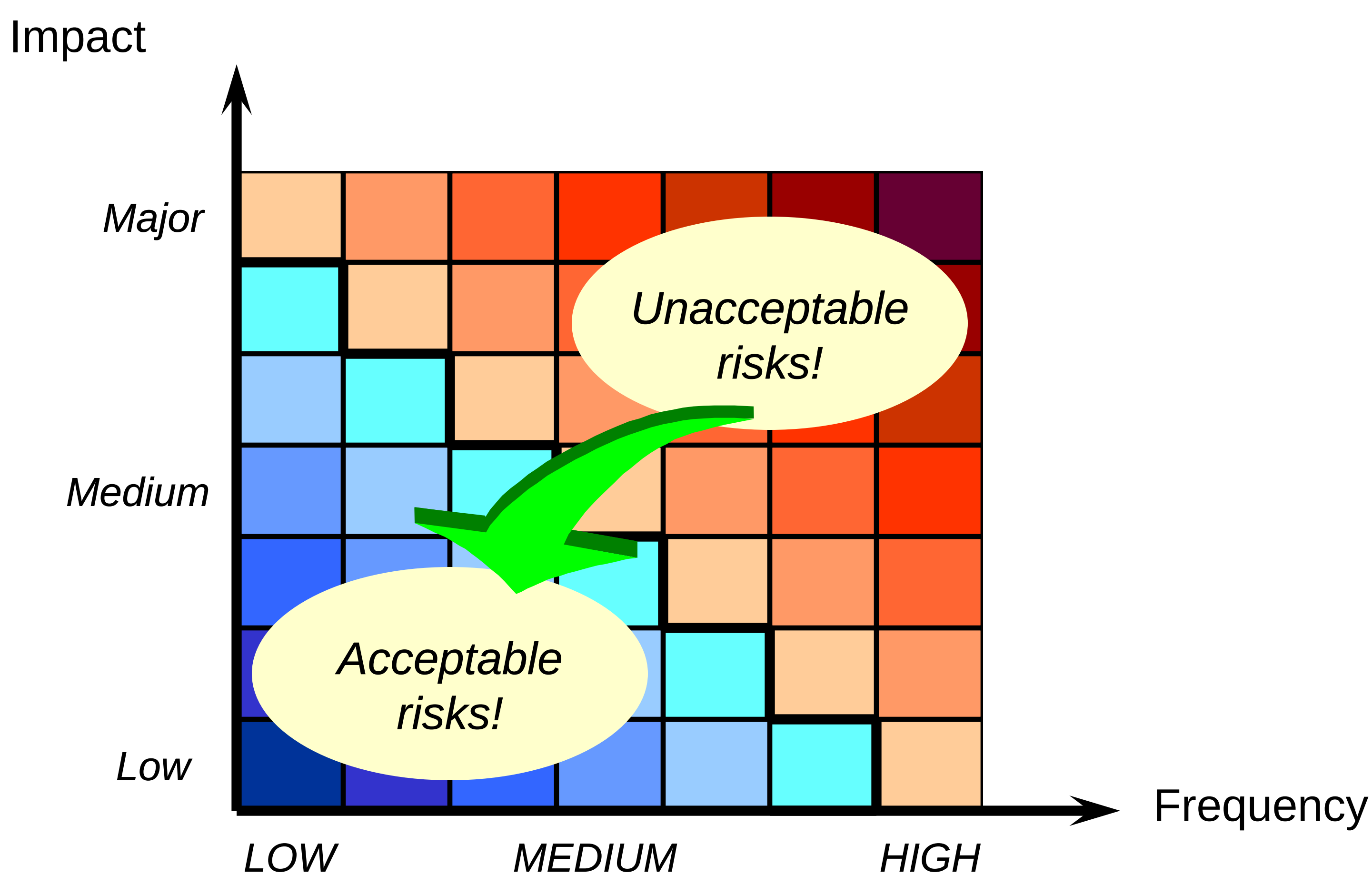
(IEC 61508 / IEC 61511)



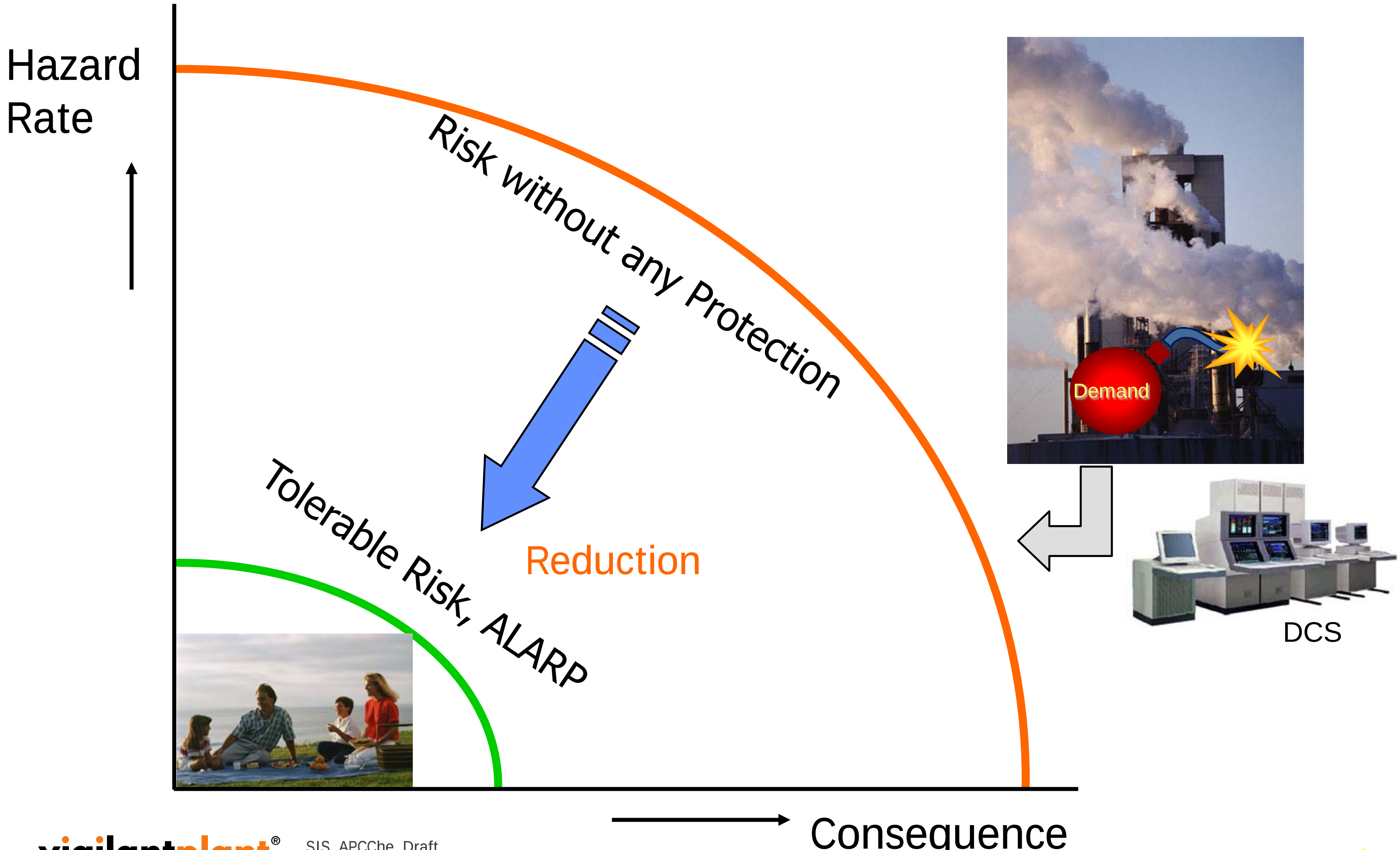
Risk= Impact X Frequency

Impact = $$, Life, Environment

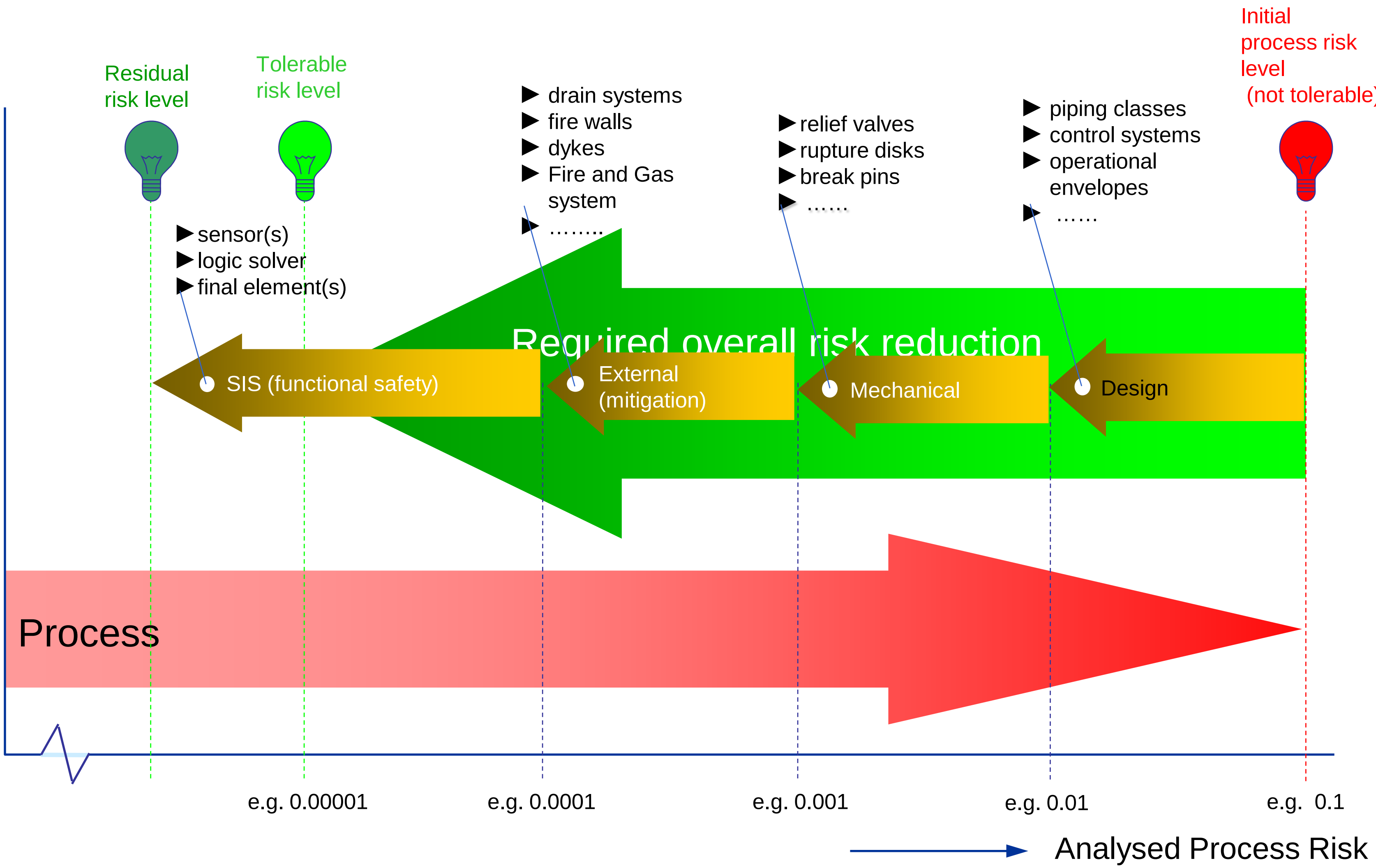
How to reduce the Risk?



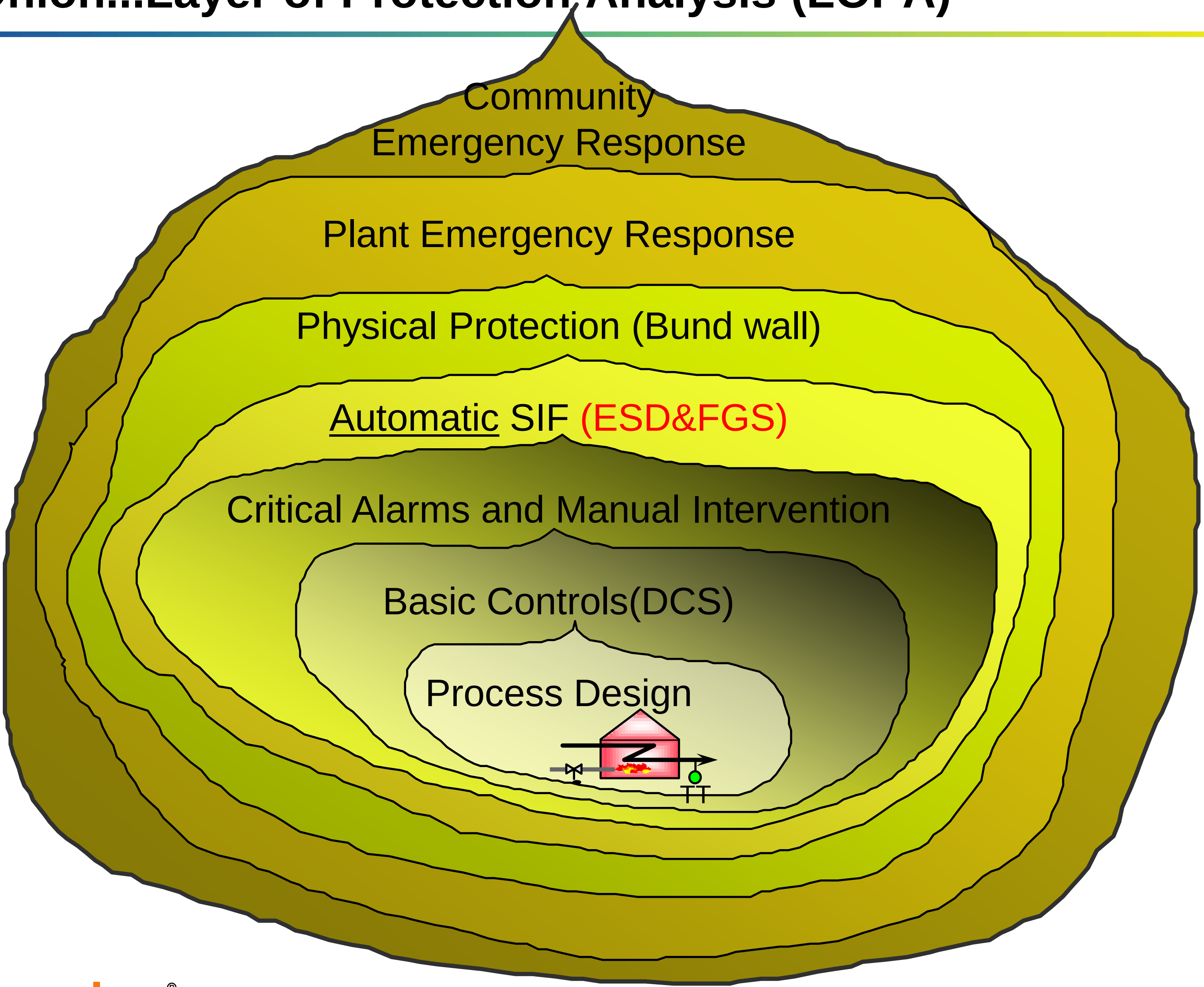
Risk Reduction



Process risk



Onion...Layer of Protection Analysis (LOPA)



- Case Study: Reliability of Instrumentation :

BP AMOCO Texas City Refinery:

Isomerization Unit Explosion, March 2005

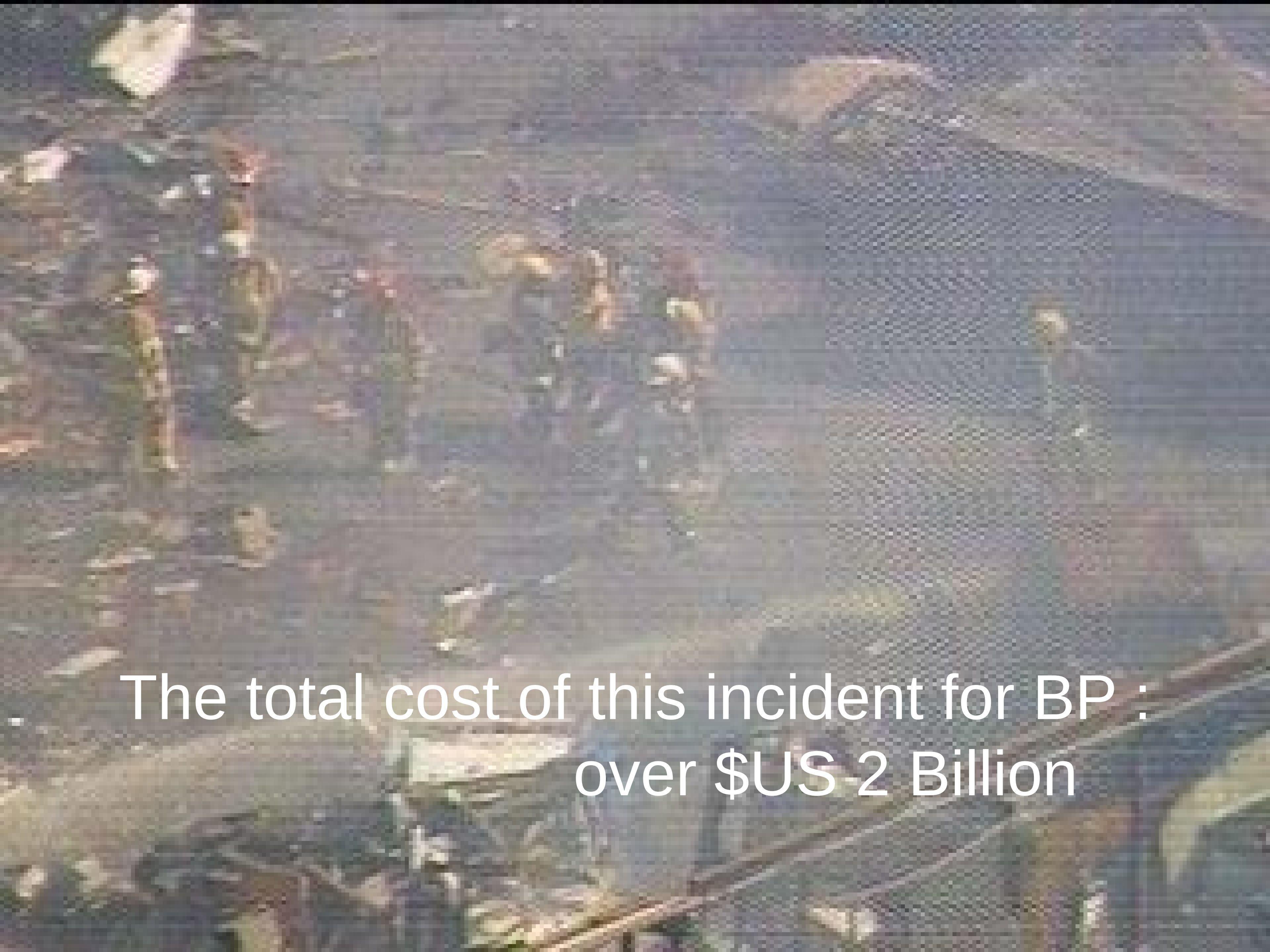
BP AMOCO EXPLOSION MARCH '05

15 DEAD

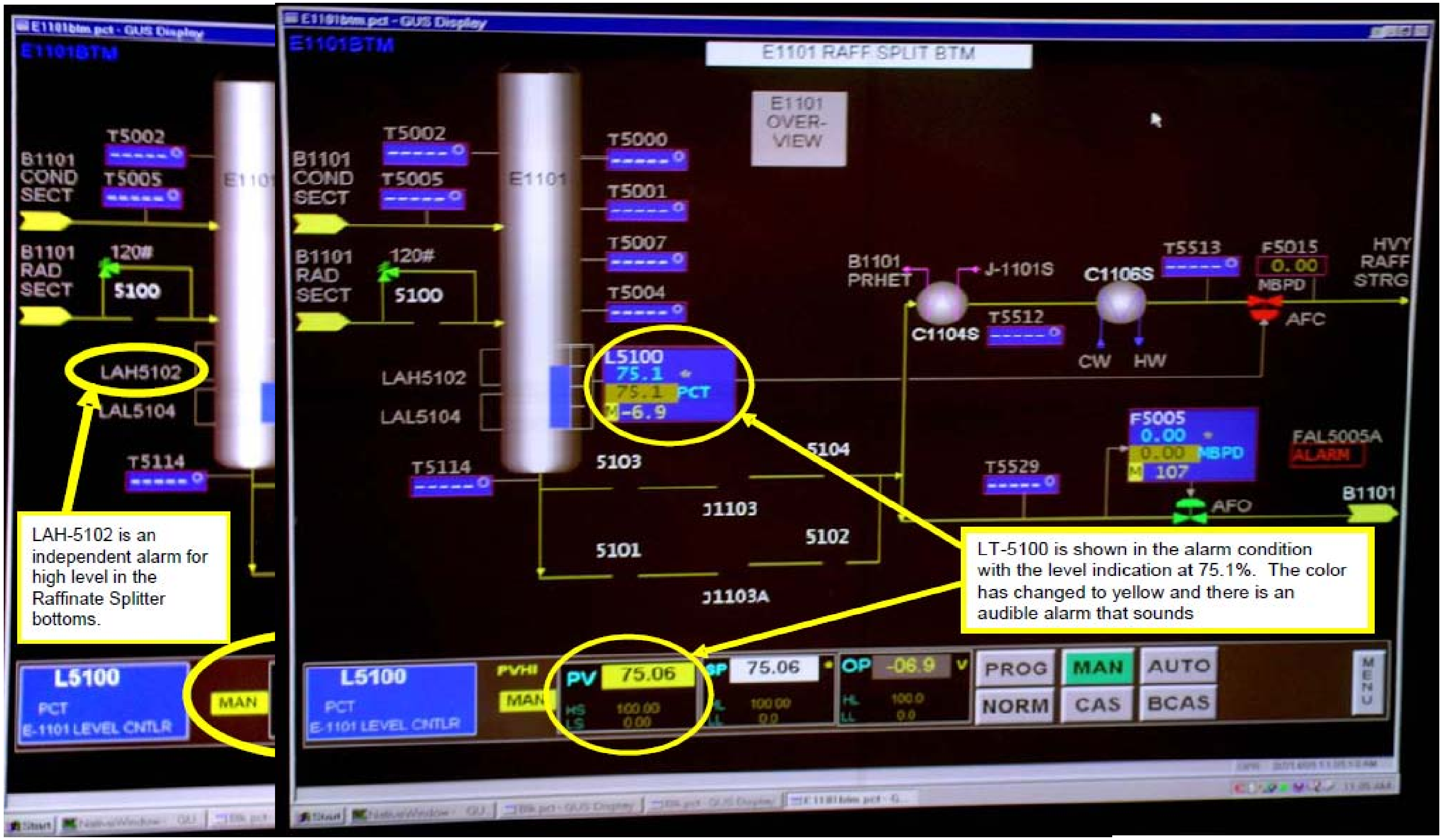
100 INJURED

30 PUBLIC INJURED

8 IN CRITICAL CONDITION


The total cost of this incident for BP :
over $US 2 Billion

Failure of Raffinate Splitter Level Instrumentation



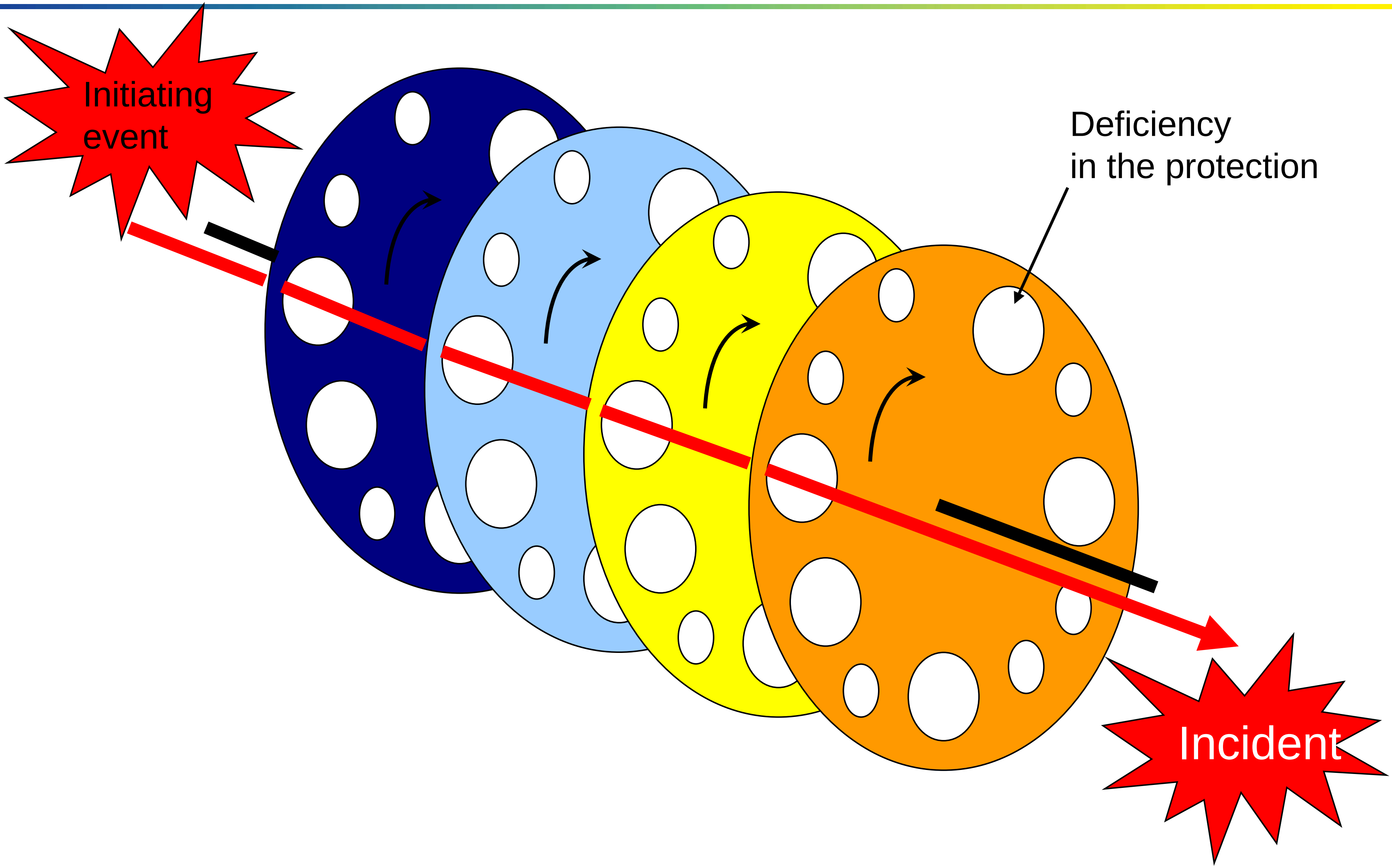
- DCS Level High Alarm was ignored
- Independent Level switch connected to alarm system did not work

Source: Fatal Accident investigation Report :
http://www.bp.com/liveassets/bp_internet/us/bp_us_english/STAGING/local_assets/downloads/t/final_report.pdf

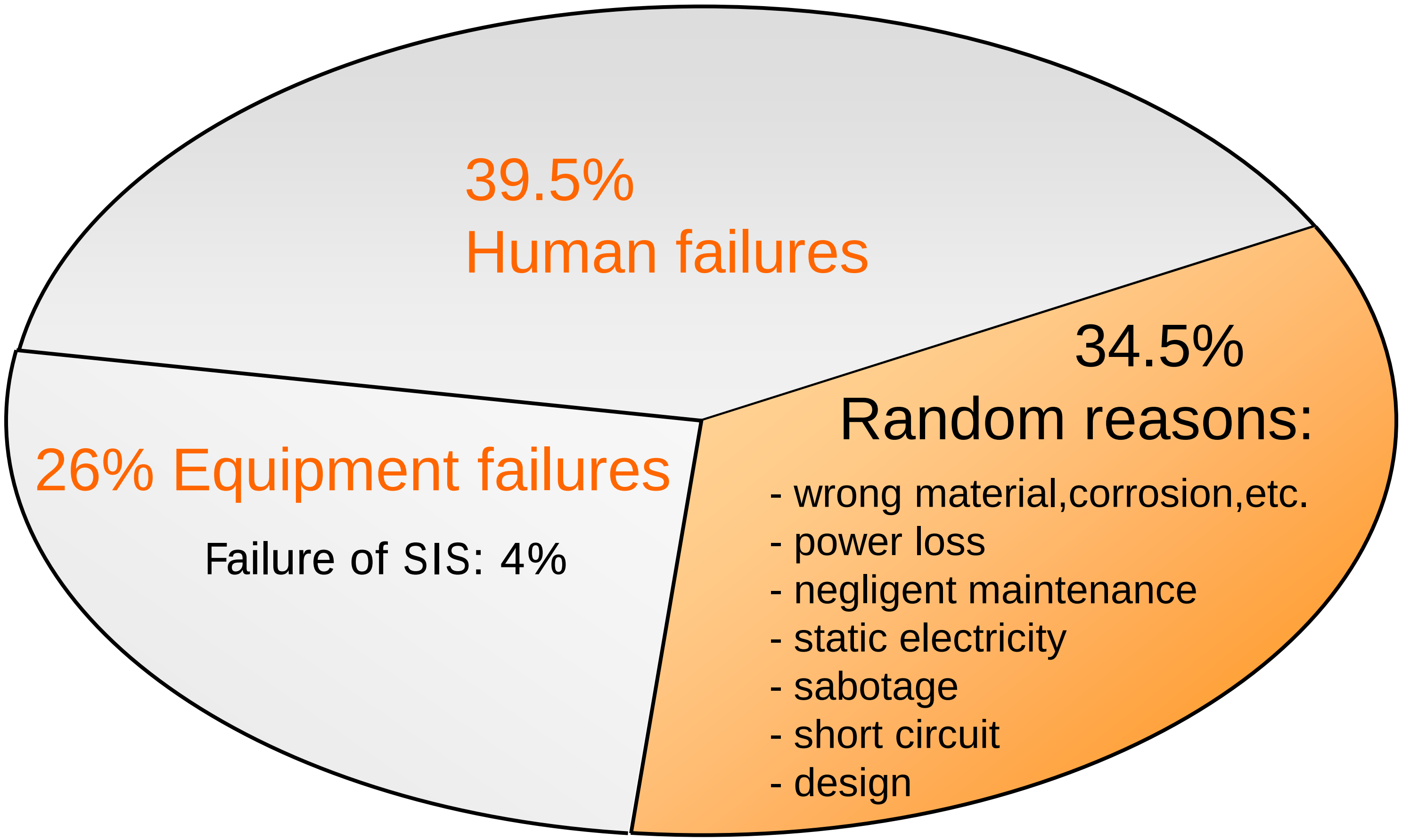
Topic

- Accidents and Causes: The Human Factor

Layers of protection



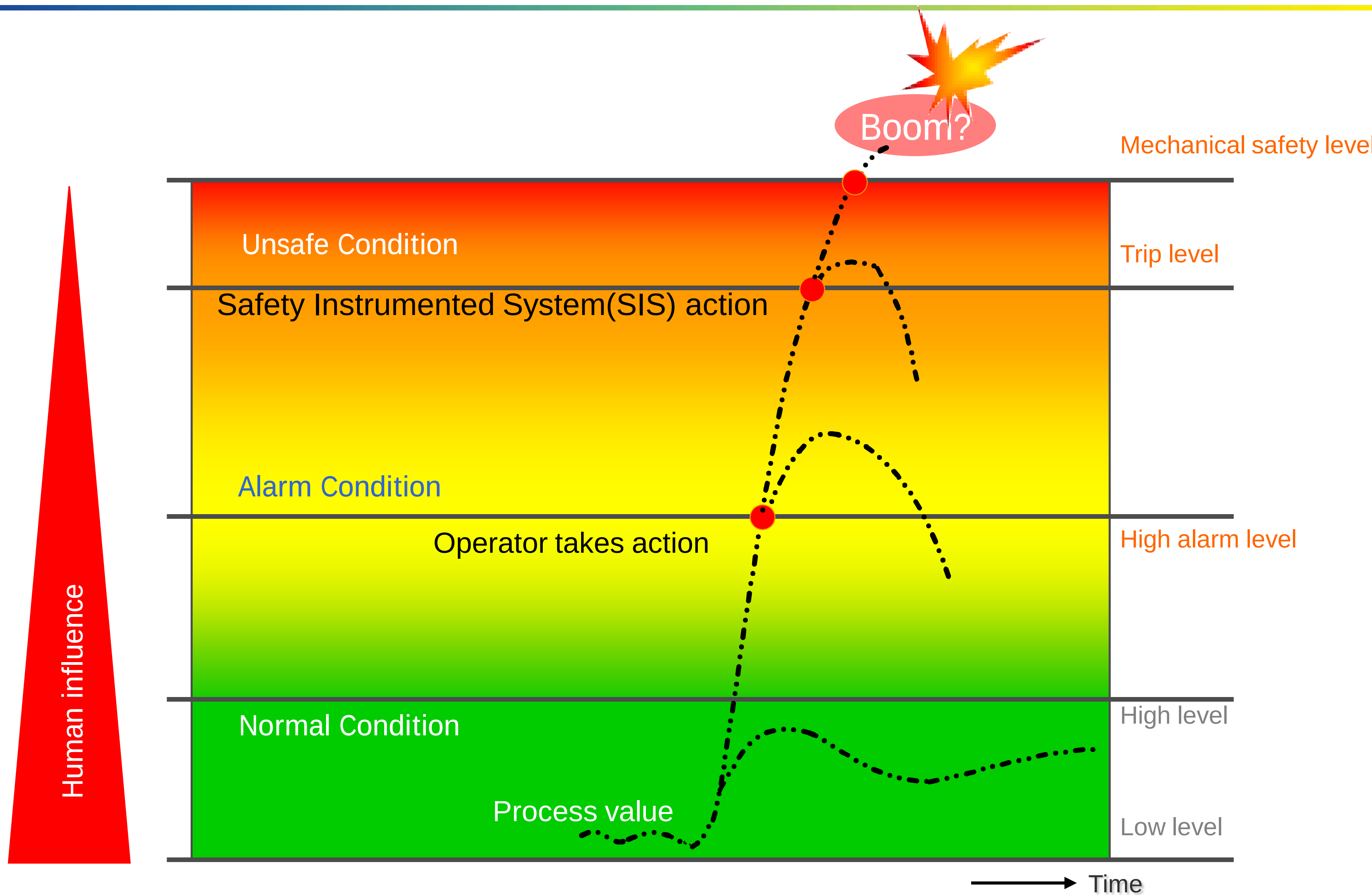
Causes of Accidents



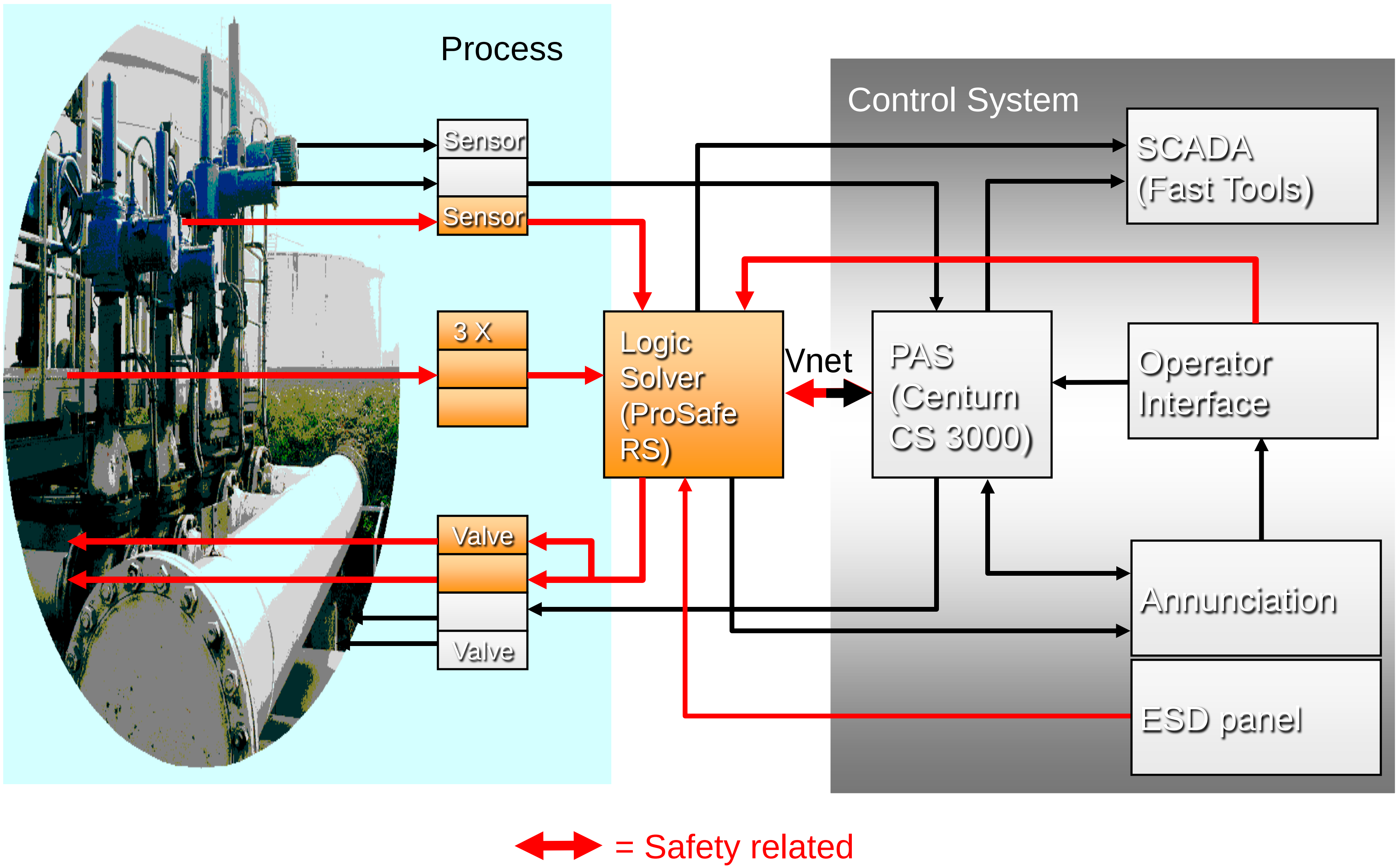
source: TNO investigations of 216 accidents

- Safety Instrumented Systems as a Safety Barrier

SIS Function in the Process



The position of SIS



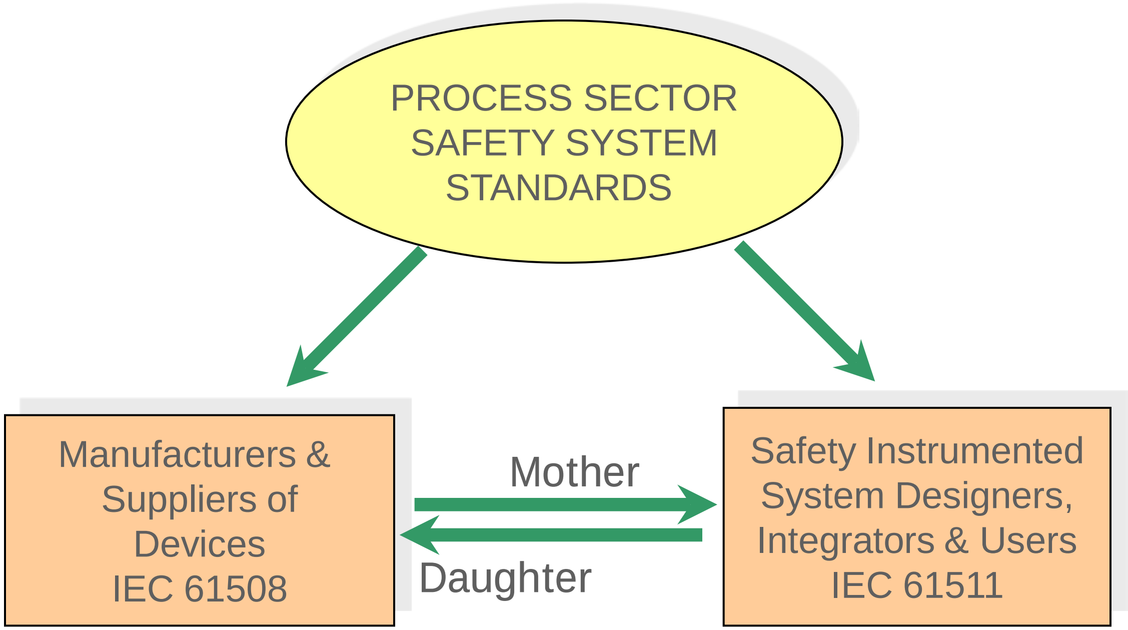
Topic

- Design & Engineering SIS: IEC 61508/ 61511 & FSM

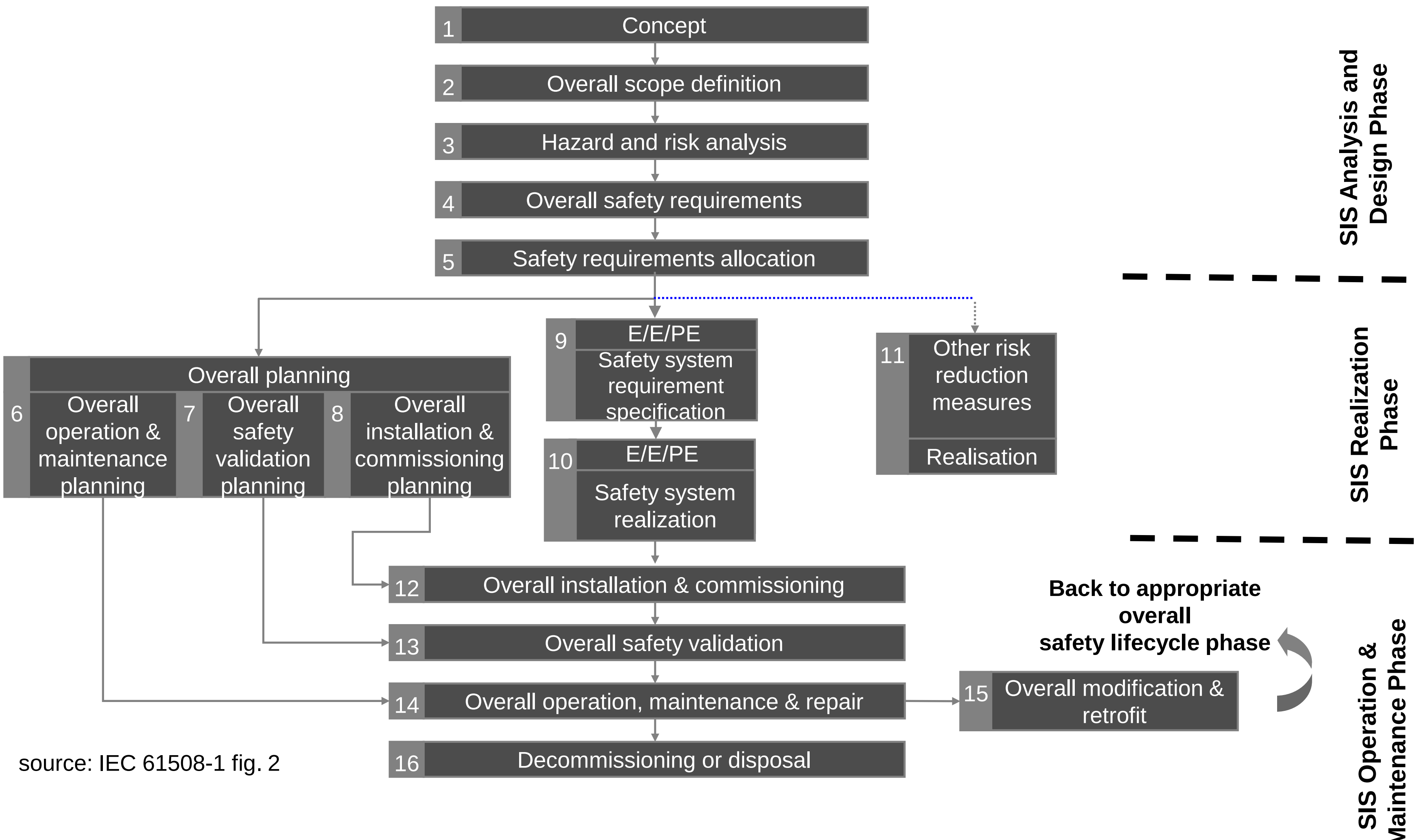
The IEC 61508 / 61511 Standard

IEC 61508 : functional safety of electrical / electronic / programmable electronic safety-related systems.

IEC 61511 : functional safety for the process industry = identical to ISA-84.00.01 (except for grandfather clause)



Safety Lifecycle



source: IEC 61508-1 fig. 2

- SIS: Analysis and Design phase

Hazard and Risk Analysis, SIL Allocation

1 Concept

2 Overall scope definition

3 Hazard and risk analysis

4 Overall safety requirements

5 Safety requirements allocation

9 E/E/PE Safety system requirement specification

10 E/E/PE Safety system realization

source: IEC 61508-1 fig. 2

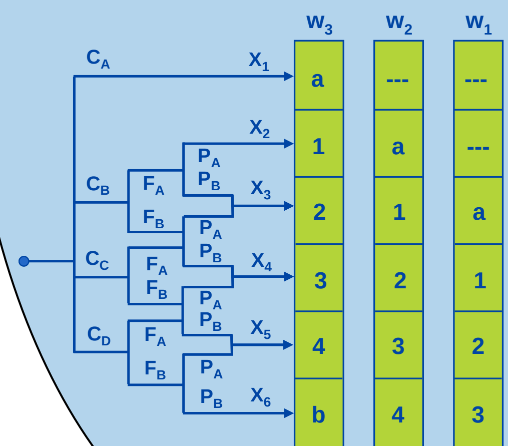
HAZOP Study

Identify Safety Functions

Allocate Safety Functions to IPLs

Safety Functions and SIL targets for SIS

- IEC 61508 : part 5
  - ALARP
  - Risk Graph
  - Risk Matrix
- IEC 61511 : part 3
  - FTA : Fault Tree Analysis
  - LOPA : Layers Of Protection Analysis



SIS: Realization Phase

Safety Integrity Level

Three basic requirements have to be fulfilled in order to claim any SIL:

1. Hardware fault tolerance for the claimed SIL to be justified.

2. PFD_{AVG} (of all elements within a SIF) shall be within the claimed SIL bandwidth

Hardware Safety Integrity

3. Systematic Capability shall comply with the requirements for the claimed SIL

Systematic Safety Integrity

Hardware Safety Integrity: SIL Classification & PFD

Safety Integrity Level	Risk Reduction Factor (RRF)	Average Probability of failure on demand (PFD)
4	> 10 000	$\geq 10^{-5}$ to $< 10^{-4}$
3	1 000 - 10 000	$\geq 10^{-4}$ to $< 10^{-3}$
2	100 - 1 000	$\geq 10^{-3}$ to $< 10^{-2}$
1	10 - 100	$\geq 10^{-2}$ to $< 10^{-1}$
0		(No Safety Requirements)

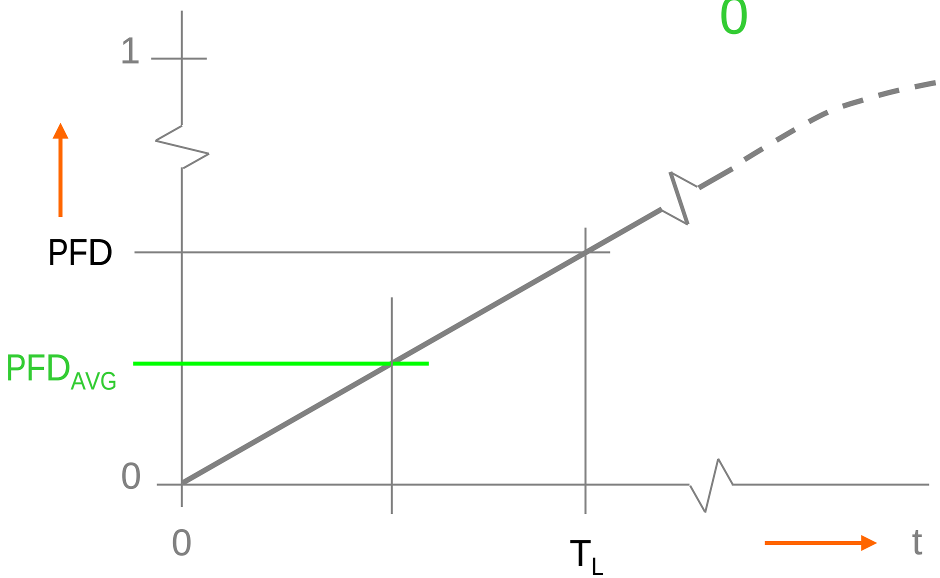
For Low Demand rate (less than once per year)

IEC 61508-1,
table 2

PFD : Probability of a Failure on Demand, derived from the safety parameters of the equipment.

$$PFD = 1 - e^{-\lambda_{Du}\, t}$$

$$PFD_{AVG} = \frac{1}{T_L}\int_0^{T_L} PFD(t)\,dt$$

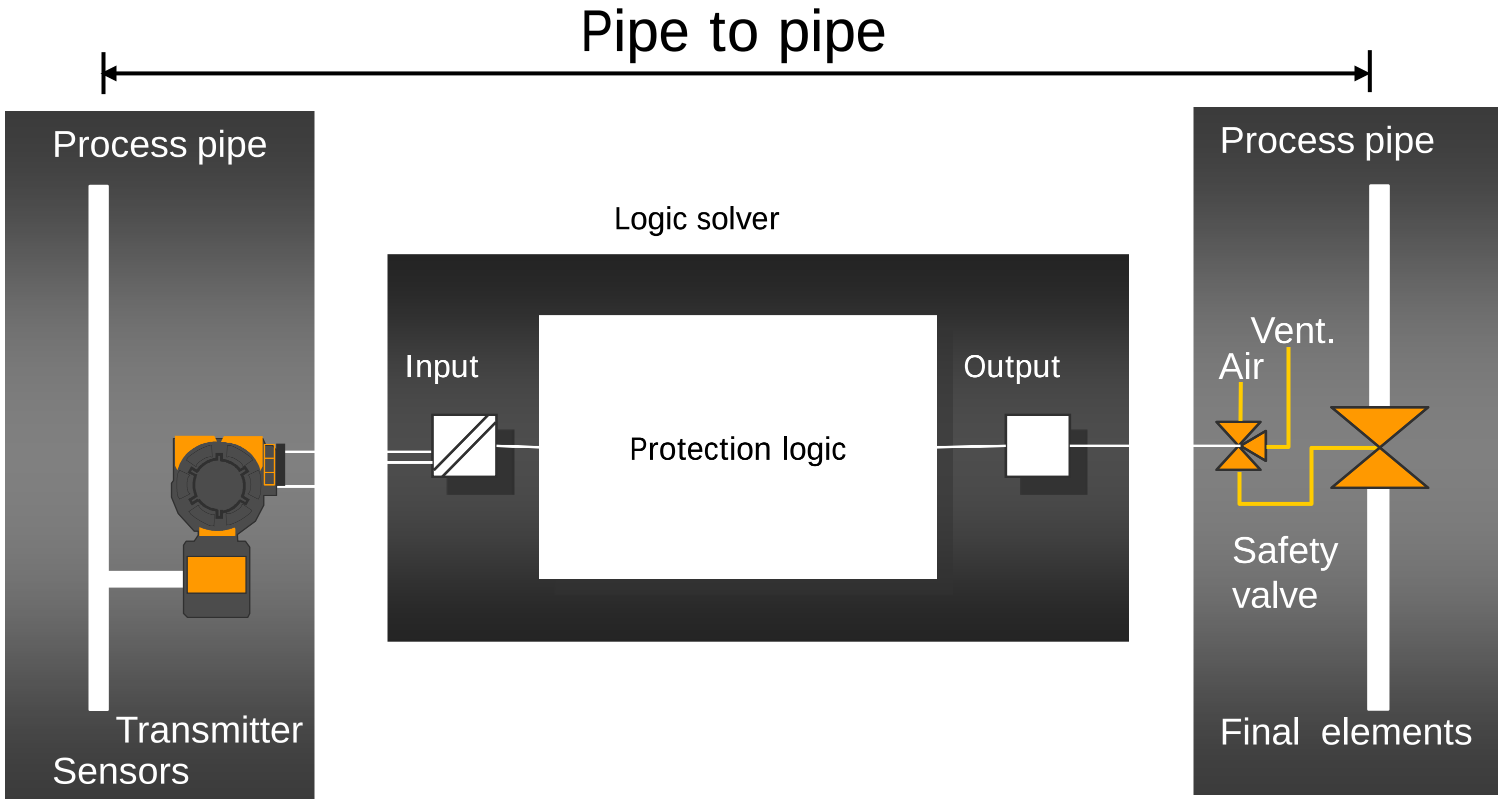


(T_L = life time)

$$PFD = \lambda_{Du} \times t$$

$$PFD_{AVG} = \tfrac{1}{2} \times \lambda_{Du} \times T_L$$

Hardware Safety Integrity: Average PFD for SIF

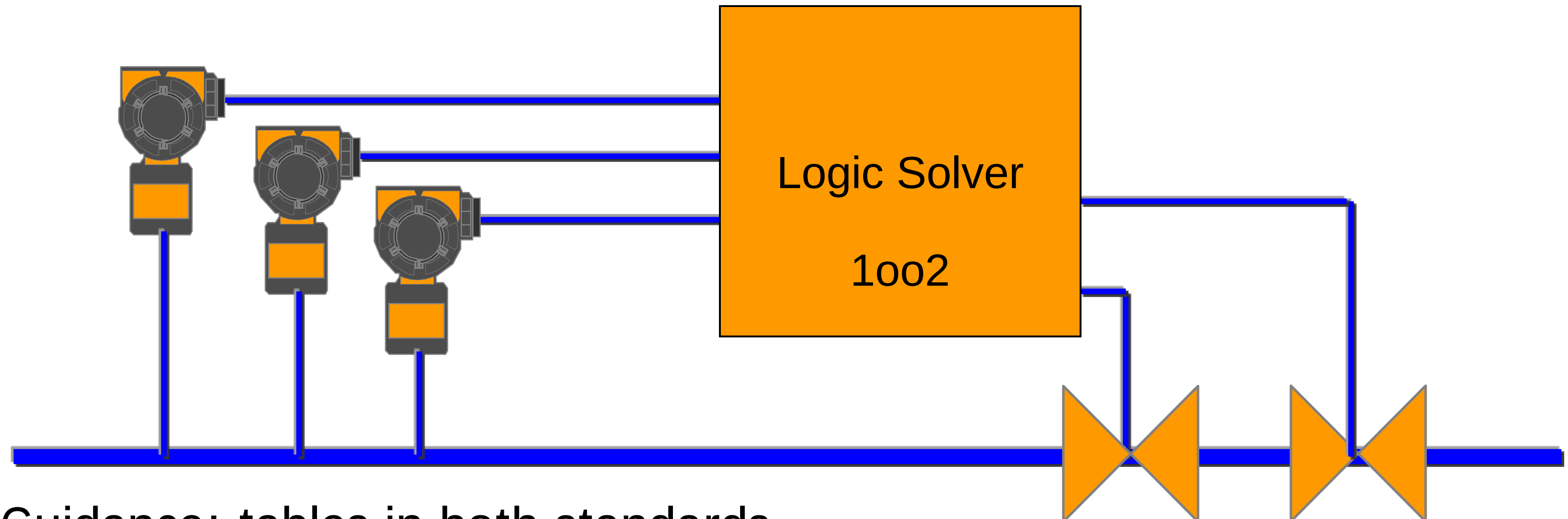


SIL → $PFD_{avg\ (target)}$ for the SIF

$$PFD_{avg\ (SIF)} = PFD_{avg\ (sensors)} + PFD_{avg\ (logic\ solver)} + PFD_{avg\ (final\ elements)}$$

Hardware fault tolerance

- The target SIL indicates the maximum PFDAVG but also depending on type and quality of the used device double / triple voting devices (1oo2, 1oo3) might be required



Guidance: tables in both standards

Fault tolerance acc. IEC 61508-2

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Type A : simple devices where the failure modes can easily be understood (mechanical devices, simple electronic devices like zener barrier, isolator etc.)

Table 3 — Hardware safety integrity: architectural constraints on type B safety-related subsystems

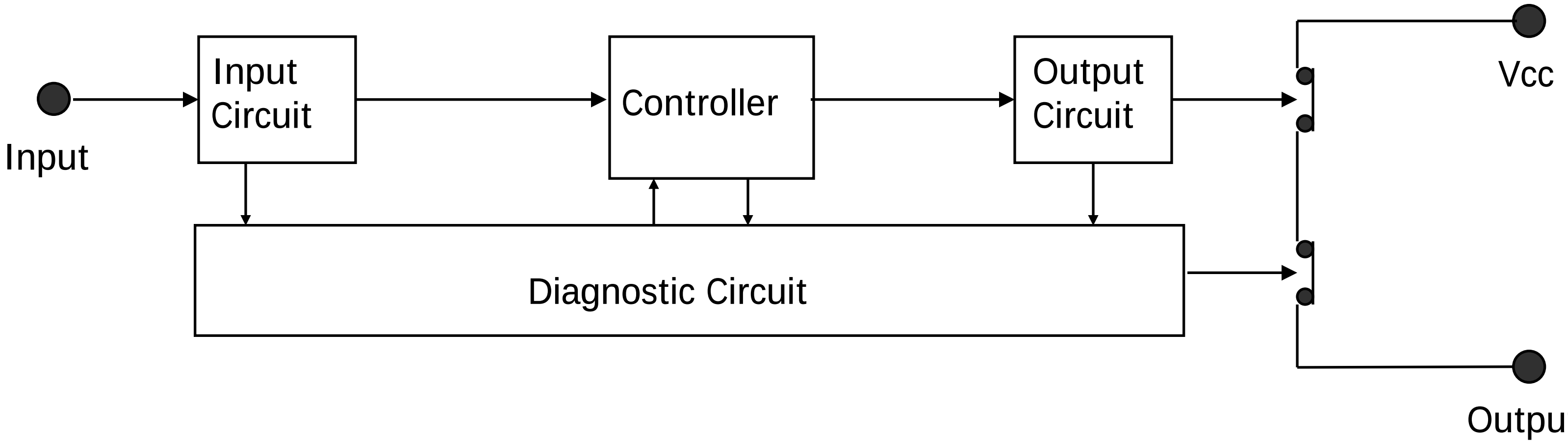
Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
NOTE 2 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Type B : everything that is not simple, not type A.

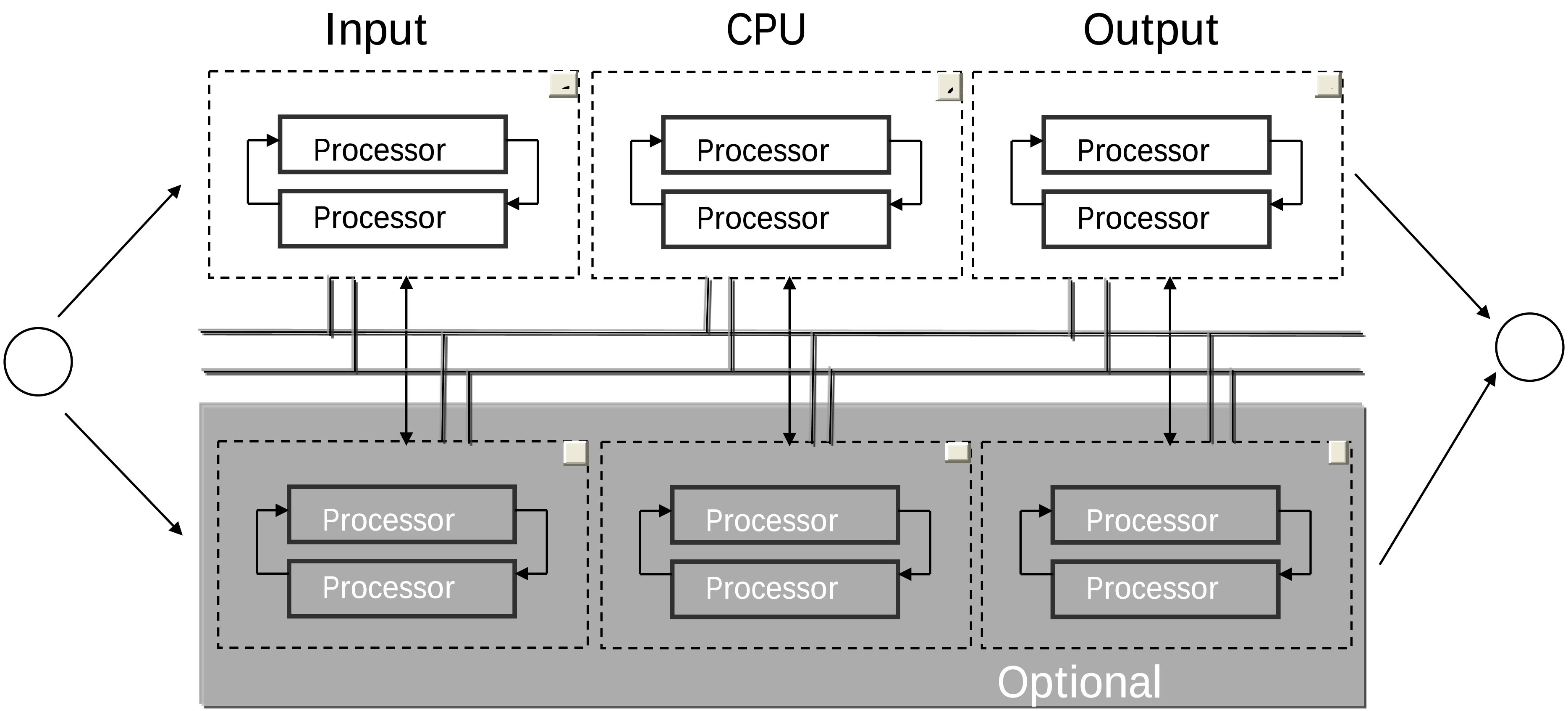
Logic Solver: Fault Tolerant Architecture

- 1oo1D architecture



- Other popular Architectures include:
  - 1oo2D
  - 2oo3
  - VMR 1oo1D

VMR 1oo1D



- Single SIL3 with high SFF
- Redundant configuration for High Availability

Systematic Safety Integrity

Measures to avoid systematic failures

Employment of safety competent personnel
Controlled realization
Verification processes
Configuration management
Document control (including software)
Functional Safety Assessment
Validation processes
Controlled operation, proof testing and maintenance
Controlled site modifications

Functional Safety Management System as per IEC 61508/61511

- Responsibility of: End-user, Contractor, SIS equipment suppliers/ integrators

Topic

- SIS: Operation and Maintenance phase
  - Proof Testing
  - Management of Change

Proof Testing

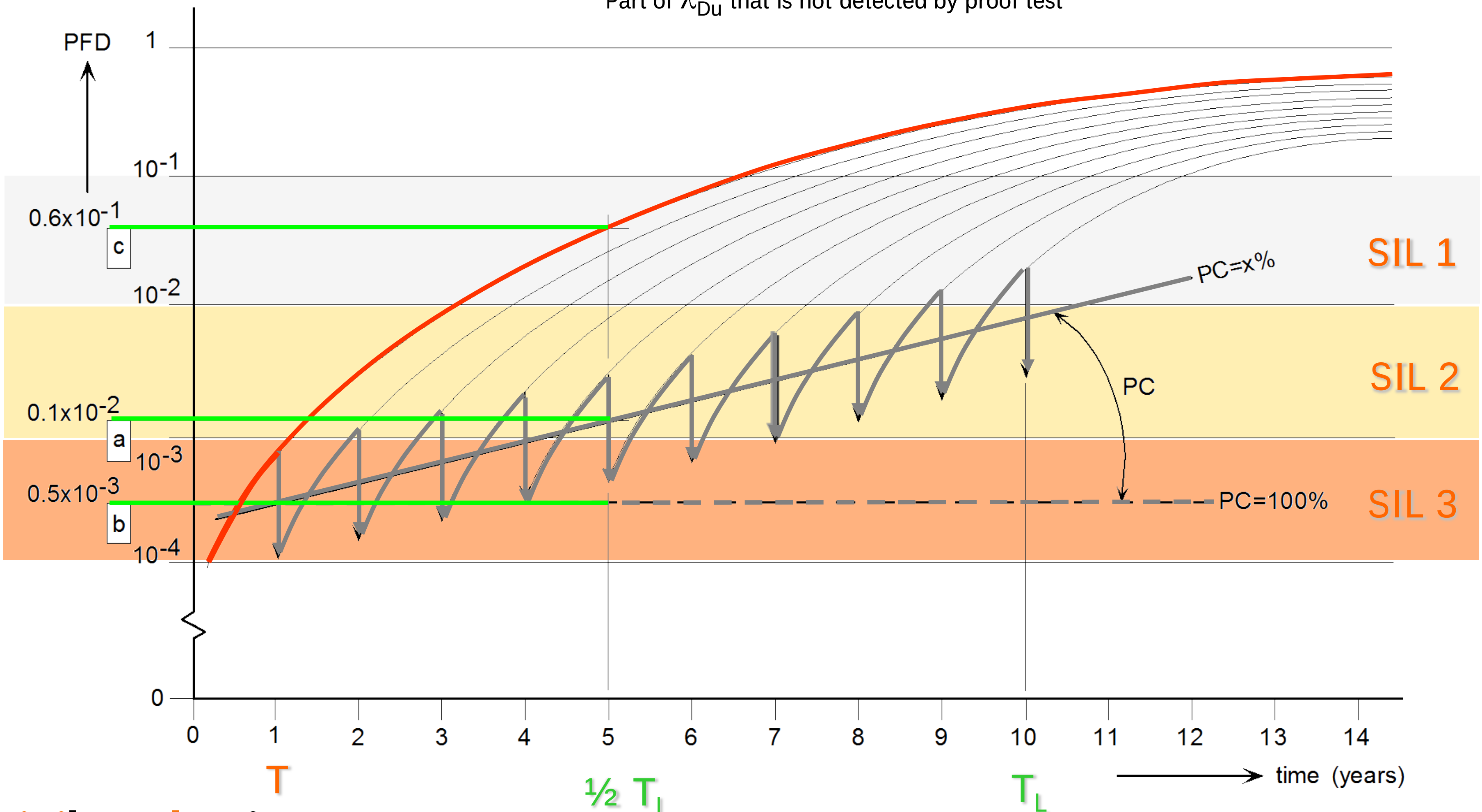
- A proof test means a complete test of the SIF, “pipe to pipe”.
- The purpose of the test is to reveal all “dangerous undetected” failures that are present in the SIF
- After the proof test the elements in the SIF should be in their initial state
- Proof Test Coverage: The proof test of the system does not completely restore the initial state due to:
  - Imperfect testing
  - Imperfect repair
  - Ageing

Impact of Proof testing on PFD_{AVG}

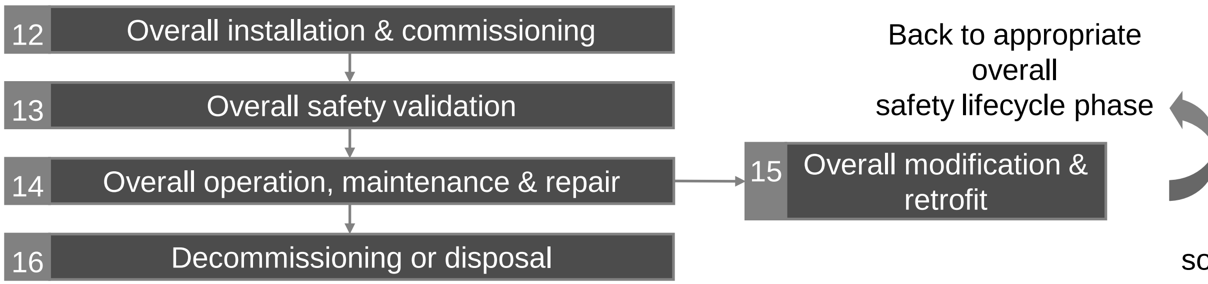
Without proof test → $PFD = 1 - e^{-\lambda_{Du} t}$ Or approximated as, $PFD = \lambda_{Du} \times t$ and $PFD_{AVG} = ½ \times \lambda_{Du} \times T_L$

With proof test → $PFD_{AVG} = ½ \times PC \times \lambda_{Du} \times T + ½ \times (1 - PC) \times \lambda_{Du} \times T_L$

Part of λ_{Du} that is not detected by proof test



Management of Change

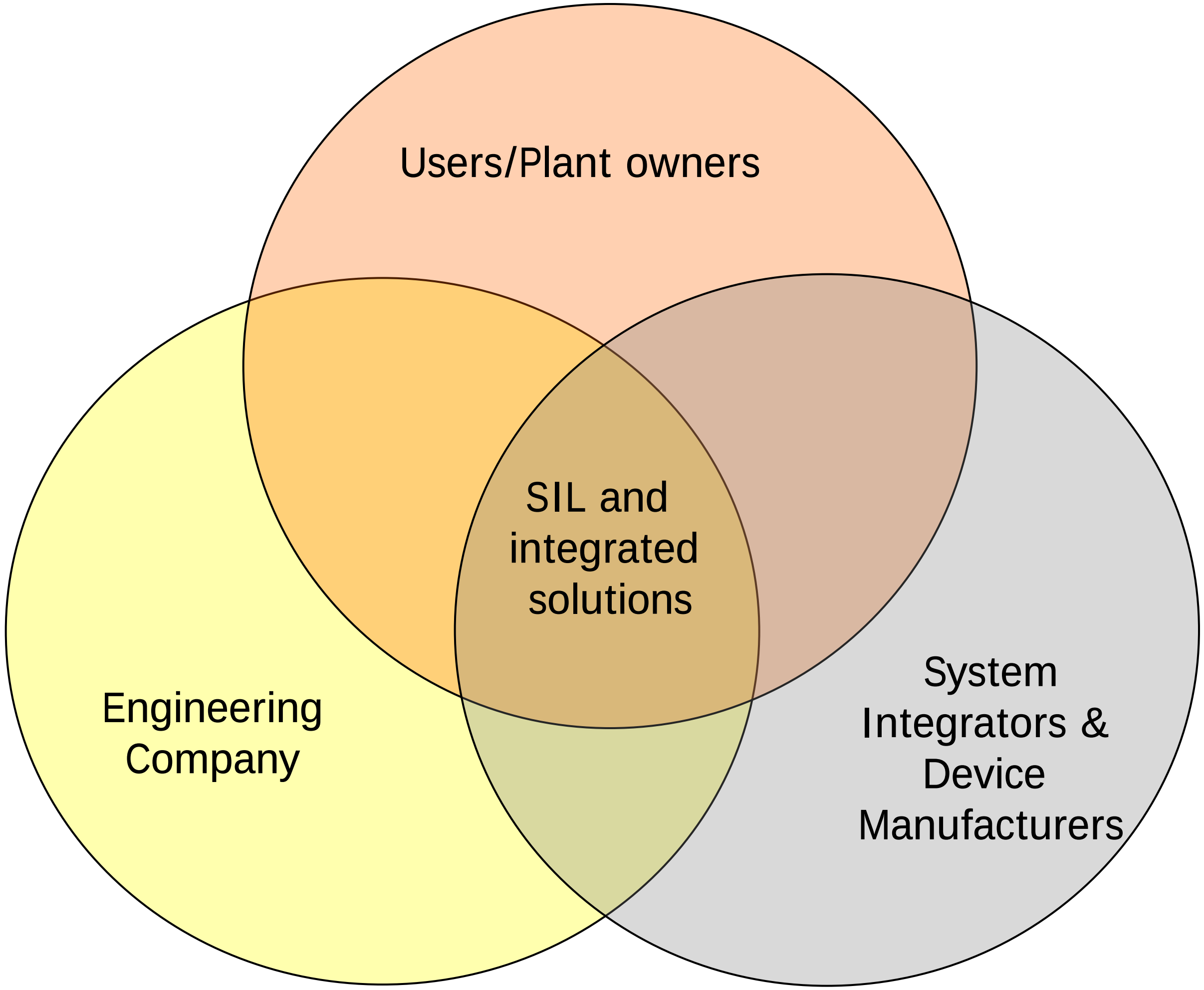


source: IEC 61508-1 fig. 2

- Prior to modifying the SIS functions on a running installation, a hazard and risk analysis needs to be carried out >> Management of Change procedure

Functional Safety Management

- Who should have a documented and auditable functional safety management system?



TÜVRheinland®

ZERTIFIKAT
CERTIFICATE

FUNCTIONAL SAFETY MANAGEMENT
- IEC 61508 / IEC 61511 -

No.: 968/FSM119.03/11

The company

Yokogawa Engineering Asia Pte Ltd
Safety Systems Business Unit
5 Bedok South Road
Singapore 469270
Republic of Singapore

YOKOGAWA

TÜVRheinland FSM

Has successfully demonstrated during an audit that a Functional Safety Management System (FSM-System) has been implemented and applied accordingly.

Purpose of the audit is to obtain evidence of compliance with the organizational requirements related to the following aspects, **Management of Functional Safety, Documentation, Functional Safety Assessment** and **company specific Safety Lifecycle Phases** according to the scope of certification based on the standards:

IEC 61508: E/E/PE- safety related System Integration
IEC 61511: SIS - Integration

This covers integration of **E/E/PE-safety related Systems** and **Safety Instrumented Systems** for the **process industry** specifically to cover the activities **configuration, application programming, assembly, test** and **safety loop calculations.**

This certification does not replace approval or certification for specific E/E/PE-safety related System Integrations.

Validity: until January 2014

Cologne, 2011-03-11

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

H. Gall

Dipl.-Ing. Heinz Gall, Head of Certification Body for FSM-Systems

Further information referring to the scope of certification is published on http://www.tuvasi.com.

Functional Safety Management System in accordance with IEC 61508 / 61511

Thanks For Your Kind Attention!