Prasad Goteti

Dec 1, 2020

SAFETY LIFE CYCLE PER IEC / ISA 61511

P^{2}SAC

Purdue Process Safety & Assurance Center

Honeywell

Presenter today

Prasad Goteti, *P.Eng, CFSE, TUV FS Expert*

Safety Engineering Consultant

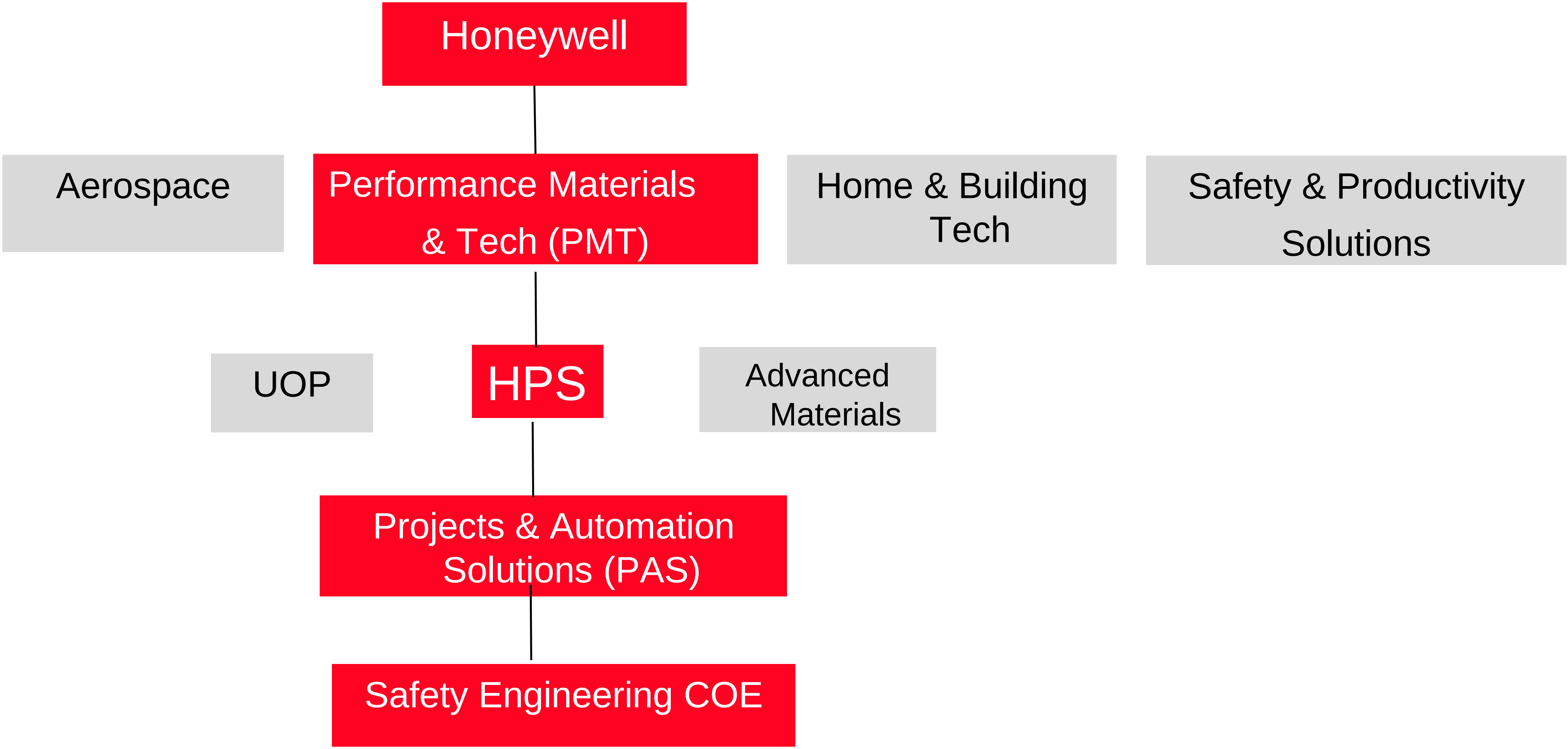
Honeywell Process Solutions

Scientific Advisory Board member, Purdue Process Safety and Assurance Center (P2SAC)

Member – ISA TR 84.00.07, Guidance on Fire and Gas for Process Industries

Honeywell

THE POWER OF CONNECTED



Honeywell

Aerospace

Performance Materials & Tech (PMT)

Home & Building Tech

Safety & Productivity Solutions

UOP

HPS

Advanced Materials

Projects & Automation Solutions (PAS)

Safety Engineering COE

Agenda

- What is Risk ?
- Introduction to Functional Safety
- Analysis phase of the Safety Life Cycle (SLC)
- Realization phase of the SLC
- Operations and Maintenance phase of the SLC
- Conclusion

Honeywell

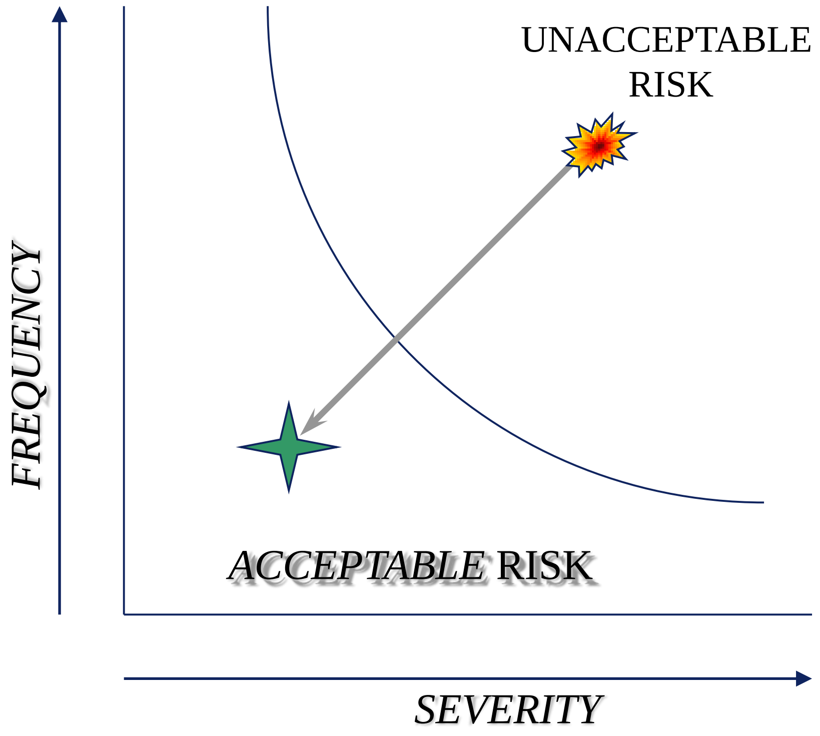
THE POWER OF CONNECTED

What is Risk ?

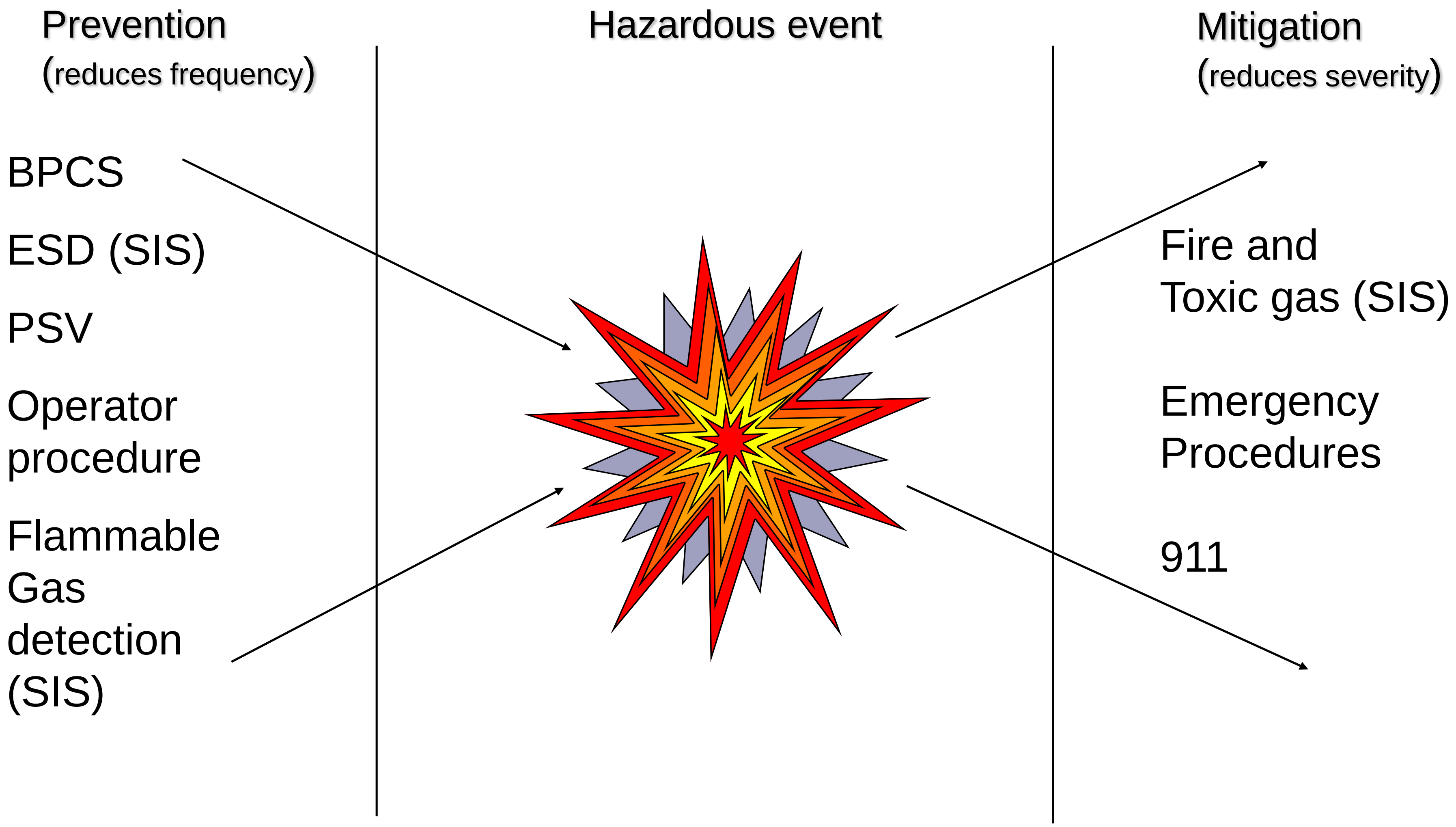
Honeywell
THE POWER OF **CONNECTED**

What is Risk ?

Risk is defined as the combination of the frequency of occurrence of harm and the severity of that harm



The Bow Tie representation



Prevention
(reduces frequency)

Hazardous event

Mitigation
(reduces severity)

BPCS

ESD (SIS)

PSV

Operator procedure

Flammable Gas detection (SIS)

Fire and Toxic gas (SIS)

Emergency Procedures

911

Layers of Protection

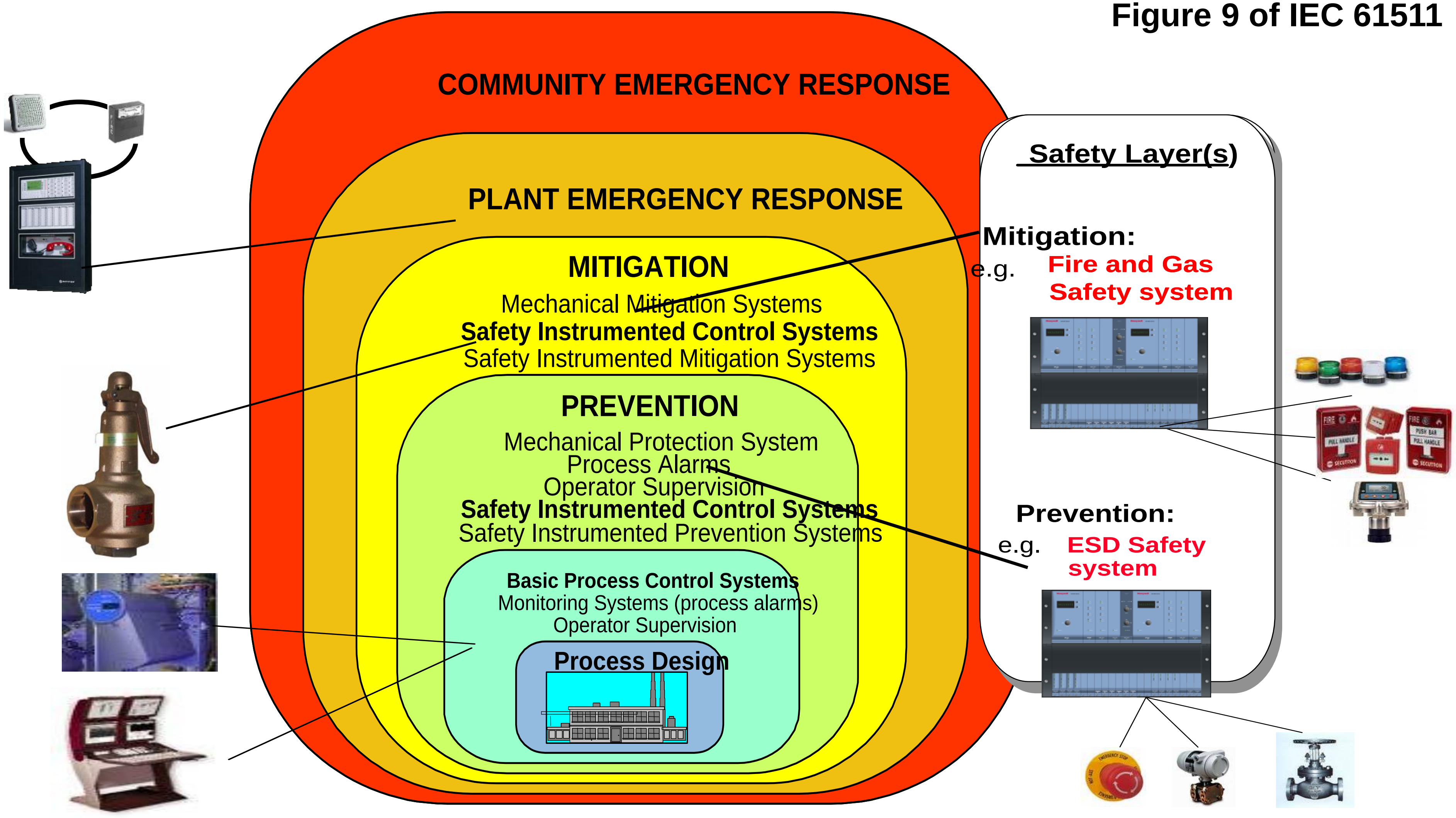


Figure 9 of IEC 61511

COMMUNITY EMERGENCY RESPONSE

PLANT EMERGENCY RESPONSE

MITIGATION

Mechanical Mitigation Systems
Safety Instrumented Control Systems
Safety Instrumented Mitigation Systems

PREVENTION

Mechanical Protection System
Process Alarms
Operator Supervision
Safety Instrumented Control Systems
Safety Instrumented Prevention Systems

Basic Process Control Systems
Monitoring Systems (process alarms)
Operator Supervision

Process Design

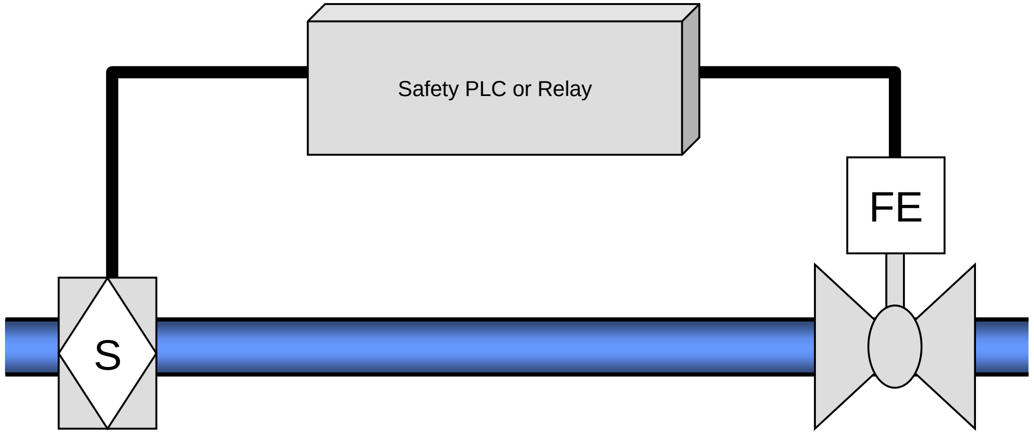
Safety Layer(s)

Mitigation:
e.g. Fire and Gas Safety system

Prevention:
e.g. ESD Safety system

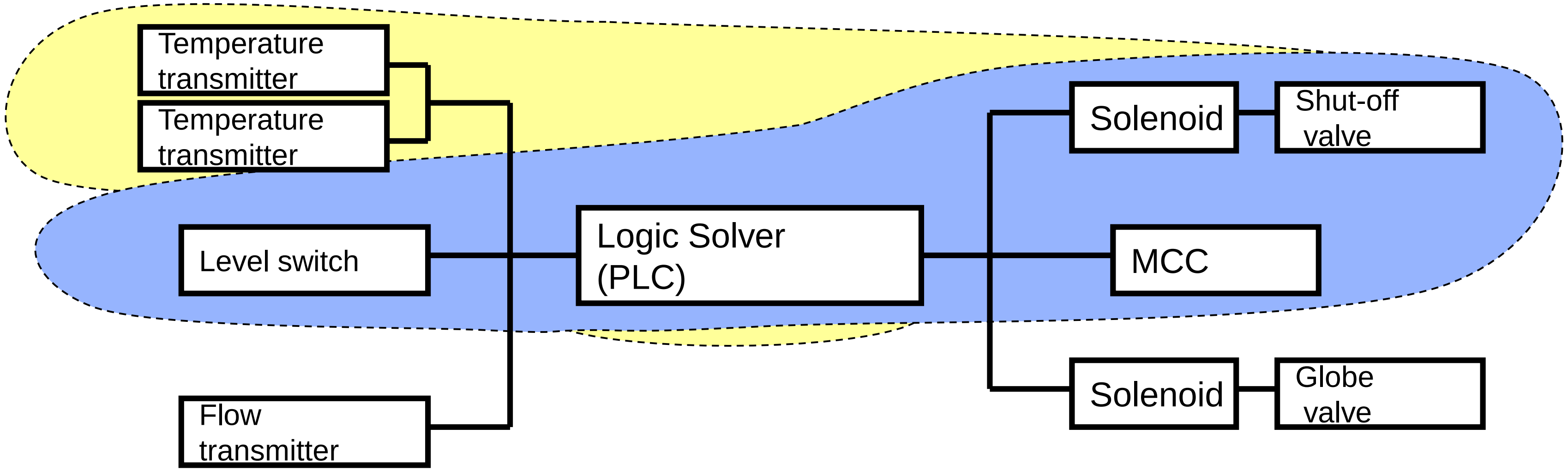
What is a Safety Instrumented System (SIS)?

- Safety instrumented system (SIS) as per IEC 61511
  - Instrumented system used to implement **one or more** safety instrumented functions (SIF)
- A SIS is
  - composed of any combination of sensor(s), logic solver(s), and final elements(s)



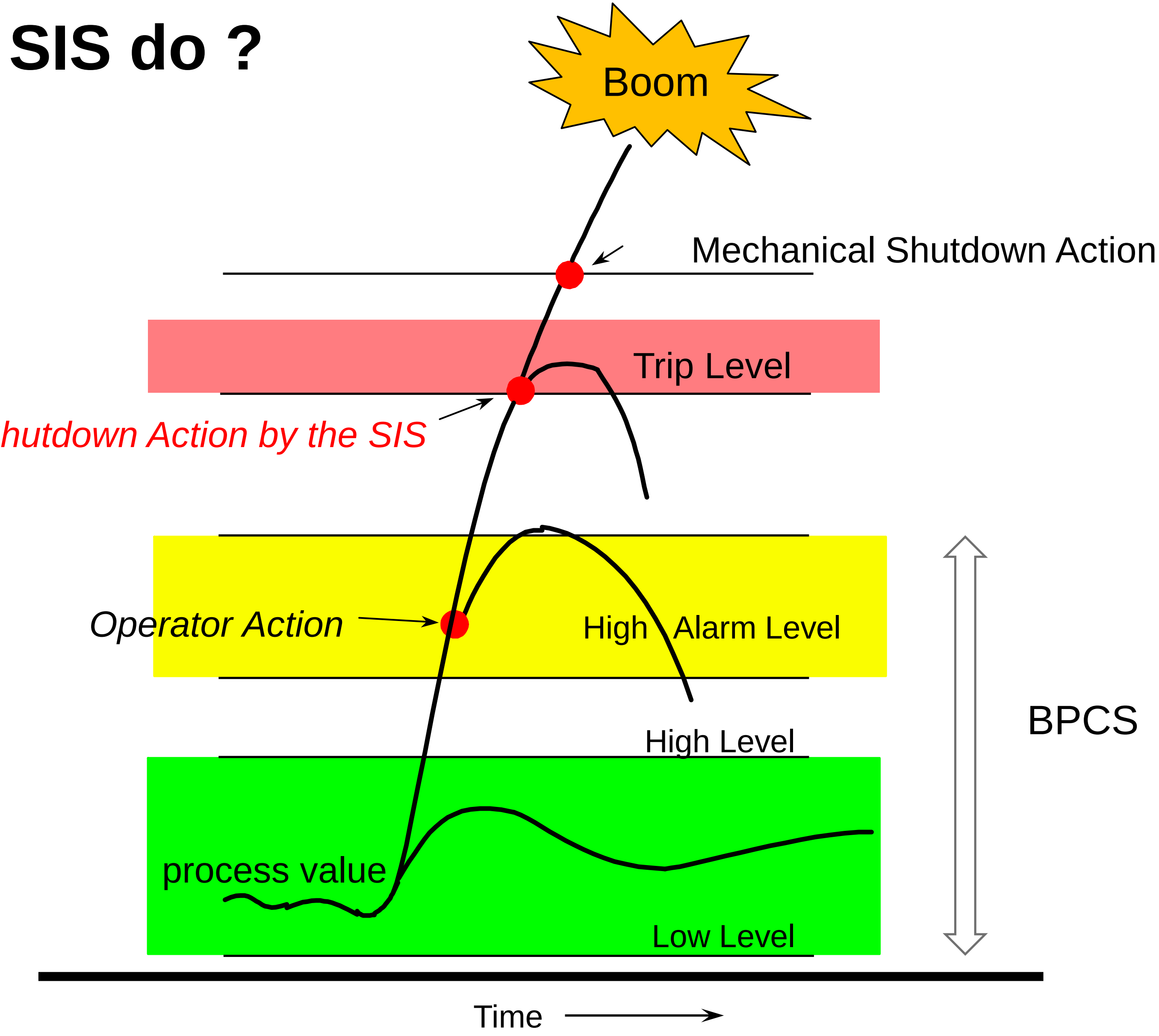
What are Safety Instrumented Functions (SIFs)

An SIS may implement one or more safety instrumented functions (SIFs), which are designed and implemented to address a **specific** process hazard or hazardous event.



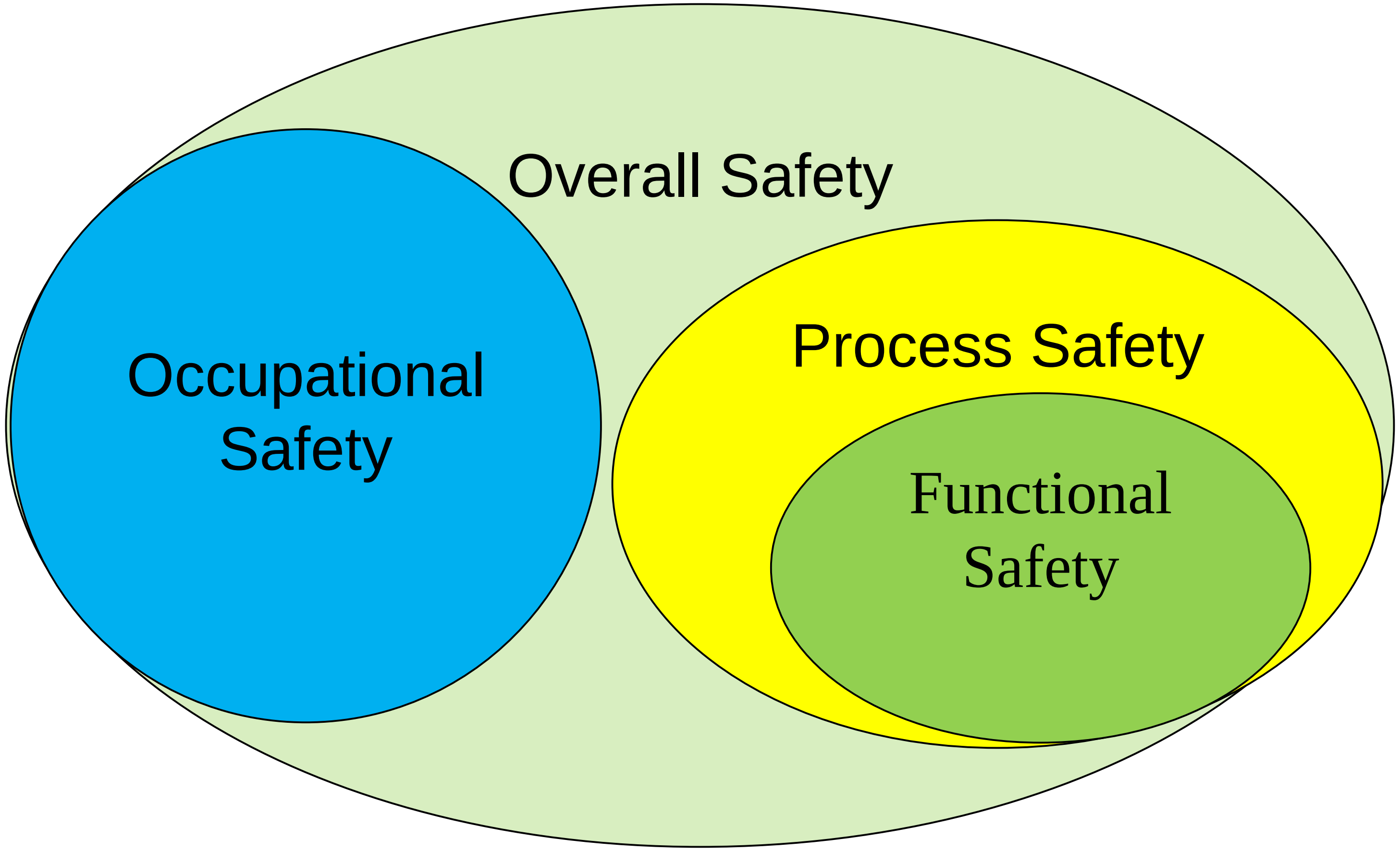
Safety Instrumented System (SIS) with multiple Safety Instrumented Functions (SIF)

What does an SIS do ?



Introduction to Functional Safety

Functional Safety, part of Overall Safety



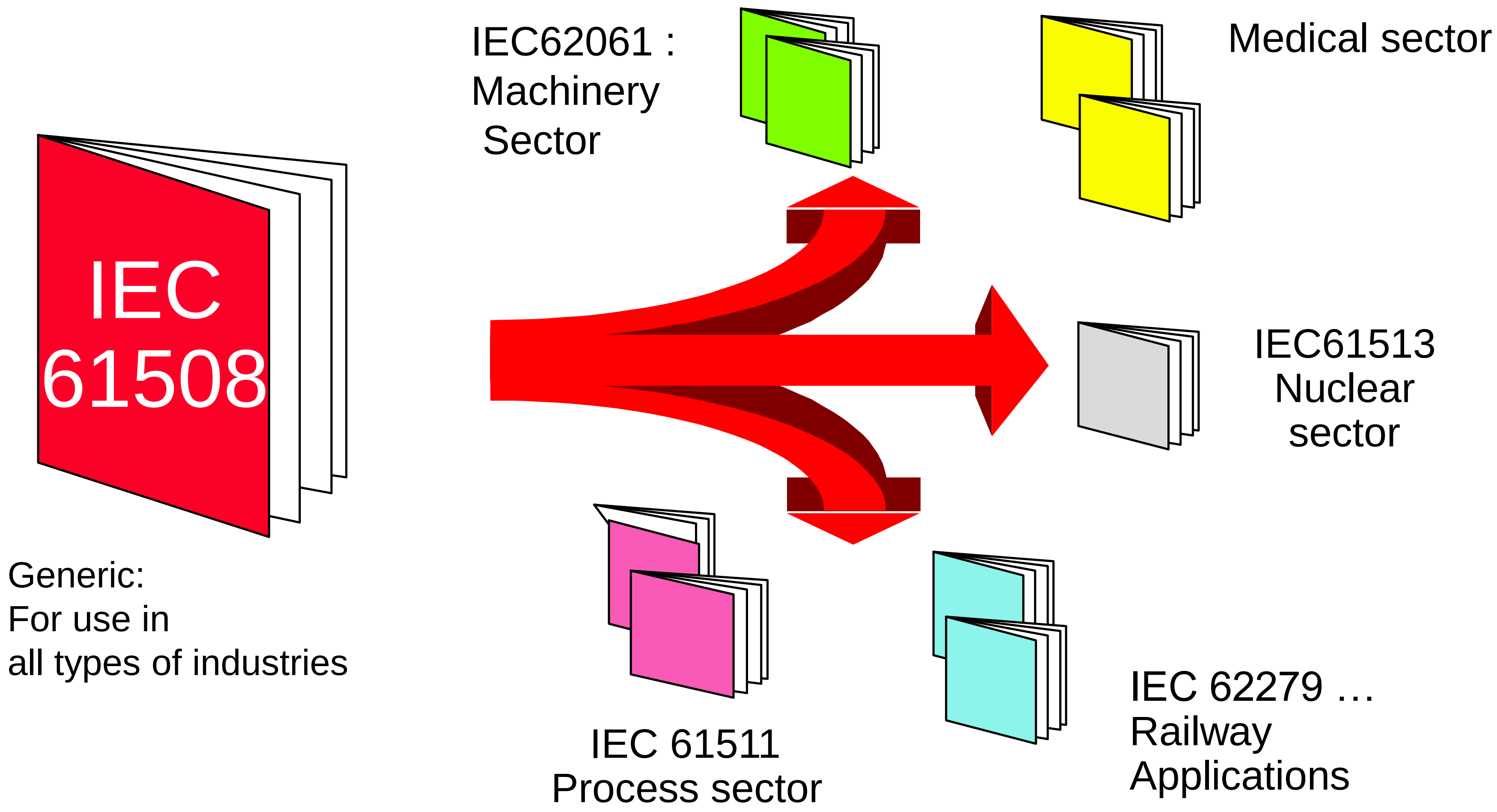
Functional Safety standards used in the industry

- IEC 61508 is a standard written with an intent to help design and develop products which are SIL rated for any industry for Electrical / Electronic / Programmable Electronic (E/EE/PE) systems.

- IEC 61511 and ISA84.00.01 are almost identical standards which have been written to help analyze, design, realize, install, commission and maintain SIL loops for the **Process industry**.

- **In the latest edition (August 2018), ISA 84.00.01 is now renamed as ISA 61511 !**

Generic and application sector standards



IEC62061 :
Machinery
Sector

Medical sector

IEC61513
Nuclear
sector

Generic:
For use in
all types of industries

IEC 61511
Process sector

IEC 62279 …
Railway
Applications

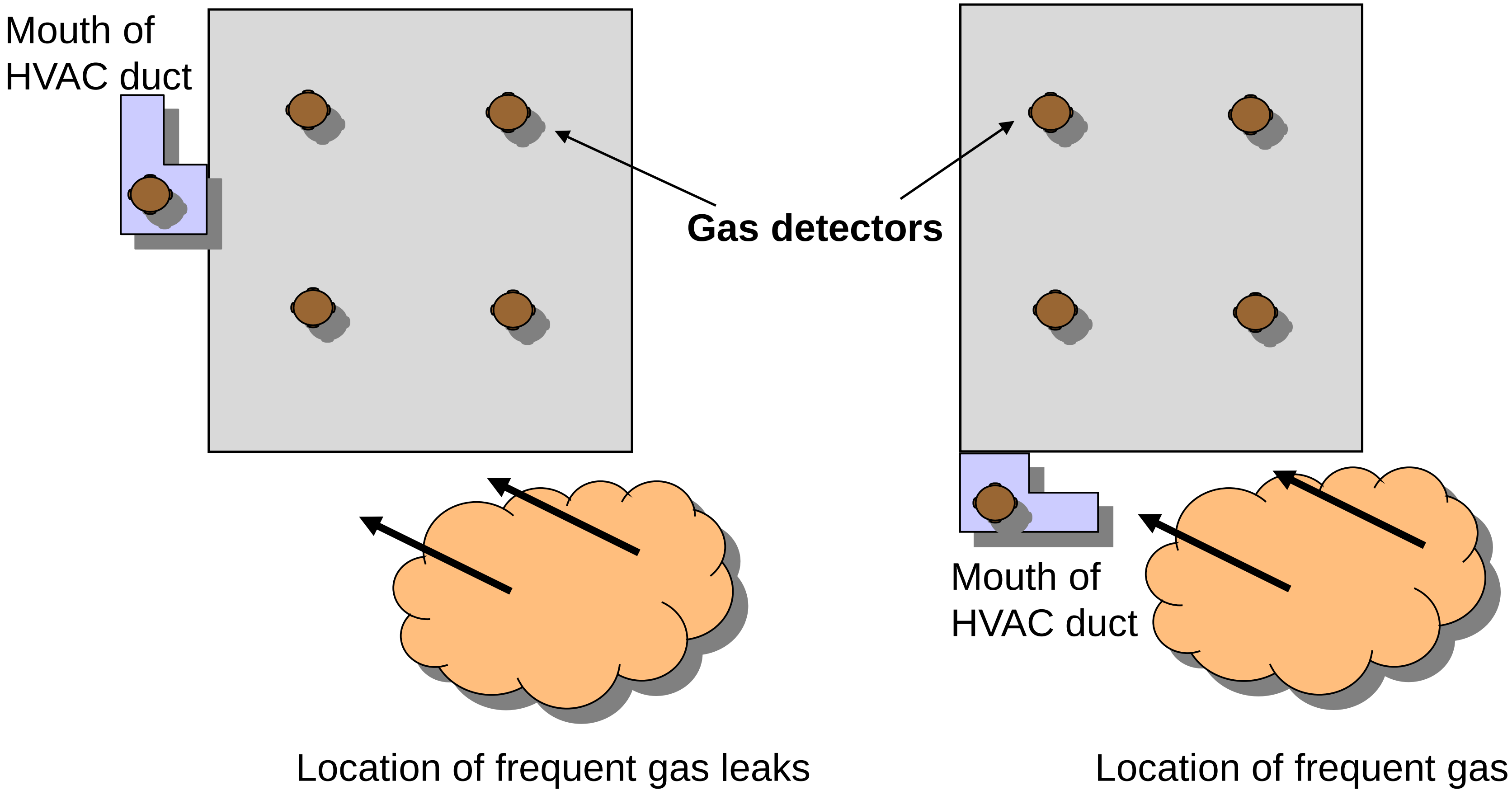
Prescriptive and Performance based standards

- **Prescriptive** standards specify the requirement to meet the code while **performance based** standards only give a guideline to the designer / end user.

- While NFPA 72 is prescriptive the IEC / ISA 61511 standards are **performance based**.

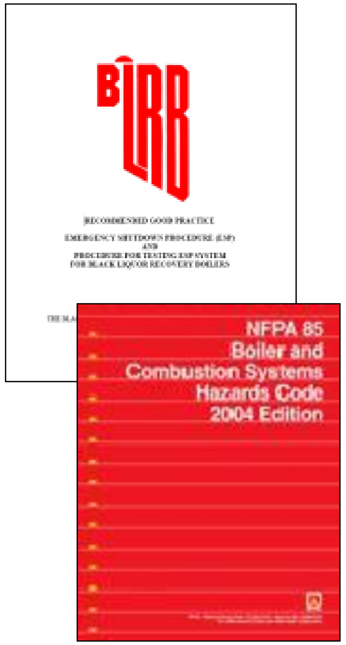
Why Prescriptive standards do not always work

Irrespective of where the mouth of the HVAC duct opens, Prescriptive standards will specify the same number of Gas Detectors inside the building


Mouth of HVAC duct
Gas detectors
Mouth of HVAC duct
Location of frequent gas leaks
Location of frequent gas leaks

Prescriptive Standards

- Prescribe materials, procedures and methods, focusing in the constructive characteristics of the resulting system, usually not stating explicitly any system goals or objectives
- Benefits
  - Easy to apply (must follow rules)
  - Certainty about compliance (do’s or don’ts)
  - User decisions are limited
  - No commitment regarding tolerable risk levels
- Drawbacks
  - Lack of flexibility to introduce new technologies and innovations
  - Safety problems may be overseen if not considered by the standard
  - Does not give directions on safety system integrity



BLRB

RECOMMENDED GOOD PRACTICE

EMERGENCY SHUTDOWN PROCEDURE (ESP)
AND
PROCEDURE FOR TESTING ESP SYSTEM
FOR BLACK LIQUOR RECOVERY BOILERS

NFPA 85
Boiler and
Combustion Systems
Hazards Code
2004 Edition

- NFPA 85 (Boiler and Combustion Systems Hazards Code)
- API 556 (Instrumentation and Control Systems for Fired Heaters and Steam Generators)
- API RP 14C (Safety for Offshore Production Platforms)
- NFPA 72 (Fire Alarm / Control Systems)
- BLRB (Black Liquor Recovery Boiler)

Performance/Functional-Based Standards

- State goals and objectives to be achieved, and methods or procedures to demonstrate that the resulting system meets the goals and objectives
  - Tell us how to proceed
- Benefits
  - Flexibility
  - Thorough coverage of risks (by risk analysis methods)
  - Maintenance and testing considered in calculations
  - Requires justification of decisions based on objective information
- Drawbacks
  - Needs more effort to implement
  - Stringent requirements to demonstrate safety integrity level
  - Requires user decision about risk tolerance

  - IEC 61508
  - IEC 61511
  - ISA 84.00.01 (IEC 61511 + grandfather clause)

ANSI/ISA-S84.01-1996
Approved March [illegible], 1997

American National Standard

Application of Safety
Instrumented Systems
for the Process Industries

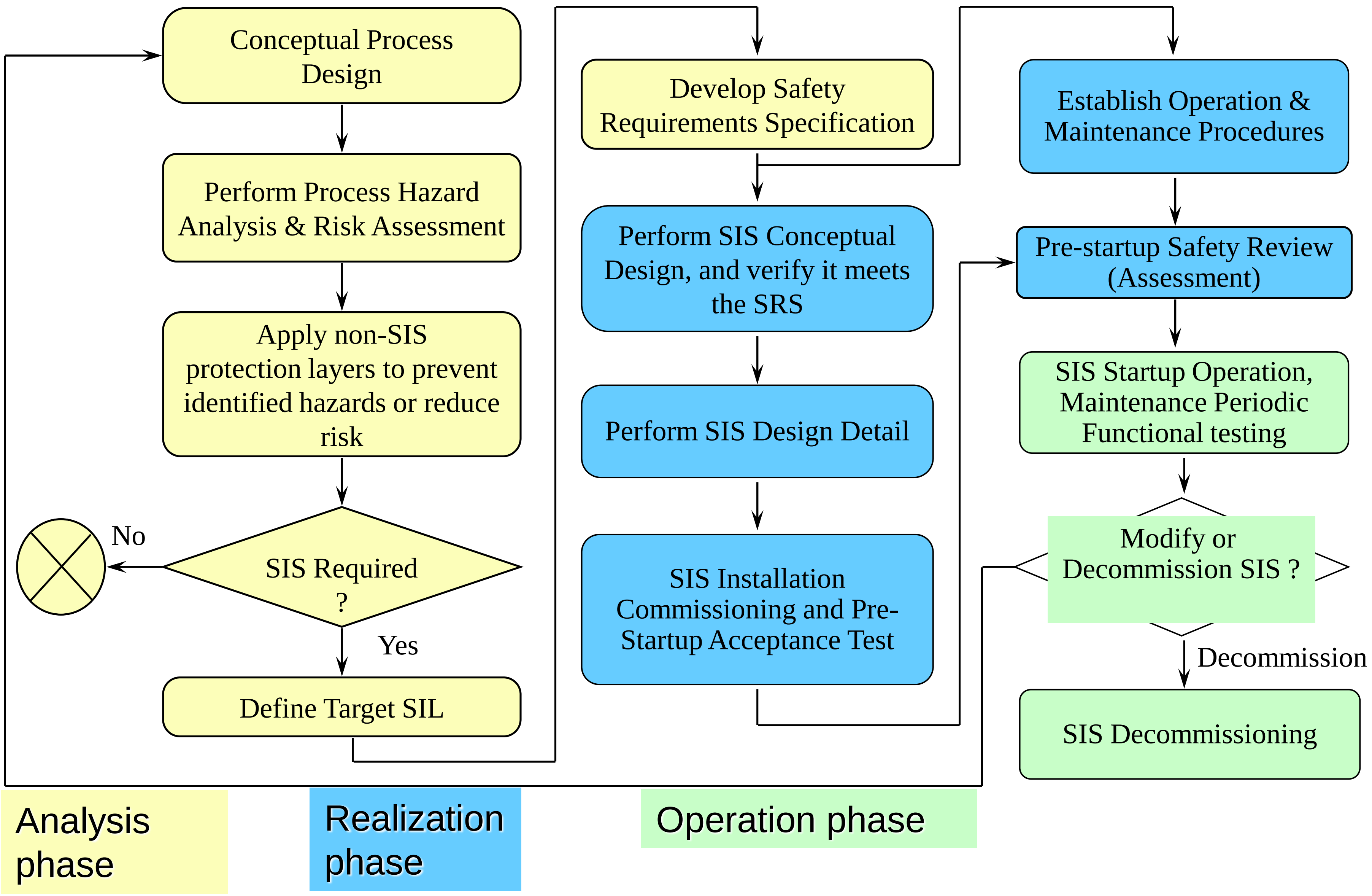
INTERNATIONAL STANDARD

IEC 61511-1

Functional safety –
Safety instrumented systems
for the process industry sector –
Part 1:
Framework, definitions, system,
hardware and software requirements

[illegible]

The Safety Life Cycle as defined in the standards



Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
SIS Required ?
No
Yes
Define Target SIL
Develop Safety Requirements Specification
Perform SIS Conceptual Design, and verify it meets the SRS
Perform SIS Design Detail
SIS Installation Commissioning and Pre-Startup Acceptance Test
Establish Operation & Maintenance Procedures
Pre-startup Safety Review (Assessment)
SIS Startup Operation, Maintenance Periodic Functional testing
Modify or Decommission SIS ?
Decommission
SIS Decommissioning
Analysis phase
Realization phase
Operation phase

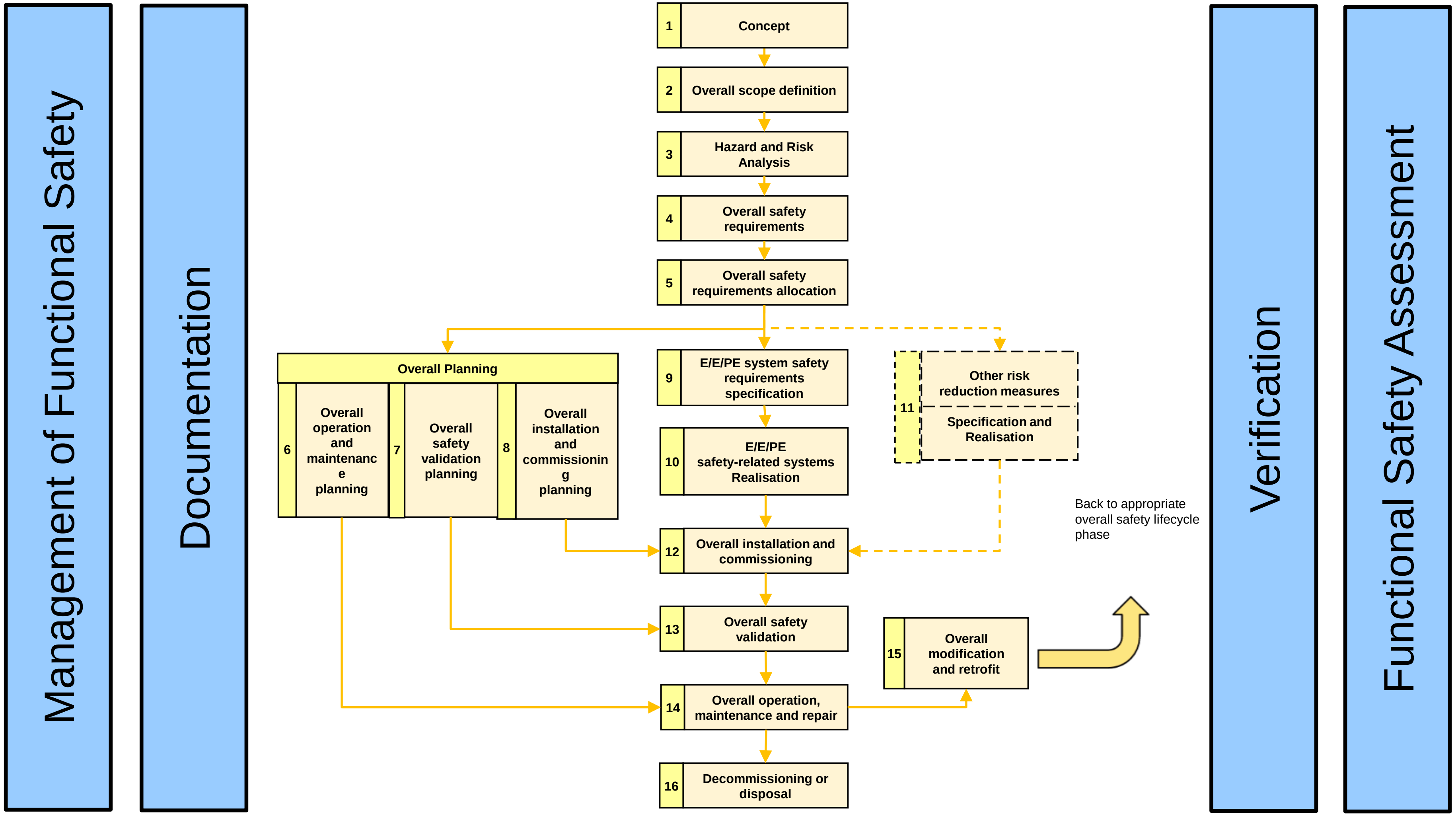
Standard Compliance throughout SLC

- **Analysis Phase** :
  - Target SIL must be specified for SIF based on hazard and risk analysis
  - Functional requirement for SIF should be detailed
- **Realization (Detailed Engineering) Phase** :
  - Each SIF must meet target SIL requirements for:
    - Random failure rate (PFD_{avg})
    - Architectural constraints
    - Development process for each component.
- **Operation and Maintenance Phase :**
  - Maintain SIF to the specified SIL
  - Any changes to the SIF should be strictly controlled

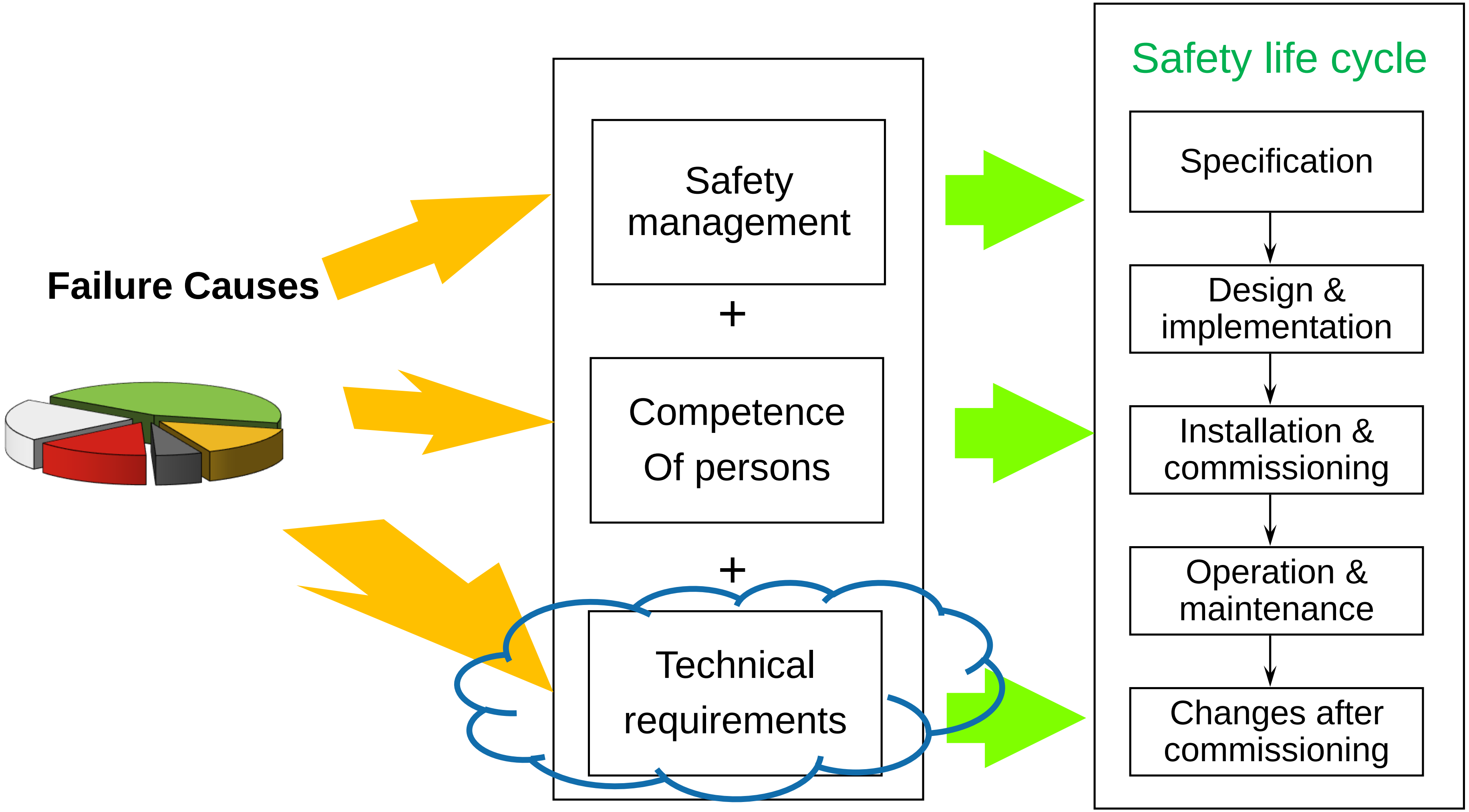
In the rest of the slides concepts from IEC 61508 and 61511 will be discussed together

Honeywell
THE POWER OF CONNECTED

IEC 61508 - Safety Lifecycle


Management of Functional Safety
Documentation
1 Concept
2 Overall scope definition
3 Hazard and Risk Analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Overall Planning
6 Overall operation and maintenanc e planning
7 Overall safety validation planning
8 Overall installation and commissionin g planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems Realisation
11 Other risk reduction measures
Specification and Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal
Back to appropriate overall safety lifecycle phase
Verification
Functional Safety Assessment

Strategy to achieve Functional Safety



Failure Causes

Safety management

+

Competence Of persons

+

Technical requirements

Safety life cycle

Specification

Design & implementation

Installation & commissioning

Operation & maintenance

Changes after commissioning

Question 1:

Which of the following gives the best definition of risk?

a). hazardous situation which results in harm

b). potential source of harm

c). combination of the probability of occurrence of harm and the severity of that harm.

d). circumstances in which a person is exposed to hazard(s).

Question 2:

Which statement is true?

a). Occupational safety is part of functional safety.

b). Functional safety is part of process safety

c). Process and functional safety are part of occupational safety

d). None are correct

Question 3:

IEC 61508 is a standard addressing:

a) Burner management systems

[✓ b) Programmable electronic safety-related systems]

c) Pneumatic control systems

d) Distributed control systems

Question 4:

How are IEC 61508 and IEC 61511 related to each other?

a) IEC 61508 is the standard for the process industry and IEC 61511 contains all the techniques that should be considered.

b) IEC 61511 is the functional safety standard for safety instrumented systems for the process industry sector that was developed under the umbrella of the general functional safety standard IEC 61508.

c) They are not related to each other.

d) IEC 61508 describes the qualitative requirements and IEC 61511 the quantitative requirements that have to be taken into account for safety-related systems.

Honeywell
THE POWER OF **CONNECTED**

Question 5:

The Three main phases of the Safety Life Cycle are :

[✓ a) Analysis, Realization, Operation & Maintenance]

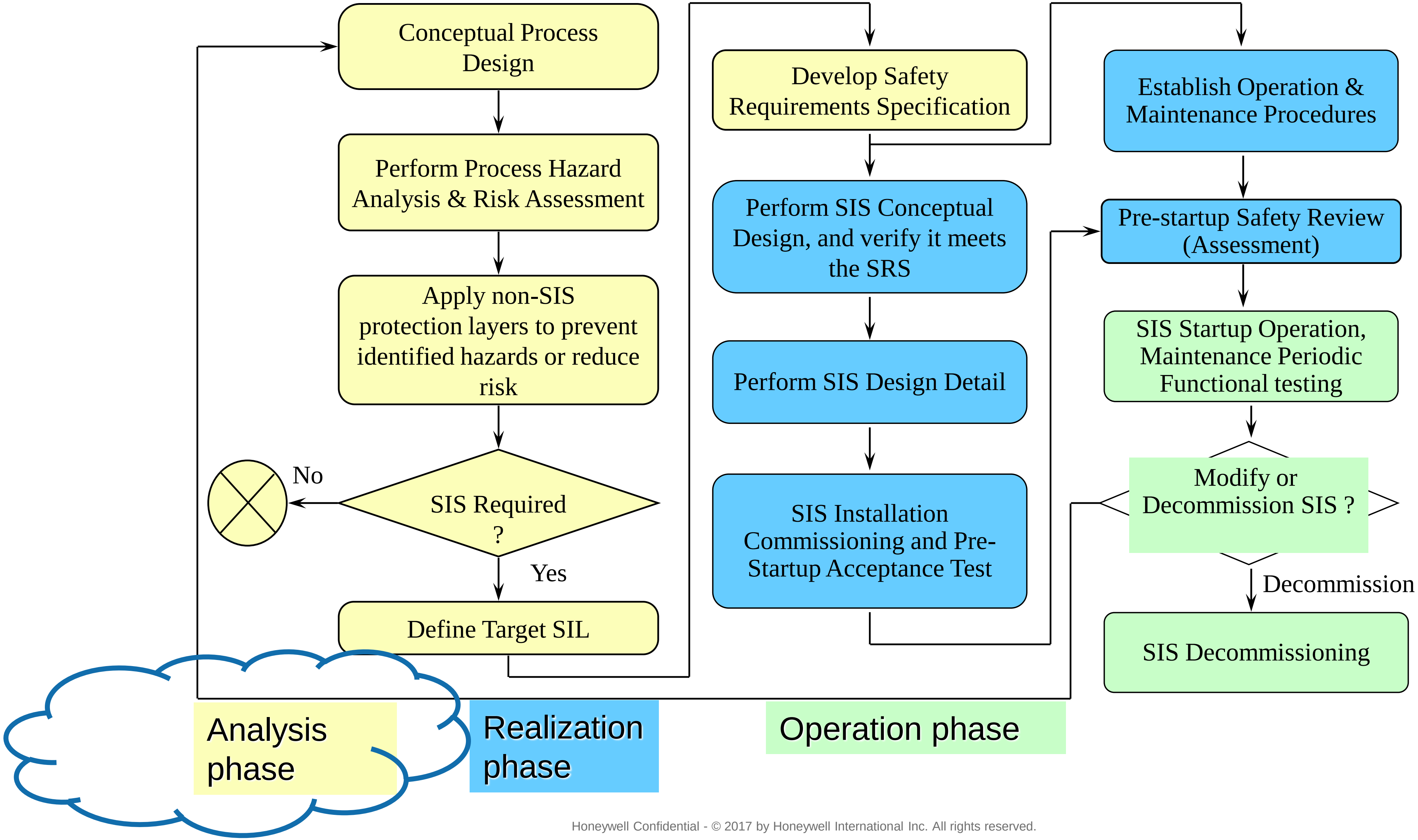
b) Analysis, SIS, SRS

c) Realization, Functional Safety Management, SIS

d) Control, Safety, Risk reduction

Analysis Phase

The Safety Life Cycle as defined in the standards

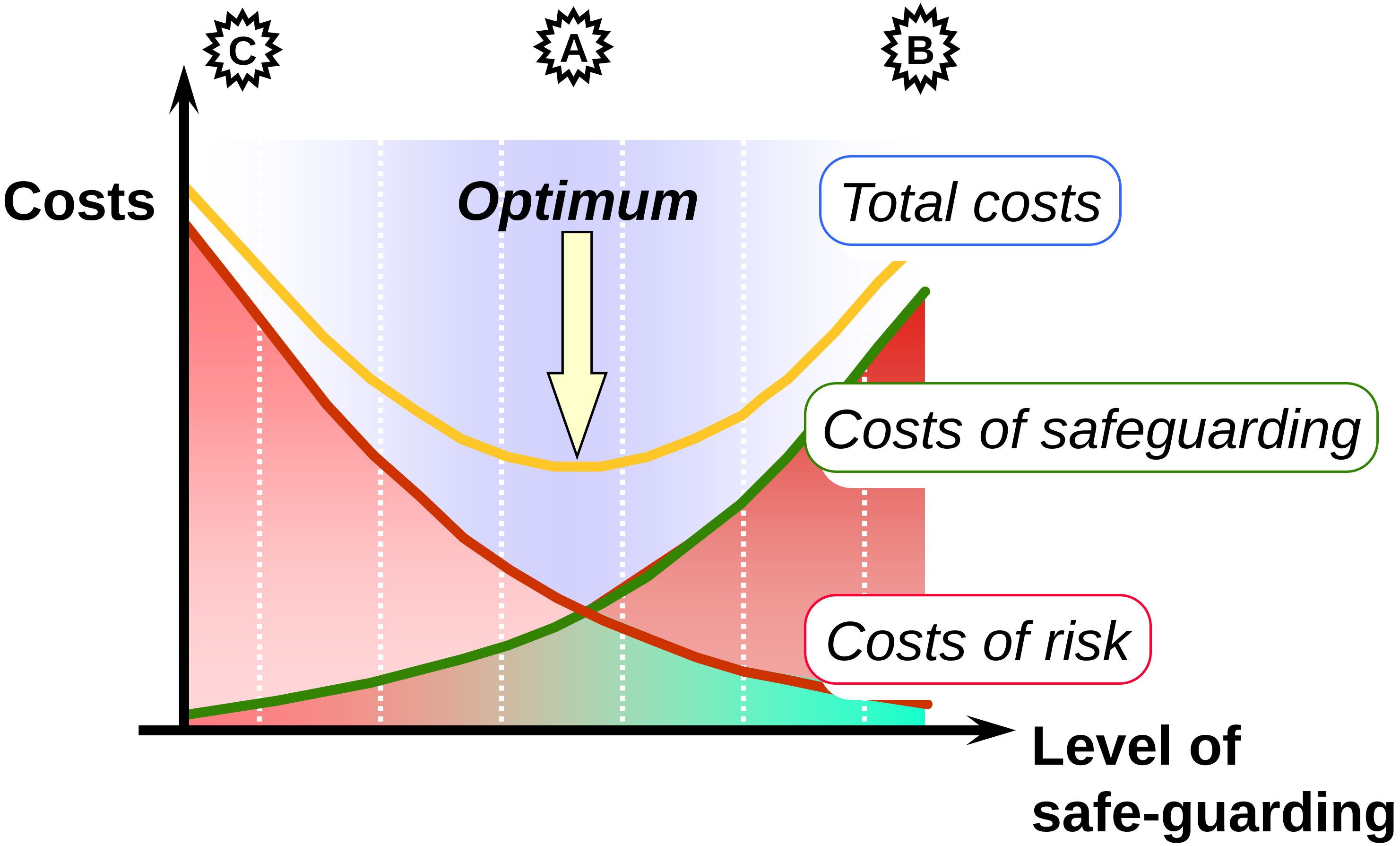

Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
SIS Required ?
No
Yes
Define Target SIL
Develop Safety Requirements Specification
Perform SIS Conceptual Design, and verify it meets the SRS
Perform SIS Design Detail
SIS Installation Commissioning and Pre-Startup Acceptance Test
Establish Operation & Maintenance Procedures
Pre-startup Safety Review (Assessment)
SIS Startup Operation, Maintenance Periodic Functional testing
Modify or Decommission SIS ?
Decommission
SIS Decommissioning
Analysis phase
Realization phase
Operation phase

Honeywell
THE POWER OF CONNECTED

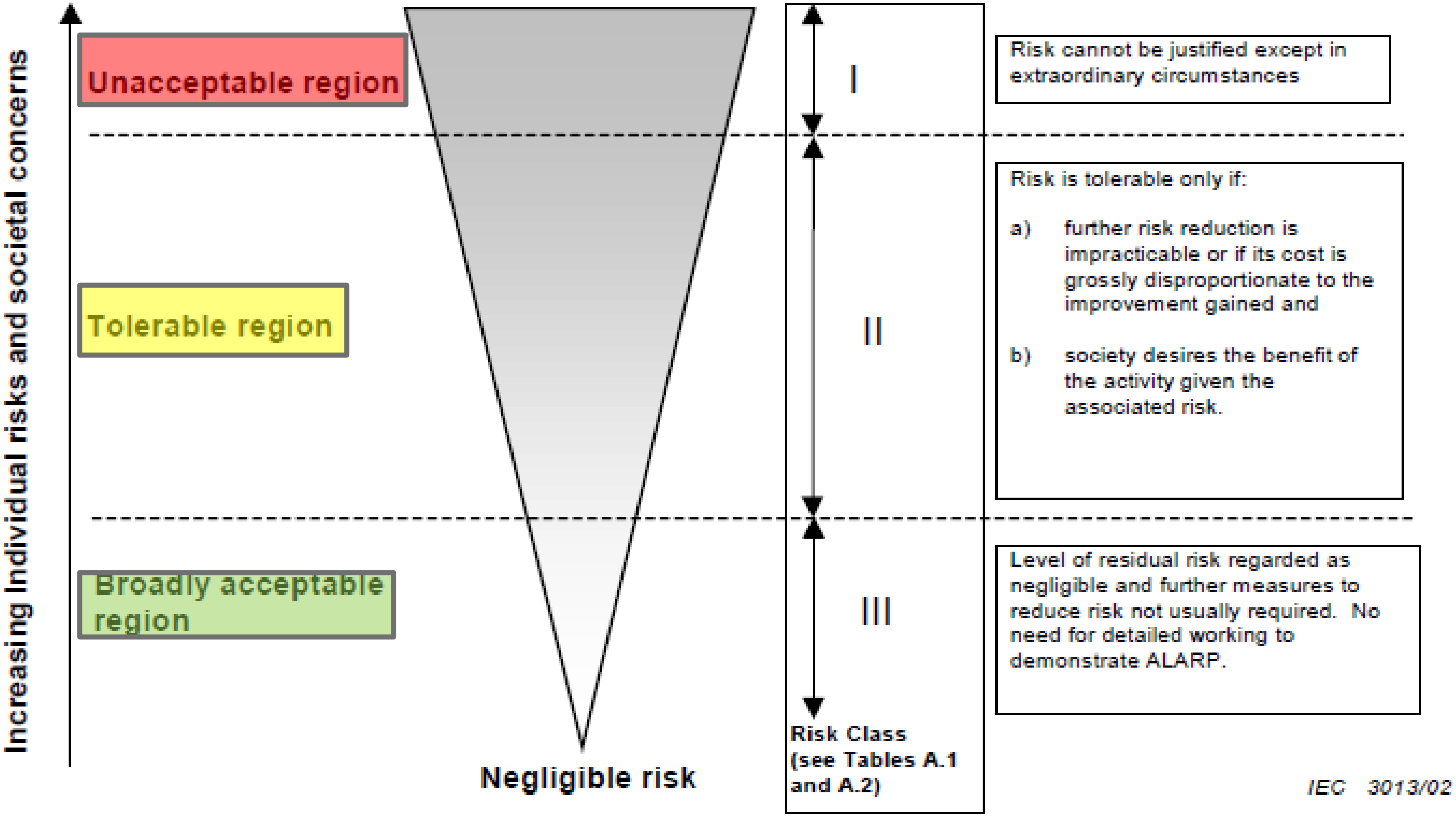
Sequence of events for a Process Accident to occur

- **Hazard**
  - Materials + Conditions (Process)
- **Initiating Event**
  - Technological failure
  - Human error
  - External event
- **Intermediate events**
  - Propagation factors
  - Containment failure
- **Result**
  - Hazardous event
  - Loss of Containment (LOC)
  - Consequences

Costs of risk <-> Costs of Safeguarding



Risk levels based on ALARP


Increasing Individual risks and societal concerns
Unacceptable region
Tolerable region
Broadly acceptable region
Negligible risk
I
II
III
Risk Class (see Tables A.1 and A.2)
IEC 3013/02

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.

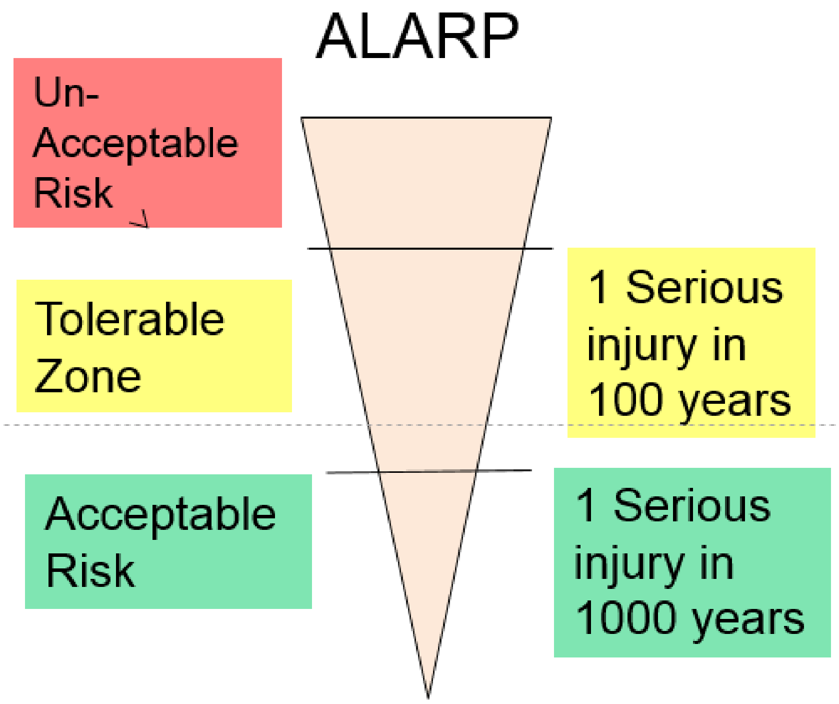
Level of residual risk regarded as negligible and further measures to reduce risk not usually required. No need for detailed working to demonstrate ALARP.

Figure A.1 – Tolerable risk and ALARP

Example of a company’s 3 x 3 Risk matrix

Frequency (per year)	1	10	100
1	H1	H2	HH
.01	M	H1	H2
.001	L	M	H1

Consequence (serious injury)



ALARP

Un-Acceptable Risk

Tolerable Zone

1 Serious injury in 100 years

Acceptable Risk

1 Serious injury in 1000 years

The Risk Matrix usually evaluate Consequence based on Serious injury, Financial loss and Environmental effects due to the Hazardous Event

SIL Determination techniques

- Safety Layer Matrix (IEC 61511, Appendix – C)
- Calibrated Risk Graph (IEC 61511, Appendix – D/E)
- Layer Of Protection Analysis (LOPA) (IEC 61511, Appendix – F)
- Fault Tree Analysis (FTA) (IEC 61511, Appendix – B)
- Event Tree Analysis (ETA) (IEC 61511, Appendix – B)

Let us review Risk graph and LOPA in detail

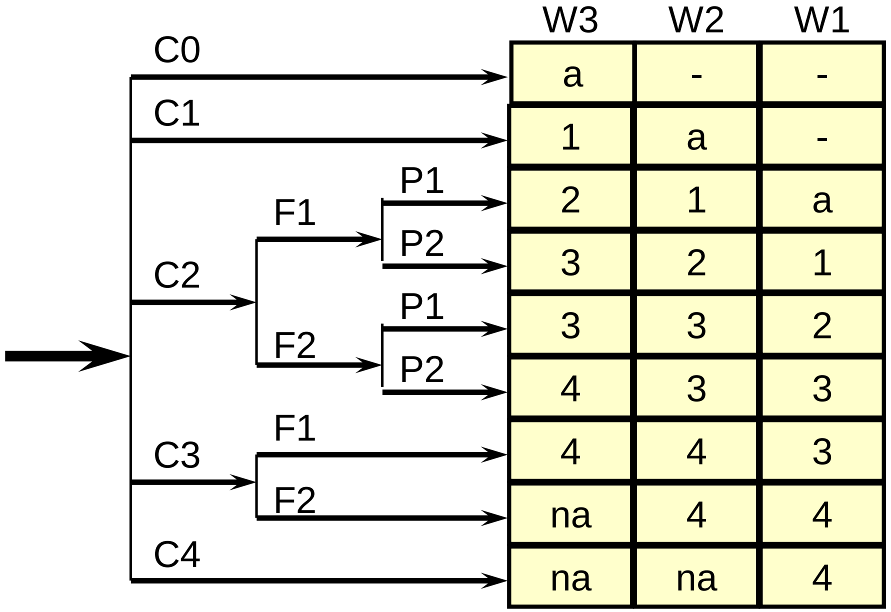
Risk graph

C0: Slight damage to equipment
C1: One injury
C2: One death
C3: Several deaths
C4: Catastrophic, many deaths

F1: Small probability of persons present in the dangerous zone
F2: High probability of persons present in the dangerous zone

P1: Good chance to avoid the hazard
P2: Hardly possible to avoid the hazard

W1: Probability of hazardous event very small
W2: Probability of hazardous event small
W3: Probability of hazardous event relative high



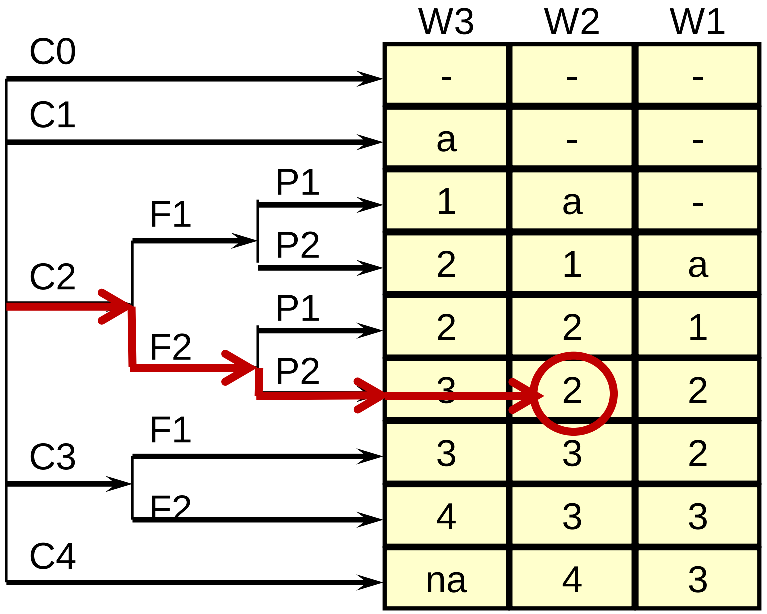
W3	W2	W1
a	-	-
1	a	-
2	1	a
3	2	1
3	3	2
4	3	3
4	4	3
na	4	4
na	na	4

This calibration shows a company with a more strict Safety Policy

Risk Classification – Example

Risk scenario ,

- Estimated consequence one casualty. (C2)
- Large prob. of persons present, (F2) assume 90%.
- No possibility to avoid the hazard, (P2) assume 0%.
- Frequency of occurrence, assumed once per 10 years. (W2)
  - Calculate: 1 * 0.90 * 1 * 0.1 = 0.09 or 9 casualties per 100 year.



W3	W2	W1
-	-	-
a	-	-
1	a	-
2	1	a
2	2	1
3	2	2
3	3	2
4	3	3
na	4	3

Required protection: SIL 2.

Risk Graph considerations

- When applying the risk graph method, it is important to consider risk requirements from the End user and any applicable regulatory authority.
- The interpretation and evaluation of each risk graph branch should be described and documented in a clear and understandable terms to ensure consistency in the method application.
- It is important that the risk graph is agreed to at a senior level within the organization taking responsibility for safety.

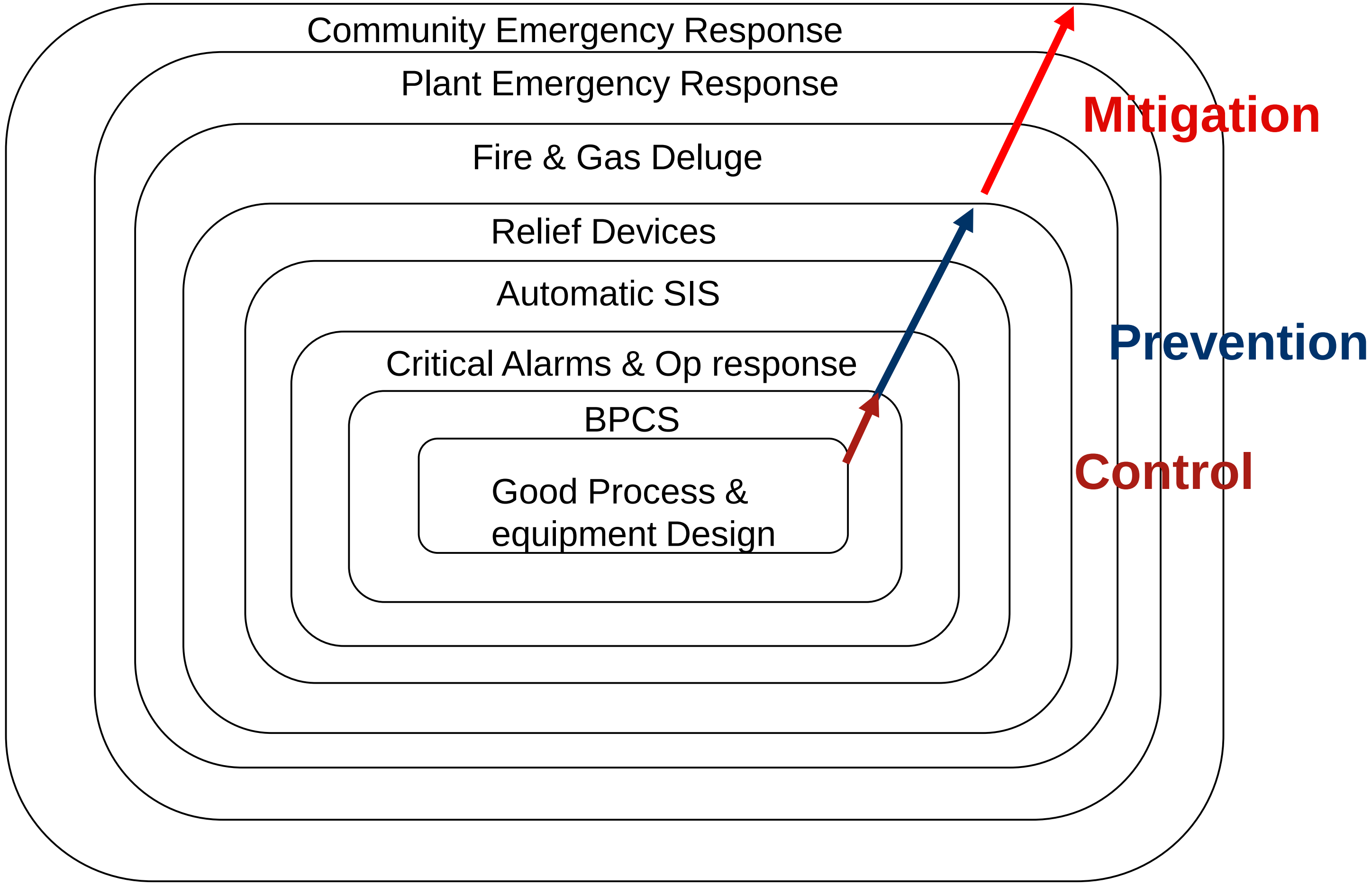
Honeywell
THE POWER OF CONNECTED

Layer Of Protection Analysis (LOPA)

- LOPA analyzes hazards to determine if SIFs are required and if so, the required Safety Integrity Level (SIL) of each SIF.
- Uses the Protection Layer model.
- For each identified hazardous event, the initiating causes and corresponding protective layers are evaluated
- LOPA does not include the protective contribution of the SIF.
  - The purpose is to determine how much RRF is needed to be provided by the SIF to fill the Risk gap left by considering other protection layers

Layers of Protection

Independent mechanism that reduces risk by control, prevention or mitigation



Independent Protection Layers (IPL)

Protection Layer is “any independent mechanism that reduces risk by control, prevention or mitigation”

Independent Protection Layers should have:

- Independency between protection layers
- Diversity between protection layers
- Physical separation between different protection layers
- Low common cause failures between protection layers

IPL credits

Protection layer	PFD
BPCS Control loop	1.0×10^{-1}
Human performance (trained, no stress)	1.0×10^{-1} to 1.0×10^{-2}
Human performance (under stress)	0.5 to 1.0
Operator response to alarms	1.0×10^{-1}
Pressure Relief Valves	$1.0 x 10^{-2}$

Probability Theory

What is the Probability of Tossing a coin and getting ‘Heads’ ?

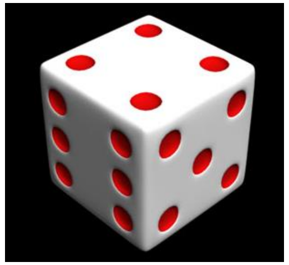
Various possible events (2) – Heads and Tails

Wanted event (1) – Heads

Answer – 1/2

Probability Theory

What is the Probability of rolling a dice and getting ‘4’.



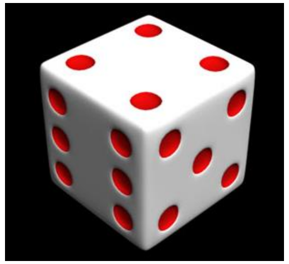
Various possible events (6) – 1, 2, 3, 4, 5, 6

Wanted event (1) – 4

Answer – 1/6

Probability Theory

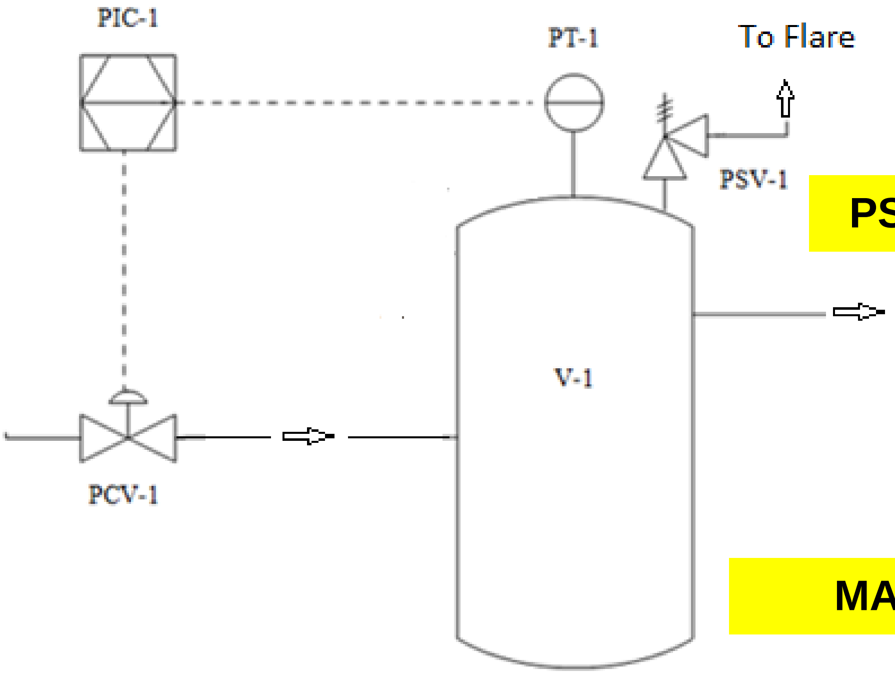
What is the Probability of Tossing a coin and getting ‘Heads’
AND
rolling a dice and getting ‘4’.



Various possible events (12) – H1, H2, H3, *H4*, H5, H6
T1, T2, T3, T4, T5, T6

Wanted event (1) – H4
Answer – 1/12
OR
1/2 x 1/6 = 1/12 (for INDEPENDENT events)

Case study - HazOp



SP= 3 BAR

PSV SP = 4.0 BAR

MAWP of V-1 = 5 BAR

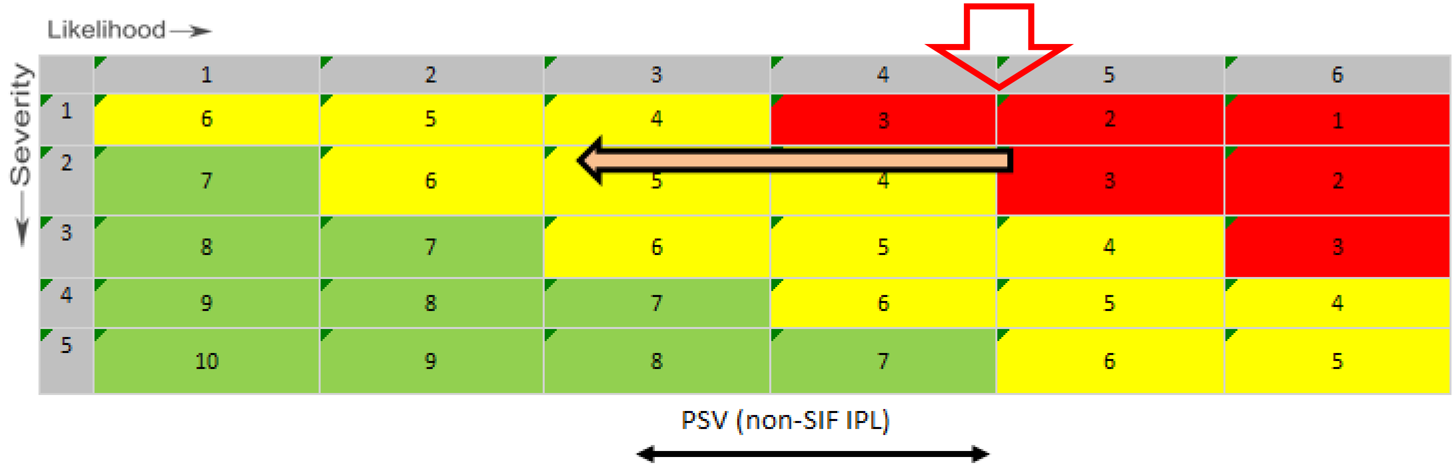
- Node: Vessel V-1
- Guideword: HIGH PRESSURE
- Consequence: High Pressure, possible vessel rupture & major fire
- Cause of failure: **PIC-1 (BPCS), Control valve (PCV-1) stuck open**
- Existing Safeguards : PSV-1
- Additional Protection Layers : **Introduce a new High pressure alarm @ 3.5 BAR in PIC-1**

Honeywell
THE POWER OF CONNECTED

Risk Reduction (with PSV only)

From the HAZOP risk matrix for this Process, with PSV as safeguard :

1. Frequency of Initiating Event (IE) – (L=3) (L=5 without any safeguards)
2. Severity – Single fatality (S=2)
3. Risk (with PSV as safeguard) = (Box 5) (Base Risk without PSV, Box 3)

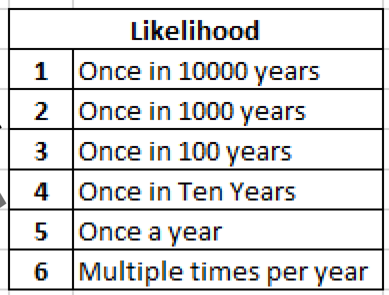


Likelihood →

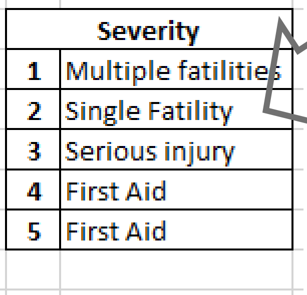
Severity

	1	2	3	4	5	6
1	6	5	4	3	2	1
2	7	6	5	4	3	2
3	8	7	6	5	4	3
4	9	8	7	6	5	4
5	10	9	8	7	6	5

PSV (non-SIF IPL)



	Likelihood
1	Once in 10000 years
2	Once in 1000 years
3	Once in 100 years
4	Once in Ten Years
5	Once a year
6	Multiple times per year

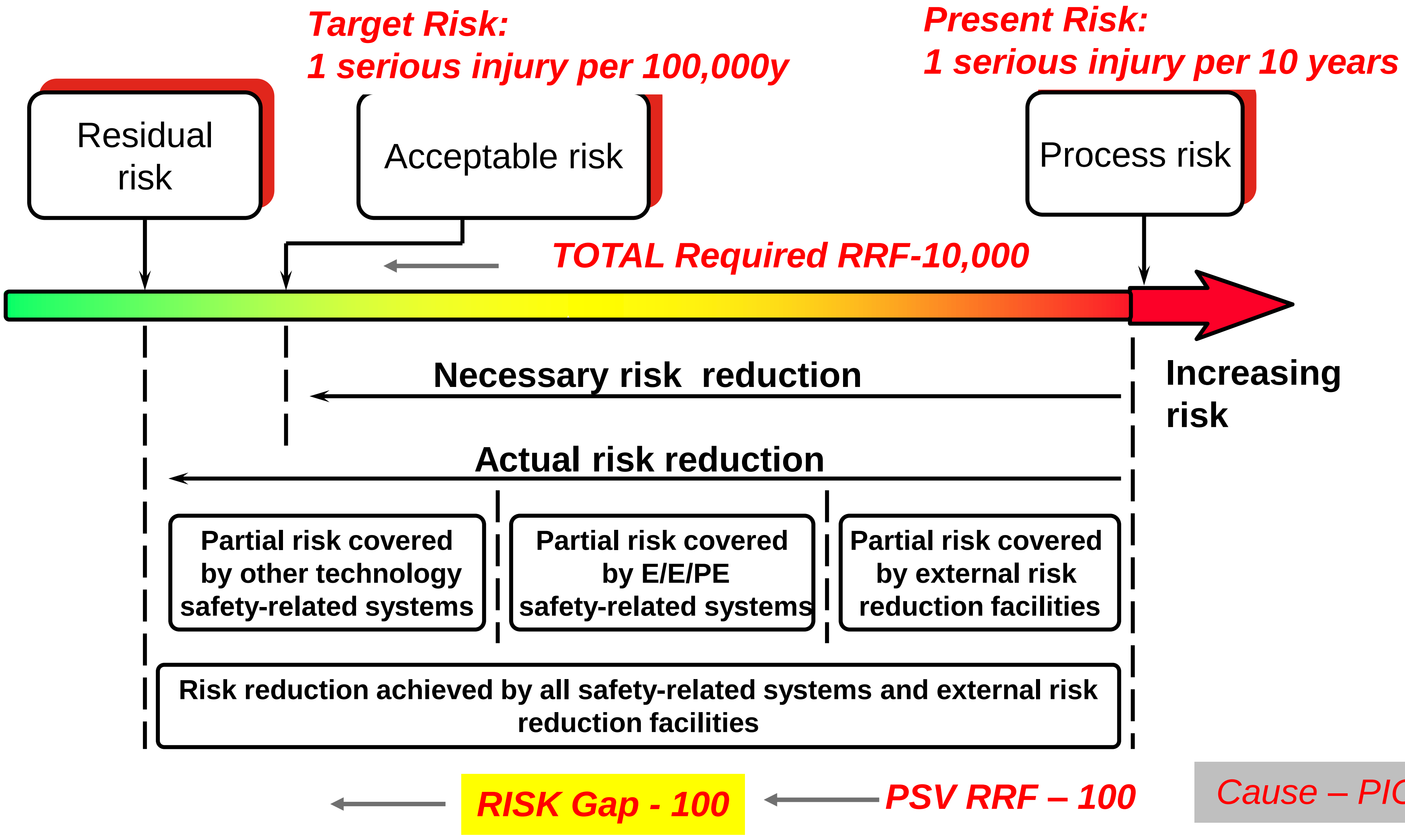


	Severity
1	Multiple fatilities
2	Single Fatility
3	Serious injury
4	First Aid
5	First Aid

LOPA TMEL (Single Fatality) :

1E-05 per year

Case study - Risk and Risk Reduction



Target Risk:
1 serious injury per 100,000y

Present Risk:
1 serious injury per 10 years

Residual risk

Acceptable risk

Process risk

TOTAL Required RRF-10,000

Increasing risk

Necessary risk reduction

Actual risk reduction

Partial risk covered by other technology safety-related systems

Partial risk covered by E/E/PE safety-related systems

Partial risk covered by external risk reduction facilities

Risk reduction achieved by all safety-related systems and external risk reduction facilities

RISK Gap - 100

PSV RRF – 100

Cause – PIC-1 fails

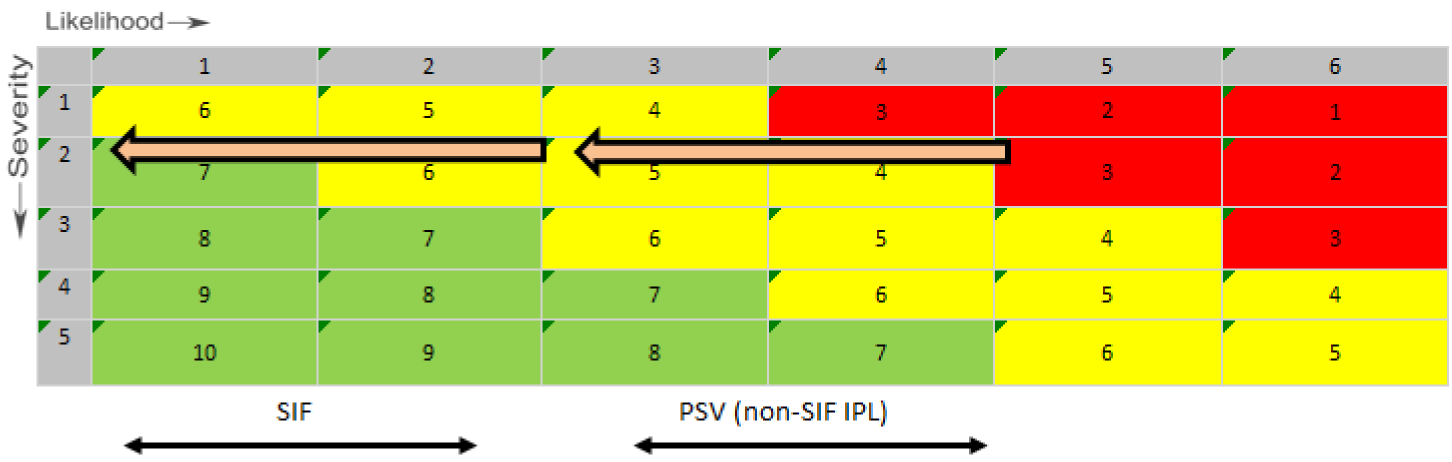
Honeywell
THE POWER OF CONNECTED

PFD	R in %	RRF	SIL	AK
			4	8 7
0.0001	99.99	10,000		
			3	6 5
0.001	99.9	1,000		
			2	4
0.01	99	100		
			1	3 2
0.1	90	10		
			-	1 -
Average Probability to Fail on Demand	Reliability of Safety Functions	Risk Reduction Factor	ISA S84.01 IEC 61508	DIN-V 19250

Risk Reduction (with PSV and SIF)

From the HAZOP risk matrix for this Process, with the Two safeguards :

1. Frequency of Initiating Event (IE) – (L=1)
2. Severity – (S=2)
3. Risk (with Two safeguards) = (Box 7) (Acceptable Risk level)



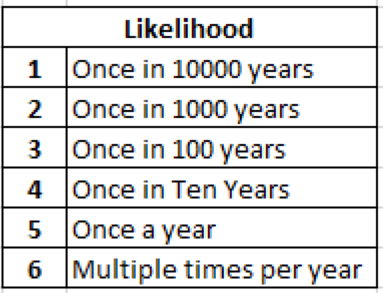
Likelihood →

Severity ↓

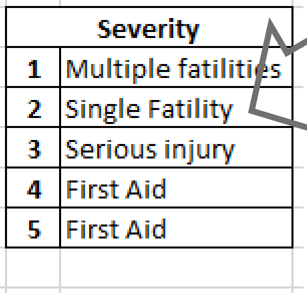
	1	2	3	4	5	6
1	🟨 6	🟨 5	🟨 4	🟥 3	🟥 2	🟥 1
2	🟩 7	🟨 6	🟨 5	🟨 4	🟥 3	🟥 2
3	🟩 8	🟩 7	🟨 6	🟨 5	🟨 4	🟥 3
4	🟩 9	🟩 8	🟩 7	🟨 6	🟨 5	🟨 4
5	🟩 10	🟩 9	🟩 8	🟩 7	🟨 6	🟨 5

SIF

PSV (non-SIF IPL)



Likelihood	
1	Once in 10000 years
2	Once in 1000 years
3	Once in 100 years
4	Once in Ten Years
5	Once a year
6	Multiple times per year

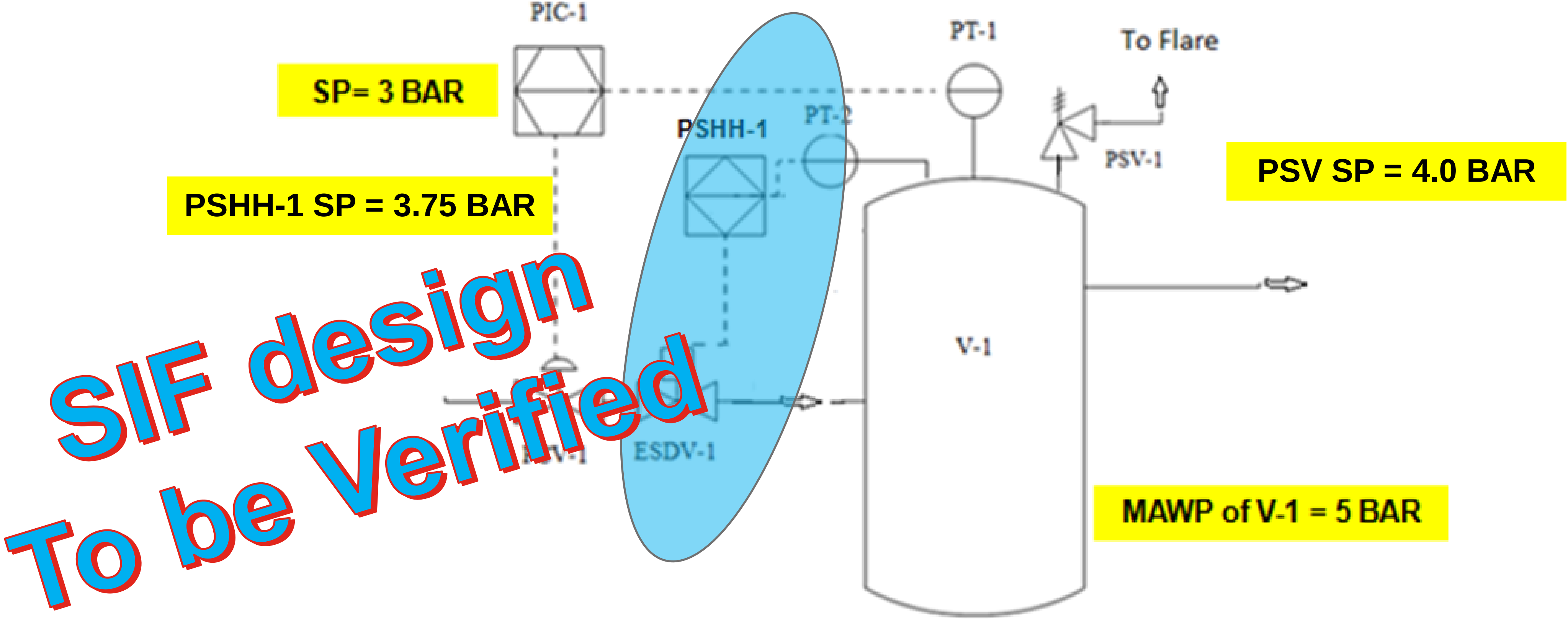


Severity	
1	Multiple fatilities
2	Single Fatility
3	Serious injury
4	First Aid
5	First Aid

LOPA TMEL (Single Fatality) :

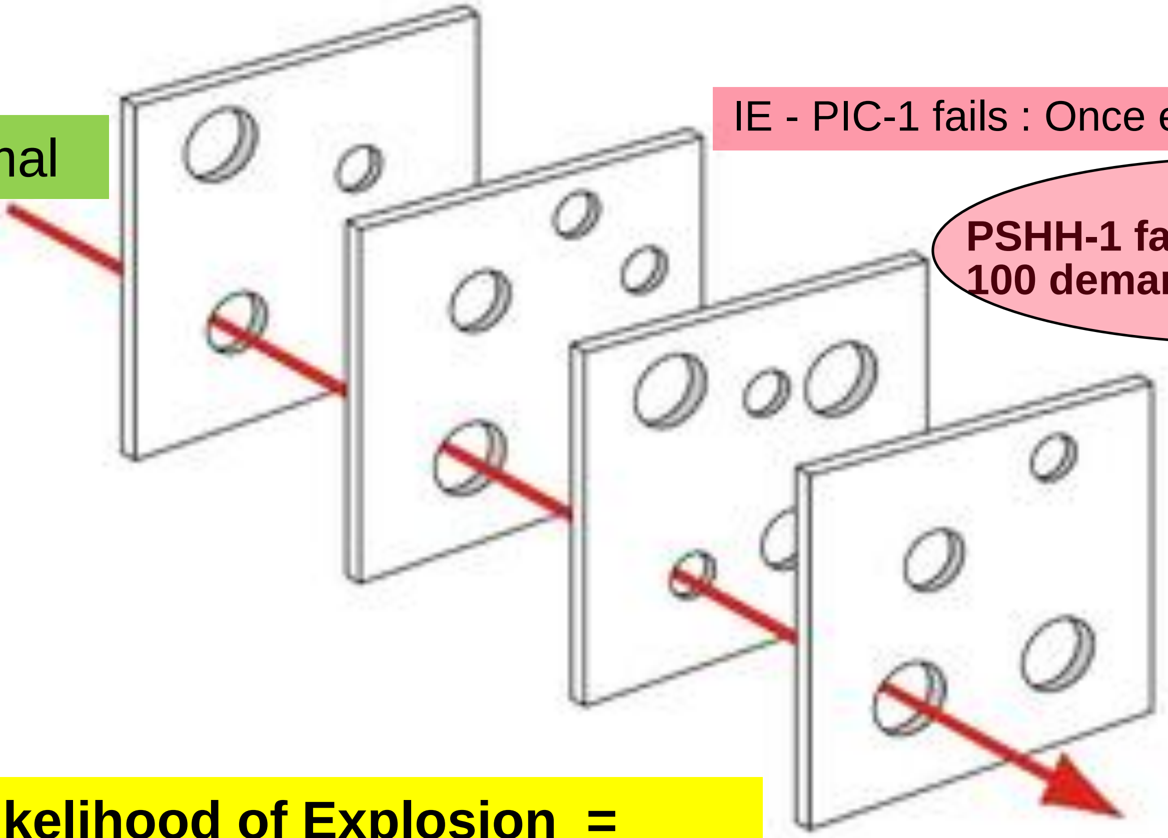
1E-05 per year

Case Study - Add a SIF (SIL2, RRF-100)



- High Pressure Trip PSHH-1 added
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

Case study - With additional SIS protection layer



System normal

IE - PIC-1 fails : Once every 10 years (0.1)

PSHH-1 fails : Once every 100 demands (0.01)

PSV fails : Once every 100 demands (0.01)

Vessel V-1 ruptures and finds a source of ignition (100%)

Probable Likelihood of Explosion =
PL(Loss Of Containment) x P(Ignition) =
0.1 x 0.01 x 0.01 x 1 = 1E-05 per year (= 1E-05)

Case study - Safety Requirement Specification (SRS)

- For the SIF , the Integrity (SIL) and Functional requirements need to be specified :

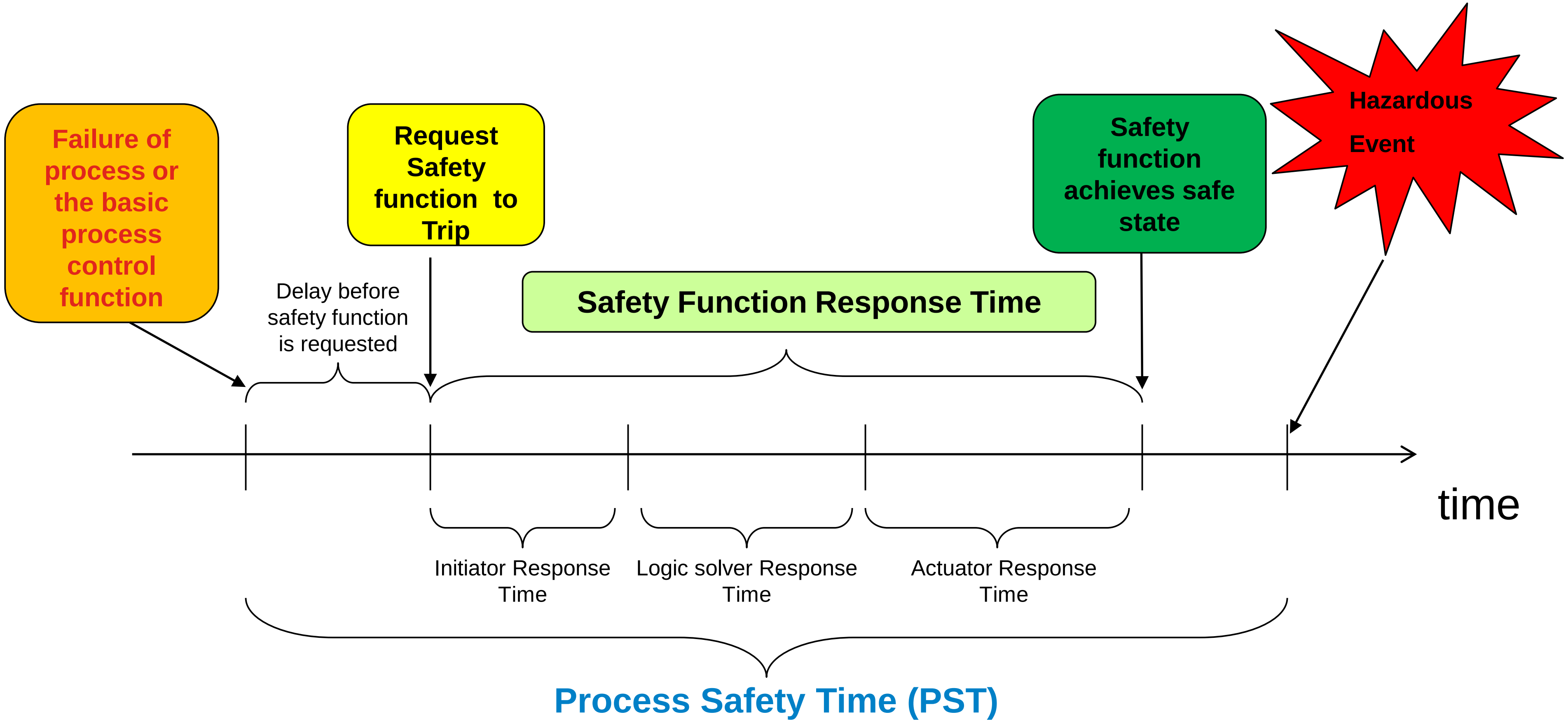
  - Integrity requirement for SIF PSHH-1 : to be SIL2 reliable with RRF 100

  - Functional requirement for SIF PAHH-1 :
    - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
    - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Reset (Open) when Pressure is less than 3.75 BAR
    - When PT-2 fails (BadPV), start MTTR timer . If MTTR expires, Shut off ESDV-1
    - How to Reset after trip ?
    - How to Bypass input ?
    - ….etc……

Honeywell
THE POWER OF CONNECTED

Process Safety Time (PST)

PST: Time period between a failure occurring in the process (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.


Failure of process or the basic process control function
Request Safety function to Trip
Safety function achieves safe state
Hazardous Event
Delay before safety function is requested
Safety Function Response Time
time
Initiator Response Time
Logic solver Response Time
Actuator Response Time
Process Safety Time (PST)

Question 1:

What is ALARP

a). As less as reasonably predicted

b). As low as recent problem

[✓ c). As low as reasonably practicable]

d). None of the above

Question 2:

What is an Initiating Event in Risk Assessment

a). The event which ends the hazardous event

b). It is the initial event before the Safety system stops working

c). It is the initial event before the Control system stops working

d). The event which starts the process that can escalate to a hazardous event

Question 3:

A SIF with a RRF of 50 is a

[✓ a) SIL1 loop]

b) SIL2 loop

c) SIL3 loop

d) ‘No SIL’ loop

Question 4:

What is LOPA

a) Layers of Prevention Act

b) Layers of Possible Actions

c) [✓ Layers of Protection Analysis]

d) Layers of Possible Analysis

Question 5:

What is Process Safety Time

[✓ a) The time between the Initiating Event and the Hazardous event]

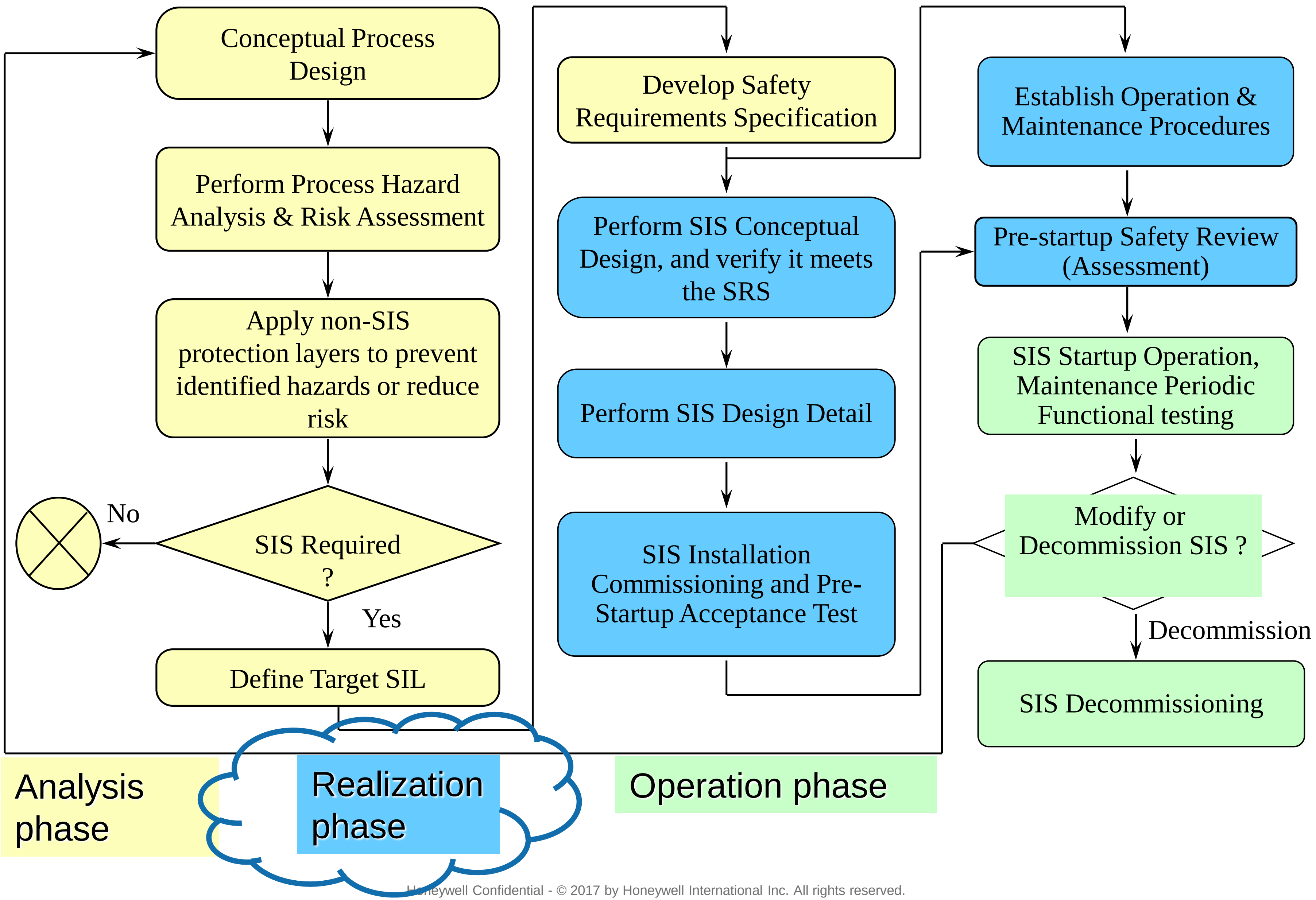
b) The time between the Initiating Event and the BPCS response

c) The time between the Initiating Event and the SIF response

d) The time between the Initiating Event and the Operator response

Realization (Detailed Engineering) Phase

The Safety Life Cycle as defined in the standards


Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
SIS Required ?
No
Yes
Define Target SIL
Develop Safety Requirements Specification
Perform SIS Conceptual Design, and verify it meets the SRS
Perform SIS Design Detail
SIS Installation Commissioning and Pre-Startup Acceptance Test
Establish Operation & Maintenance Procedures
Pre-startup Safety Review (Assessment)
SIS Startup Operation, Maintenance Periodic Functional testing
Modify or Decommission SIS ?
Decommission
SIS Decommissioning
Analysis phase
Realization phase
Operation phase

Honeywell
THE POWER OF CONNECTED

Realization phase of the Safety Life cycle

- With the SRS generated, the SIFs need to be engineered to meet the identified functional and integrity requirements.
- As part of the realization phase:
  - The SIF components are specified and designed as per integrity requirements (and some functional requirements)
  - The Logic solver program is written and tested as per the functional requirements in the SRS (assuming it is a Programmable Electronic Logic Solver)
- The realization phase ends with Validation of the SIS, ie making sure before system commissioning that the SIS has been designed and tested per the requirements in the SRS

Introduction to failure rates, failure modes, PFDavg, Safe Failure Fraction

Basic concepts

- Before we get into the design , let us first try to understand basic concepts like :
    - Type of failures
    - Failure modes
    - Diagnostic coverage
    - Safe Failure Fraction (SFF)
    - And more

Types of failures: Random Failures

- A failure occurring at a random time, which results from one or more of the possible degradation mechanisms.
  - thermal stressing
  - wear-out
  - ……
- Expressed as Failure Rate (λ)
- Many sources of failure rate data
- PFD calculation are based on Random Physical Hardware Failures only

Honeywell
THE POWER OF CONNECTED

Failure rate and FIT

- Failure Rate (λ) - Number of failures per unit time
  - Failures/hour
  - Failures per million hours (OREDA)
  - Failures per billion hours (FIT’s, MIL HDBK 217)
    - FIT : Failures in Time
    - 5 FIT: 5 Failures per 10^9 hours

      (or 5 failures in approx. 10^5 years)
- Failure rate = 1/MTTF (Mean Time To Fail)

Types of failures: Systematic failures

- A failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

- Faults are produced by human error during system development and operation
  - Software bugs
  - Wrong specification
  - Bad hardware design

- Presently there is no mathematical model to express Systematic failures

Honeywell
THE POWER OF CONNECTED

Failure Modes

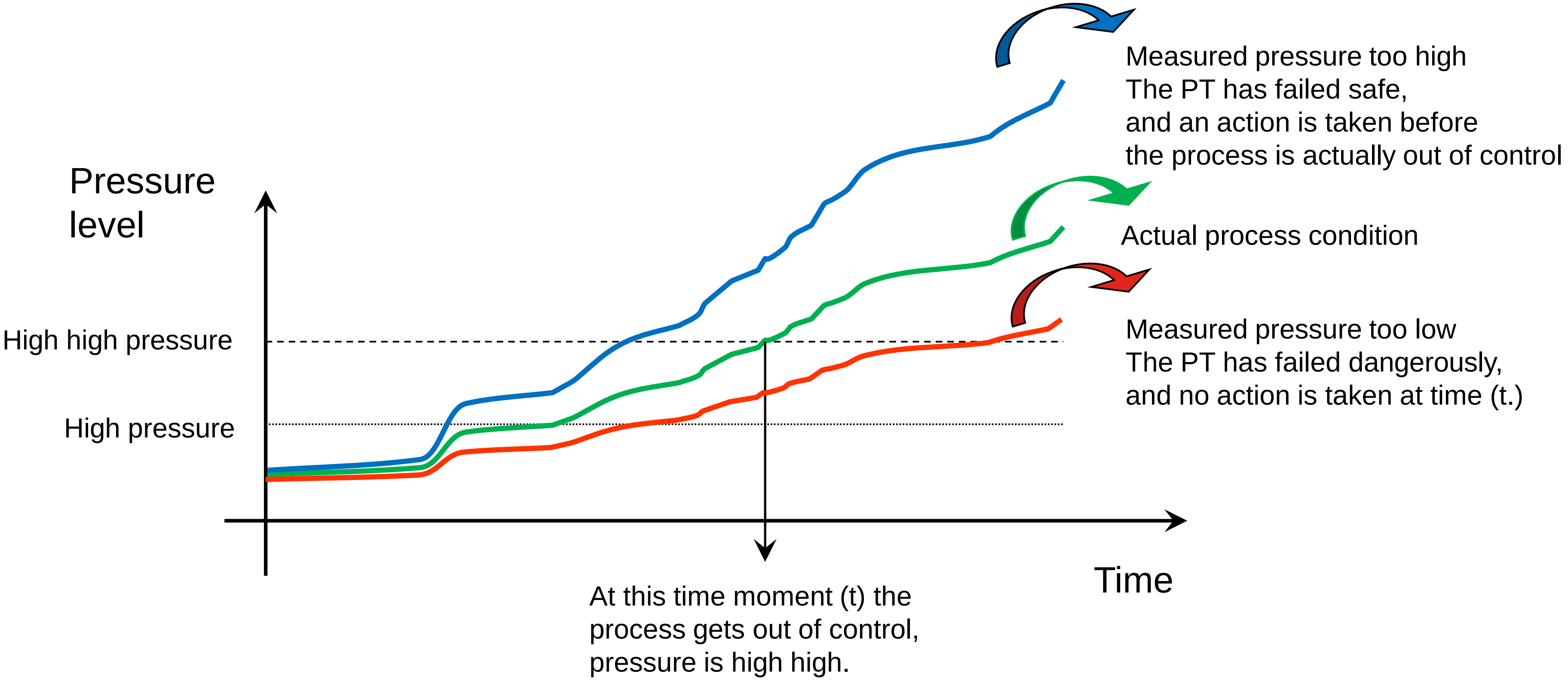
- Safe failure (λ_S)
  - failure which does not have the potential to put the safety related system in a hazardous or fail to-function state
  - Used in PFS (Probability of Failure Spurious) calculations

- Dangerous failure (λ_D)
  - failure which has the potential to put the safety-related system in a hazardous or fail-to-function state
  - Used in PFD calculations

- λ (Total Failure rate) = $\lambda_S + \lambda_D$

Safe vs. Dangerous failure of a Sensing Element

- Pressure Transmitter in a High Pressure interlock



Measured pressure too high
The PT has failed safe,
and an action is taken before
the process is actually out of control

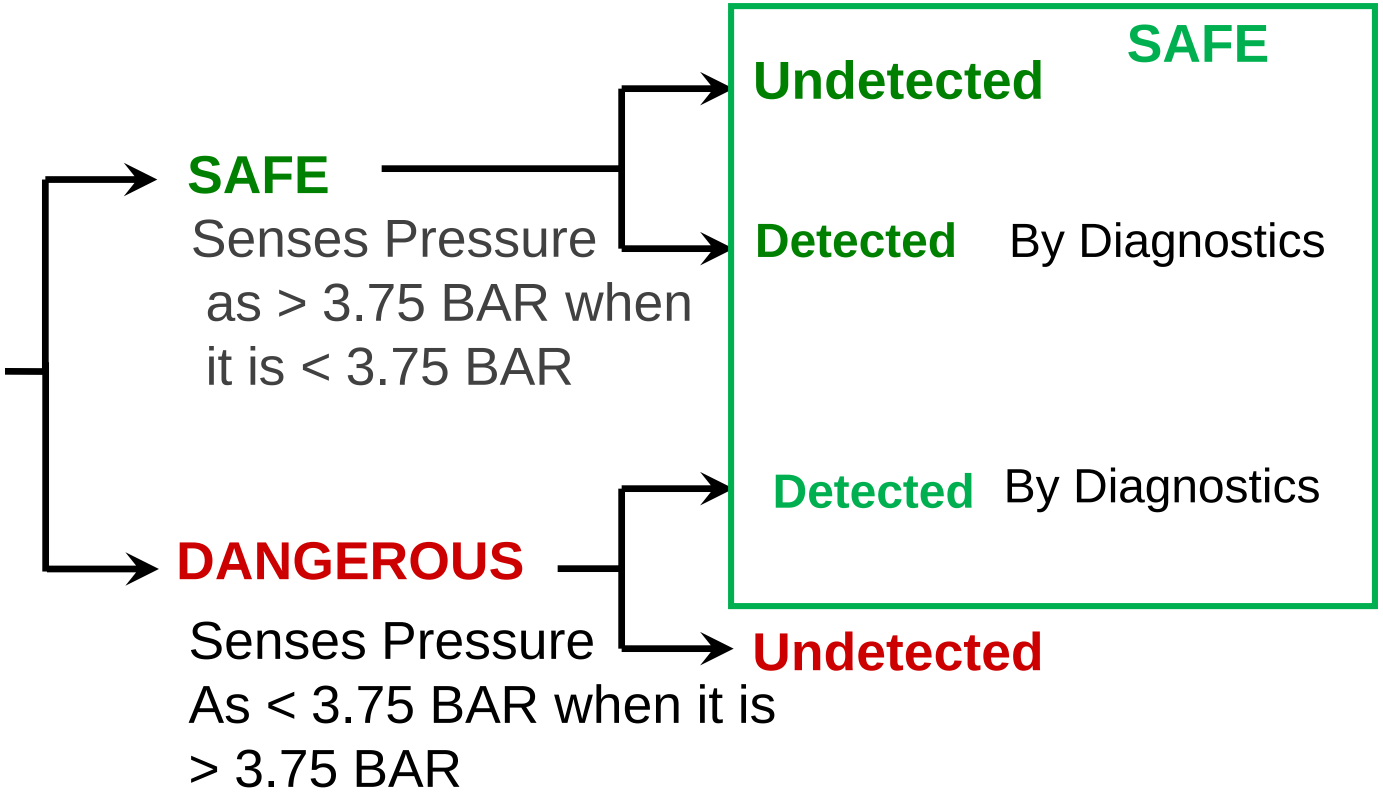
Actual process condition

Measured pressure too low
The PT has failed dangerously,
and no action is taken at time (t.)

At this time moment (t) the
process gets out of control,
pressure is high high.

Types of Failures

- Pressure Transmitter
- On High Pressure (> 3.75 BAR), the PT should sense and send a signal to the Logic Solver



SAFE

Senses Pressure as > 3.75 BAR when it is < 3.75 BAR

DANGEROUS

Senses Pressure As < 3.75 BAR when it is > 3.75 BAR

SAFE

Undetected

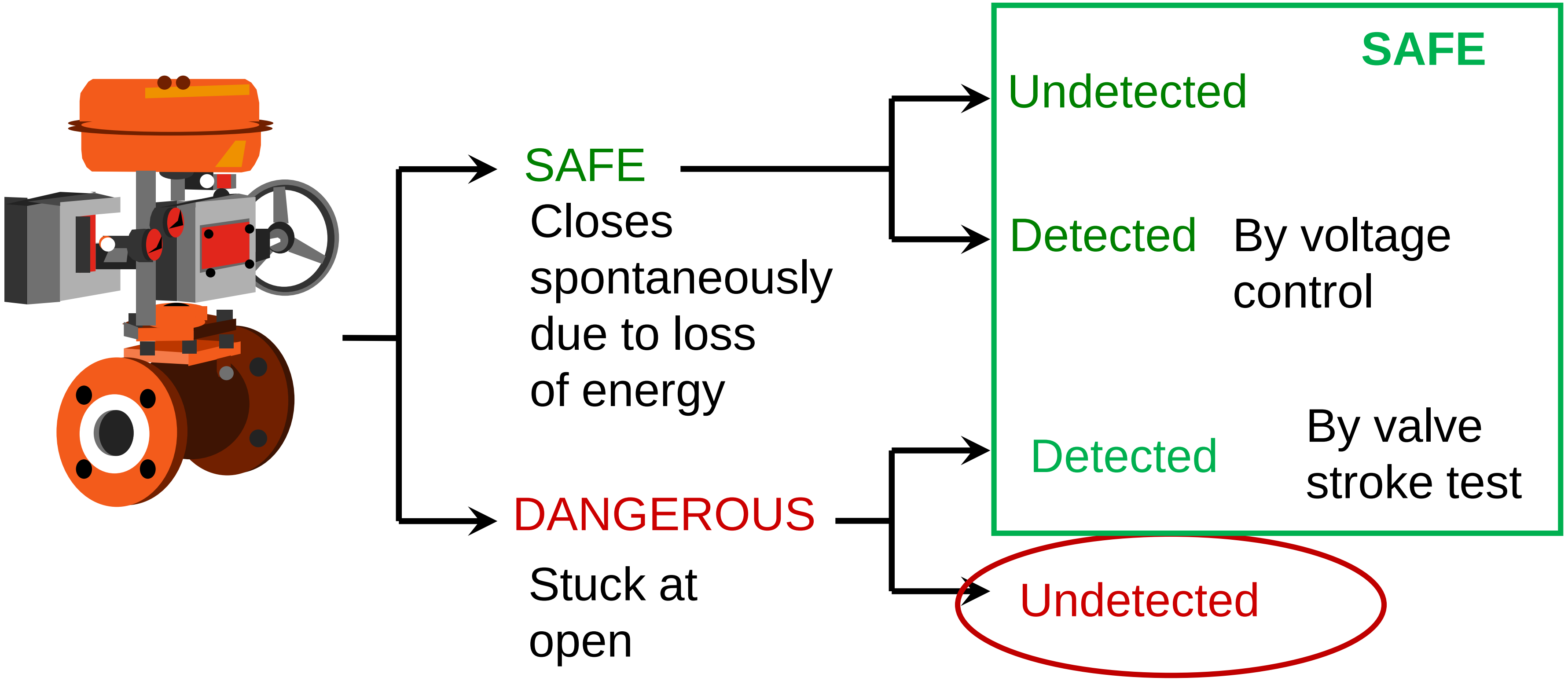
Detected By Diagnostics

Detected By Diagnostics

Undetected

Failure modes and types for a final element

- Safety valve, normally open & normally energized
  In case of an out of control process, the valve has to close



SAFE

Closes spontaneously due to loss of energy

DANGEROUS

Stuck at open

SAFE

Undetected

Detected By voltage control

Detected By valve stroke test

Undetected

Diagnostic Coverage

- Diagnostic Coverage (DC):
  - Fraction of dangerous failures detected by automatic on-line diagnostic tests.
  - The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures

- Diagnostic Test Interval
  - Interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage

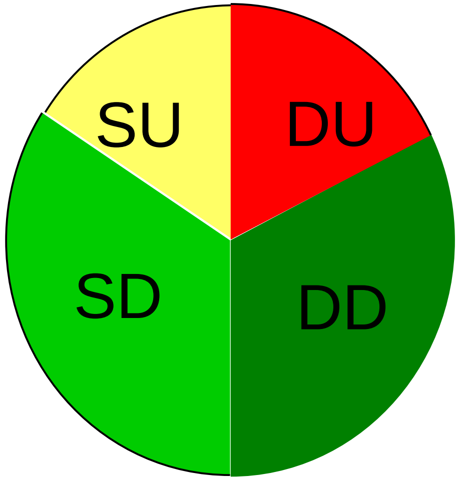
Note – 61508 only refers to dangerous failures while 61511 refers DC to both dangerous and safe failures

Honeywell
THE POWER OF CONNECTED

Detected & Undetected Failures

- **Safe failure (λ_S)**
  - Safe detected (λ_{SD})
  - Safe Undetected (λ_{SU})

- **Dangerous failure (λ_D)**
  - Dangerous detected (λ_{DD})
  - Dangerous Undetected (λ_{DU})



- **Diagnostics is a tool to detect failures**

Diagnostic Coverage and Failure rates

Formulae :

1. $\lambda_T = \lambda_s + \lambda_D$

Total failure rate = Sum of Safe and dangerous failure rates

2. $\lambda_S = \lambda_{SU} + \lambda_{SD}$

Safe failure rate = Sum of Safe undetected and detected failure rates

3(a) $\lambda_{SD} = DC_S * \lambda_S$

3(b) $\lambda_{SU} = (1- DC_S)*\lambda_S$

DC_S = Diagnostic Coverage for Safe Failures

4. $\lambda_D = \lambda_{DU} + \lambda_{DD}$

Dangerous failure rate = Sum of Dangerous undetected and detected failure rates

5(a) $\lambda_{DD} = DC_D * \lambda_D$

5(b) $\lambda_{DU} = (1- DC_D)*\lambda_D$

DC_D = Diagnostic Coverage for Dangerous Failures

Example

The total failure rate of a Transmitter is 5 x 1E-06 failures / hour. Assuming the Safe and Dangerous failures are the same, what is the Dangerous Undetected failure rate if the Diagnostic Coverage (dangerous) is 80%

$\lambda_T =$ 5 x 1E-06 failures / hour

$\lambda_s = \lambda_D = 2.5 \times 1E\text{-}06$

$\lambda_{DU} = (1\text{- } DC_D)*\lambda_D = (1\text{-}0.8) \times 2.5 \times 1E\text{-}06 = 5 \times 1E\text{-}05$ failures / hour

Redundancy Concepts: Hardware Fault Tolerance

- Redundancy: The existence of more than one means for performing a required function or for representing information.
  - EXAMPLE: Duplicated functional components and the addition of parity bits are both instances of redundancy.

- Diversity: Different means of performing a required function
  - EXAMPLE: Diversity may be achieved by different physical methods or different design approaches. (Pressure transmitter & Pressure switch)

- Hardware Fault Tolerance (HFT): A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.
  - EXAMPLE : HFT of 2oo3 voting is 1

Honeywell
THE POWER OF CONNECTED

Hardware Fault Tolerance

- Voting, XooY System
- A SIS sub-system made up of a number of channels (Y), where (X) of which is/are sufficient to perform the correct safety function
- HFT = (Y – X)

Architecture	Channels	HFT
1oo1	1	0
2oo2	2	0
1oo2	1	1
2oo3	3	1
1oo3	3	2
2oo4	4	2

Different types of HFT arrangements

For Safety Instrumented subsystem with identical channels:

- High

  To

- Low

Safer arrangement

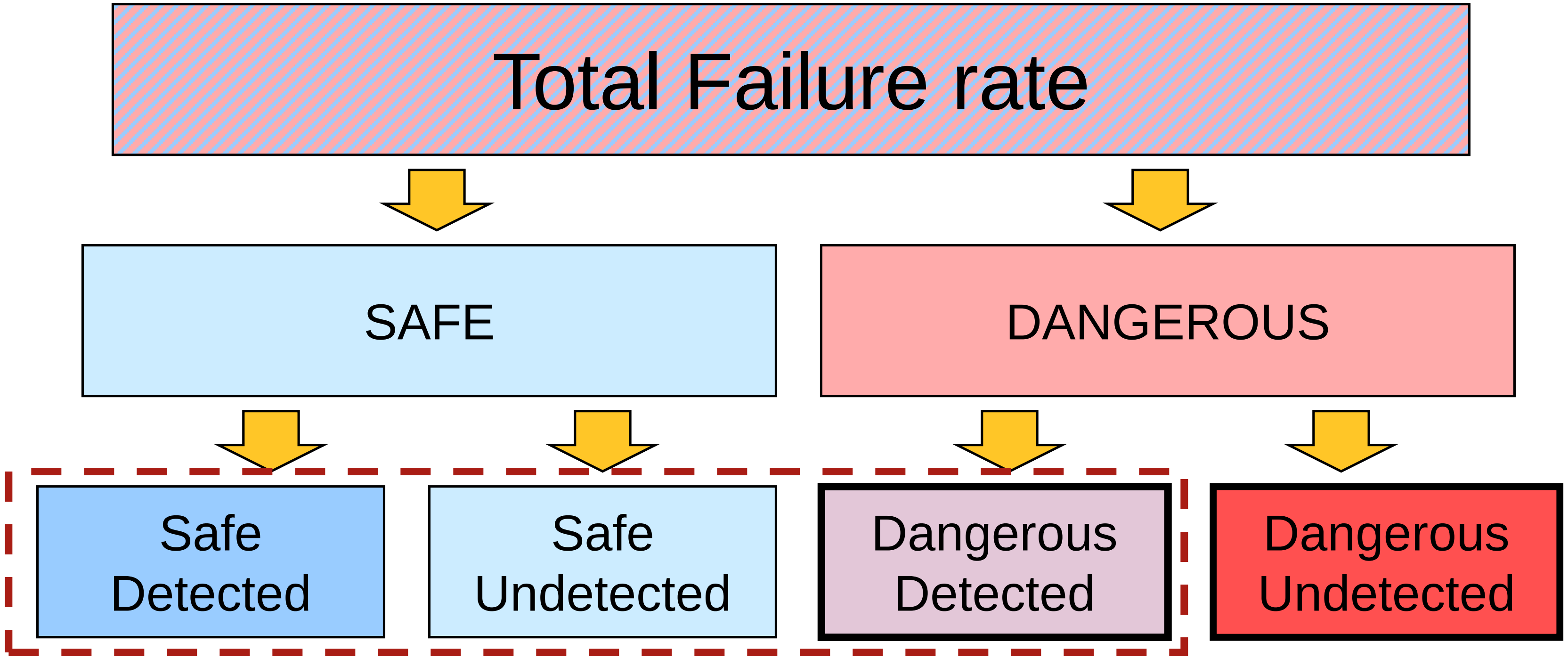
- 1oo2
- 2oo3
- 1oo1
- 2oo2

Process Availability

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

Note - High Process Availability, means Low Spurious trips
Low Process Availability, means High Spurious trips

Safe Failure Fraction (SFF)



$$\text{Safe Failure Fraction} = \frac{\Sigma\,\text{Safe failure rate} + \Sigma\,\text{DD failure rate}}{\Sigma\,\text{Total failure rate}}$$

Honeywell
THE POWER OF CONNECTED

Requirements to meet SIL during the Realization phase

IEC 61508/61511 Design Requirements to meet SIL

All SIF components should meet :

- Architectural Constraints
  - Diagnostic coverage of component failure
  - Safe Failure Fraction of component failure
  - Fault tolerance of subsystems
  - Type of components
- Reliability of components → PFD
- Systematic Capability influences
  - Requirements specification
  - Hardware
  - Software
  - Environmental

Reliability equations

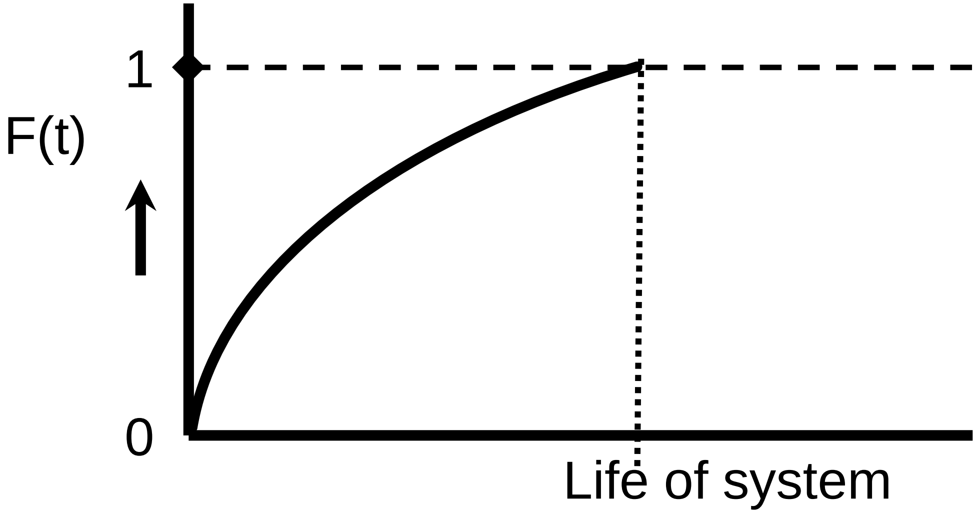
From Reliability engineering, for non-repairable systems, Reliability over a period of time is given as:

$$R(t) = e^{-\lambda t}$$

Where ‘λ’ = failure rate of the device and ‘t’ = time in use

Then, Probability of Failure over a period of time is defined as :

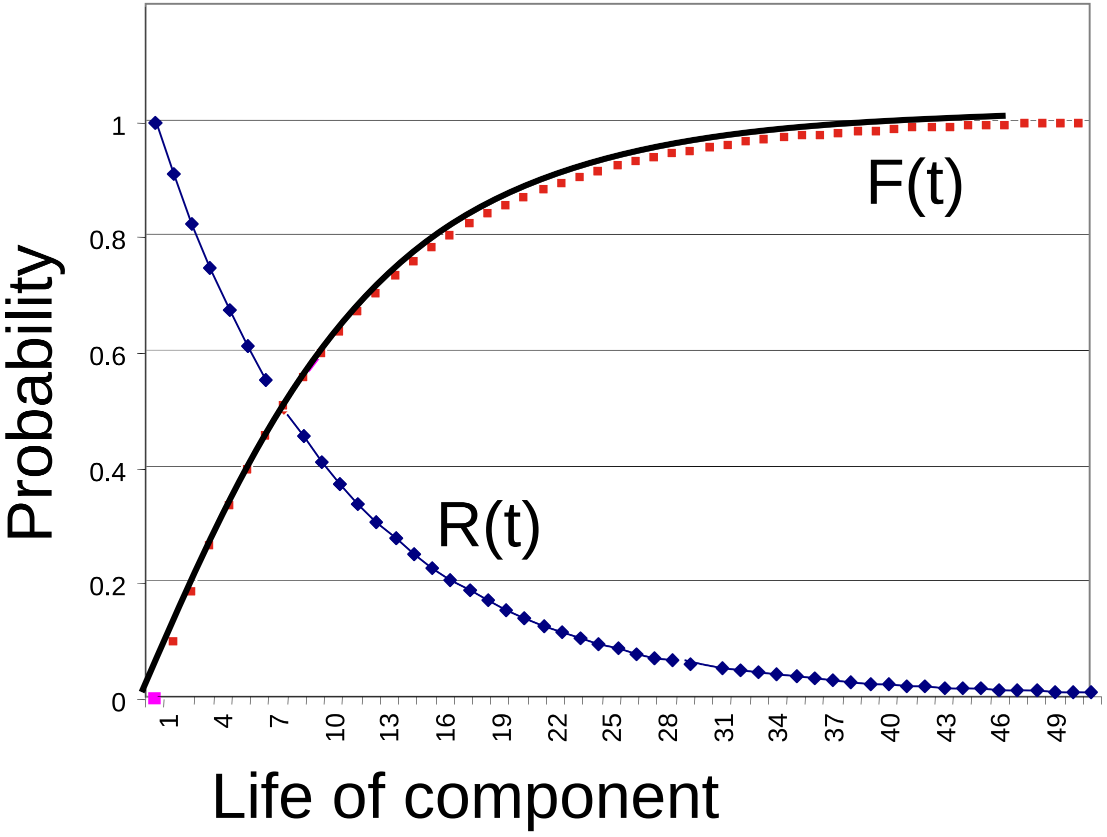
$$F(t) = 1-e^{-\lambda t}$$



Component Reliability

$$R(t) = e^{-\lambda t}$$

$$F(t) = 1 - e^{-\lambda t}$$



Finally component will fail !

Reliability equations

Taylor series states that :

$e^x = x^0/0! + x^1/1! + x^2/2! + \ldots\ldots\ldots\ldots\ldots$

When ‘x’ is very small, we can eliminate $x^2/2!$ onwards and are left with

$e^x = x^0/0! + x^1/1!$

$e^x = 1 + x$

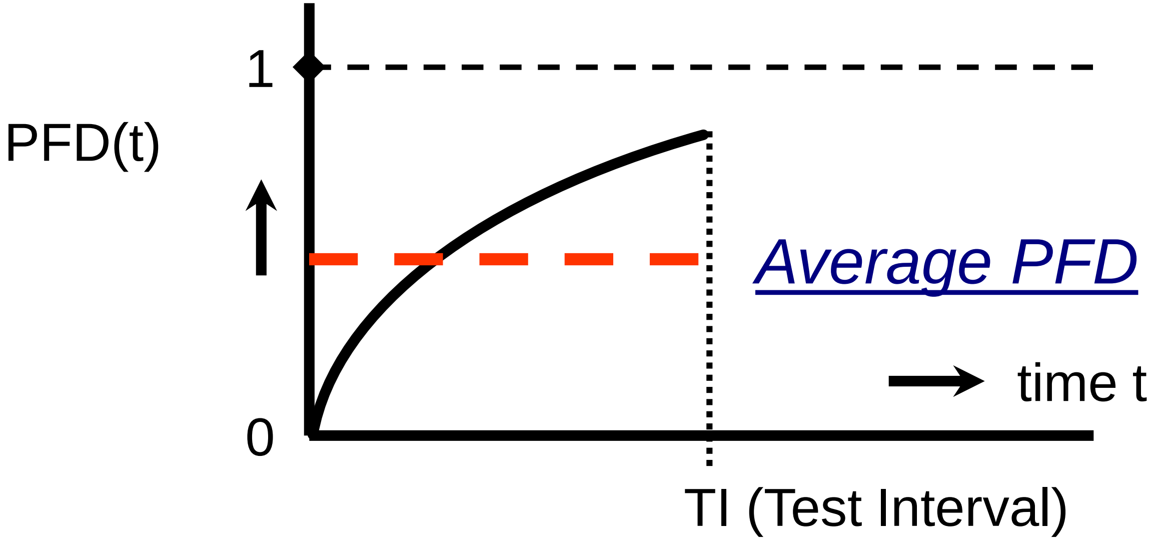
Substitute $x = -\lambda t$, we get :

$e^{-\lambda t} = 1 - \lambda t$

So $F(t) = 1-e^{-\lambda t} = 1-(1 - \lambda t) = \lambda t$

$F(t) = PFD(t) = \lambda t$ (when ‘λt’ is very small)

Average PFD for time period TI

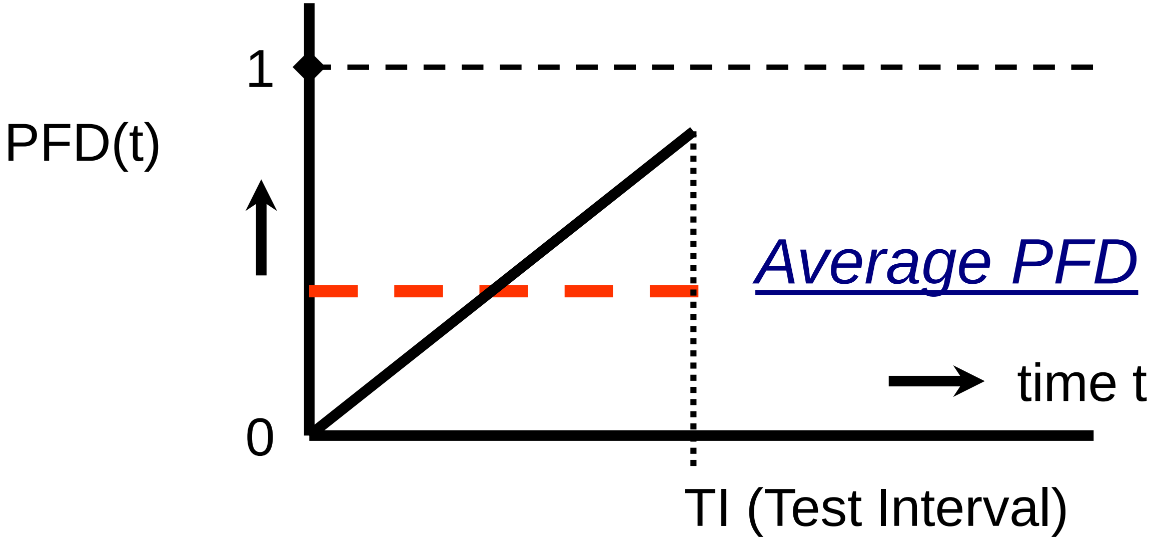


$$PFD_{AVG} = \frac{\int_{0}^{T_I} PFD(t)dt}{T_I}$$

, where PFD(t) = λt

Linear approximation

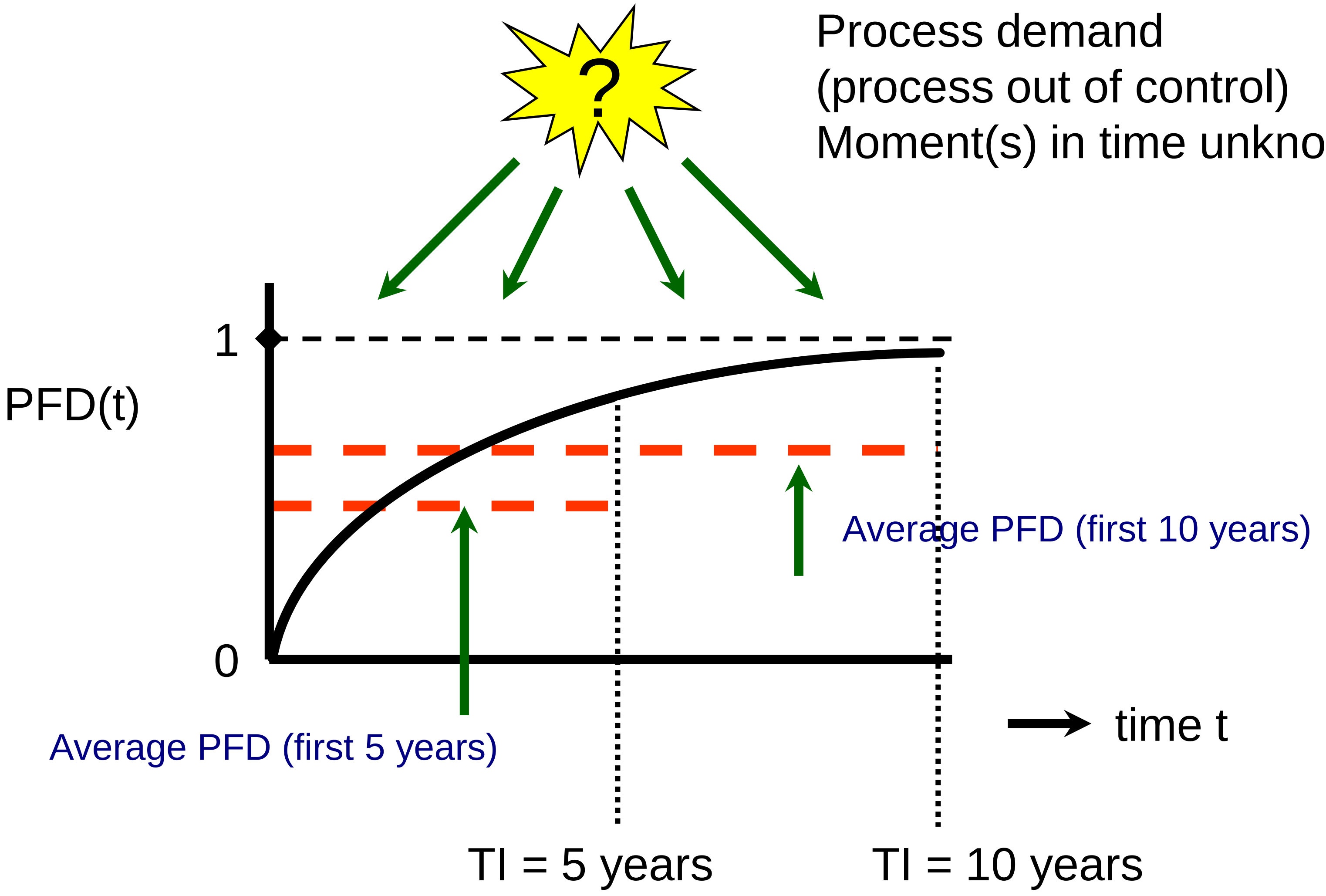
Linear approximation acceptably accurate if Lambda << 1/TI



$$\mathbf{PFD_{AVG}} = \frac{\lambda * \mathbf{TI}}{\mathbf{2}}$$

Honeywell
THE POWER OF CONNECTED

Why PFDavg instead of PFD(t)?



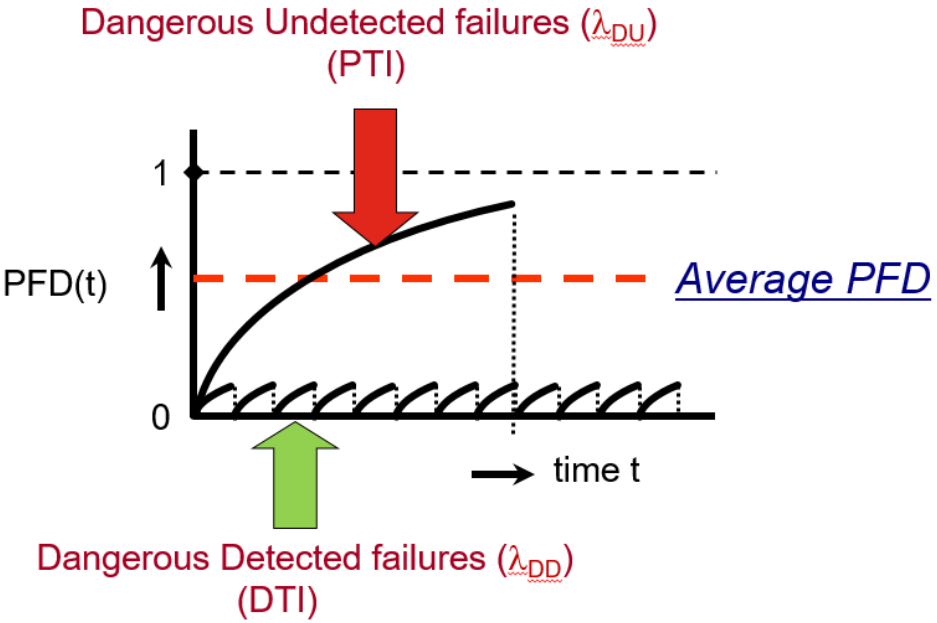
Process demand
(process out of control)
Moment(s) in time unknown

Average PFD (first 10 years)

Average PFD (first 5 years)

Device Average Probability Of Failure on Demand (PFDavg)

$$\textbf{PFDavg} = (\lambda_{DU} \cdot \text{PTI}) / 2 + (\lambda_{DD} \cdot \text{DTI}) / 2$$


Dangerous Undetected failures (λ_{DU})
(PTI)

Dangerous Detected failures (λ_{DD})
(DTI)

Where :

λ = Failure rate of device
DU = Dangerous Undetected
DD = Dangerous Detected
PTI = Proof Test Interval
DTI = Diagnostic Test Interval

generally $(\lambda_{DU} \cdot \text{PTI}) / 2 \gg (\lambda_{DD} \cdot \text{DTI}) / 2$

$$\textbf{PFDavg (approx.)} = (\lambda_{DU} \cdot \text{PTI}) / 2$$

Note - This is the PFDavg equation in its simplest form. In reality, other parameters like common cause (beta), Mean Time To restore (MTTR), Diagnostic Coverage (DC) etc also need to be considered

PFDavg equations on 1oo1 voting (IEC 61508, part 6)

1. $\lambda_D = \lambda_{DU} + \lambda_{DD} \qquad \lambda_{DD} = \lambda_D DC \qquad \lambda_{DU} = \lambda_D (1 - DC)$

2. $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

3. $PFD_{AVG} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$

Honeywell
THE POWER OF CONNECTED

PFDavg equations on 1oo2D voting (IEC 61508, part 6)

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + \left(\lambda_{DD} + \lambda_{SD}\right)MTTR}{\lambda_{DU} + \left(\lambda_{DD} + \lambda_{SD}\right)}$$

$$t_{GE}' = \frac{T_1}{3} + MRT$$

$$PFD_{AVG} = 2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\right)t_{CE}'t_{GE}' + 2(1-K)\lambda_{DD}t_{CE}' + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

SIF demand modes

- **Low demand mode:**
  - where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year Low Demand Mode
  - ***Use: probability of dangerous failure on demand PFD***
- **High demand mode:**
  - where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
- **Continuous mode:**
  - where the safety function retains the EUC in a safe state as part of normal operation
- *The last two use: average frequency of a dangerous failure per hour PFH*

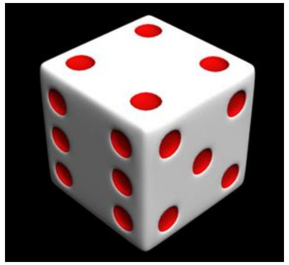
Honeywell
THE POWER OF CONNECTED

Low Demand mode – SIL vs PFDavg

PFDavg	R in %	RRF	SIL	AK
			4	8 7
0.0001	99.99	10,000		
			3	6 5
0.001	99.9	1,000		
			2	4
0.01	99	100		
			1	3 2
0.1	90	10		
			-	1 -
Average Probability to Fail on Demand	Reliability of Safety Functions	Risk Reduction Factor	ISA S84.01 IEC 61508	DIN-V 19250

Probability Theory

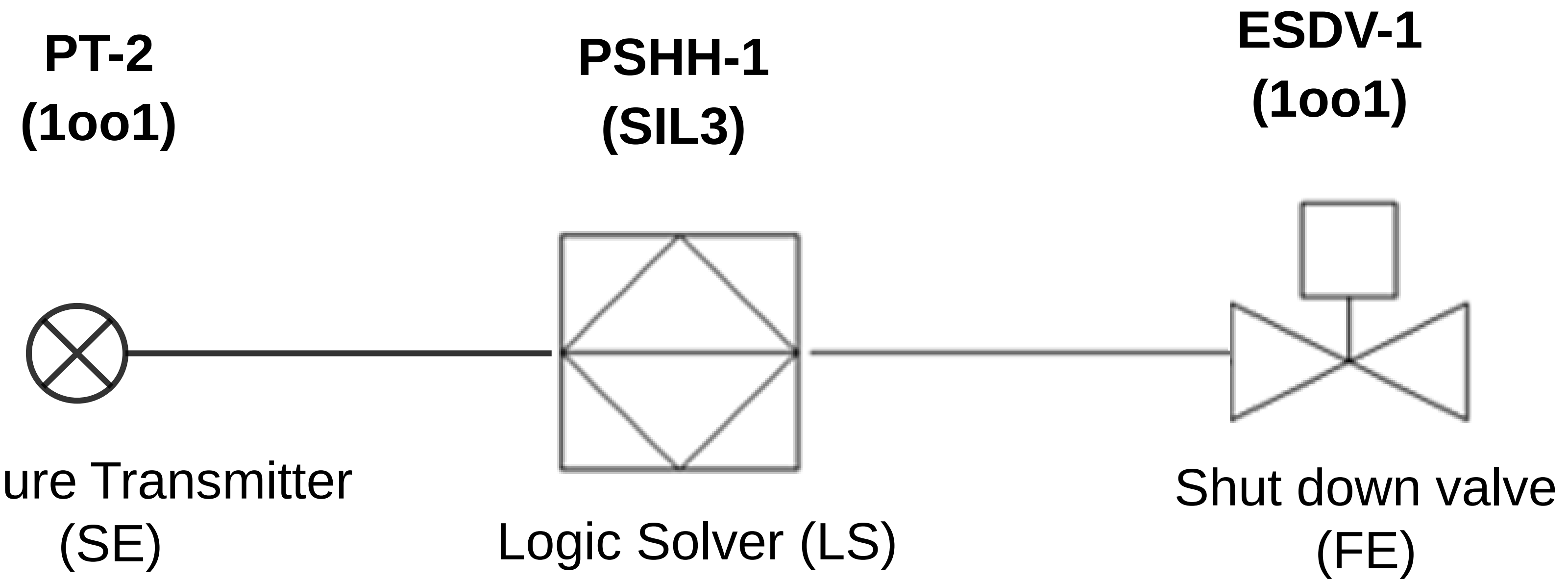
What is the Probability of Tossing a coin and getting ‘Heads’
OR
rolling a dice and getting ‘4’.



P(Heads) + P(4 on dice) – [P(Heads) x P(4 on dice)]
1/2 + 1/6 - (1/2) x (1/6) = 4/6 – 1/12 = 7/12

Note - For small Probability values we can eliminate the product part

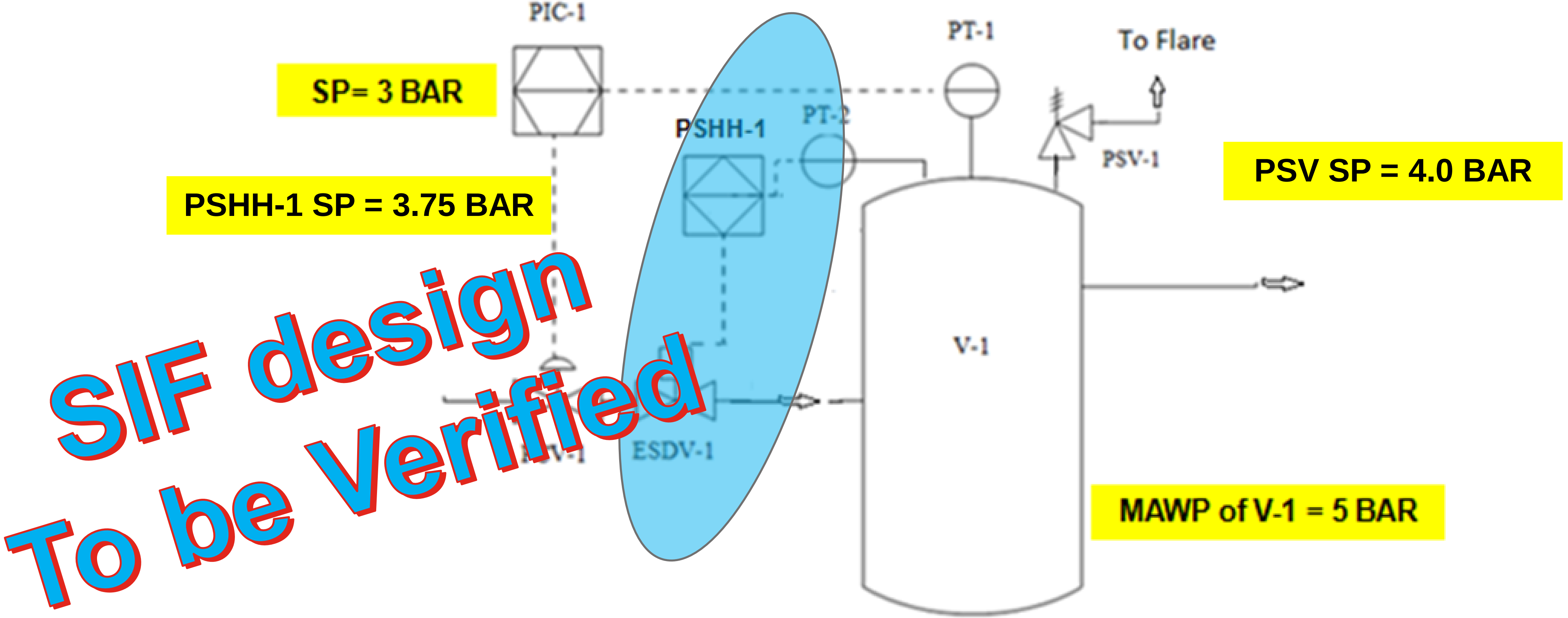
SIF PFDavg calculation



$$PFD_{avg}(SIF\text{-}1) = PFD_{avg}(SE) + PFD_{avg}(LS) + PFD_{avg}(FE)$$

Honeywell
THE POWER OF CONNECTED

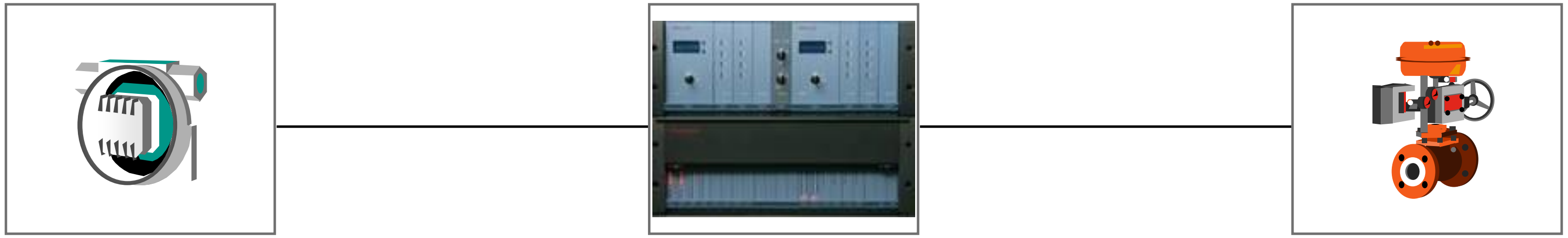
Case Study - Add a SIF (SIL2, RRF-100)



- High Pressure Trip PSHH-1 added
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

Honeywell
THE POWER OF CONNECTED

Case study - PFDavg Calculation (A)



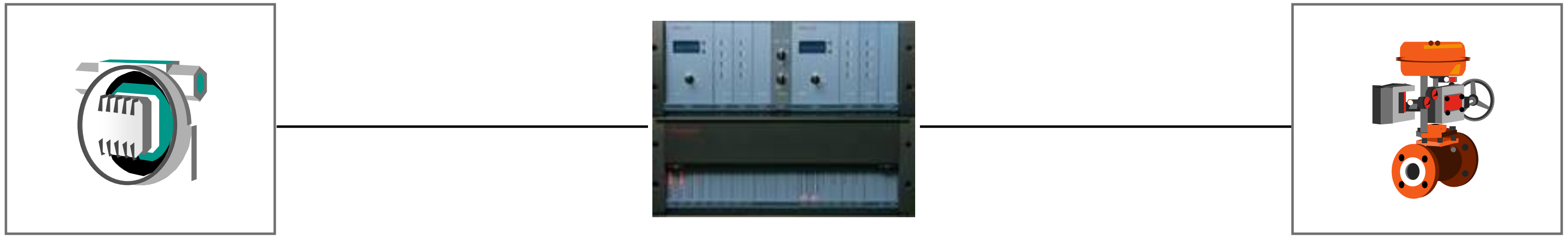
SIL2 Xmtr

SIL3 Logic Solver

Generic valve assembly

- Proof Test interval = 1 y
- Reliability data:
  - Valve: λ_{DU} = 1/10y (= 0.1 y^{-1})
  - Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
  - Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})
- PFD_{avg} = λ_{DU} x PTI / 2
  = 0.1 x 1 / 2 = 0.05 for valve
  0.001 x 1 / 2 = 0.0005 for logic solver
  0.01 x 1 / 2 = 0.005 for transmitter
  Total PFD_{avg} = 0.05 + 0.0005 + 0.005 = 0.0555
- Calculated SIL = 1 (range 0.01 – 0.1)
- Required SIL = 2 !

Case study - PFDavg calculation (B) - Adjust Test Interval



SIL2 Xmtr

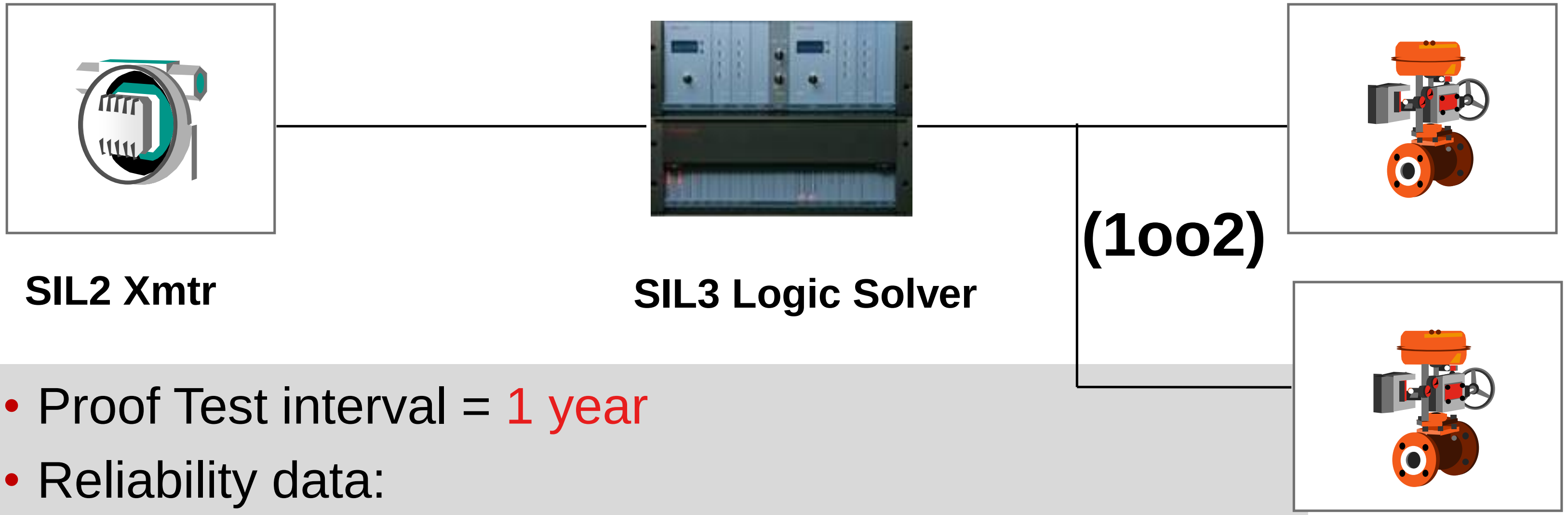
SIL3 Logic Solver

Generic valve assembly

- Proof Test interval = 1 month
- Reliability data:
  - Valve: λ_{DU} = 1/10y (= 0.1 y^{-1})
  - Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
  - Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})
- PFD_{avg} = λ_{DU} x PTI / 2
  = 0.1 / (12 x 2) = 0.004 for valve
  0.001 / (12 x 2) = 0.00004 for logic solver
  0.01 / (12 x 2) = 0.0004 for transmitter
  Total PFD_{ave} = 0.004 + 0.00004 + 0.0004 = 0.00444
- Calculated SIL = 2 (range 0.001 – 0.01)
- Required SIL = 2 OK

THE POWER OF CONNECTED

Case study - PFDavg calculation (C) – Consider 2 valves



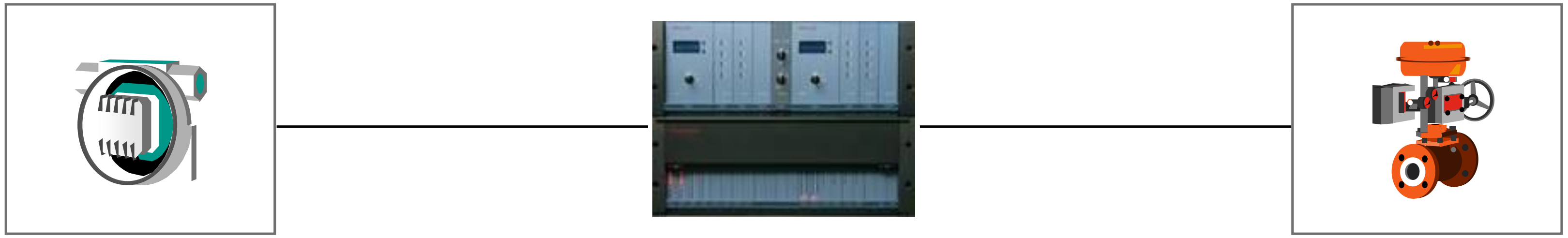
SIL2 Xmtr

SIL3 Logic Solver

Generic valve assemblies

- Proof Test interval = 1 year
- Reliability data:
  - Valve: λ_{DU} = 1/10y (= 0.1 y^{-1})
  - Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
  - Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})
- PFD_{avg} = 0.0025 + 0.0005 + 0.005 = 0.0080
- Calculated SIL = 2 (range 0.001 – 0.01)
- Required SIL = 2 OK .

Case study - PFDavg Calculation (D) – One SIL2 rated valve



SIL2 Xmtr

SIL3 Logic Solver

SIL2 rated valve assembly

- Proof Test interval = 1 y
- Reliability data:
  - Valve: λ_{DU} = 1/100y (= 0.01 y^{-1})
  - Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
  - Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})
- PFD_{avg} = λ_{DU} x PTI / 2

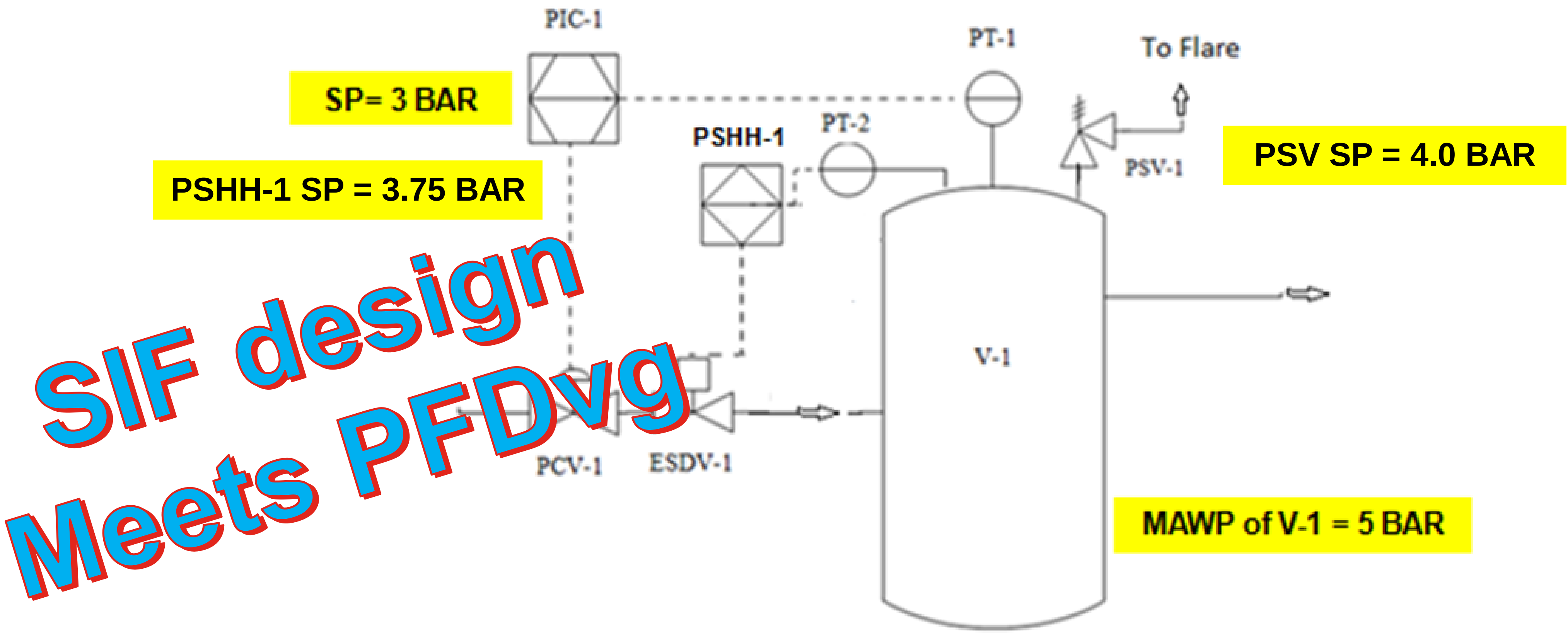
  = 0.01 x 1 / 2 = 0.005 for valve

  0.001 x 1 / 2 = 0.0005 for logic solver

  0.01 x 1 / 2 = 0.005 for transmitter

  Total PFD_{avg} = 0.005 + 0.0005 + 0.005 = 0.0105
- Calculated almost SIL = 2 ! (range 0.01 – 0.1)
- Required SIL = 2

Case Study, Add a new SIF (select - scenario D)



- High Pressure Trip PSHH-1 added
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

IEC 61508/61511 Design Requirements to meet SIL

All SIF components should meet :

- Architectural Constraints
  - Diagnostic coverage of component failure
  - Safe Failure Fraction of component failure
  - Fault tolerance of subsystems
  - Type of components

- Reliability of components → PFD

- Systematic Capability influences
  - Requirements specification
  - Hardware
  - Software
  - Environmental

Subsystem Types: Type A

- **Type A subsystem:**
  - The Failure modes of all constituent components are well defined

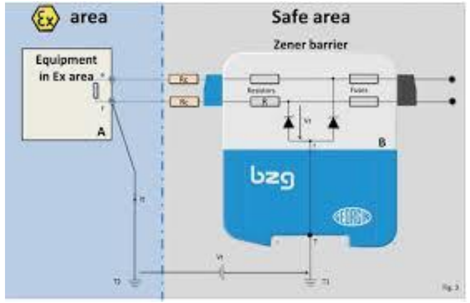
    AND

  - The behavior of the subsystem under fault conditions can be completely determined

    AND

  - Dependable failure data from field experience exists for the subsystem, sufficient to show that the required target failure is met

Examples

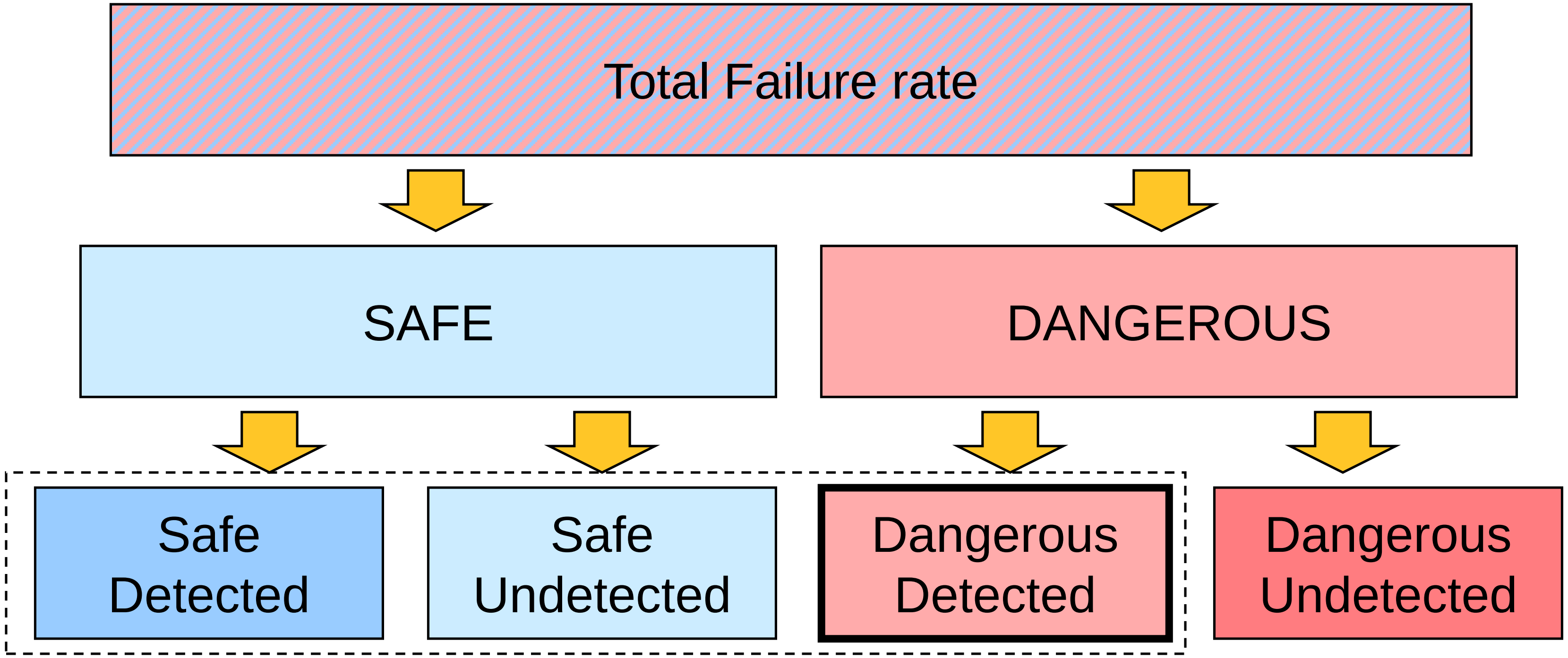


Subsystem Types: Type B

- **Type B subsystem:**
  - The failure modes of at least one constituent component is not well defined
    OR
  - The behavior of the subsystem under fault conditions cannot be completely determined
    OR
  - Insufficient dependable failure data from field experience exists for the subsystem, to show that the required target failure is met

Examples:

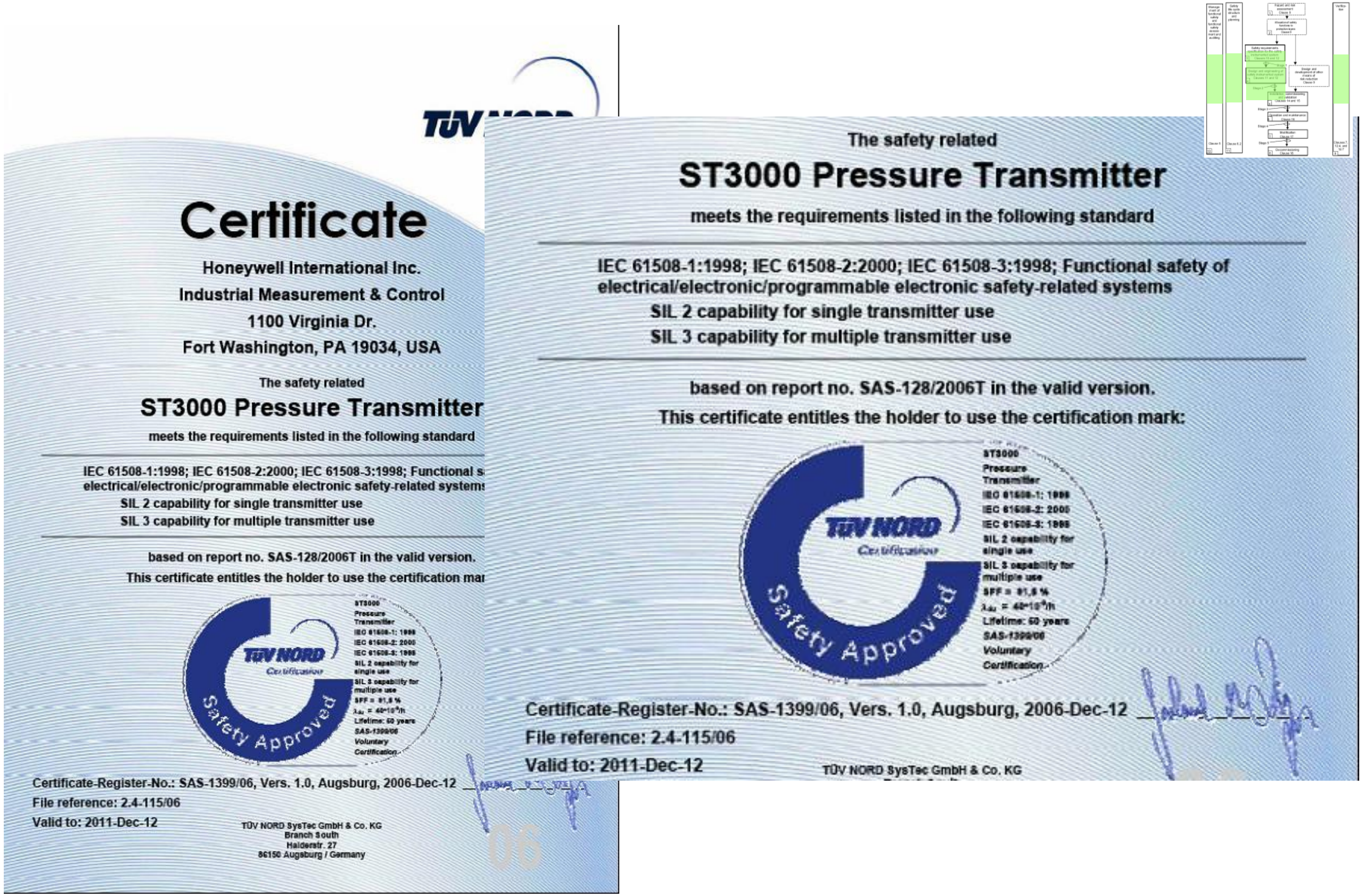
Safe Failure Fraction (SFF)



$$\text{Safe Failure Fraction}: \frac{\Sigma\,\text{Safe failure rate} + \Sigma\,\text{DD failure rate}}{\Sigma\,\text{Total failure rate}}$$

Honeywell
THE POWER OF CONNECTED

Transmitter TÜV Certificate



TÜV NORD

Certificate

Honeywell International Inc.
Industrial Measurement & Control
1100 Virginia Dr.
Fort Washington, PA 19034, USA

The safety related

ST3000 Pressure Transmitter

meets the requirements listed in the following standard

IEC 61508-1:1998; IEC 61508-2:2000; IEC 61508-3:1998; Functional safety of electrical/electronic/programmable electronic safety-related systems
SIL 2 capability for single transmitter use
SIL 3 capability for multiple transmitter use

based on report no. SAS-128/2006T in the valid version.

This certificate entitles the holder to use the certification mark:

TÜV NORD Certification
Safety Approved
ST3000
Pressure
Transmitter
IEC 61508-1: 1998
IEC 61508-2: 2000
IEC 61508-3: 1998
SIL 2 capability for single use
SIL 3 capability for multiple use
SFF = 91,5 %
λ_{du} = 40*10^{-9}/h
Lifetime: 50 years
SAS-1399/06
Voluntary
Certification

Certificate-Register-No.: SAS-1399/06, Vers. 1.0, Augsburg, 2006-Dec-12
File reference: 2.4-115/06
Valid to: 2011-Dec-12

TÜV NORD SysTec GmbH & Co. KG
Branch South
Halderstr. 27
86150 Augsburg / Germany

06

The safety related

ST3000 Pressure Transmitter

meets the requirements listed in the following standard

IEC 61508-1:1998; IEC 61508-2:2000; IEC 61508-3:1998; Functional safety of electrical/electronic/programmable electronic safety-related systems
SIL 2 capability for single transmitter use
SIL 3 capability for multiple transmitter use

based on report no. SAS-128/2006T in the valid version.

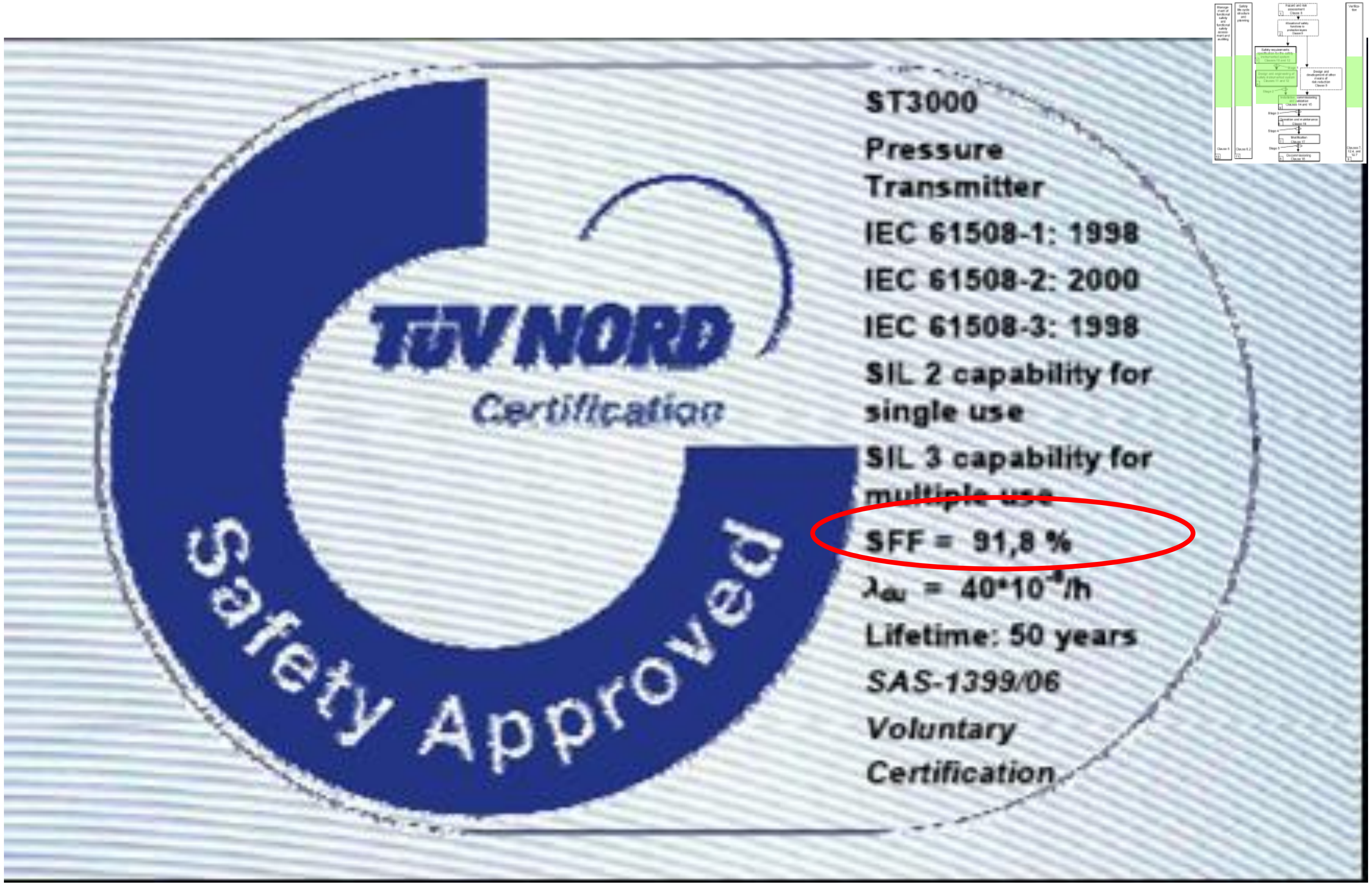
This certificate entitles the holder to use the certification mark:

TÜV NORD Certification
Safety Approved
ST3000
Pressure
Transmitter
IEC 61508-1: 1998
IEC 61508-2: 2000
IEC 61508-3: 1998
SIL 2 capability for single use
SIL 3 capability for multiple use
SFF = 91,5 %
λ_{du} = 40*10^{-9}/h
Lifetime: 50 years
SAS-1399/06
Voluntary
Certification

Certificate-Register-No.: SAS-1399/06, Vers. 1.0, Augsburg, 2006-Dec-12
File reference: 2.4-115/06
Valid to: 2011-Dec-12

TÜV NORD SysTec GmbH & Co. KG

Transmitter TÜV Certification Mark


TÜV NORD
Certification
Safety Approved

ST3000

Pressure Transmitter

IEC 61508-1: 1998

IEC 61508-2: 2000

IEC 61508-3: 1998

SIL 2 capability for single use

SIL 3 capability for multiple use

SFF = 91,8 %

λ_{du} = 40•10^{-9}/h

Lifetime: 50 years

SAS-1399/06

Voluntary Certification

Honeywell
THE POWER OF **CONNECTED**

Architectural Constraints (Route 1H)

IEC 61508,
Part 2

Table 2:

Type A subsystems

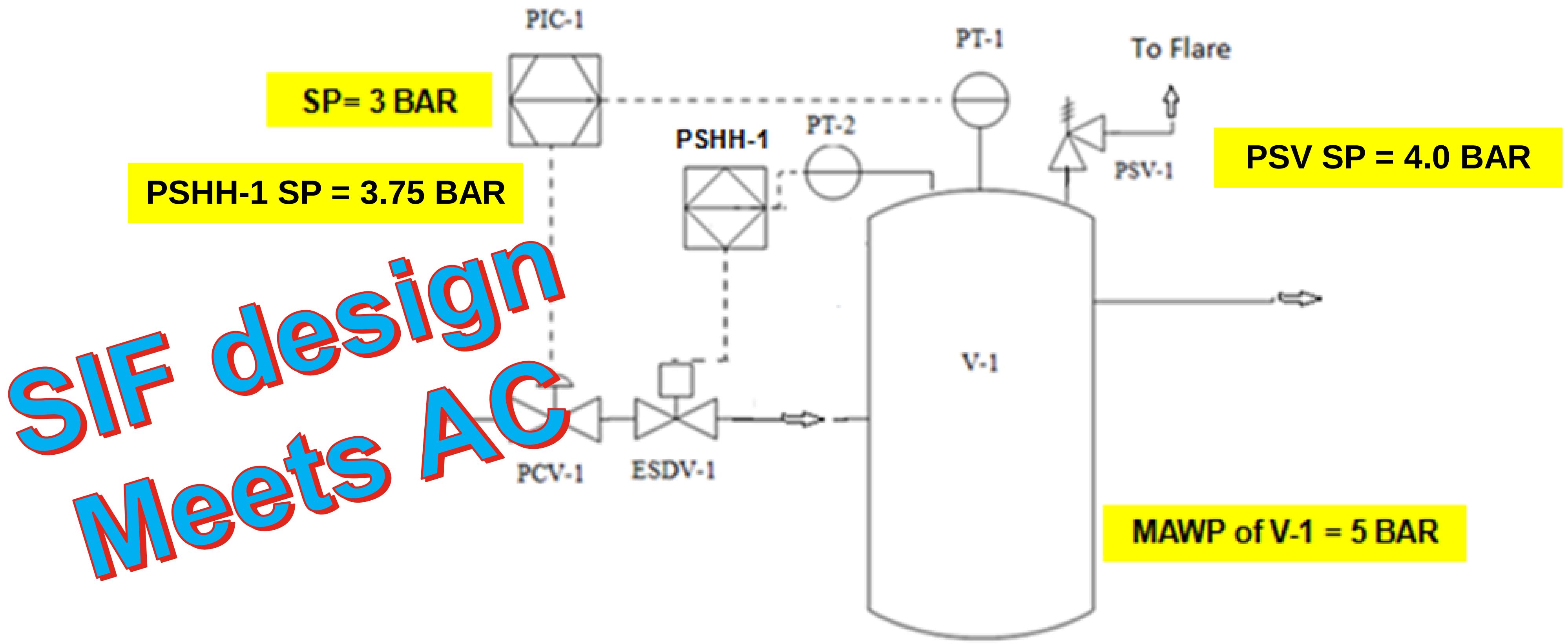
Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - 90 %	SIL2	SIL3	SIL4
90 % - 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Table 3:

Type B subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % - 90 %	SIL1	SIL2	SIL3
90 % - 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Case Study, Add a new SIF (select - scenario D)



- High Pressure Trip PSHH-1 added
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

Honeywell
THE POWER OF CONNECTED

IEC 61508/61511 Design Requirements to meet SIL

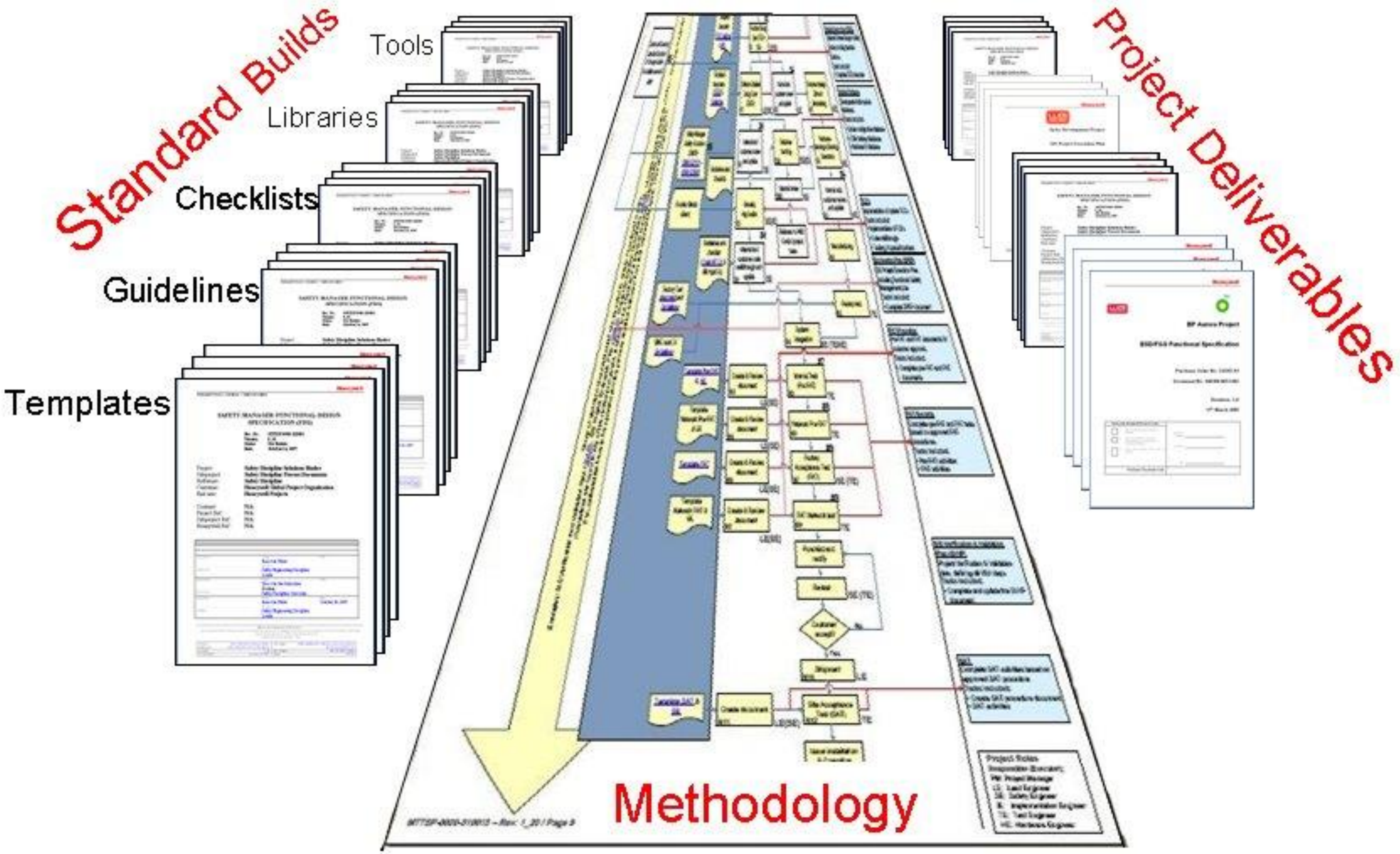
All SIF components should meet :

- Architectural Constraints
    - Diagnostic coverage of component failure
    - Safe Failure Fraction of component failure
    - Fault tolerance of subsystems
    - Type of components

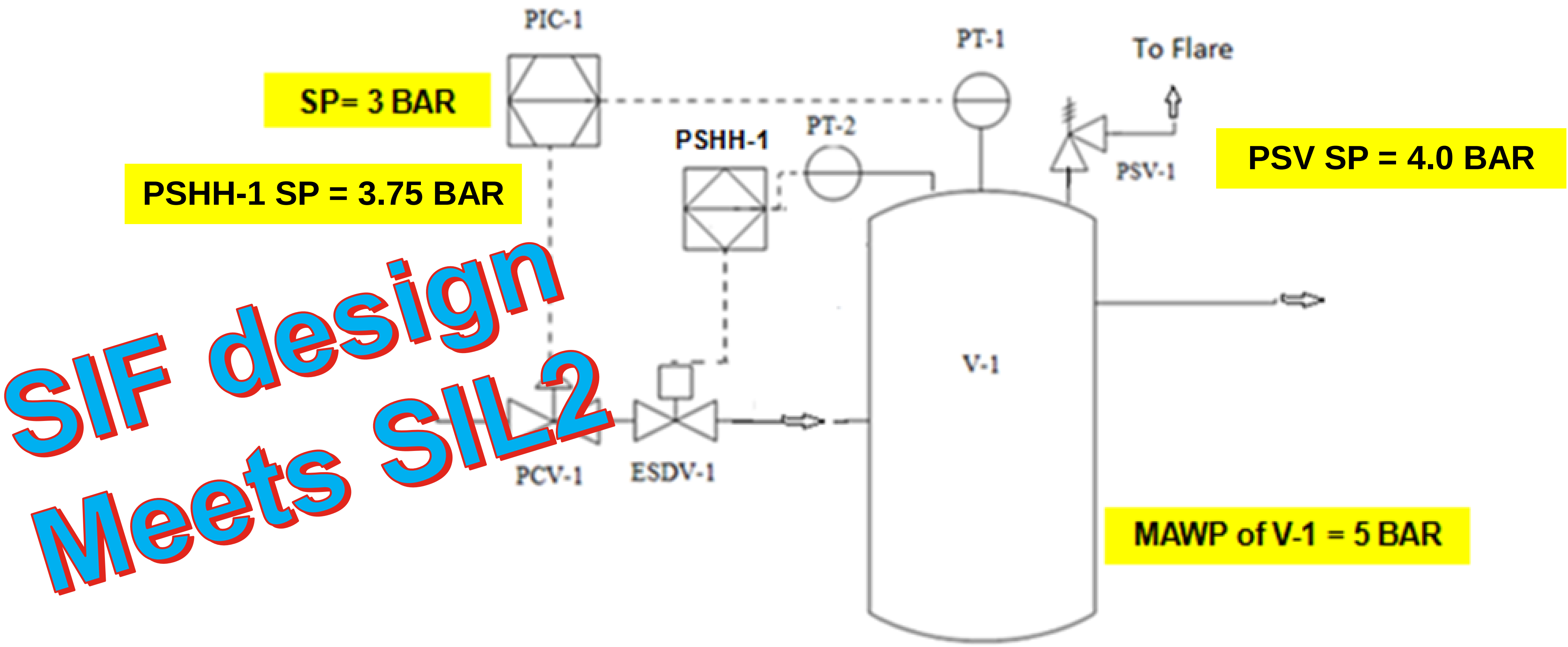
- Reliability of components → PFD

- Systematic Capability influences
    - Requirements specification
    - Hardware
    - Software
    - Environmental

Standard Build Concept for Safety product development and project execution



Case Study, Add a new SIF (select - scenario D)

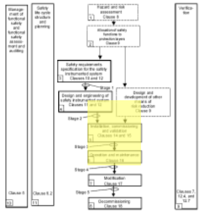


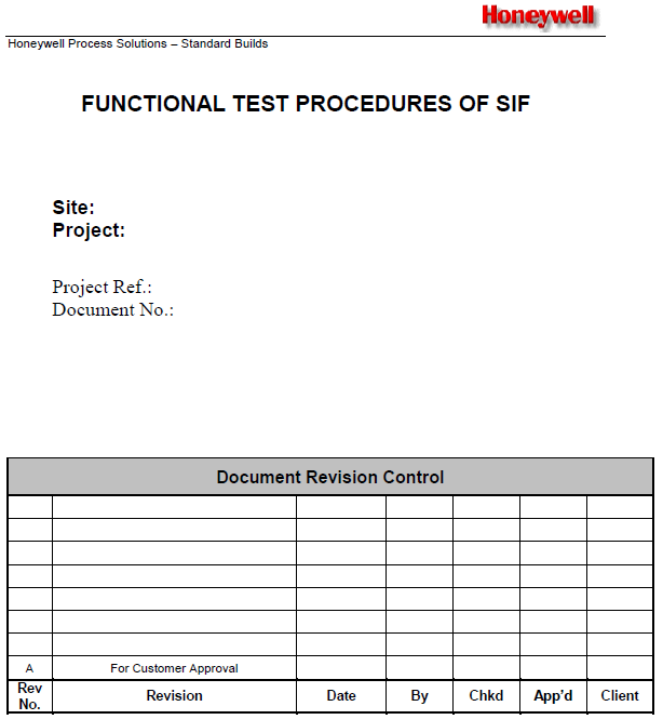
- High Pressure Trip PSHH-1 added
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

Honeywell
THE POWER OF CONNECTED

SIS Validation

- SIS Validation at site to make sure that all the SIFs in the SIS are functioning as per the requirements in the SRS
- Use Functional Test Procedures for SIS validation





Honeywell

Honeywell Process Solutions – Standard Builds

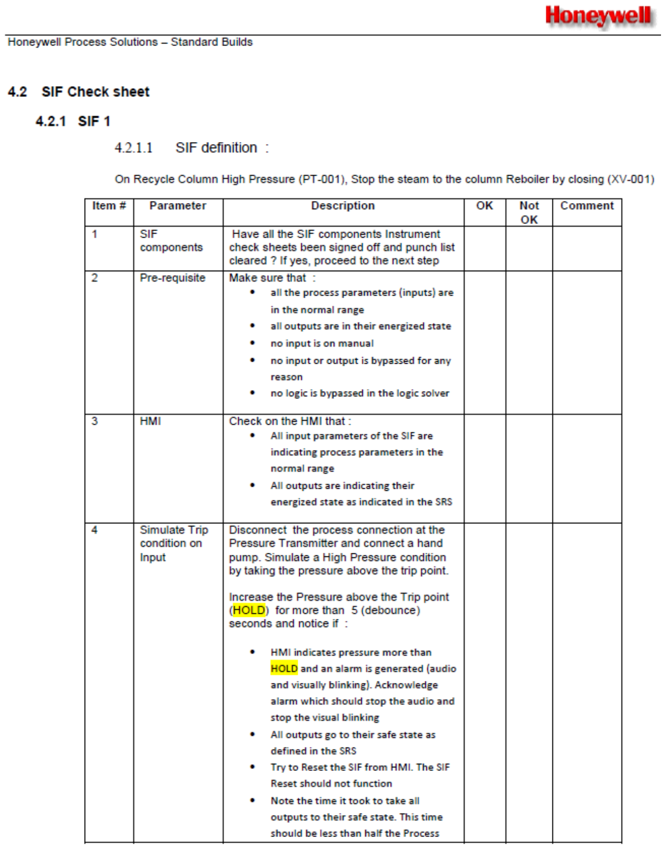
FUNCTIONAL TEST PROCEDURES OF SIF

Site:
Project:

Project Ref.:
Document No.:

Document Revision Control

A	For Customer Approval					
Rev No.	**Revision**	**Date**	**By**	**Chkd**	**App'd**	**Client**



Honeywell

Honeywell Process Solutions – Standard Builds

4.2 SIF Check sheet

4.2.1 SIF 1

4.2.1.1 SIF definition :

On Recycle Column High Pressure (PT-001), Stop the steam to the column Reboiler by closing (XV-001)

Item #	Parameter	Description	OK	Not OK	Comment
1	SIF components	Have all the SIF components Instrument check sheets been signed off and punch list cleared ? If yes, proceed to the next step			
2	Pre-requisite	Make sure that : • all the process parameters (inputs) are in the normal range • all outputs are in their energized state • no input is on manual • no input or output is bypassed for any reason • no logic is bypassed in the logic solver			
3	HMI	Check on the HMI that : • All input parameters of the SIF are indicating process parameters in the normal range • All outputs are indicating their energized state as indicated in the SRS			
4	Simulate Trip condition on Input	Disconnect the process connection at the Pressure Transmitter and connect a hand pump. Simulate a High Pressure condition by taking the pressure above the trip point. Increase the Pressure above the Trip point (HOLD) for more than 5 (debounce) seconds and notice if : • HMI indicates pressure more than HOLD and an alarm is generated (audio and visually blinking). Acknowledge alarm which should stop the audio and stop the visual blinking • All outputs go to their safe state as defined in the SRS • Try to Reset the SIF from HMI. The SIF Reset should not function • Note the time it took to take all outputs to their safe state. This time should be less than half the Process			

Honeywell
THE POWER OF **CONNECTED**

Question 1:

The SRS is used to document the following :

a) The initiating events of all SIFs

b) The Functional requirements of all SIFs

c) The SIL calculations of all SIFs

d) The Functional and Integrity requirements of all SIFs

Honeywell
THE POWER OF **CONNECTED**

Question 2:

What is PFD

a). Probability of Failing Dangerously

b). Probability of Falling Dead

[✓ c). Probability of Failure on Demand]

d). None of the above

Question 3:

What is Diagnostic coverage

a). Fraction of failures detected During Proof tests

[✓ b). Fraction of failures detected by automatic on-line diagnostic tests]

c). Fraction of failures detected during SIS validation

d). None of the above

Question 4:

To meet SIL, all SIF components should meet the following requirements :

[✓ a) Architectural Constraints, PFDavg and Systematic capability]

b) SFF, PFDavg and Systematic capability

c) Architectural Constraints, Failure rates and Systematic capability

d) None of the above

Question 5:

The HFT of 1oo3 voting of transmitters is:

a) 0

b) 1

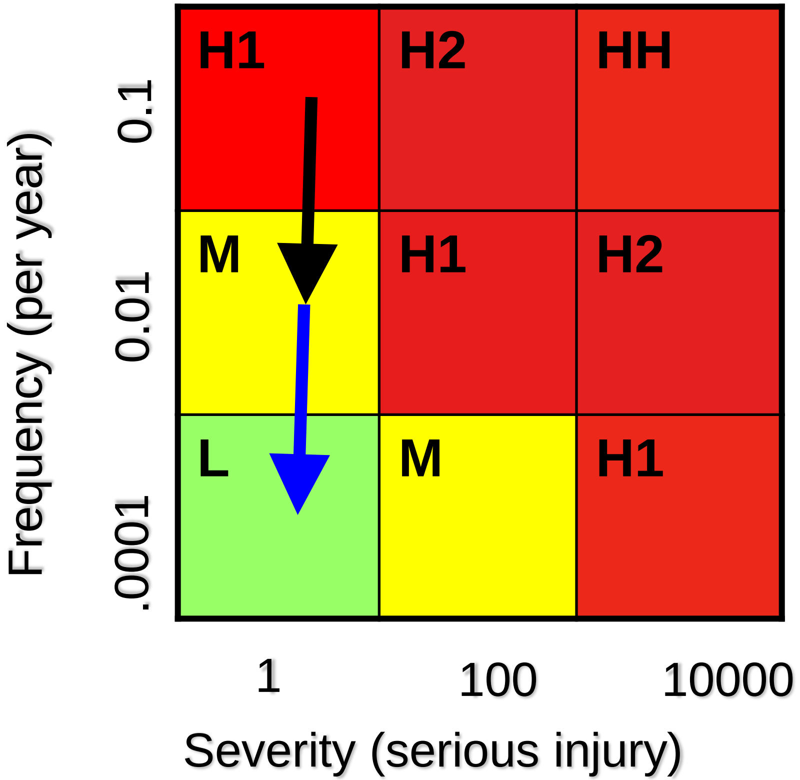
[✓ c) 2]

d) 3

Independence between BPCS and SIS

Honeywell
THE POWER OF CONNECTED

Example – Consider RRF BPCS loop = 10, SIS loop = 100



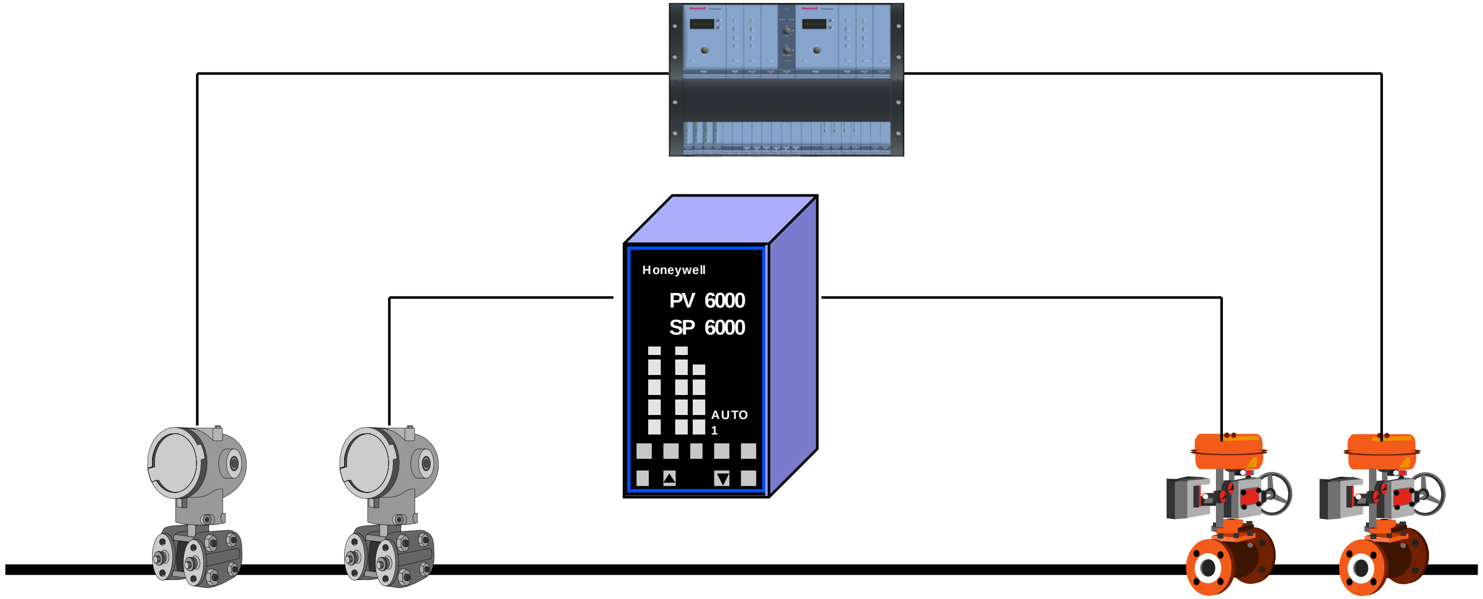
Frequency (per year)	1	100	10000
0.1	H1	H2	HH
0.01	M	H1	H2
.0001	L	M	H1

Present Risk “H1” = 0.1 (1 Serious injury in 10 years)
Risk at “M”- .01 (1 Serious injury in 100 years)
Risk Reduction Factor =10 (**By BPCS loop**)

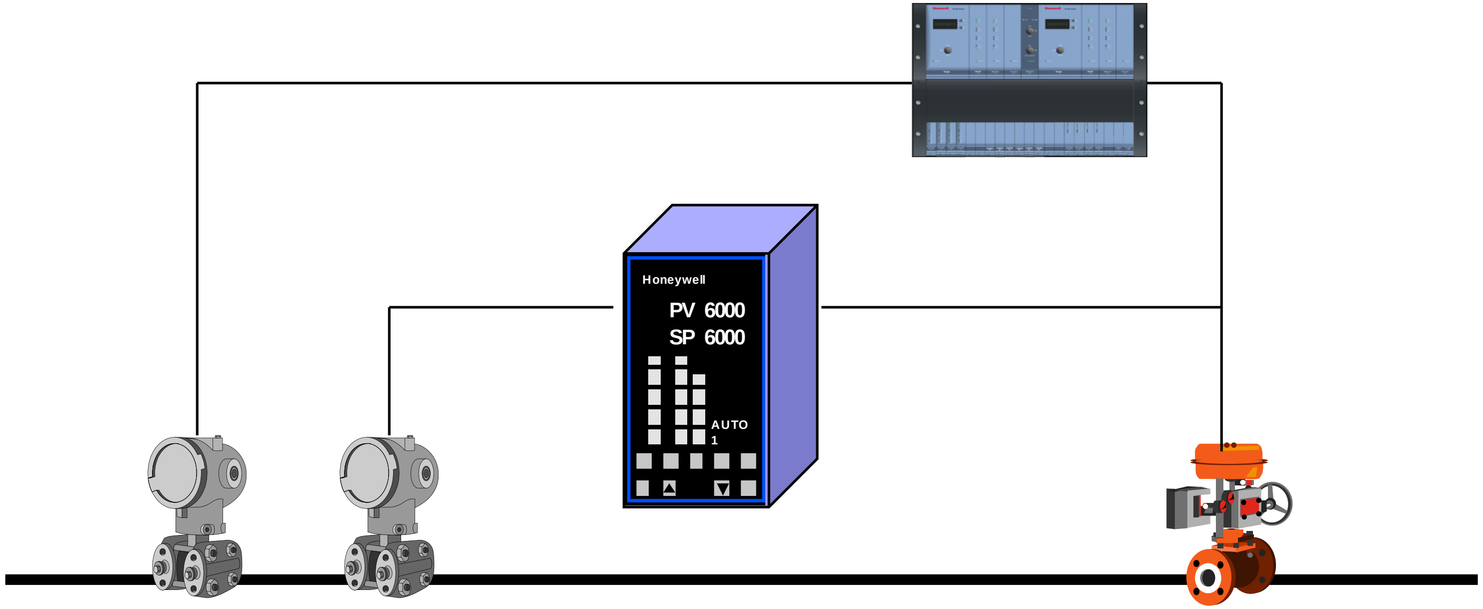
Risk at “M”- .01 (1 Serious injury in 100 years)
Risk at “L”- .0001 (1 Serious injury in 10000 years)
Risk Reduction Factor = 100 (**By SIS loop**)

Total Required RRF = 10 x 100 = 1000

Config 1 - BPCS and SIS loop independent



Config 2 - BPCS and SIS loop with common valve



RRF calculation – Config 1 vs 2

- Config 1 - independent IPLs

- BPCS RRF = 10
- SIS loop RRF = 100
- Total RRF = 10 x 100 = 1000

- If BPCS valve fails dangerous (remains open), BPCS RRF = 1
- Achieved RRF = 1 x 100 = 100

- Even with a BPCS failure, a RRF of 100 is still available because of SIS loop (per HAZOP Risk matrix in YELLOW zone)

- Config 2 - common valve

- BPCS RRF = 10
- SIS loop RRF = 100
- Total RRF = 10 x 100 = 1000

- If BPCS valve fails dangerous (remains open), BPCS RRF = 1 and SIS Loop RRF = 1
- Achieved RRF = 1 x 1 = 1

- No Risk reduction available ! (per HAZOP Risk matrix in RED zone)

Honeywell
THE POWER OF CONNECTED

Fire and Gas Functions

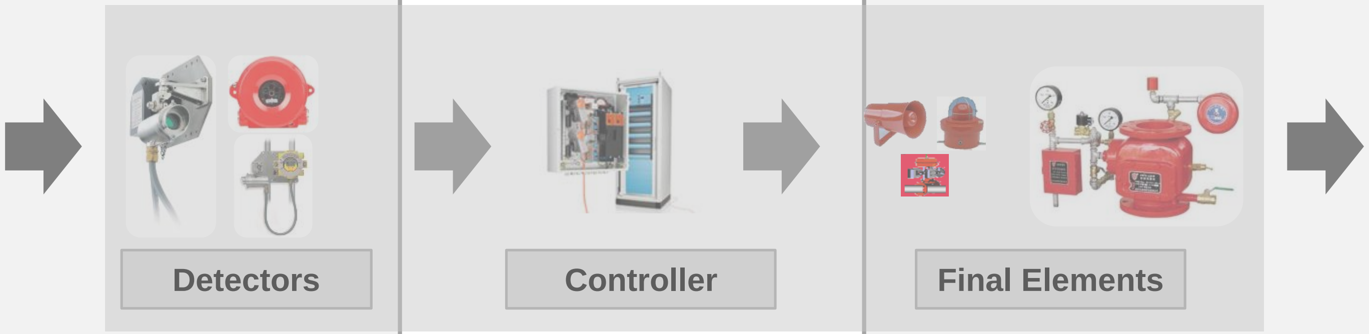
Honeywell
THE POWER OF CONNECTED

FGS Instrumented Function (FIF) Effectiveness

Detector coverage

FGS Loop availability

Mitigation action effectiveness



Detectors

- Gas
- Fire
- Flame
- Smoke
- ……

Controller

- SIL3 PLC for F&G
- DCS
- Fire Alarm Panel for Buildings
- …..

Final Elements

- Dry Powder
- Expansion foam
- Water Curtains
- Annunciation Systems
- Shutdown systems
- …..

FIF Detection Effectiveness = Detector coverage x FGS loop availability

FIF Loop Effectiveness = FIF Detection Effectiveness x Mitigation action effectiveness

FGS Instrumented Function (FIF) Effectiveness

FIF Effectiveness = 0.9 x 0.99 x 0.9 = 0.80 (80%)		
Detector Coverage Say **90%**	FGS loop Availability Say **99%**	Mitigation Effectiveness **90%**

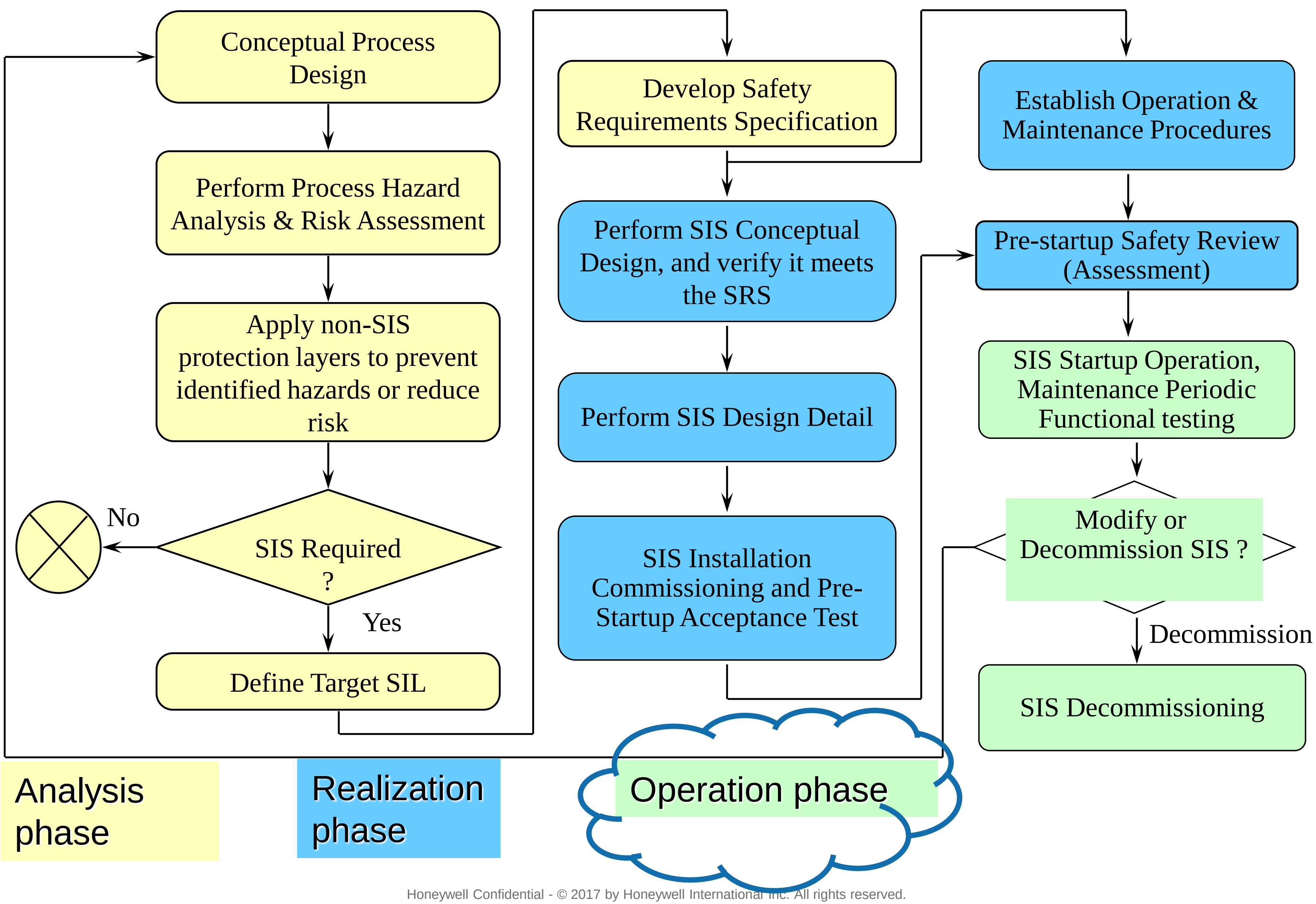
With 80% Effectiveness, not a good idea to assign a SIL value to a FGS Instrumented Function

Honeywell
THE POWER OF **CONNECTED**

Operations and Maintenance Phase

Honeywell
THE POWER OF CONNECTED

The Safety Life Cycle as defined in the standards

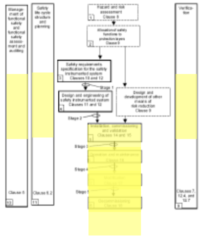

Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
SIS Required ?
No
Yes
Define Target SIL
Develop Safety Requirements Specification
Perform SIS Conceptual Design, and verify it meets the SRS
Perform SIS Design Detail
SIS Installation Commissioning and Pre-Startup Acceptance Test
Establish Operation & Maintenance Procedures
Pre-startup Safety Review (Assessment)
SIS Startup Operation, Maintenance Periodic Functional testing
Modify or Decommission SIS ?
Decommission
SIS Decommissioning
Analysis phase
Realization phase
Operation phase

Operations and Maintenance Obligations

- Proof test SIF devices at specified interval **(PFDavg = (λ_{DU}. PTI) / 2)**
- Monitor design assumptions
  - Demand rates
  - Component reliability
- Adjust test interval to suit
- SIF modifications (proper MOC process)
- System upgrade (Hardware and Software)
- Ensure Maintenance and Operational Overrides are used as designed
- Monitor and promptly follow-up diagnostics.

SIS Modification

New SIF introduced after commissioning

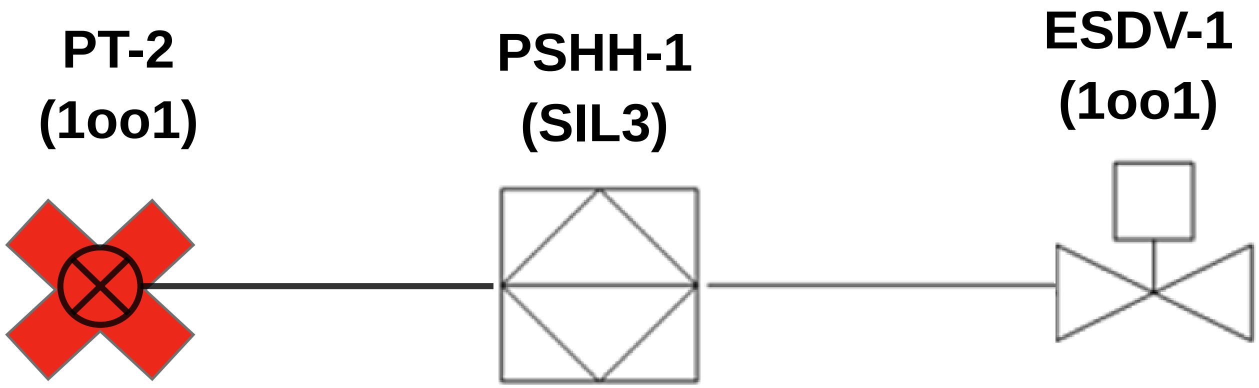


TECHNIQUE / MEASURE	Ref	SIL 1	SIL 2	SIL 3	SIL 4
1 Impact Analysis	B.35	HR	HR	HR	HR
2 Re-verify Changed Module	B.35	HR	HR	HR	HR
3 Re-verify Affected Modules	B.35	R	HR	HR	HR
4 Revalidate Complete System	B.35	---	R	HR	HR
5 Software Configuration Management	B.56	HR	HR	HR	HR
6 Data Recording and Analysis	B.13	HR	HR	HR	HR

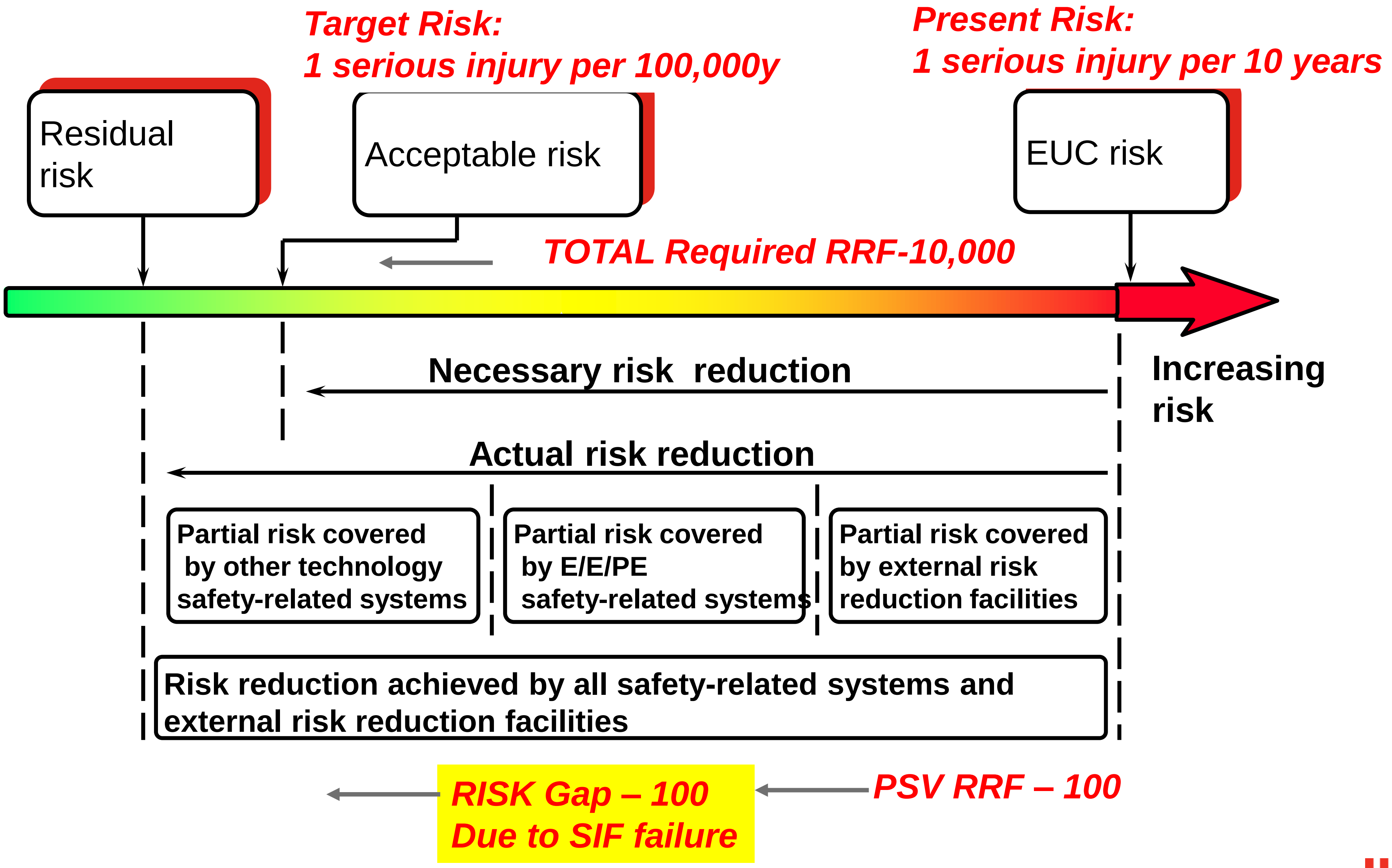
During early design consider splitting SIL 2 and SIL 3 systems.

PSHH-1 SIF failure

- During normal operations, say **PT-2 fails (indicates BadPV)**
- That would mean we do not have an Operating SIF PSHH-1



Risk and Risk Reduction



Target Risk:
1 serious injury per 100,000y

Present Risk:
1 serious injury per 10 years

Residual risk

Acceptable risk

EUC risk

TOTAL Required RRF-10,000

Necessary risk reduction

Increasing risk

Actual risk reduction

Partial risk covered by other technology safety-related systems

Partial risk covered by E/E/PE safety-related systems

Partial risk covered by external risk reduction facilities

Risk reduction achieved by all safety-related systems and external risk reduction facilities

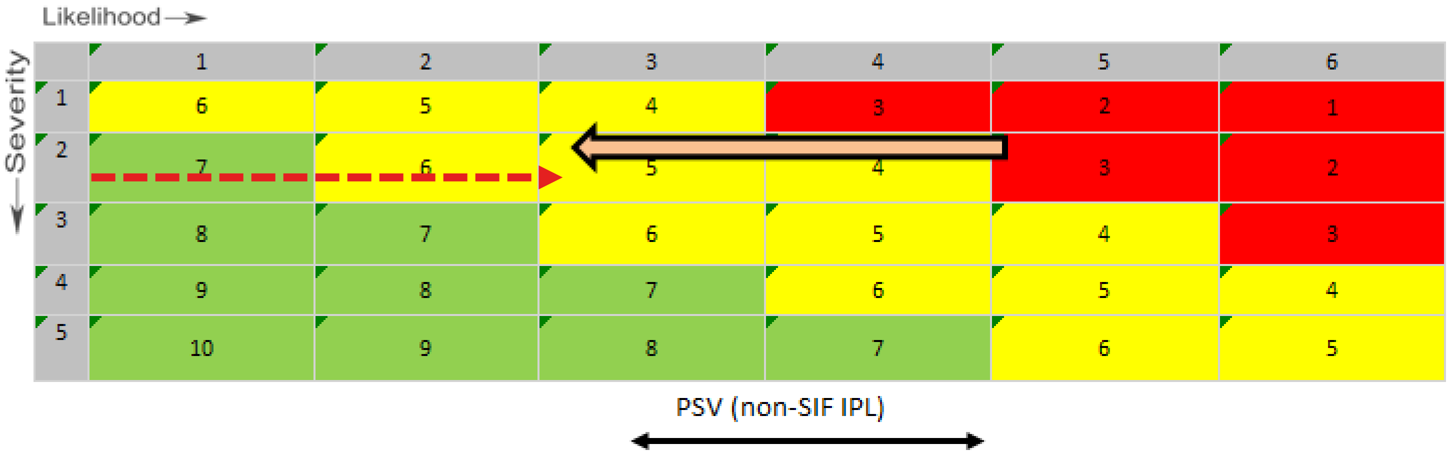
RISK Gap – 100
Due to SIF failure

PSV RRF – 100

Risk Reduction (with SIF in Bypass or Failed transmitter)

From the HAZOP risk matrix for this Process, if SIF is Bypassed:

1. Frequency of Initiating Event (IE) – (L=3)
2. Severity – Single fatality (S=2)
3. Risk (with only PSV as safeguard) = (Box 5)



Likelihood →

Severity ↓	1	2	3	4	5	6
1	6	5	4	3	2	1
2	7	6	5	4	3	2
3	8	7	6	5	4	3
4	9	8	7	6	5	4
5	10	9	8	7	6	5

PSV (non-SIF IPL)

Likelihood	
1	Once in 10000 years
2	Once in 1000 years
3	Once in 100 years
4	Once in Ten Years
5	Once a year
6	Multiple times per year

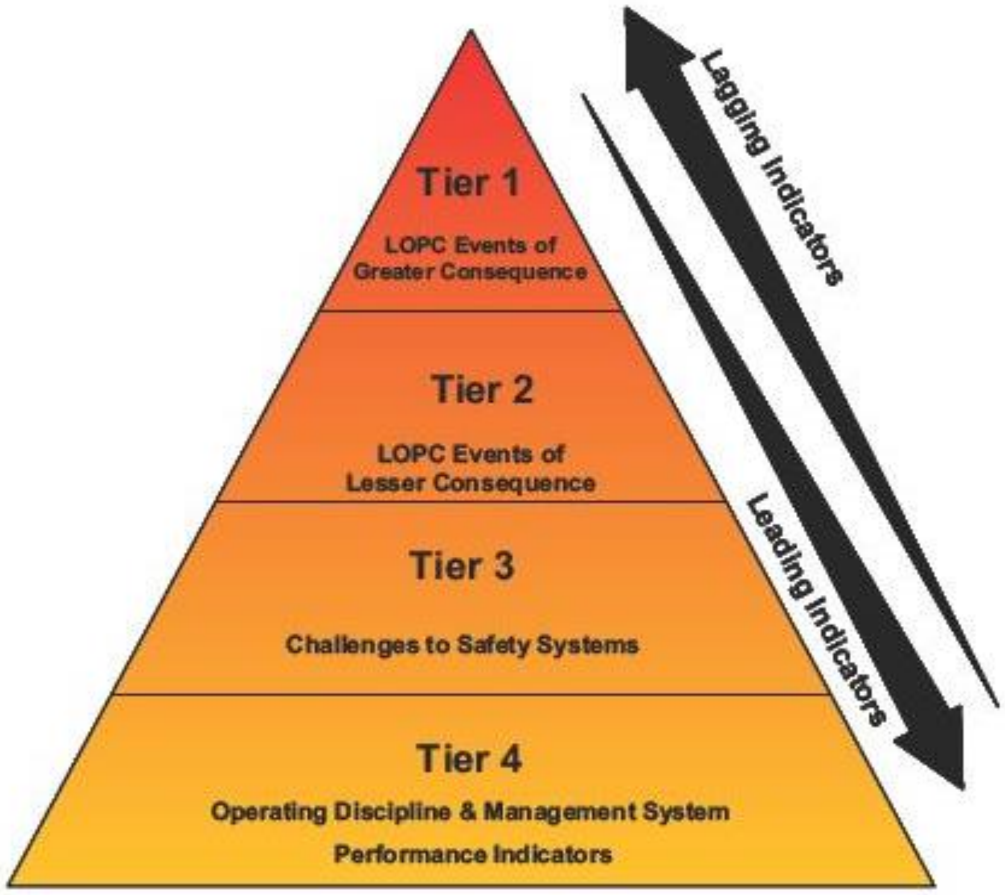
Severity	
1	Multiple fatilities
2	Single Fatility
3	Serious injury
4	First Aid
5	First Aid

LOPA TMEL (Single Fatality) :

1E-05 per year

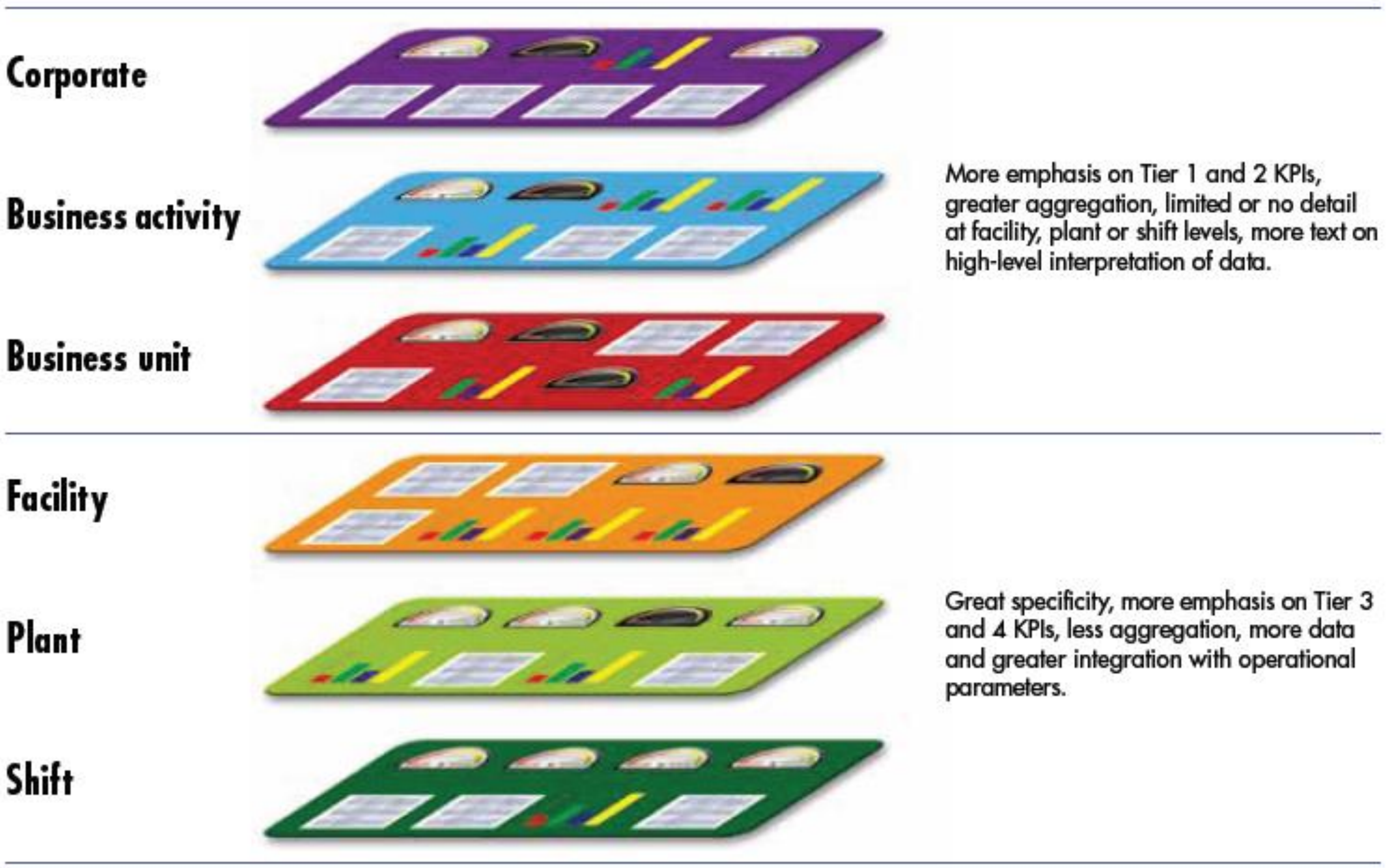
Honeywell
THE POWER OF CONNECTED

API RP 754 - Process Safety Performance Indicators for the Refining & Petrochemical Industries


Tier 1
LOPC Events of Greater Consequence
Tier 2
LOPC Events of Lesser Consequence
Tier 3
Challenges to Safety Systems
Tier 4
Operating Discipline & Management System Performance Indicators
Lagging Indicators
Leading Indicators

Honeywell
THE POWER OF **CONNECTED**

Key Performance Indicators (KPI)



More emphasis on Tier 1 and 2 KPIs, greater aggregation, limited or no detail at facility, plant or shift levels, more text on high-level interpretation of data.

Great specificity, more emphasis on Tier 3 and 4 KPIs, less aggregation, more data and greater integration with operational parameters.

Process Risk Index (Tier 2 KPI)

- **Process Risk Index (PRI)** is one number which indicates the Process Risk profile of a Process Plant during a small period (Short term) or over a period of time (Long term)

- **Short Term (ST) PRI** is for a period of **One shift or One day**. This is for the Plant Operations Manager to get an idea how their Process plant is doing based **SIFs that have been bypassed**

- **Long Term (LT) PRI** is for a period of a **few months and above**. This is for the senior management (and plant management) to know how the Process plant has been doing in the long term based on **SIF demands, SIF bypass and On Time testing of SIF components**

Short Term Risk Index

Assumptions for ST Risk Index equations:

- “Safety” is the driver for this hazardous event (not Commercial and Environment)
- PFDactual of SIF and non-SIF IPL is the same as PFD per design
- The SIF has 1oo1 input voting
- All other IPLs are working per design

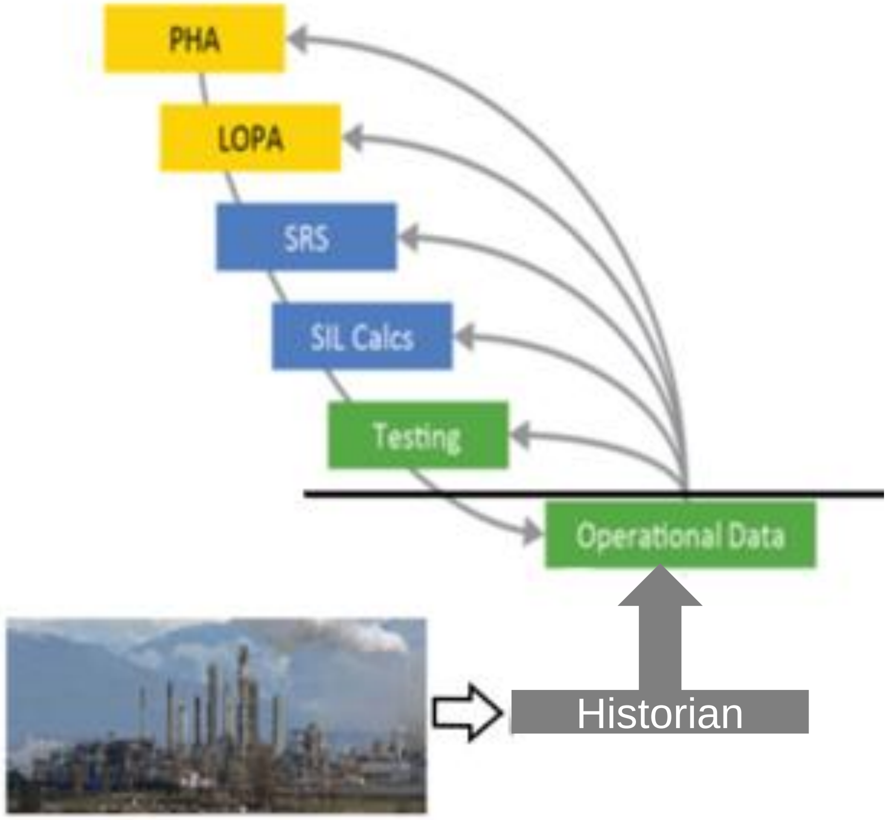
Variable which effects Short Term (ST) Risk Index

- **SIF “Time in Bypass”** over the Short term period.

This data is collected from the Historian over the specified Short term.

Honeywell
THE POWER OF **CONNECTED**

Design and Historian data compared – Short Term



PHA

LOPA

SRS

SIL Calcs

Testing

Operational Data

Historian

SIF Time in Bypass

Short Term Risk Index (One scenario)

Designed ST Safety Risk = **TMEL (for safety) x Safety Severity**
(the assumption here is that with the designed IPLs, the TMEL has been met)

Actual ST Safety Risk = **IEF x [(PFD of non-SIF IPL x SIF PFD) x (Time SIF NOT in Bypass/SST) + (PFD of non-SIF IPL) x (Time SIF in Bypass/SST)] x Safety Severity**

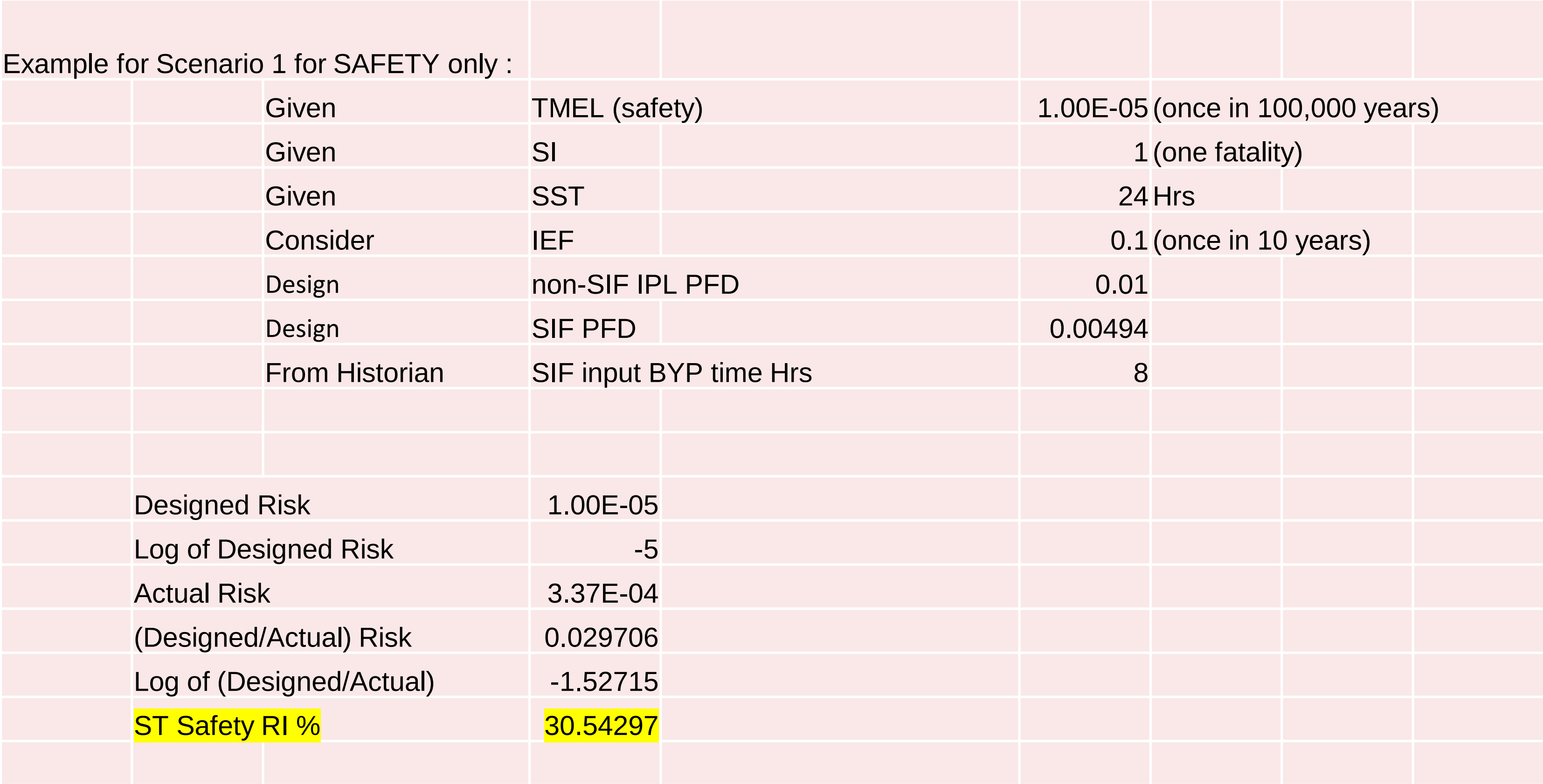
where :
IEF = Initiating Event Frequency
SST = Short Sample Time

ST Safety Risk Index = **[Log of (Designed Safety Risk/Actual Safety Risk) / Log of Designed Safety Risk)]*100**

ST Risk Indication calculation (One scenario)

In our example, if SIF-1 input (PT-2) in **24 Hours period :**

- **bypassed for 8 Hours**
- SIF design PFD = 4.94E-03

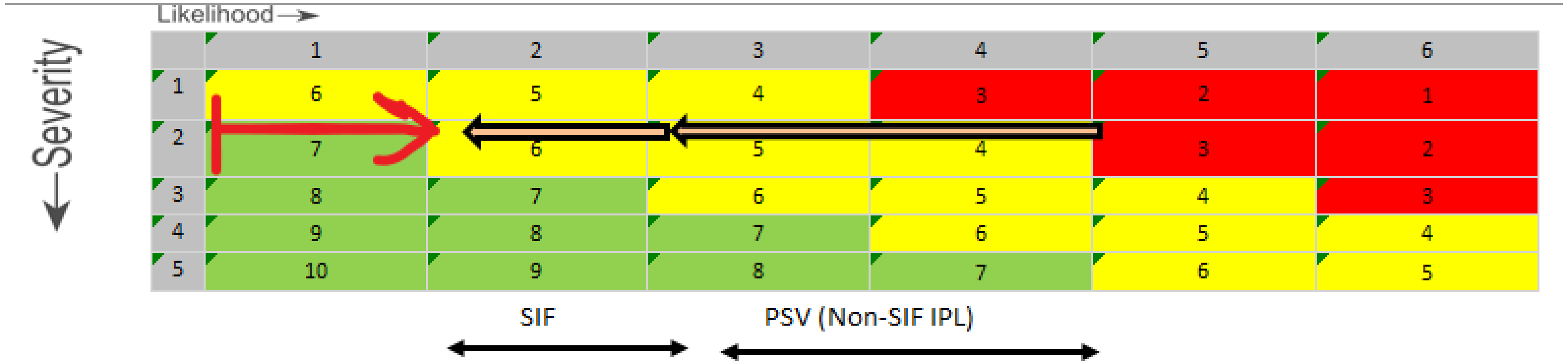


Example for Scenario 1 for SAFETY only :						
		Given	TMEL (safety)		1.00E-05	(once in 100,000 years)
		Given	SI		1	(one fatality)
		Given	SST		24	Hrs
		Consider	IEF		0.1	(once in 10 years)
		Design	non-SIF IPL PFD		0.01	
		Design	SIF PFD		0.00494	
		From Historian	SIF input BYP time Hrs		8	
	Designed Risk		1.00E-05			
	Log of Designed Risk		-5			
	Actual Risk		3.37E-04			
	(Designed/Actual) Risk		0.029706			
	Log of (Designed/Actual)		-1.52715			
	ST Safety RI %		30.54297			

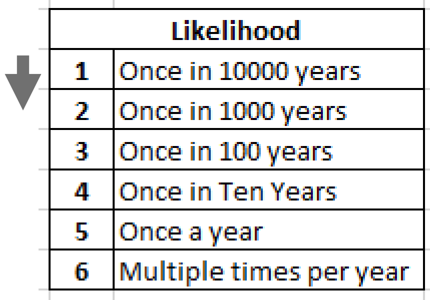
Risk Reduction (Based on ST Risk Index)

From the HAZOP risk matrix for this Process :

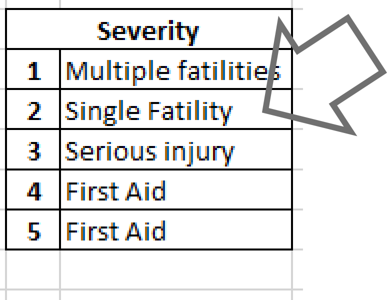
1. Short Term sample time : 24 Hours
2. SIF Bypass time : 8 hours
3. Calculated Safety ST RI = 30% (Approx)


Likelihood
Severity
SIF
PSV (Non-SIF IPL)

	1	2	3	4	5	6
1	🟨 6	🟨 5	🟨 4	🟥 3	🟥 2	🟥 1
2	🟩 7	🟨 6	🟨 5	🟨 4	🟥 3	🟥 2
3	🟩 8	🟩 7	🟨 6	🟨 5	🟨 4	🟥 3
4	🟩 9	🟩 8	🟩 7	🟨 6	🟨 5	🟨 4
5	🟩 10	🟩 9	🟩 8	🟩 7	🟨 6	🟨 5



Likelihood	
1	Once in 10000 years
2	Once in 1000 years
3	Once in 100 years
4	Once in Ten Years
5	Once a year
6	Multiple times per year



Severity	
1	Multiple fatilities
2	Single Fatility
3	Serious injury
4	First Aid
5	First Aid

LOPA TMEL (Single Fatality) :

1E-05 per year

Short Term Risk Index (Multiple scenarios)

Designed ST Safety Risk (Multiple) =
∑ (TMEL (for safety) x Safety Severity)
(the assumption here is that with the designed IPLs, the TMEL has been met for all scenarios)

Actual ST Safety Risk (Multiple) =
∑ (IEF x [(PFD of non-SIF IPL x SIF PFD) x (Time SIF NOT in Bypass/SST)
+ (PFD of non-SIF IPL) x (Time SIF in Bypass/SST)] x Safety Severity)

where :
IEF = Initiating Event Frequency
SST = Short Sample Time

ST Safety Risk Index (Multiple) = **[Log of (Designed Safety Risk (Multiple)/Actual Safety Risk(Multiple)) / Log of Designed Safety Risk(Multiple))]*100**

Worst actor of ST Safety Risk Index = **Highest ST Safety Risk Index (ONE scenario)**

Honeywell
THE POWER OF CONNECTED

Long Term Risk Index

Assumptions for LT Risk Index equations:

- “Safety” is the driver for this haz. event (not Commercial and Environment)
- PFDactual of SIF and non-SIF IPL may not be the same as PFD per design
- The SIF input has 1oo1 input voting

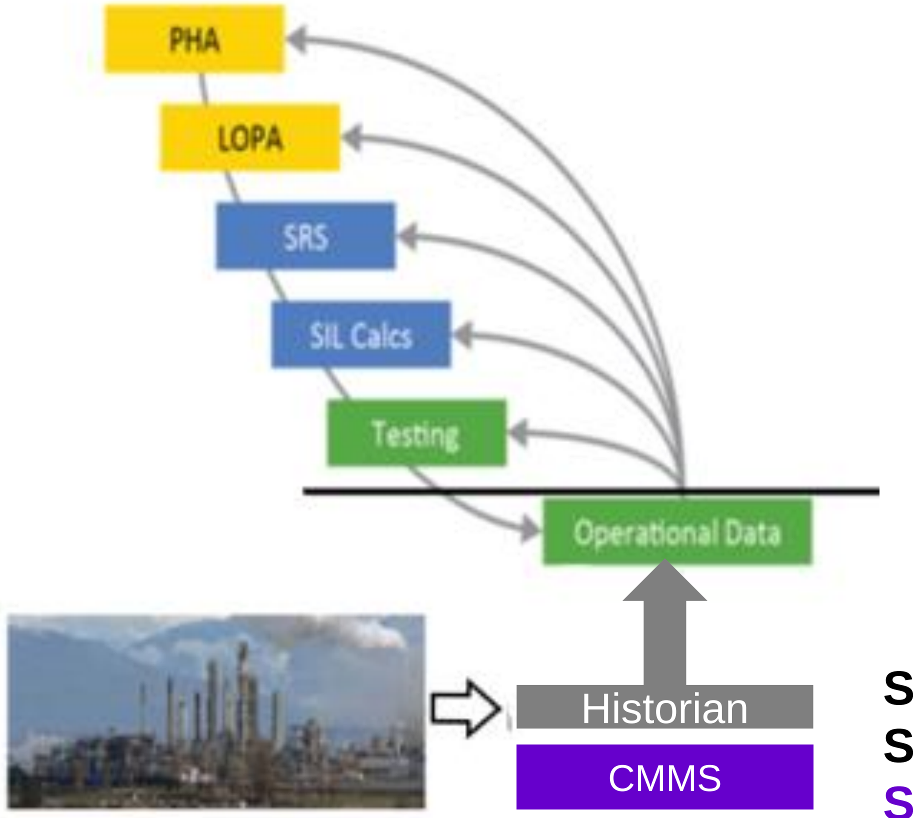
Variable which effects Long Term (LT) Risk Index

- **SIF demand rate**. If this is greater than the assumed IEF, then SIF demand rate will be considered in the “Actual LT Safety Risk” equation
- **SIF “Time in Bypass”** over the Long Term period
- **IPLs On time testing**. If this is different than what was considered during design, then this will effect the PFDactual of the IPLs

This data is collected from the Historian and plant CMMS (Computer Maintenance Management System) over the specified Long term.

Honeywell
THE POWER OF **CONNECTED**

Design and Historian data compared – Long Term



PHA

LOPA

SRS

SIL Calcs

Testing

Operational Data

Historian

CMMS

SIF Time in Bypass
SIF Demands
SIF OnTime testing

Honeywell
THE POWER OF CONNECTED

Long Term Risk Index (One Scenario)

Designed Long Term Safety Risk = **TMEL (for safety) x Safety Severity**
(the assumption here is that with the designed safeguards,TMEL has been met)

Actual LT Safety Risk = **SIF demands x [(PFDactual of non-SIF IPL x SIF PFDactual) x (Time SIF NOT in Bypass/LST) + (PFDactual of non-SIF IPL) x (Time SIF in Bypass/LST)] x Safety Severity**

where :
SIF demands considered as Initiating Event Frequency if SIF demands > IEF
LST = Large Sample Time
PFDactual (for SIF and IPL) varies based on “Real test intervals” vs “Design Test intervals”

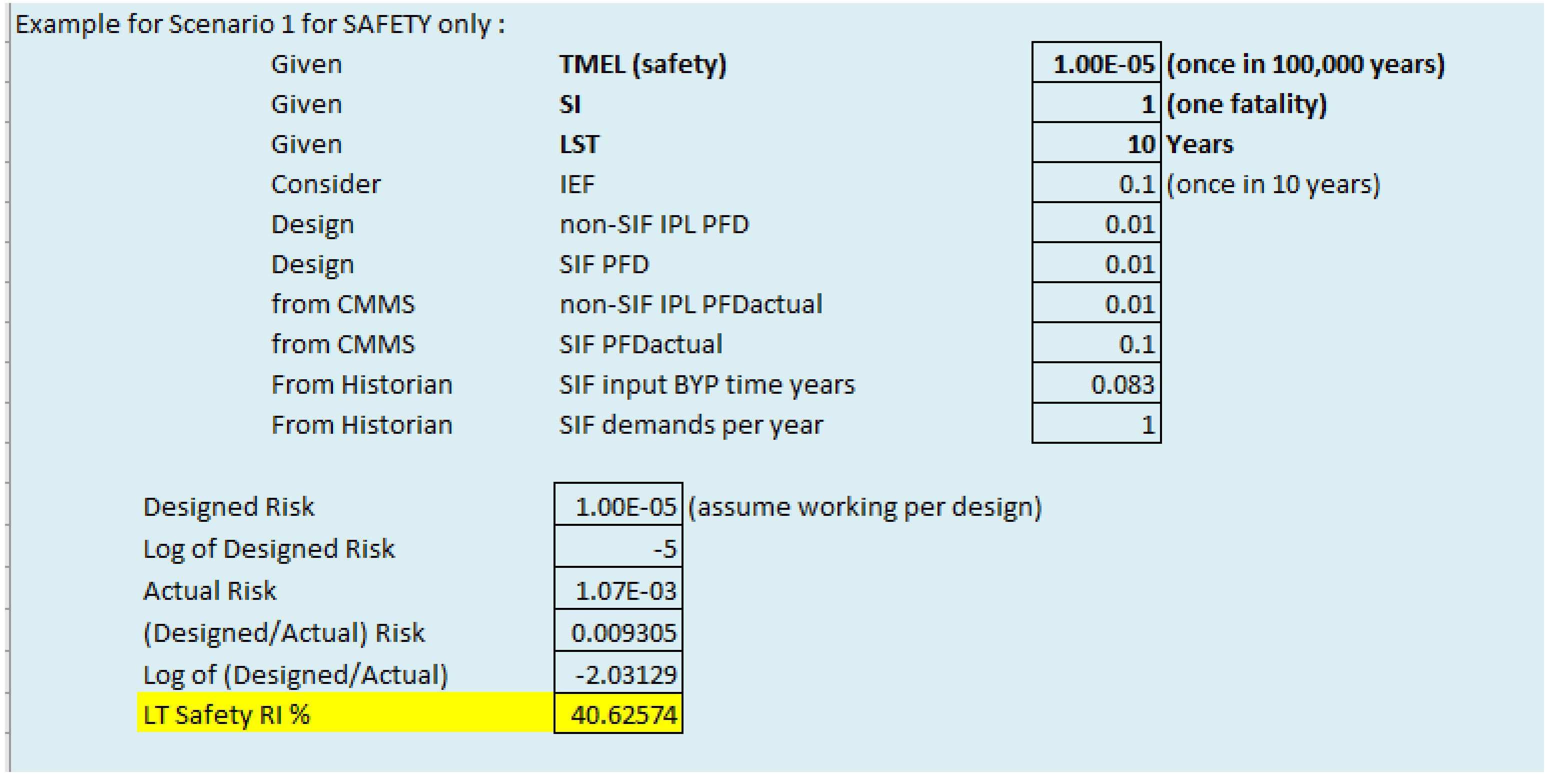
LT Safety Risk Index = **[Log of (Designed Safety Risk/Actual Safety Risk) / Log of Designed Safety Risk)]*100**

Honeywell
THE POWER OF CONNECTED

LT Risk Indication calculation (One scenario)

In our example, if SIF-1 input (PT-2) in ONE year period :

- bypassed for ONE month
- SIF has ONE demand (design IEF = 0.1 per year)
- SIF PFDactual = 0.1 (design PFD = 4.94E-03)



Example for Scenario 1 for SAFETY only :

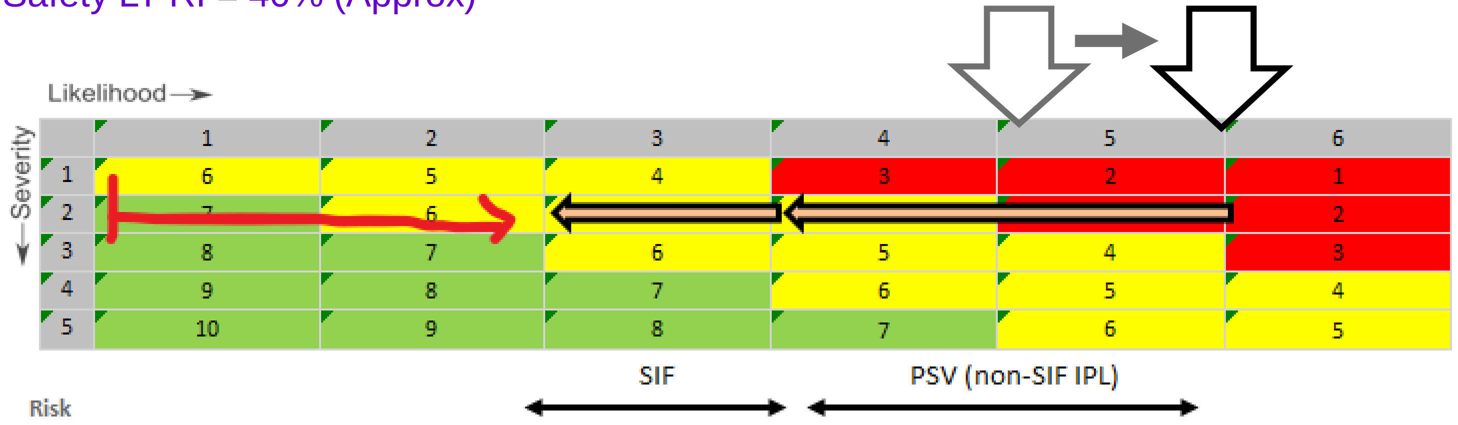
Given	**TMEL (safety)**	**1.00E-05**	**(once in 100,000 years)**
Given	**SI**	**1**	**(one fatality)**
Given	**LST**	**10**	**Years**
Consider	IEF	0.1	(once in 10 years)
Design	non-SIF IPL PFD	0.01	
Design	SIF PFD	0.01	
from CMMS	non-SIF IPL PFDactual	0.01	
from CMMS	SIF PFDactual	0.1	
From Historian	SIF input BYP time years	0.083	
From Historian	SIF demands per year	1	

Designed Risk	1.00E-05	(assume working per design)
Log of Designed Risk	-5	
Actual Risk	1.07E-03	
(Designed/Actual) Risk	0.009305	
Log of (Designed/Actual)	-2.03129	
LT Safety RI %	40.62574	

Risk Reduction (Based on LT Risk Index)

From the HAZOP risk matrix for this Process :

1. Long Term sample time : ONE year
2. SIF Bypass time : ONE month
3. SIF demand : ONE demand in ONE year
4. SIF PFDactual = 0.05
5. Calculated Safety LT RI = 40% (Approx)



Severity \ Likelihood	1	2	3	4	5	6
1	6	5	4	3	2	1
2	7	6				2
3	8	7	6	5	4	3
4	9	8	7	6	5	4
5	10	9	8	7	6	5

	Likelihood
1	Once in 10000 years
2	Once in 1000 years
3	Once in 100 years
4	Once in Ten Years
5	Once a year
6	Multiple times per year

	Severity
1	Multiple fatilities
2	Single Fatility
3	Serious injury
4	First Aid
5	First Aid

LOPA TMEL (Single Fatality) :

1E-05 per year

Long Term Risk Index (Multiple scenarios)

Designed LT Safety Risk (Multiple) =
∑ (TMEL (for safety) x Safety Severity)
(the assumption here is that with the designed safeguards, the TMEL has been met for all scenarios)

Actual LT Safety Risk (Multiple) =
∑ (SIF demands x [(PFDactual of non-SIF IPL x SIF PFDactual) x (Time SIF NOT in Bypass/LST) + (PFDactual of non-SIF IPL) x (Time SIF in Bypass/LST)] x Safety Severity)
Where :
SIF demands considered as Initiating Event Frequency if SIF demands > IEF
LST = Large Sample Time
PFDactual (for SIF and IPL) varies based on “Real test intervals” vs “Design Test intervals”

LT Safety Risk Index (Multiple) = **[Log of (Designed Safety Risk (Multiple)/Actual Safety Risk(Multiple)) / Log of Designed Safety Risk(Multiple))]*100**

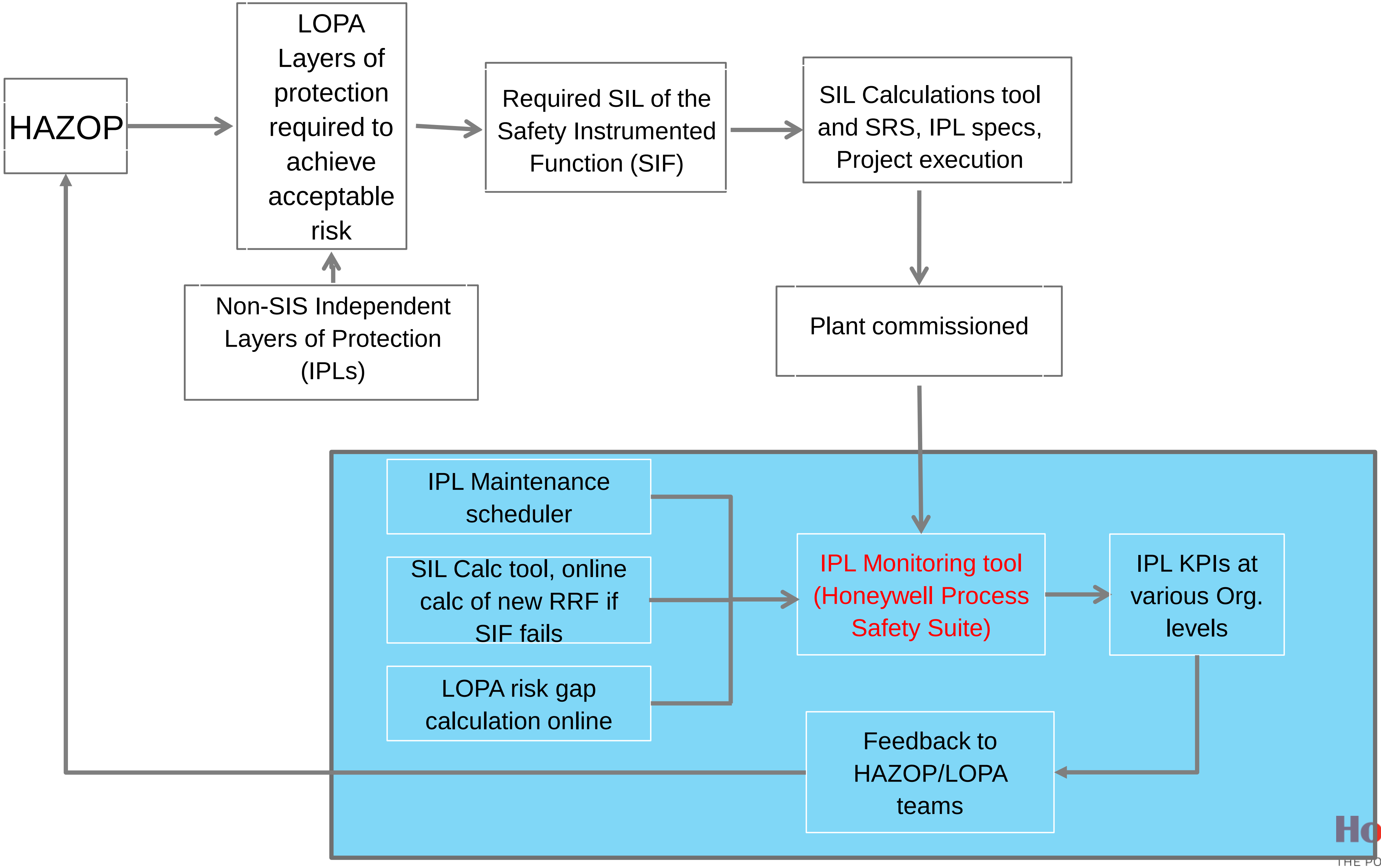
Worst actor of LT Safety Risk Index = Highest LT Safety Risk Index (ONE scenario)

Process Plant Safety Risk Index

At the Corporate level and Plant level:

- Process Plant Safety Risk Index (Long Term) = LT Safety Risk Index (Multiple)
- Worst actor for Process Plant Safety Risk Index (Long Term) = Scenario with Highest LT Safety Risk Index
- This will give Senior management at the corporate an insight on how the plant has been running based on the Long Term safety track record
- The Long Term Safety Risk Index will help the Plant / Operations Manager to reanalyze risk and take appropriate action based on some of the worst actors which are driving the Safety Risk index up.

Safety Life Cycle process……


HAZOP
LOPA Layers of protection required to achieve acceptable risk
Required SIL of the Safety Instrumented Function (SIF)
SIL Calculations tool and SRS, IPL specs, Project execution
Non-SIS Independent Layers of Protection (IPLs)
Plant commissioned
IPL Maintenance scheduler
SIL Calc tool, online calc of new RRF if SIF fails
LOPA risk gap calculation online
IPL Monitoring tool (Honeywell Process Safety Suite)
IPL KPIs at various Org. levels
Feedback to HAZOP/LOPA teams

Honeywell
THE POWER OF CONNECTED

Honeywell’s Process Safety Suite

Compliant with ISA-84 / IEC 61511

Today the key information in the Process Safety Lifecycle is handled through many manual and disconnected steps.

Honeywell’s Process Safety Suite automates this lifecycle helping to reduce errors, lower costs, continuously monitor operations for hazard conditions and provide safety alerts in a timely fashion.

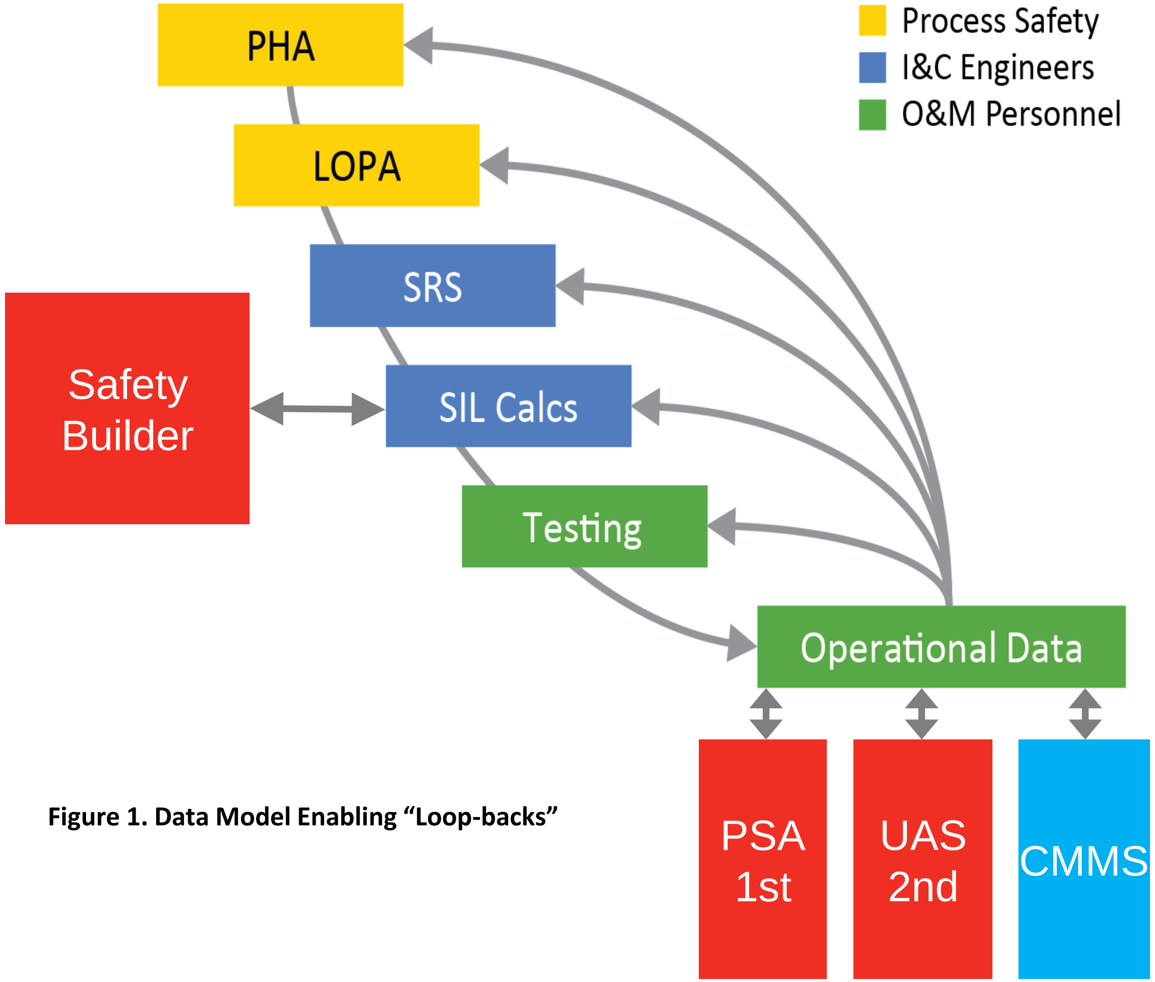


Figure 1. Data Model Enabling “Loop-backs”

Conclusion

- Functional Safety is a subset of Process Safety
- IEC61511, ISA84.00.01 (ISA 61511) are functional safety standards used in the Process industry
- Functional safety standards are normative and not prescriptive. These are based on Risk assessment and Risk management
- Functional safety standards define a “safety life cycle”, which need to be managed from “cradle” to “grave” by the end user
- Presently these standards are not mandated by law in any part of the world but are considered as “Good Engineering Practices “

Thank You...

THE POWER OF CONNECTED