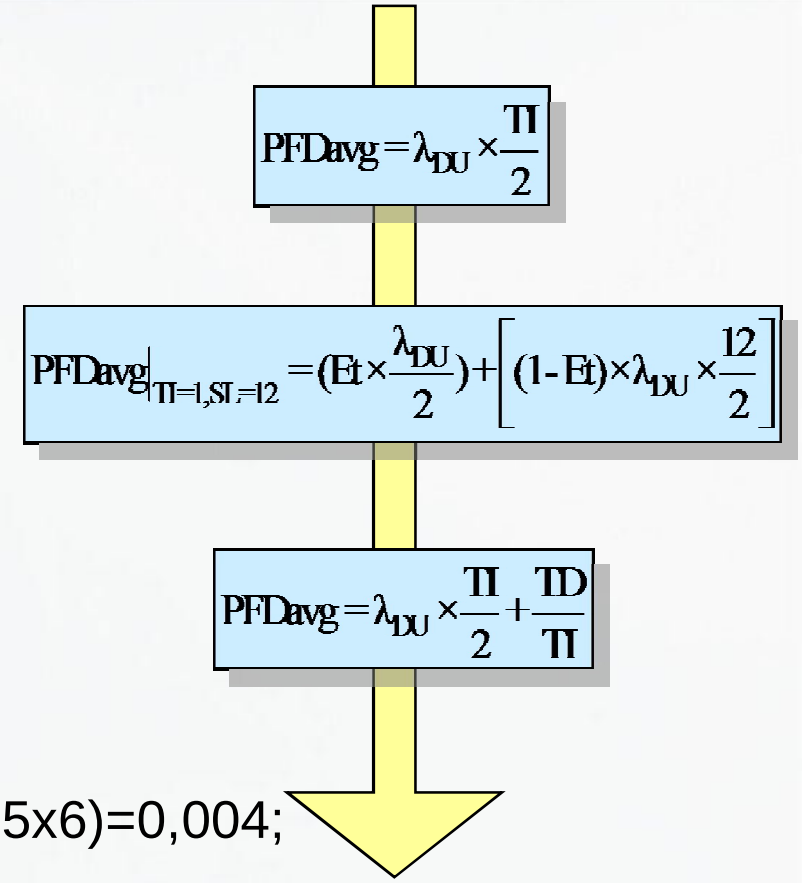
Test Effectiveness & Duration on PFDavg

Example f:

λdu = 0,0025 / yr
TI = 1 yr
TD = 8 hrs
TE = 80%
SL = 12 yrs



At installation:

PFDavg = 0,0025/2 = 0,00125;

RRF = 1/ PFDavg = 1/0,00125 = **800**

After one year:

PFDavg=(0,8x0,00125)+(0,0009)+(0,2x0,0025x6)=0,004;

RRF = 1/PFDavg = 1/0,004 = **250**

Note: **As can be noted the initial SIL level is lowered by influence of T-proof tests effectiveness & duration.**

Specifications

It make sense to include in specification:

- Required minimum T-proof Test Time Intervals;
- Max. percentage used to claim the SIL level;

Eg: SIL 2; T-proof T.I. 5 years; Max 10% of PFD.

Better to include minimum SIL level required in RRF

Eg: SIL 2 Minimum RRF of 500.

Claiming SIL 2 / RRF 500 or a SIL 2 / RRF 150. Not the same!

INTERNATIONAL
TECHNOLOGY FOR SAFETY

G.M. International S.r.l
Via San Fiorano, 70
20852 Villasanta (Milano)
ITALY

www.gmintsrl.com
info@gmintsrl.com

ISA Delhi - PNID 2011

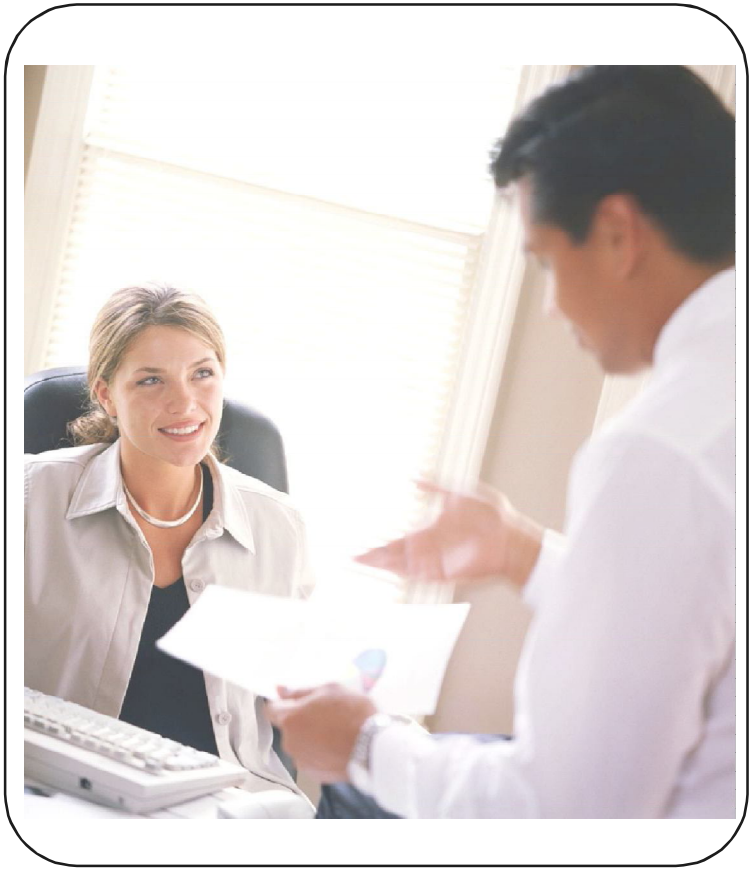
Safety Instrumented Systems for Achieving Process Safety

Amit Aglave
Safety Consultant
TUV FS ENG ID: 2827 / 10
Honeywell Automation India Ltd.

Honeywell

Agenda

- Safety Trends
- Process Safety
- Functional Safety Standards
- Key Safety Applications
- Application of Safety Standards
- Design Considerations
- Summary



What may happen when a process gets out of control

OR

Safeguarding Equipments Fail?

Honeywell

Results of Failure are devastating…

Deep Water Horizon, Gulf of Mexico - 2010

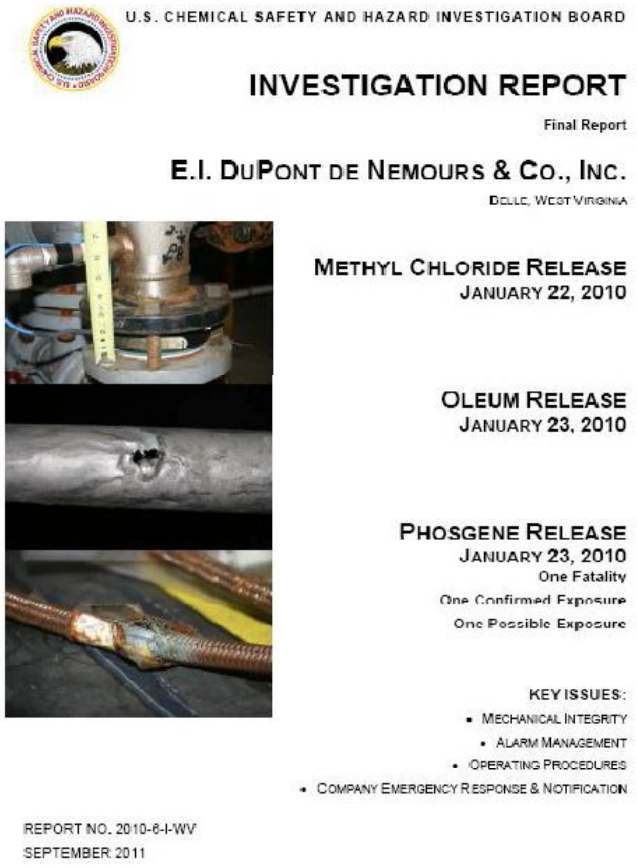
Buncefield Oil Terminal, UK - 2005

Union Carbide, Bhopal, India - 1984

Phillips Petroleum, Pasadena, USA - 1989

Accidents are very expensive – Comprehensive Process Safety is Key

What can we learn from these incidents?


U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

INVESTIGATION REPORT

Final Report

E.I. DUPONT DE NEMOURS & CO., INC.

DELLE, WEST VIRGINIA

METHYL CHLORIDE RELEASE
JANUARY 22, 2010

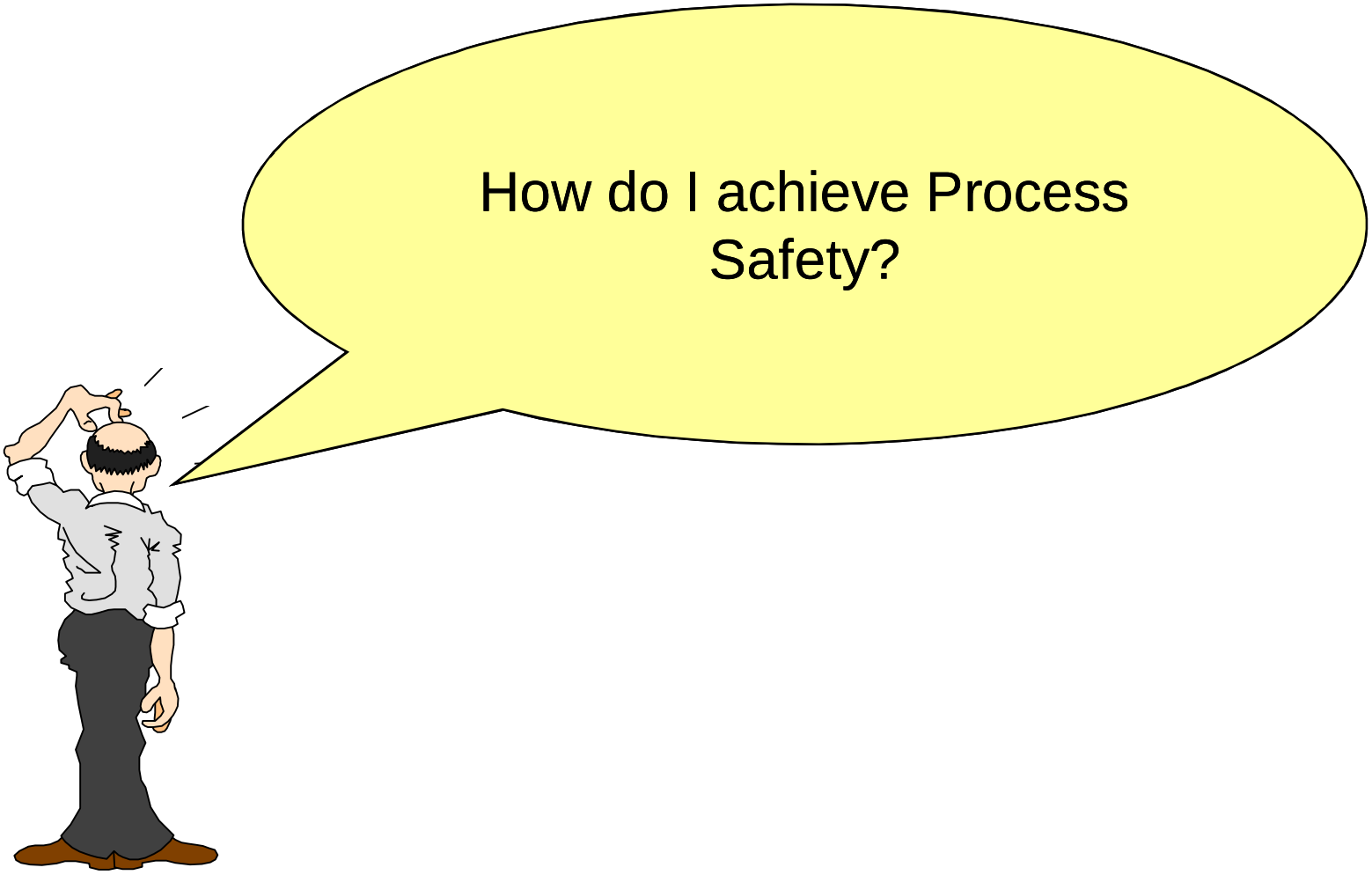
OLEUM RELEASE
JANUARY 23, 2010

PHOSGENE RELEASE
JANUARY 23, 2010
One Fatality
One Confirmed Exposure
One Possible Exposure

KEY ISSUES:
- MECHANICAL INTEGRITY
- ALARM MANAGEMENT
- OPERATING PROCEDURES
- COMPANY EMERGENCY RESPONSE & NOTIFICATION

REPORT NO. 2010-6-I-WV
SEPTEMBER 2011

- Study the reports
  - They come with recommendations
- Continued focus on safety standards
  - Not limited to the Equipment Under Control but also
    - Procedures
    - Competence of people
- Increase focus on leading indicators, not just the process parameters (high pressure, temperature etc…%)


How do I achieve Process Safety?

Ways to Achieve Process Safety.

- PROCESS DESIGN: [illegible]
  - DESIGN PHASE [illegible]
- *Inherent* — Eliminating the hazard by using materials and process conditions which are non-hazardous.
- *Passive* — Minimizing the hazard by process and equipment design features which reduce either the frequency or consequence of the hazard without the active functioning of any device.
- *Active* — Using facilities to detect and correct process conditions: [illegible]
  - monitoring systems for hazards that develop over a long term
  - and emergency shutdown systems to detect and correct process deviations
- *Procedural* — [illegible]
- Safe operating procedures and operator training
- Administrative safety checks
- Management of Change
- Plant emergency response
  - Certified Components and Instruments
  - Location of facilities – separation of ignition sources and fuels from other facilities
  - Design equipment for design pressure in excess of the adiabatic pressure from a reaction.
  - *Minimize* — Reduce quantities of hazardous substances
  - *Substitute* — Use less hazardous substances
  - *Moderate* — Use less hazardous process conditions, less hazardous forms of materials, or configure facilities to minimize impact from hazardous material releases or uncontrolled energy release
  - *Simplify* — Configure facilities to simplify operation
- *TARGET IS A FAIL-SAFE INSTALLATION*

Honeywell

Active Safety achieved by ?????

General Purpose PLC

Safety PLC

?????

Process Operations

F&G Safety System

SIS controlled

Mechanical Shutdown Action

Trip Level

ESD Safety System

Emergency Shutdown Action

Operator Action

High Alarm Level

Process Operators

High Level

process value

Low Level

Process PLC/DCS

Time

Functional Safety Standards !

IEC 61508

Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems

- IEC 61508 applies to safety-related systems when one or more of such systems incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices.

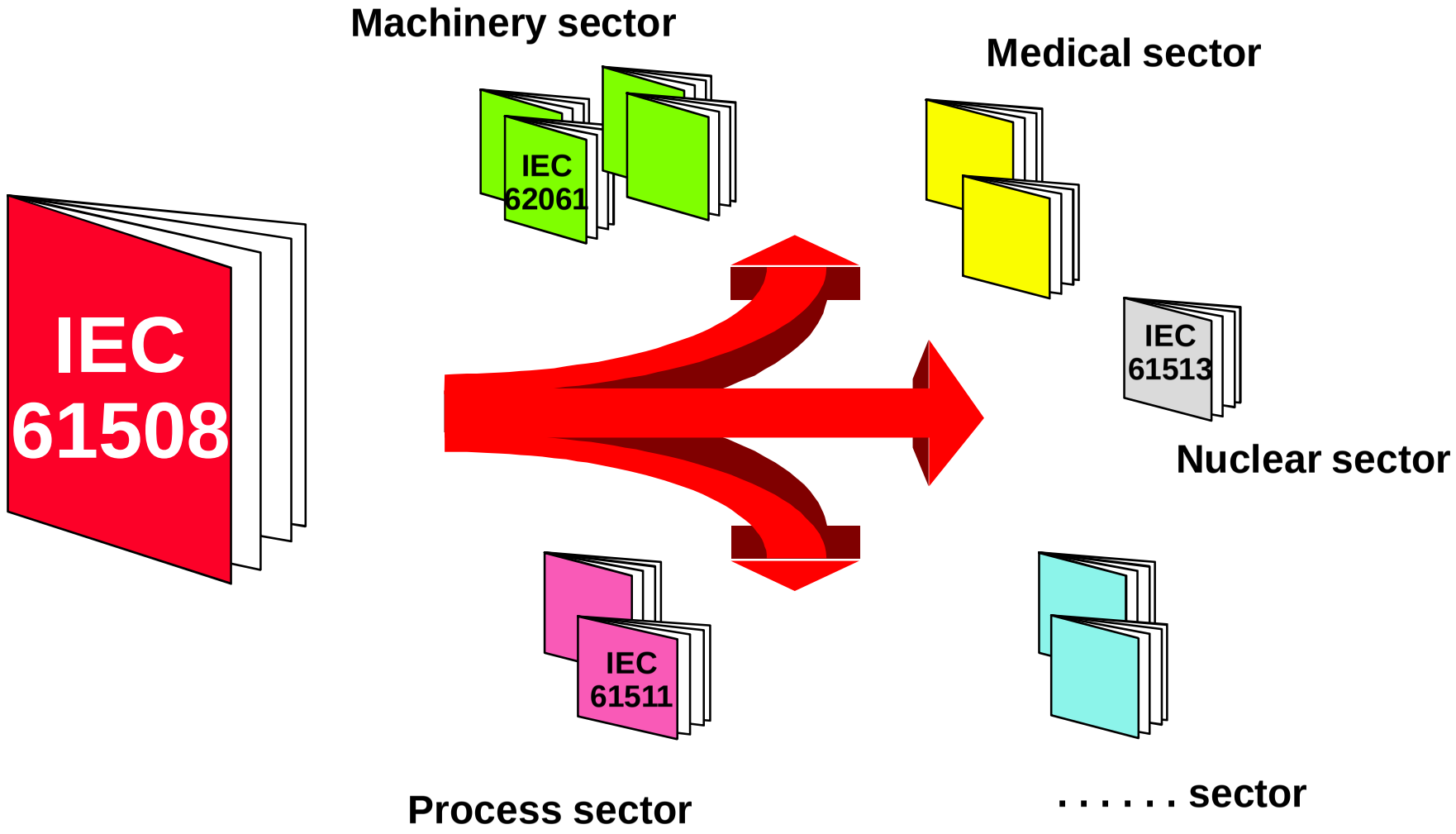
  It covers possible hazards caused by failure of the safety functions to be performed by the E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock etc).

  It is generically based and applicable to all E/E/PE safety-related systems irrespective of the application.

IEC 61511

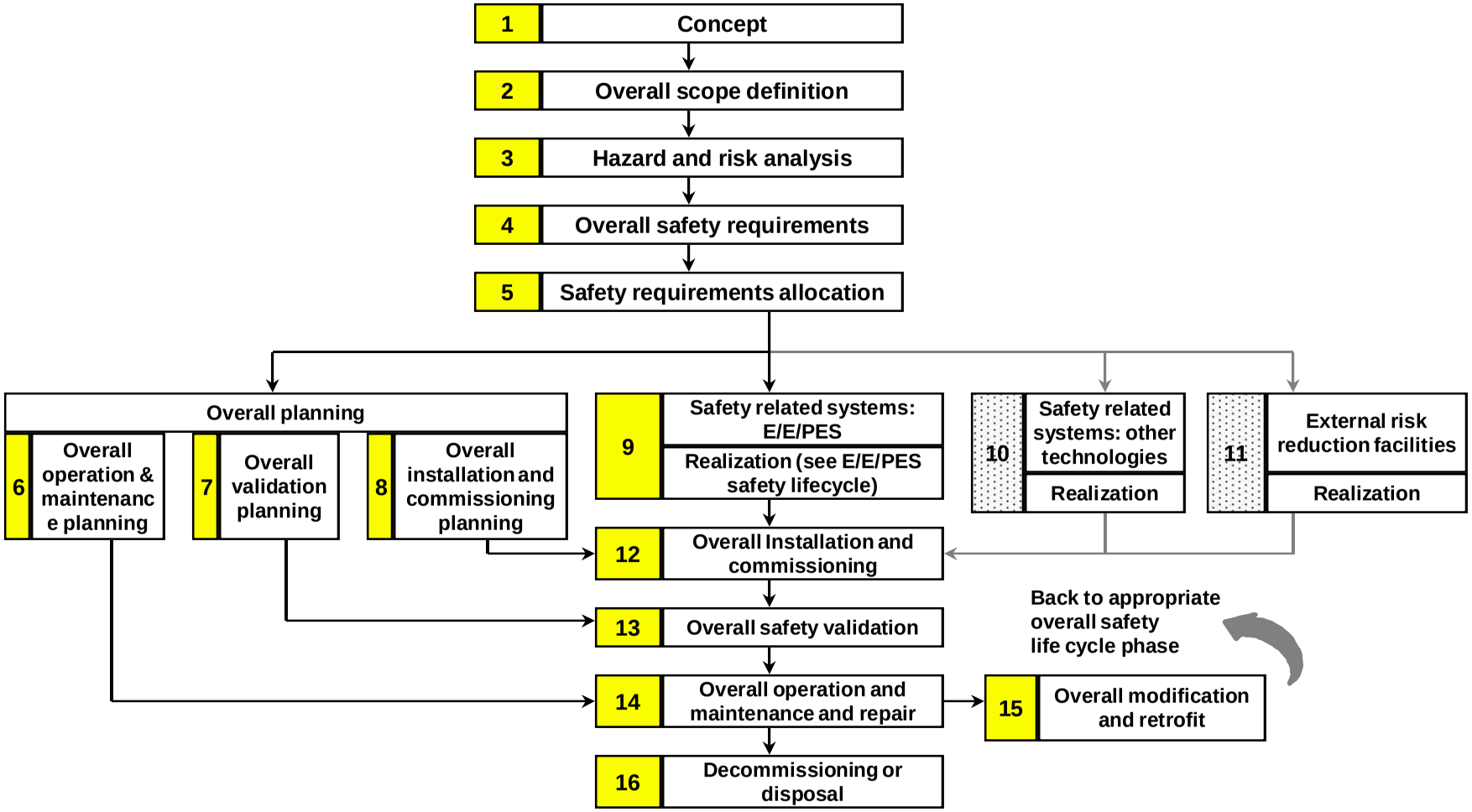
Functional Safety: Safety Instrumented System (SIS) for Process Industry Sector

Generic and application sector standards



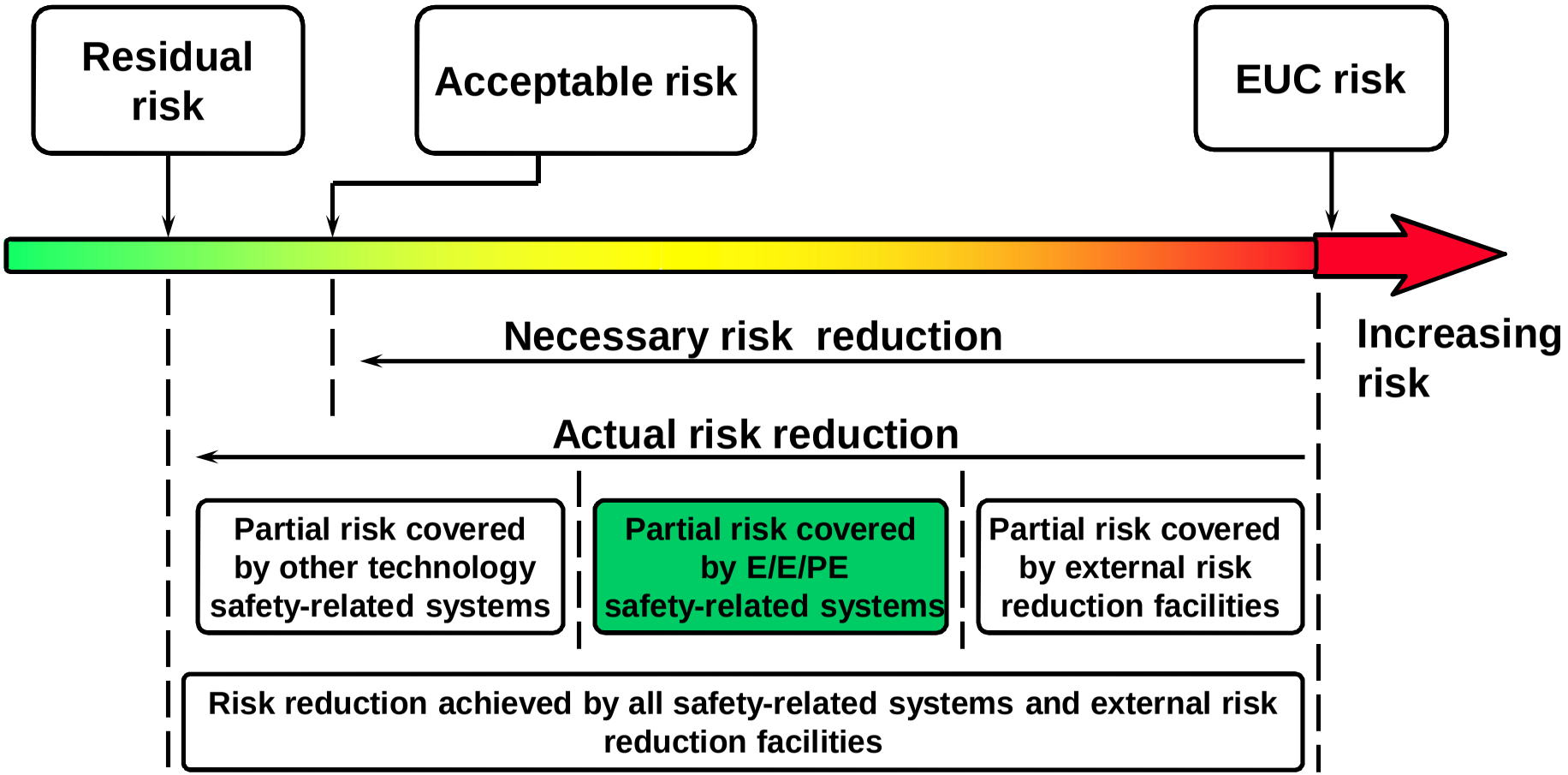
Honeywell

IEC 61508 - Key Item 1 - Safety Lifecycle



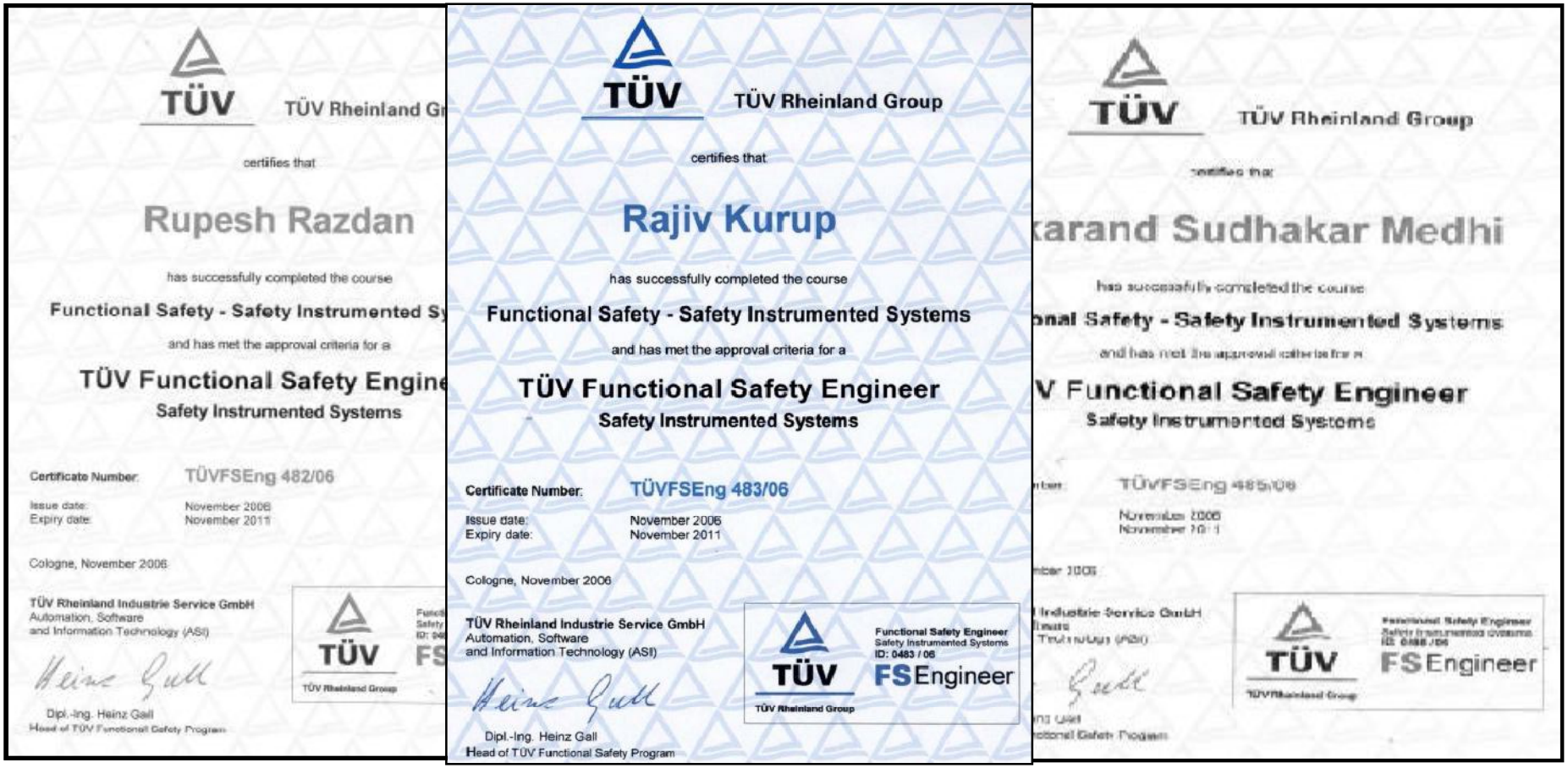
Honeywell

IEC 61508 - Key Item 2 - Risk Reduction



Honeywell

IEC 61508 - Key Item 3 - Competence of People



TÜV Rheinland Gr

certifies that

Rupesh Razdan

has successfully completed the course

Functional Safety - Safety Instrumented Sy

and has met the approval criteria for a

TÜV Functional Safety Engine

Safety Instrumented Systems

Certificate Number: TÜVFSEng 482/06

Issue date: November 2006
Expiry date: November 2011

Cologne, November 2006

TÜV Rheinland Industrie Service GmbH
Automation, Software
and Information Technology (ASI)

Dipl.-Ing. Heinz Gall
Head of TÜV Functional Safety Program

TÜV Rheinland Group

certifies that

Rajiv Kurup

has successfully completed the course

Functional Safety - Safety Instrumented Systems

and has met the approval criteria for a

TÜV Functional Safety Engineer

Safety Instrumented Systems

Certificate Number: TÜVFSEng 483/06

Issue date: November 2006
Expiry date: November 2011

Cologne, November 2006

TÜV Rheinland Industrie Service GmbH
Automation, Software
and Information Technology (ASI)

Dipl.-Ing. Heinz Gall
Head of TÜV Functional Safety Program

Functional Safety Engineer
Safety Instrumented Systems
ID: 0483 / 06
FS Engineer

TÜV Rheinland Group

karand Sudhakar Medhi

onal Safety - Safety Instrumented Systems

V Functional Safety Engineer

Safety Instrumented Systems

FS Engineer

Honeywell

IEC 61508 - Key Item 4 - Safety Integrity Levels

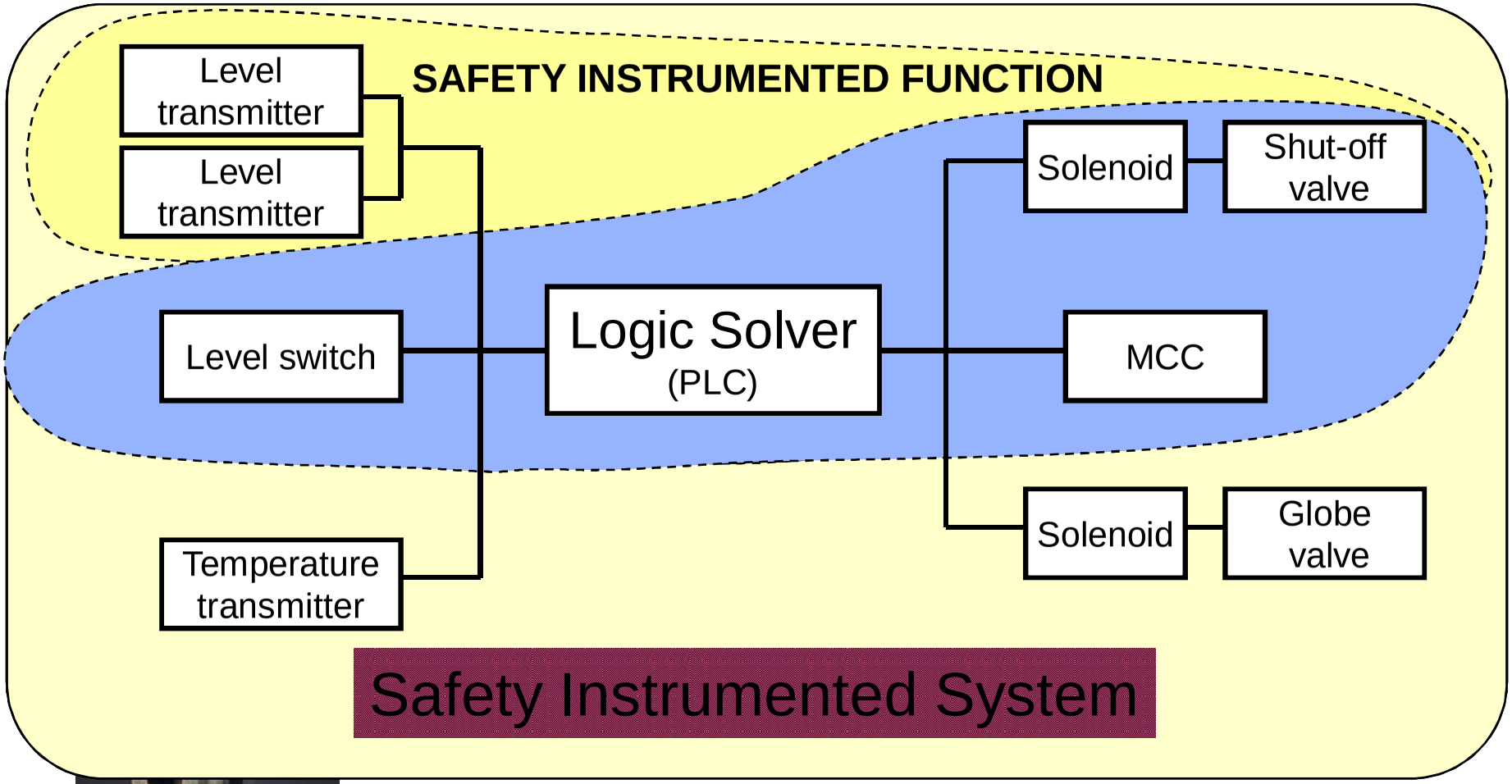
Integrity Level	Safety Availability Required	Safety Unavailability	Equivalent RRF
4	> 99.99%	0.001% - 0.01%	>10,000
3	99.9 - 99.99%	0.01% - 0.1%	1,000 - 10,000
2	99 - 99.9%	0.1% - 1%	100 - 1,000
1	90 - 99%	1% - 10%	10 - 100
-		*PFD*	(Control - N/A)

Risk reduction Factor (RRF)

Honeywell

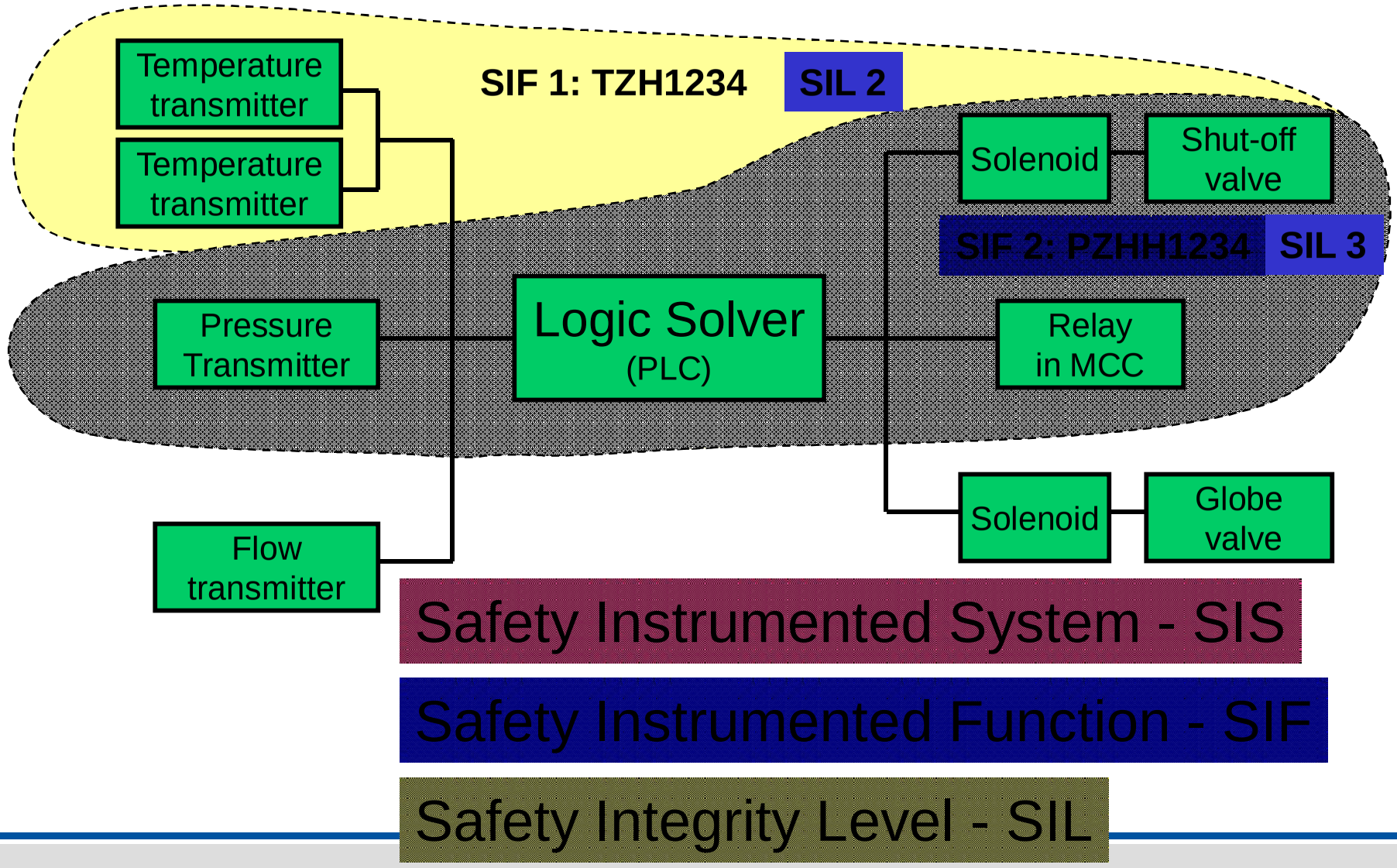
IEC 61508 - Key Item : Safety Integrity Levels

So to what does this SIL applies?



Honeywell

SIS, SIF and SIL



Honeywell

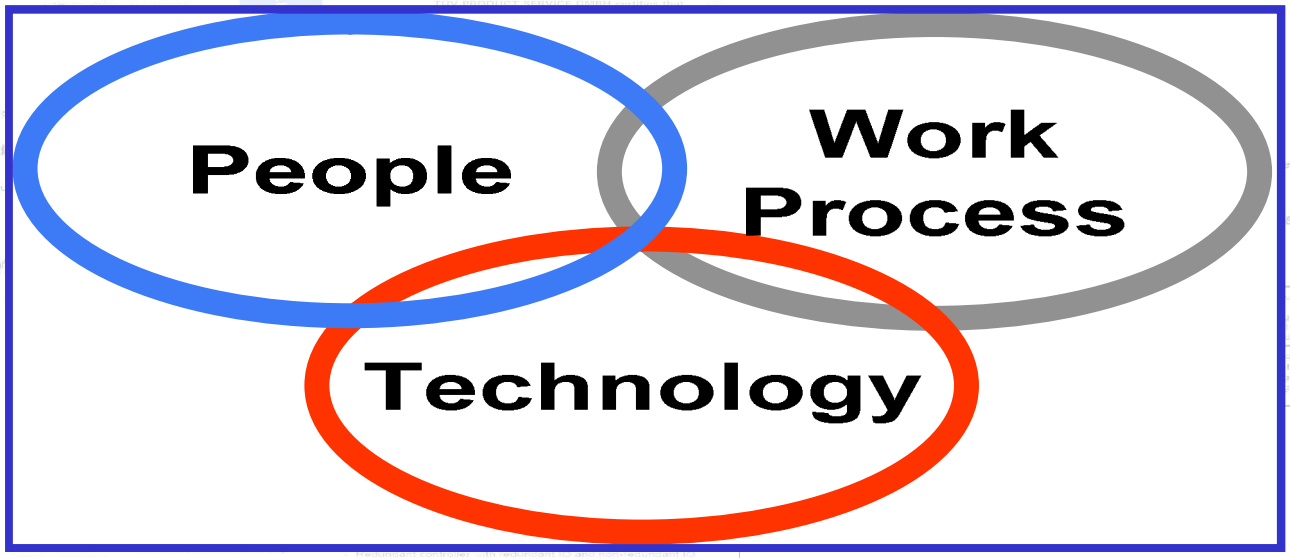
BUT… SIL is much more than PFD!

- Hardware design requirements
  - Safe Failure Fraction (SFF)
  - Hardware Fault Tolerance (HFT)
  - Process Safety Time (PST)
  - Diagnostic Coverage (DC) and off-line proof Test Intervals (TI)
- SR-software development requirements
- Techniques, methods, procedures to be applied
- …

This all, to prevent or minimize systematic failures, common cause failure, human errors, etc.

Honeywell

Compliance to IEC61508 : What is required?



Honeywell

IEC61511 - Segregation of Layers of Safety

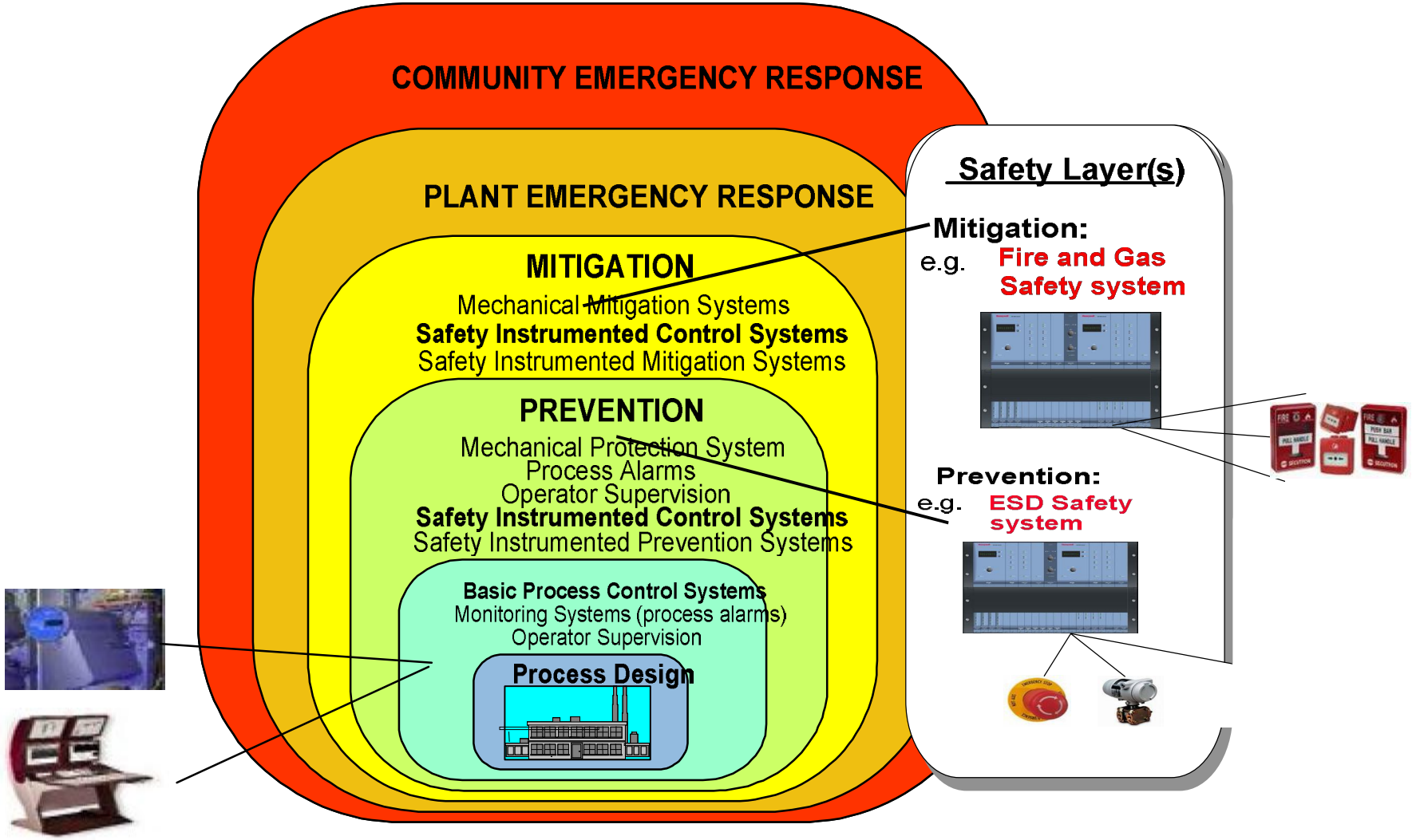


Figure 9 of IEC 61511

Honeywell

Functional Safety standards helps for . . .

Achieving Reliability

Robustness maximize process availability

- SIL 3 Safety Instrumented system
- Full Redundancy (Processor, IO, Communication)
- Support for Integrated and Segregated topologies
- System Audits
  - Modifications, maintenance practices, diagnostic messages
  - Environmental consideration (corrosion)
- People Certification

Operating Efficiently

Remote management and data exchange

- TUV approved On Line Modification technique
  - H/w additions and changes
  - Application additions and changes
  - Firmware updates
- Remote management
  - Configurable per Safety System
- Easy data exchange with process controllers

Maximize uptime

Key Safety Applications…

The typical applications of the Safety Instrumented Systems (SIS) for process industry are:

- *Emergency Shutdown Systems (ESD)*
  For Shutdown of the plant/processes
- *Process Shutdown Systems (PSD)*
  For Shutdown of equipment or unit
- *Fire & Gas Protection (FGS)*
  For plant wide protection against fires and gas leaks (NFPA72 applies)
- *Burner Management System (BMS)*
  For Boilers, HRSG Boilers, Heaters, Furnaces (NFPA85 / NFPA86 applies)

High Integrity Pressure Protection System (HIPPS)
For protection against over pressures – typically on oil platforms

- *Tunnel Ventilation System (TVS)*
  For applications of tunnel ventilation for Metro/Rail Tunnels
- *Many more . . . . .*

Honeywell

What is a BMS and what does it do?

1.3.27 Burner Management System.

A burner management system is responsible for the safe start-up, operation, and shutdown of a burner.

The control system dedicated to combustion safety and operator assistance in the starting and stopping of fuel preparation and burning equipment and for preventing mis-operation of and damage to fuel preparation and burning equipment.

– NFPA 85

The BMS:

- Controls – Purge sequence, Light off sequence for Pilot and Main Burner;
- Continuously monitors Interlocks, Fuel Valve Positions, Flame status and Field Devices;
- Automatically shutdowns individual or all burners for protection upon violation of process limits;
- links the burner management system of auxiliary boilers to the main burner management system and with the basic process control system

BMS Standards and Solutions

What is NFPA 85?

–NFPA 85 is a Boiler and Combustion system Hazards code that provides common and specific requirements for-
–Single burner boiler
–Multiple burner boiler
–Heat recovery Steam Generator etc

What is NFPA 86?

NFPA 86 is a standard for Ovens and Furnaces and applies to Class A and Class B ovens, dryers and furnaces

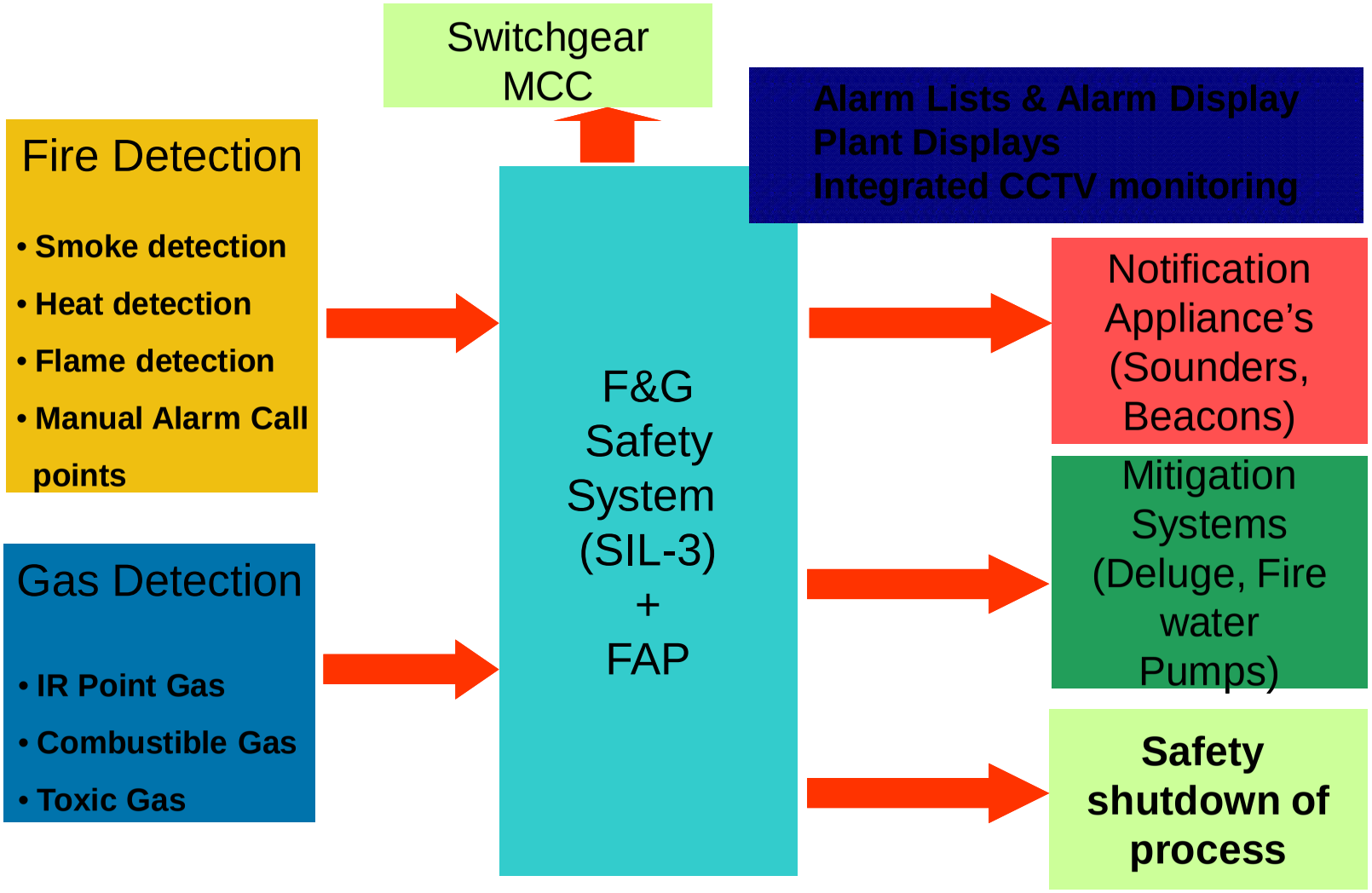
Why is Fire and Gas Safety Solution required?

The intent is “fire and gas related risk reduction” and is defined as the application of technological and administrative measures to reduce fire or explosion risk to a tolerable level.

Reduced fire risk means fewer fire losses, less production downtime, better employee morale, better public relations, and greater profit potential.

Honeywell

Fire & Gas System Components



Standards governing F&G

NFPA – 72 ➔ **"***National Fire Alarm Code***"**

EN54 -> Europe " *Fire Protection Norm***"**

A.1.9.5 The user of this code is encouraged to use judgment in the application of these guidelines for all process and safety functions contained in a distributed control system.

(4) The hardware should be capable of stable dynamic control.
(5) The hardware should be capable of thorough self-diagnosis.
(6) Consideration should be given to all levels and types of electrical interference that can be tolerated by the hardware without compromising its reliability or effectiveness.
(7) Fail-safe operation should be obtained through a thorough and complete analysis of each control loop and by providing for a failure of that loop (i.e., valve/actuator) to cause a fail-safe position.

Self diagnostics.. An essence of safety

Fail Safe operation to ensure safety

Standards governing F&G

F&G System – As per ISA Standard

OISD Standard 152: Requirements for F&G Systems

3.13 **FIRE, GAS & SMOKE DETECTION (FGSD) SYSTEM:**

A system that detects following at an early stage:

- Presence of flammable and toxi gases;
- Presence of a fire;
- Presence of smoke from smoulderin or incipient fires.

FGSD system generates alarms, warnings and / or initiates shutdown functions and / or actuates fire fighting system. Also, based on pre-defined criticality on identified scenarios, it may be configured to initiate evacuation process, reports generation, historisation of data & events at predetermined level of concentrations. Associated electrical or electronics circuits connecting with the field devices of detection system require high availability and reliability in line with IEC 61508 or equivalent international standards.

F&G Controller shall be reliable and comply to IEC 61508 implying it should be SIL certified


What need to be done for application of Safety Standards for SIS design?

Honeywell

Process Control and Safety Instrumented System
A Comparison, Reference (OISD – 152)

Features	Process Control	Safety Control
Control type	Active, complex, optimizing	Passive, simple, direct acting
Tasks	Many variables, expanding, experimental	Limited, strictly defined
Modes of control	Auto / manual, supervisory	Automatic, no manual intervention, no external command levels
Communications	Open systems, Field bus etc	Limited, specialized, difficult with bus networks
Changes	Easy to make, password protected, configurable, parameter changes	Strictly controlled, password protected, verified and documented, parameter changes strictly controlled
Diagnostics	Limited	Intensive proof-testing
Redundancy	Used for high **availability** for continuous use	Used for high **reliability**
Documentation	For convenience	Essential for validation of each function
Testing	Nominal loop testing	Failure modes testing
Legal	Not regulated	Subject to regulation, audit and certification

Honeywell

Few SIS Design Considerations?

- Apply IEC61508/IEC61511 Standards
- Identify SIFs and apply appropriate SIL to each SIF
- Develop ‘Safety Requirement Specification’
- Specify and deploy certified Safety System for all SIF whenever SIL assigned is more than SIL1
- Apply built in redundancy to Safety System for more availability
- Consider and minimize impact of ‘Human Factor’ by design
- Design, engineering and implementation should be done by certified engineers at certified locations.
- Validation of system meeting desired SIL should be done
- Test the design by force to fail where ever possible

  .

  .

  .

- Remember, standards are only the start

Additional FSD/FGS Design Considerations?

- Apply NFPA 72 standard requirements
- FSD/FGS System requirements as mitigation/prevention system
- Consider energise to trip system requirements
- Loop monitoring system requirements
- Back-up power requirements including battery sizing
- Trip signals to ESD, MCC
- Integration to plant SCADA
- F&G Detector coverage

Honeywell

Process Safety…more than ‘Safety Systems’ and ‘Standards’

- Employee Participation – Documented employee involvement in Process Safety Management and Risk Management Program
- Process Safety Information – Hazards of the chemical, technology of process and equipment in the covered process
- Hazard Review (RMP only) – Offsite consequence analysis of worst case and alternate case release scenario,
- Process Hazard Analysis - Thorough, organized, systematic approach to identifying, evaluating and controlling the hazards of covered processes
- Operating Procedures – Written instructions for safely conducting activities involved in the covered process
- Training – Employees, involved in a covered process, trained in an overview of process and the operating procedures

Honeywell

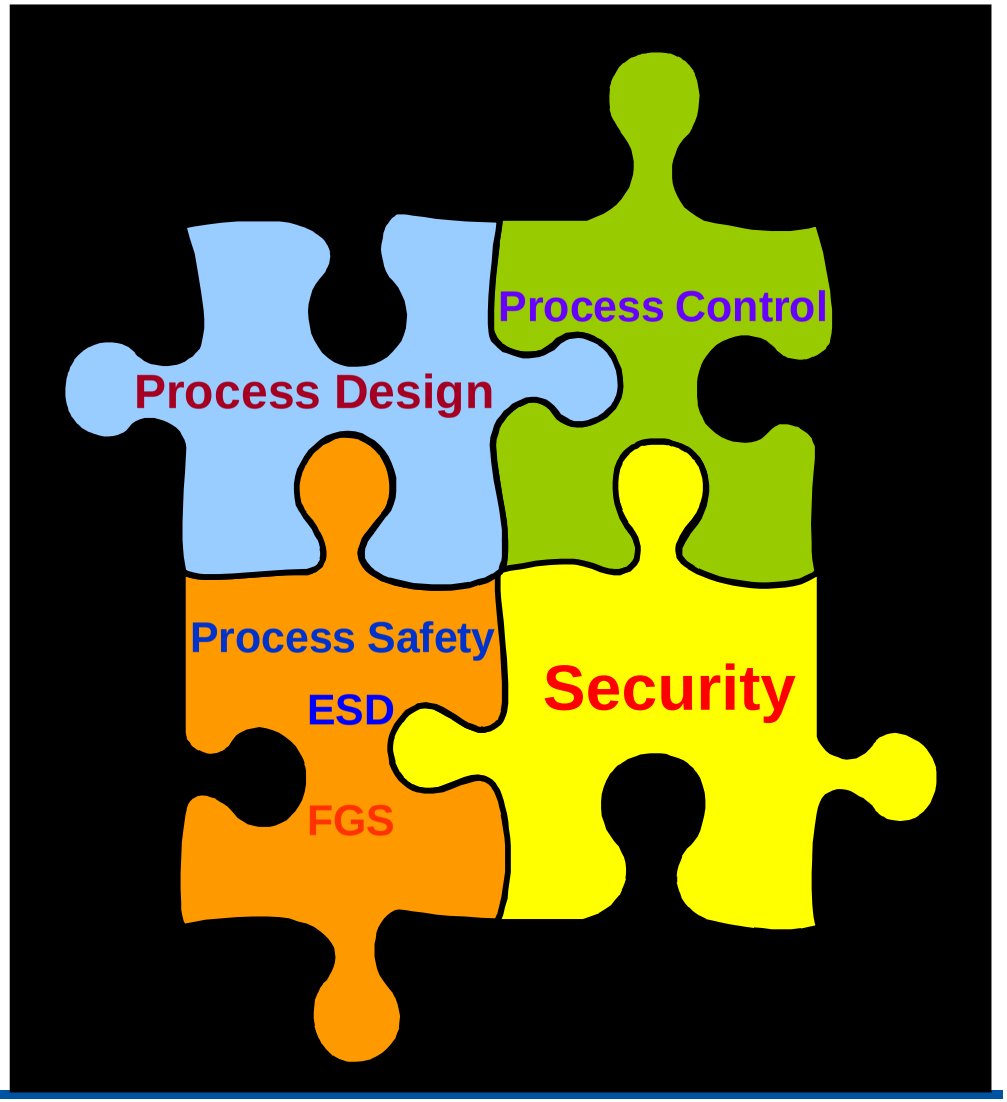
Process Safety…more than ‘Safety Systems’ and ‘Standards’

- Contractors – Management of contractors and contractor employees
- Pre-Startup Safety Review – Review prior to startup of new or significantly modified facilities
- Mechanical Integrity – Maintain critical process equipment to ensure proper design and that the equipment operates properly
- Permit to Work – Proper permit system shall be in place to carry any field work
- Management of Change – Manage changes (except “replacement-in-kind”) to process chemicals, technology, procedures and equipment
- Incident Investigation – Investigation and documentation of incidents
- Emergency Planning and Response – Written emergency action plan including provisions for training and drills
- Compliance Audits – Documented periodic evaluation of compliance with program requirements

Integrated Safety Solution

Though independent protection layers for Safety should exist, these independent layers should be tightly integrated with the Process Control layer for monitoring. The intention of this is:

- System Diagnostics
- Field Devices Diagnostics
- Alarm Visualization
- Event Historian & Event status
- Process CCTV Integration
- Security Integration



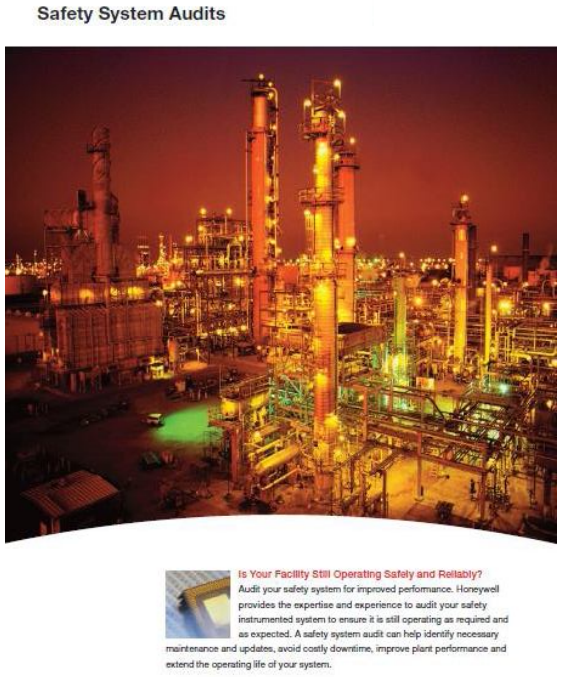
Honeywell

Sustenance is key . . .
Audit the Safety Systems

Audit the current condition of the Safety System.

This should be aimed to find:

- Is the system designed in a correct way?
- Is the environment effecting system?
- Did modifications affect the safety & reliability of the system?
- Are diagnostics messages revealing a hidden issue?
- Is system maintenance performed in a correct way?



Is my system running safe & reliable?

Summary

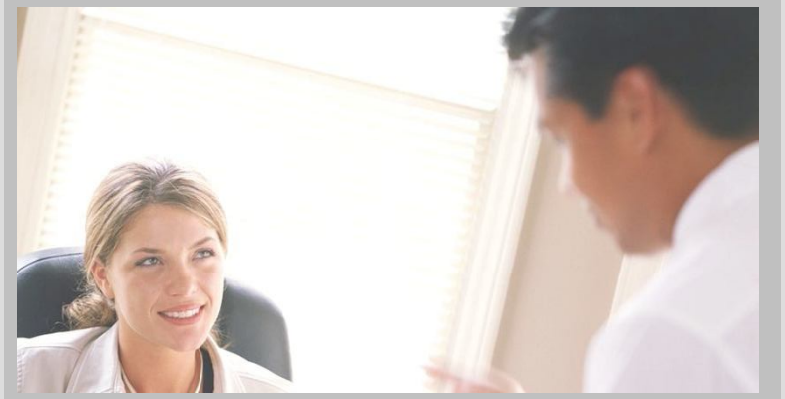
What we Know:

- Process related incidents cost $
- Process safety automation is key
- Sustaining safety is critical

Consider:

- Process Safety is the goal.
- Functional Safety is subset of safety.
- To achieve functional safety, consider factors such as:

➢ Functional Safety Management
➢ Safety Lifecylce activities
➢ Competence of People

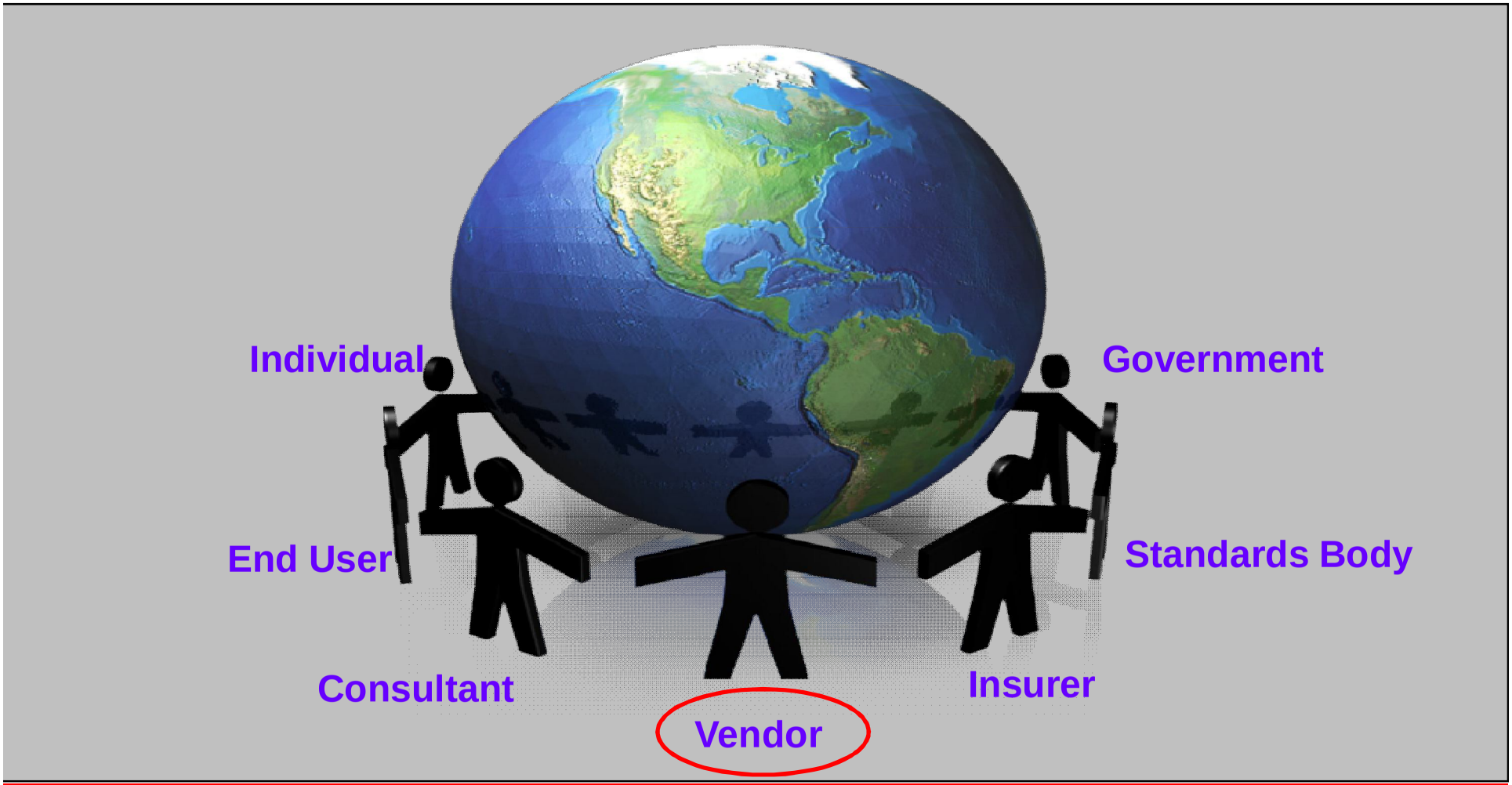


Improve business performance through better safety, reliability, and efficiency.

Automation can help.

Honeywell

Joint Efforts for Safe Society



Joint Industry Platform to promote safety

Honeywell

Joint Efforts for Safe Society

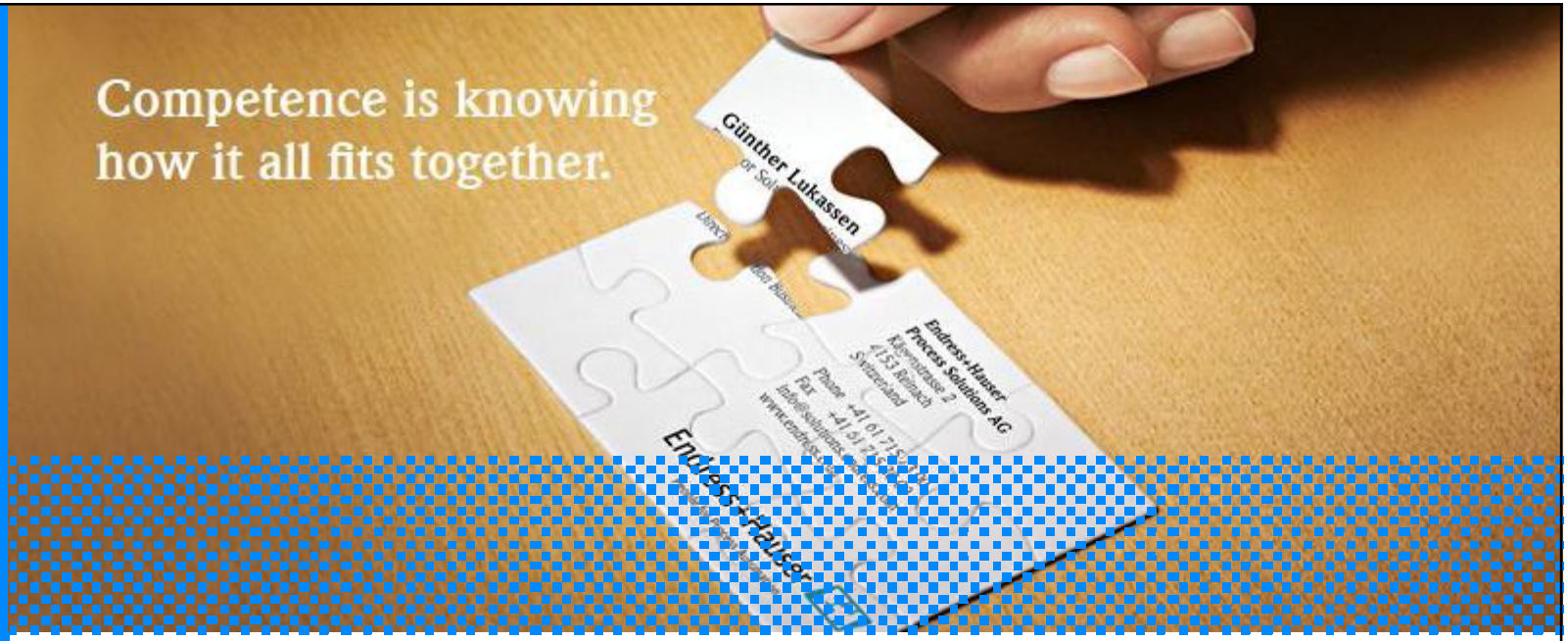
Individual	- Training & Awareness
End User	- Create Safety Culture, Trainings
Consultant	- Update, promote & prescribe latest standards & technology
Vendor	- Invest in Technology / Research
Insurer	- Incentivise end users for investments in risk reducing technology
Standards Body	-Benchmark global standards -Relentless enforcement of standards
Government	- Promote & Incentivise safety & security

Joint Industry Platform to promote safety

Honeywell

Thank You !

Amit Aglave
Safety Consultant
TUV FS ENG ID: 2827 / 10
Honeywell Automation India Ltd.
amit.aglave@honeywell.com



Level Pressure Flow Temperature Liquid Analysis Registration Systems Components Services Solutions

Functional Safety from Field Device Perspective

Hemal Desai

Endress+Hauser
People for Process Automation

Endress+Hauser

Synopsis

■This presentation will outline the selection of sensors for SIS applications that meet the requirements of IEC 61511 standard while minimizing lifecycle costs.

Endress+Hauser

Agenda

- Introduction
- SIS Failures - Where do they occur & causes
- Safety Standards
- Sensor Selection per IEC 61511
  - Designed per IEC 61511 Section 2 &3 & Prior Use
  - Technology Selection
  - Architecture Selection
  - Test Philosophy
  - Other considerations

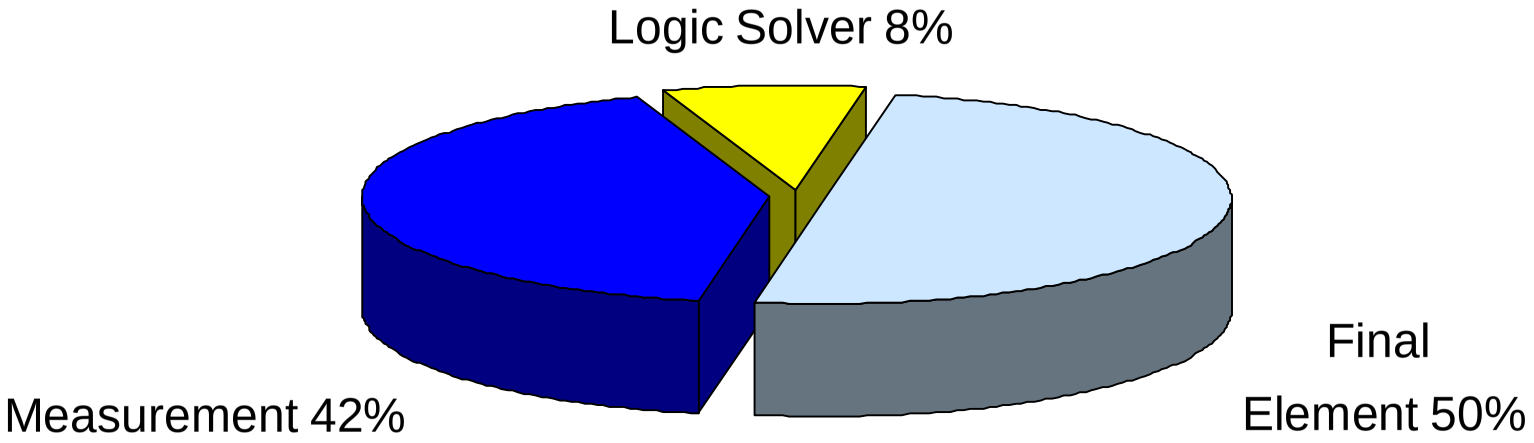
Endress+Hauser

Accidents that changed Safety Considerations

Bhopal
Texas City
Buncefield
Jaipur
.....

Endress+Hauser

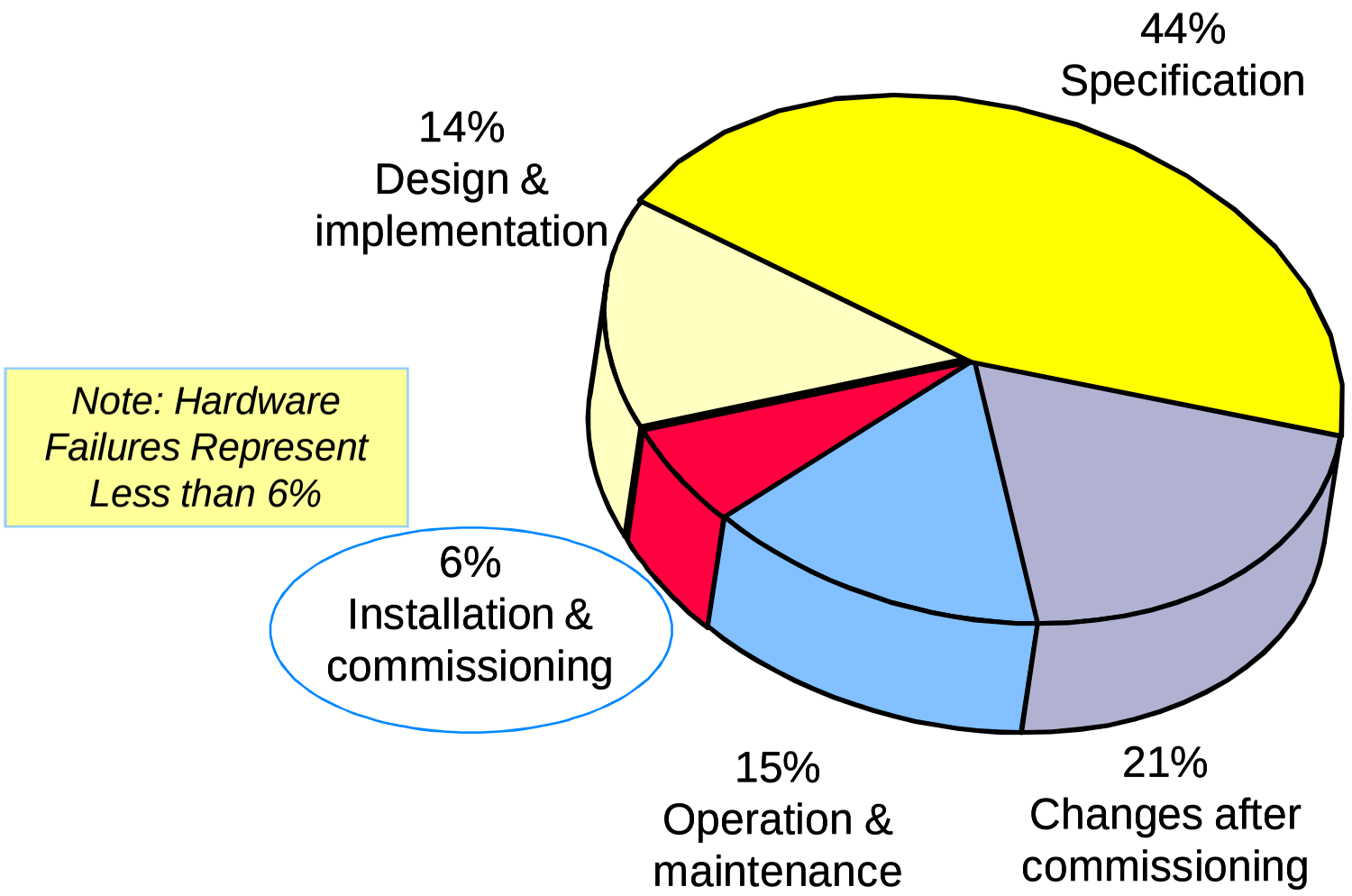
SIS Failures-Where do they occur?



Source OREDA

Primary Causes of SIS Failures
HSE Study of accident causes

Endress+Hauser



"Out of Control: Why systems go wrong & how to prevent failure"
Source Health, Safety & Environmental Agency UK Ed. 2 - 2003

International Standards for Functional Safety

Endress+Hauser

Objectives:
- International Standard for Safety thru LC
- Cost effectiveness
- Published in 1998
- Best Engg Practices

IEC 61508

Generic Standard
»Functional Safety«

Generic standard

Valid for all relevant sectors
• Process • Power Plants
•Traffic• Machinery

IEC 61513
Application Standard
»Nuclear Sector«

IEC 61511/ISA 84.00.01
Application Standard
»Process industry«

IEC 62061
Application Standard
»Machinery Sector«

Application standard Implementation for

Process industries
• Chemical • Petro-Chemical •Oil&Gas

Developed by End Users

2003

Relationship Between IEC 61508 & 61511

Endress+Hauser

SIS Standard
»Process industry«

Performance over
Lifecycle
Vs
Prescriptive

Umbrella Standard

IEC 61508
Equipment Suppliers
&
Manufacturers

IEC 61511
SIS Designers
Integrators
& Users
-ISA 84.00.01 (2004)

Only guidelines. Not law

IEC 61511 Lifecycle

Endress+Hauser

End user/ Consultant
»Analysis«

End user/ Contractor/Vendor
»Realization«

End user/ Contractor
»Operation«

Identify Hazards
Estimate Risks
Are Risks Tolerable??

- HAZOP
- Analysis of Likelihood & Consequences
- Non SIS Layers of Protection

Access Likehood
based on all
Protection Layers

- Identify Layers of Protection
- Use Qualitative & Quantitative Methods to access Risk

Specify Risk reduction in terms of SIL.

Determine difference
Between Actual Tolerable

- Use SIL Table

Develop Safety
Requirement Specification
SRS

- Identify SIF
- Document SIL for SIF
- Document logic & Cause+Effect diag.
- Document Proof test, Maintenance bypass etc.

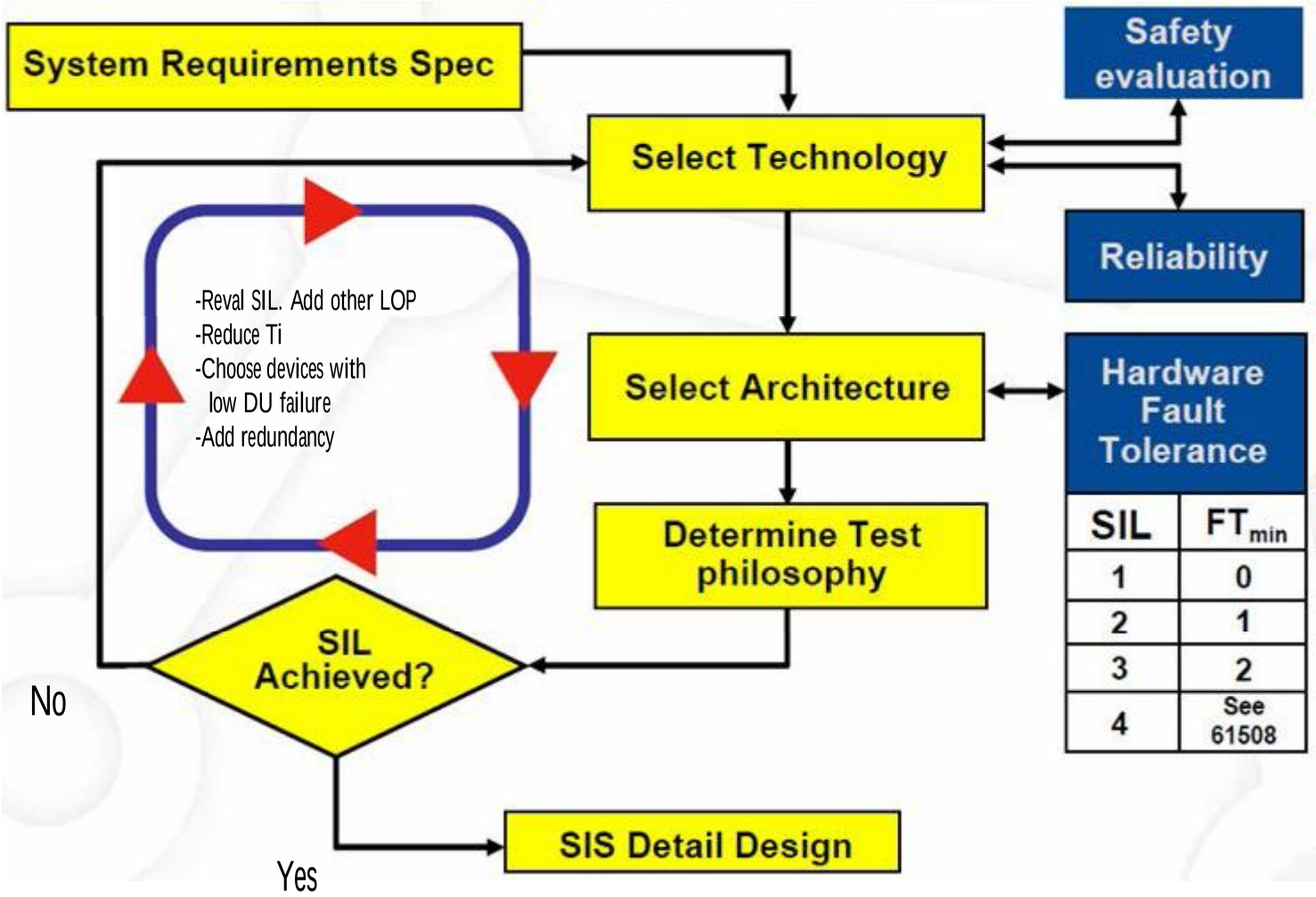
Endress+Hauser

How to Select Sensor per IEC 61511

- Sections1-7 Scope and Management
- Sections 8-9 Evaluation
- Section 10 Safety Requirements Spec.
- Sections 11-12 Design and Engineering
- Sections 13-14 Testing, Installation
- Section 15 Validation
- Section 16 Operations and Maintenance
- Section 17-18 Modification

Endress+Hauser

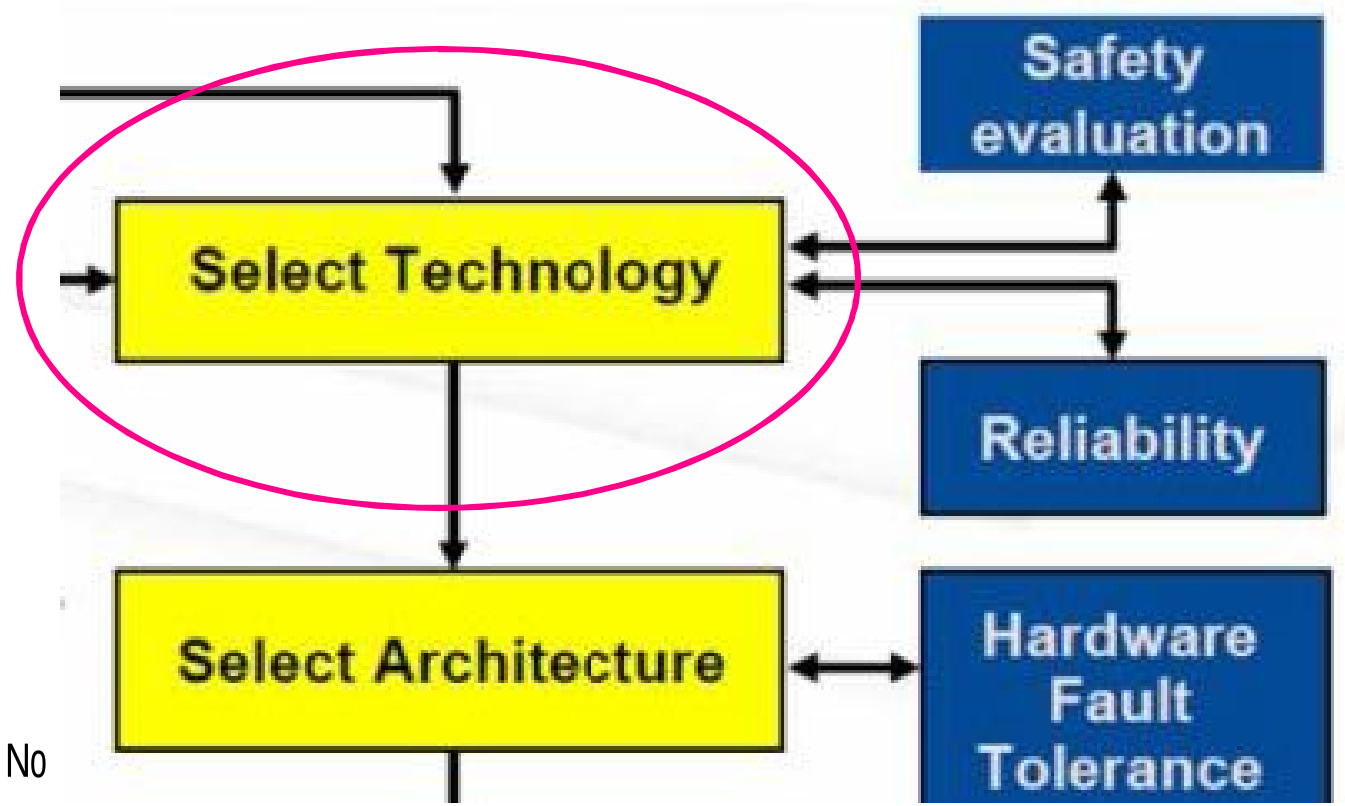
Iterative Method of Sensor Selection per IEC 61511



SIL	FT_{min}
1	0
2	1
3	2
4	See 61508

Endress+Hauser

Iterative Method of Sensor Selection per IEC 61511



Endress+Hauser

Classification of Sensors used in SIS

- IEC 61511 documents requirements for hardware used in SIS
- IEC 61511 section 11.5.2 list two options end users have
  - Components and subsystems selected for use as part of SIS for SIL1 to SIL3 shall be either in accordance with IEC 61508 sections 2 (HW, Systems) & 3 (Software)
  - Meet the requirements of IEC 61511 section 11.4 & 11.5.3 to 11.5.6 requirements for selection of components & subsystems based on prior use

Difference between the two?

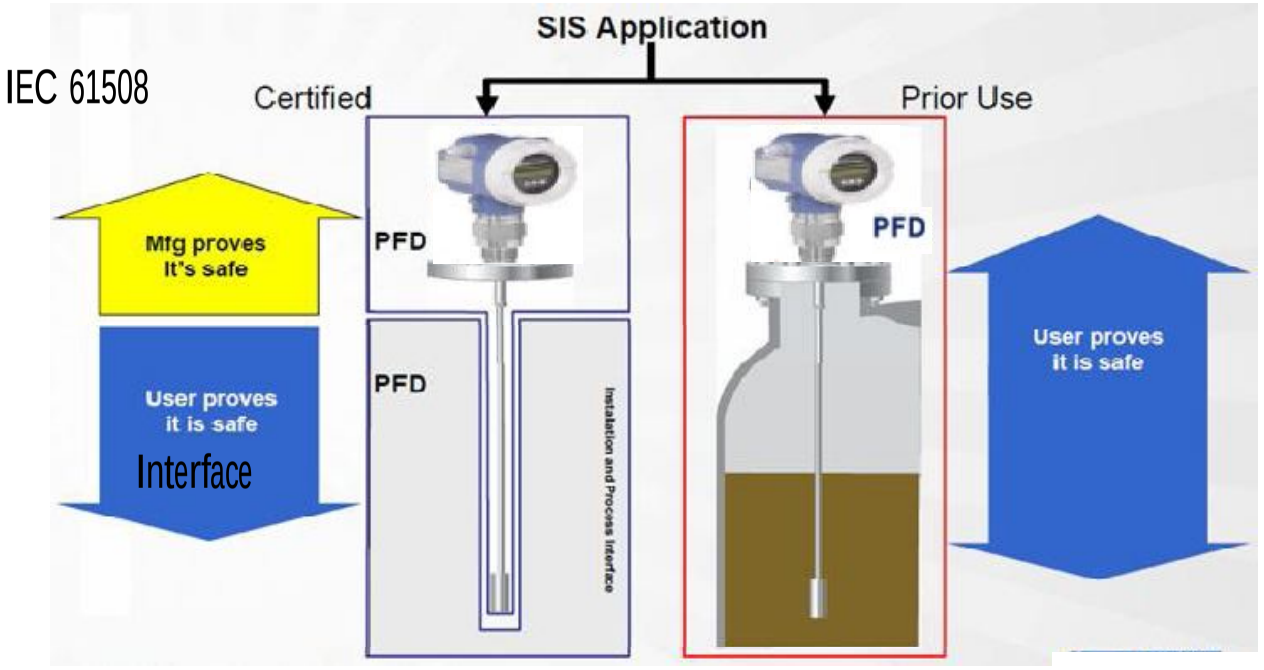
BURDEN OF PROOF

Burden of Proof

Endress+Hauser

Manufacturer proves safety level, capabilities & Limitations od sensor

End User determines PFD, capabilities & Limitations of sensor



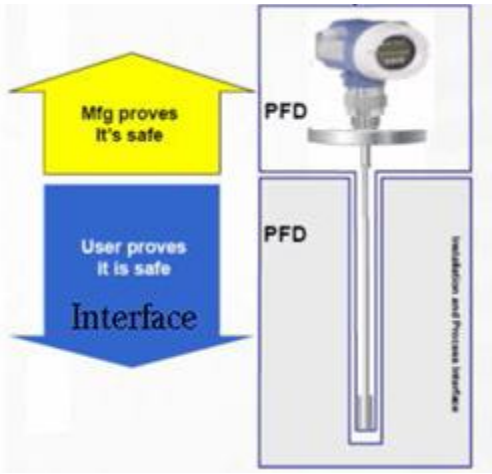
User need to evaluate Undetected Failure rates for interface due to physical damage from hammering, corrosion, gas permeation, embrittlement

User need to evaluate Undetected Failure rates for interface due to physical damage from hammering, corrosion, gas permeation, embrittlement

Characteristics of Sensors Designed per IEC 61508 sections 2&3

Endress+Hauser

1. Sensor design has Safe-Failure-Fraction (SSF) >90%
2. Sensor design complies with requirements of
   - IEC61508 Section 2 - Hardware
   - IEC61508 Section 3 - Software
3. Operations
   - Design change management
   - Manufacturing process controls
4. Suppler has provided a Safety Manual
   - Documents Use, Limitations, and Proof-Test requirements
5. Failure Mode Effect Diagnostic Analysis (FMEDA)
6. Probability of Failure on Demand (PFD)
7. Third Party certification & report by notified body



Certifications

Endress+Hauser

Third Party Certification


CERTIFICATE

No. Z10 08 03 20351 004

Holder of Certificate: Endress+Hauser GmbH+Co. KG

Factory(ies):

Certification Mark:

Product:

Pressure Meters

Model(s):

Parameters:

Tested according to:

ZERTIFIKAT ◆ CERTIFICATE ◆ CERTIFICADO ◆ CERTIFICAT

Safety Manual


Typically list

Sensor installation
Configuration & Operation
Product life
Proof tests
Limitations

Endress+Hauser

Notified Bodies: RWTUV, TUV Sud
TUV Rhineland, FM

Experts like Exida, Risknowledgy
Assist activities like FMEDA &
Developing safety requirements

Endress+Hauser

Benefits of Designed per IEC 61508

- Simpler compliance to IEC 61511
- Supplier responsible for documenting the safety level of device
- Assurance the PDF values & failure rate data are correct
- Assurance equipment design meets Good Engg Practice defined in IEC 61511
- Assurance that manufacturer has processes for "Management of Change"
- Availability of Safety Manual & Certifications

Characteristics of Sensors Designed on Prior Use (Proven in Use)

Endress+Hauser

1. Consideration of the manufacturers' Quality, management and configuration management systems

2. Adequate identification and specification of the components or subsystems

3. Demonstration of performance of the components or subsystems in similar operation profiles and physical environments

4. The volume of operating experience (e.g 2 yrs without significant change in design or SW)

Proven in Use Tools

Endress+Hauser

PROVEN-IN-USE WORKSHEET

PROJECT: **Project ID#:**

CLIENT:

DEVICE DESCRIPTION

Equipment Type:

Manufacturer:

Model:

Service Description:

Is actual Service similar to Proposed Application? (Y/N):

Physical Environment Decription:

Is actual Environment similar to Proposed Application? (Y/N):

MANUFACTURER MANAGEMENT INFORMATION

	Answer	Discussion
1. Does the Manufacturer has a Quality Management System for hardware? How is it known?		
2. Does the Manufacturer has a Quality Management System for software? How is it known?		
3. Does the Manufacturer has a Configuration Management? How is it known?		
4. Have there been quality problems and/or failure issues with this device that are unresolved?		

FAILURE DATA

	Data	Notes on method for obt[illegible]
Number of devices on service (in this profile):	10	

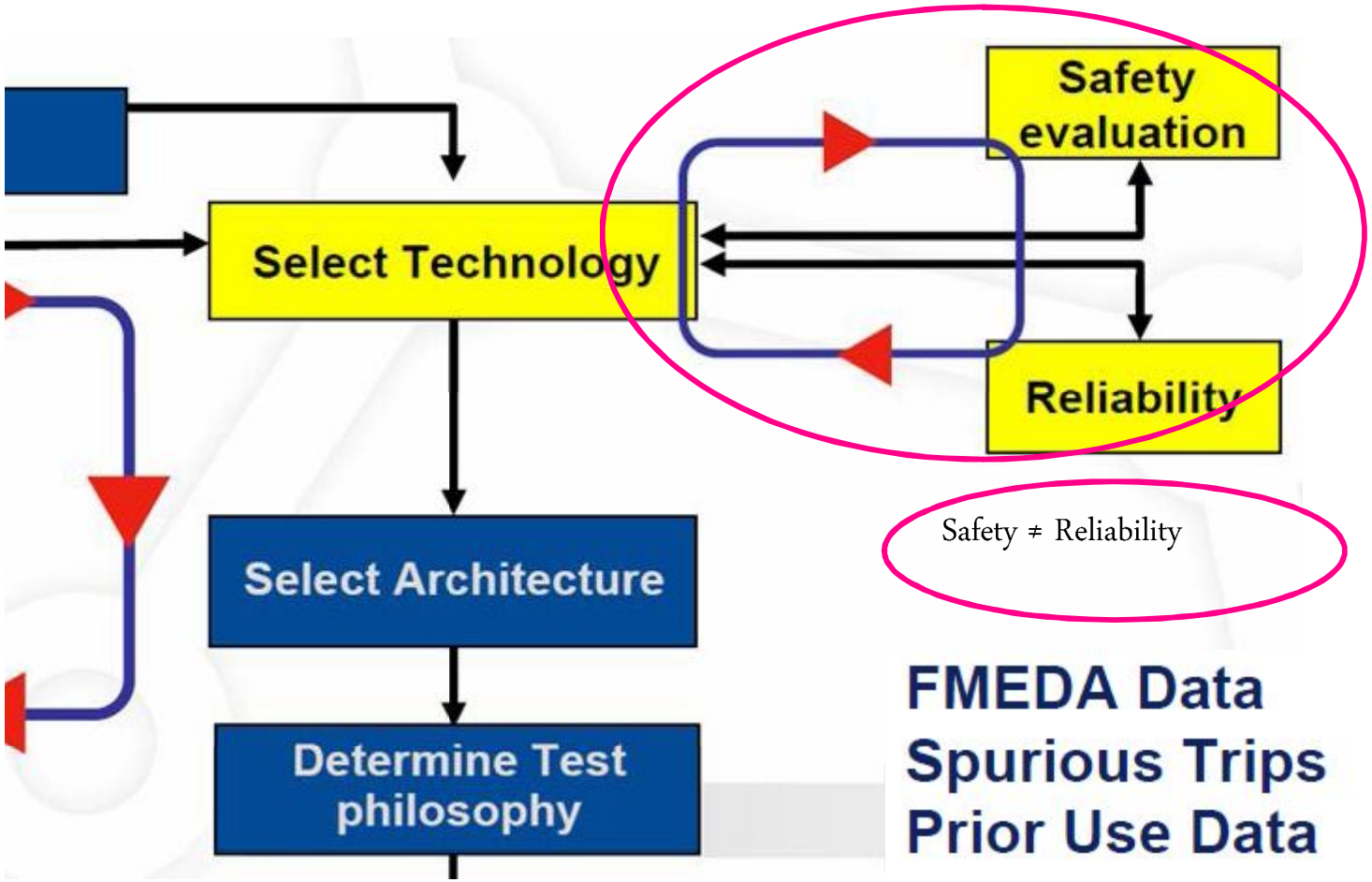
Exida

Silvertool

Source Kenexis

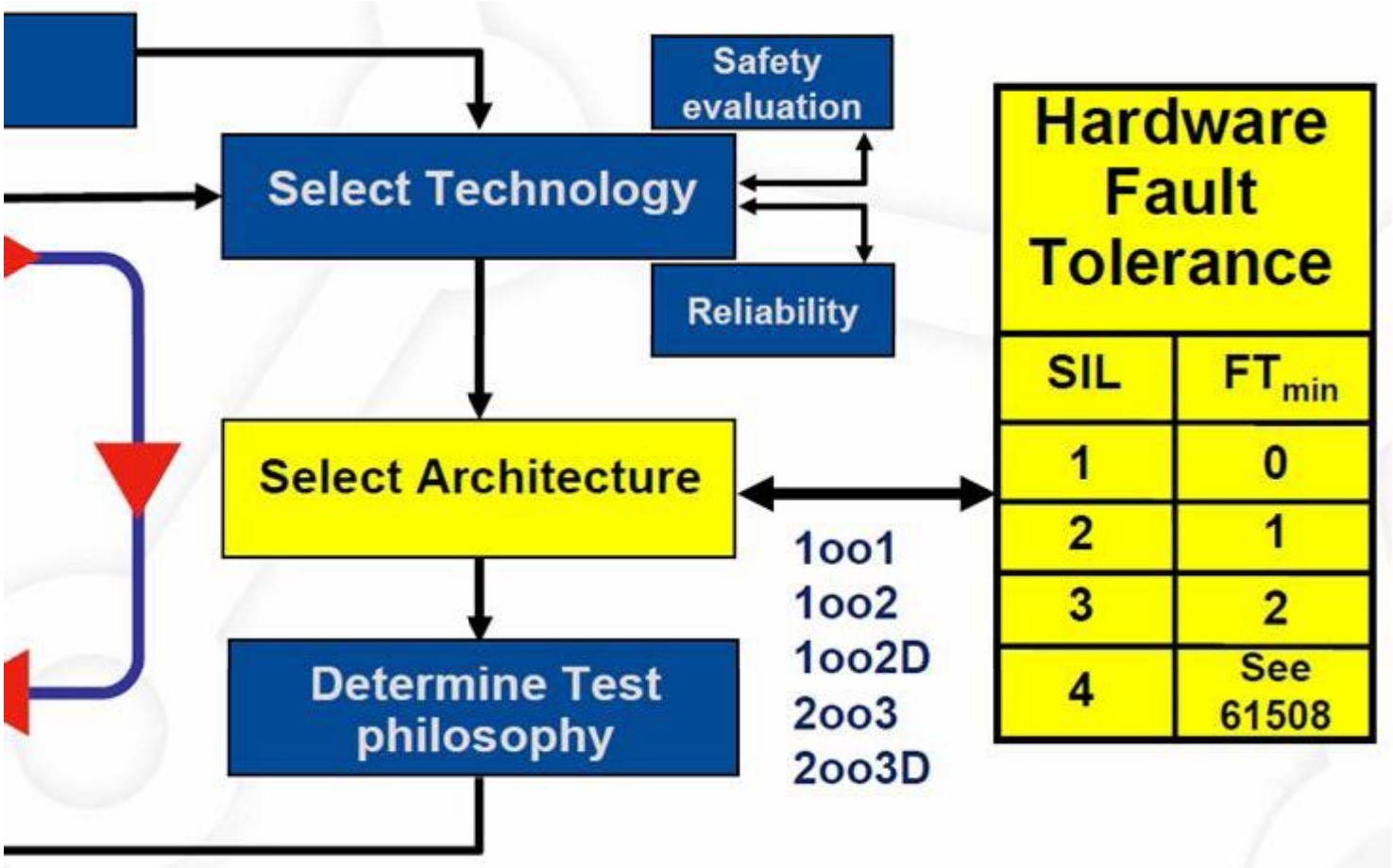
Endress+Hauser

Safety vs Reliability



Endress+Hauser

Select Sensor Architecture IEC 61511-1 (HFT Table 6)



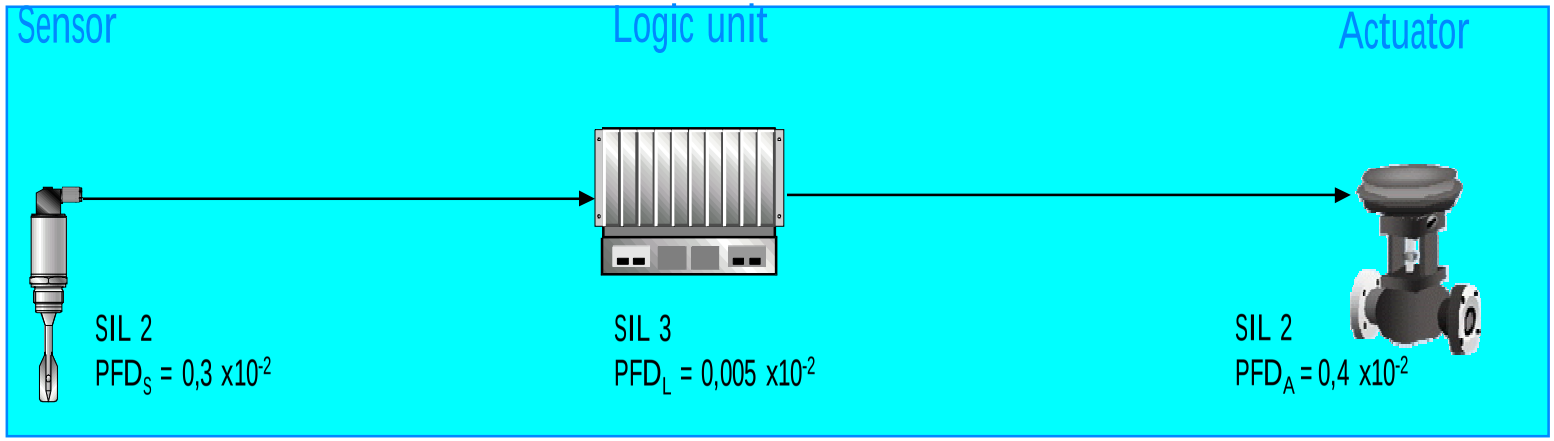
Hardware Fault Tolerance	
SIL	FT_{min}
1	0
2	1
3	2
4	See 61508

Single Channel System

Endress+Hauser

Determination of a Single Channel System

Example: required level ➔SIL 2 (PFD < $1x10^{-2}$)



Design Rules:

$SIL = Min(SIL_S , SIL_L , SIL_A)$

$PFDav = PFD_S+PFD_L+PFD_A < PFD(SIL)$

	Sensor	Logic unit	Actuator	System
SIL	2	3	2	2 √
PFD_{av}	$0,3x10^{-2}$	$0,005x10^{-2}$	$0,4x10^{-2}$	$0,71 \times 10^{-2}$ √

Multi-channel system

Design of a Multi-Channel System

Homogenuous redundant 2 identical sensors	 + 
Diverse redundant 2 different sensors (to avoid a simultaneous occurrence of a systematic fault) 2 different technologies (different measuring principles or different physical measuring variables)	 +  Pressure transmitter A Pressure transmitter B  +  Hydrostatic level Level Radar

Endress+Hauser

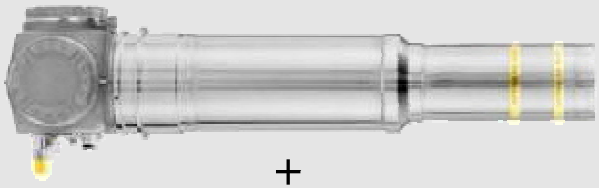
Homogeneous Redundancy: SIL 2 + SIL 2 = SIL 3?

PMP41
Hardware SIL 2
Software SIL 2

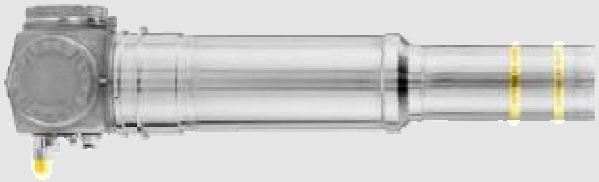
+

PMP41
Hardware SIL 2
Software SIL 2

= SIL 2



+



FMG60
Hardware SIL 2
Software SIL 3

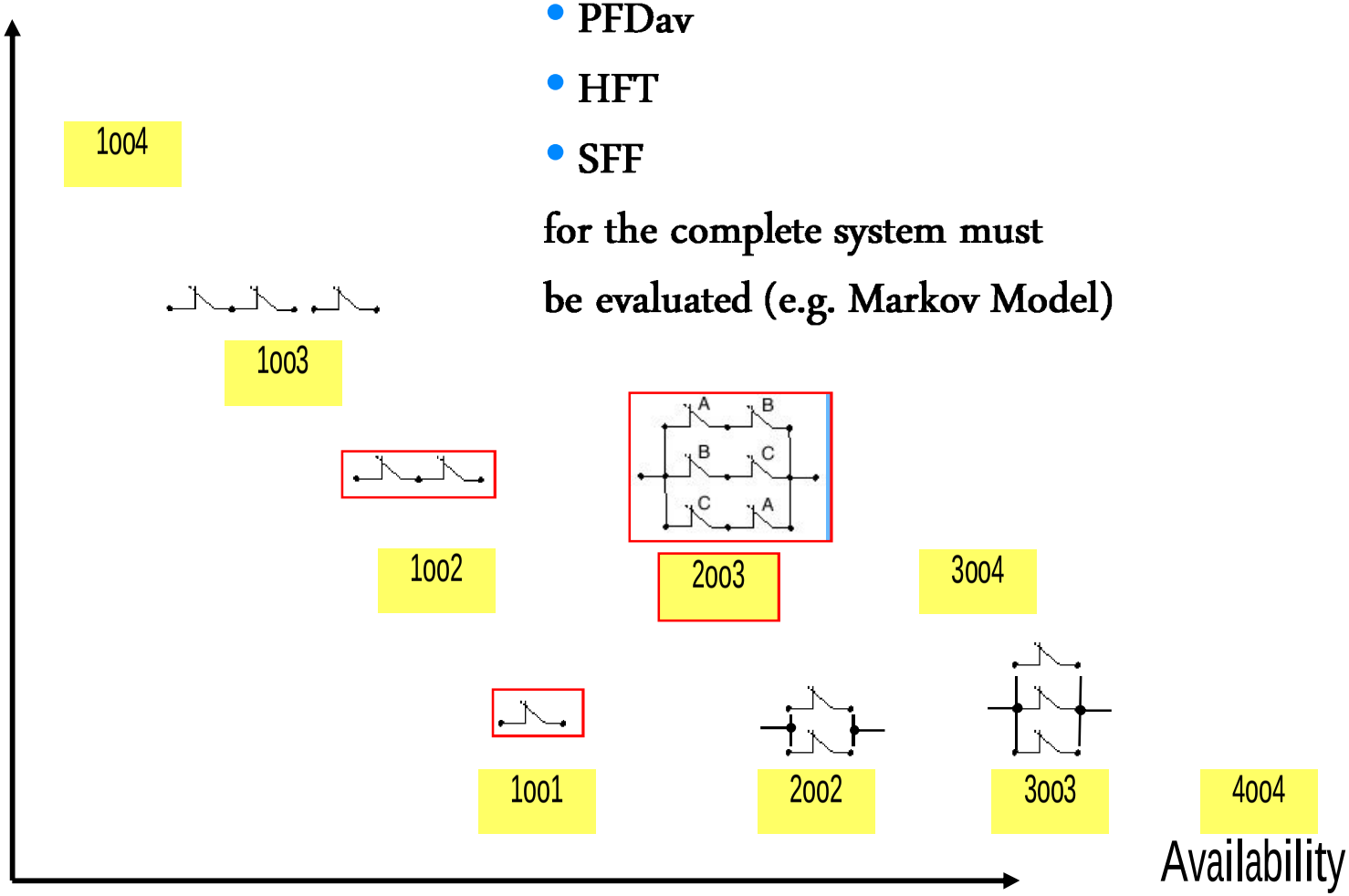
FMG60
Hardware SIL 2
Software SIL 3

= SIL 3

Endress+Hauser

Architecture of Multi-Channel Systems

Safety

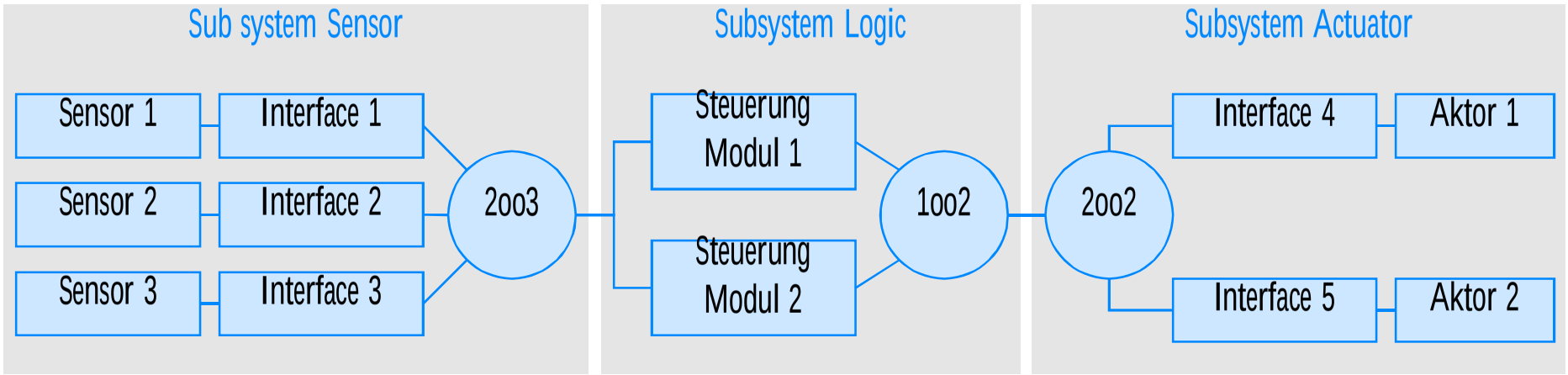


Fundamental Safety Parameters

- **PFDav**
- **HFT**
- **SFF**

for the complete system must be evaluated (e.g. Markov Model)

Determination of a Multi-Channel System



PFD calculation of System:

Step 1: Calculation of PFD_x of sub systems (e.g. Markov model)

Step 2: $PFD_{System} = PFD_S + PFD_L + PFD_A$

Calculation tools: e.g. exSILentia (Exida)

Endress+Hauser

Approximation formula (Source: VDI/VDE 2180, Sheet 4)

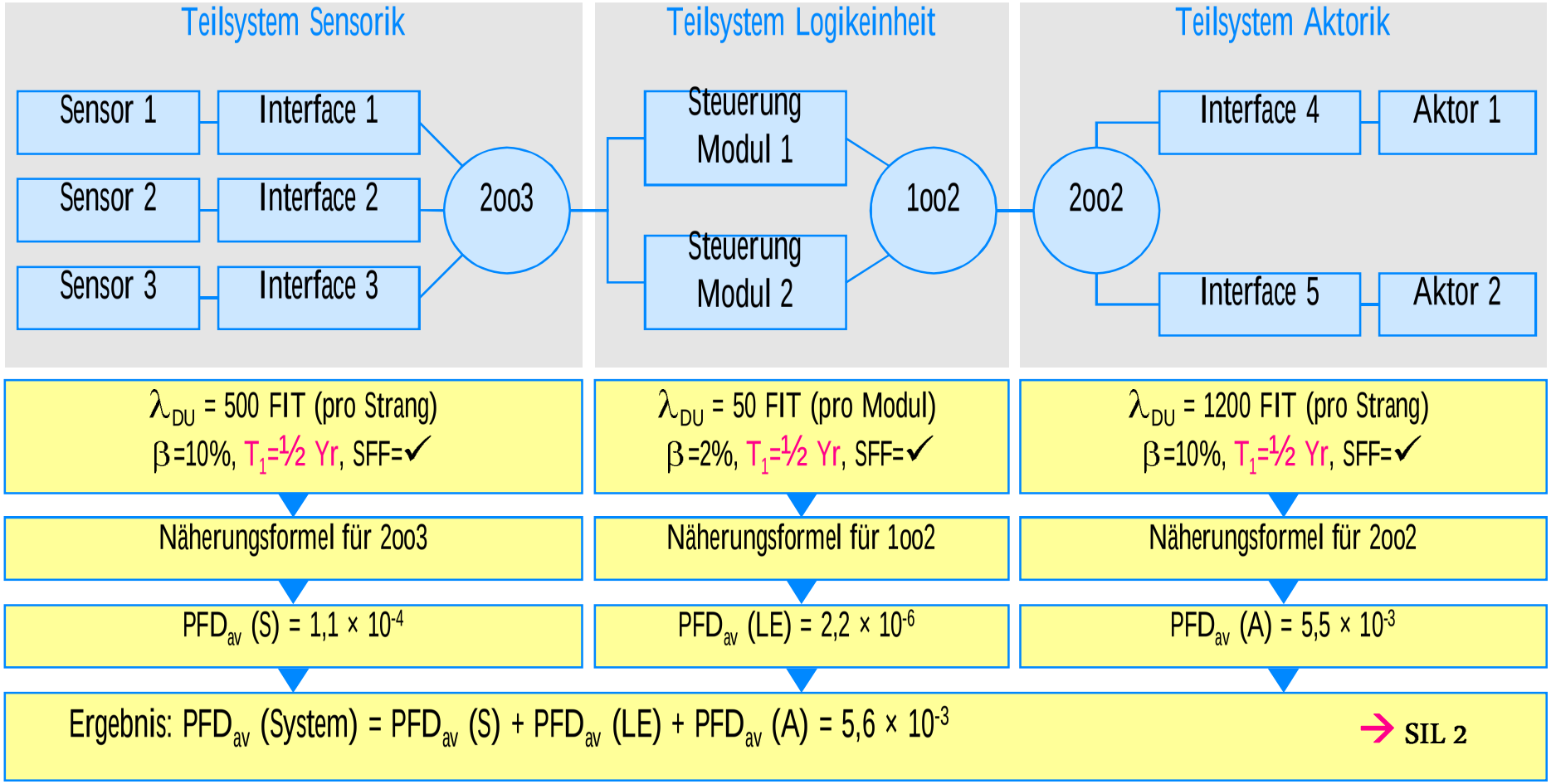
Options of Circuit	Approximation formula for PFD_{av}
1oo1	$PFD_{1oo1} \approx \frac{\lambda_{DU} T_1}{2}$
1oo2	$PFD_{1oo2} \approx \frac{(\lambda_{DU} T_1)^2}{3} + \frac{\beta \lambda_{DU} T_1}{2}$
1oo3	$PFD_{1oo3} \approx \frac{(\lambda_{DU} T_1)^3}{4} + \frac{\beta \lambda_{DU} T_1}{2}$
1oo4	$PFD_{1oo4} \approx \frac{(\lambda_{DU} T_1)^4}{5} + \frac{\beta \lambda_{DU} T_1}{2}$
2oo2	$PFD_{2oo2} \approx \lambda_{DU} T_1$
2oo3	$PFD_{2oo3} \approx (\lambda_{DU} T_1)^2 + \frac{\beta \lambda_{DU} T_1}{2}$
2oo4	$PFD_{2oo4} \approx (\lambda_{DU} T_1)^3 + \frac{\beta \lambda_{DU} T_1}{2}$

λ_{DU} = Failure „dangerous undetected“, β = Common cause Factor,
T_1 = Time interval for proof testing [h] (1 Year = 8.760 h)

SIL Calculation

Endress+Hauser

Ziel:SIL2



IEC 61511 Allows Credit for Fault Tolerance by 1 in Architecture if....

In a Prior Use sensor

- Device is password / jumper protected

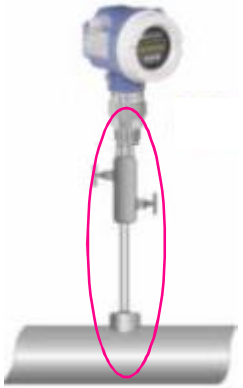
Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60%	Not Allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL4	SIL 4

Designed per IEC 61511

- Alternate fault tolerance based on IEC 61508 HFT table for Type B with specified SFF%

Alternative Hardware Fault Tolerance	
SIL	FT_{min}
1	0
2	0
3	1
4	See 61508

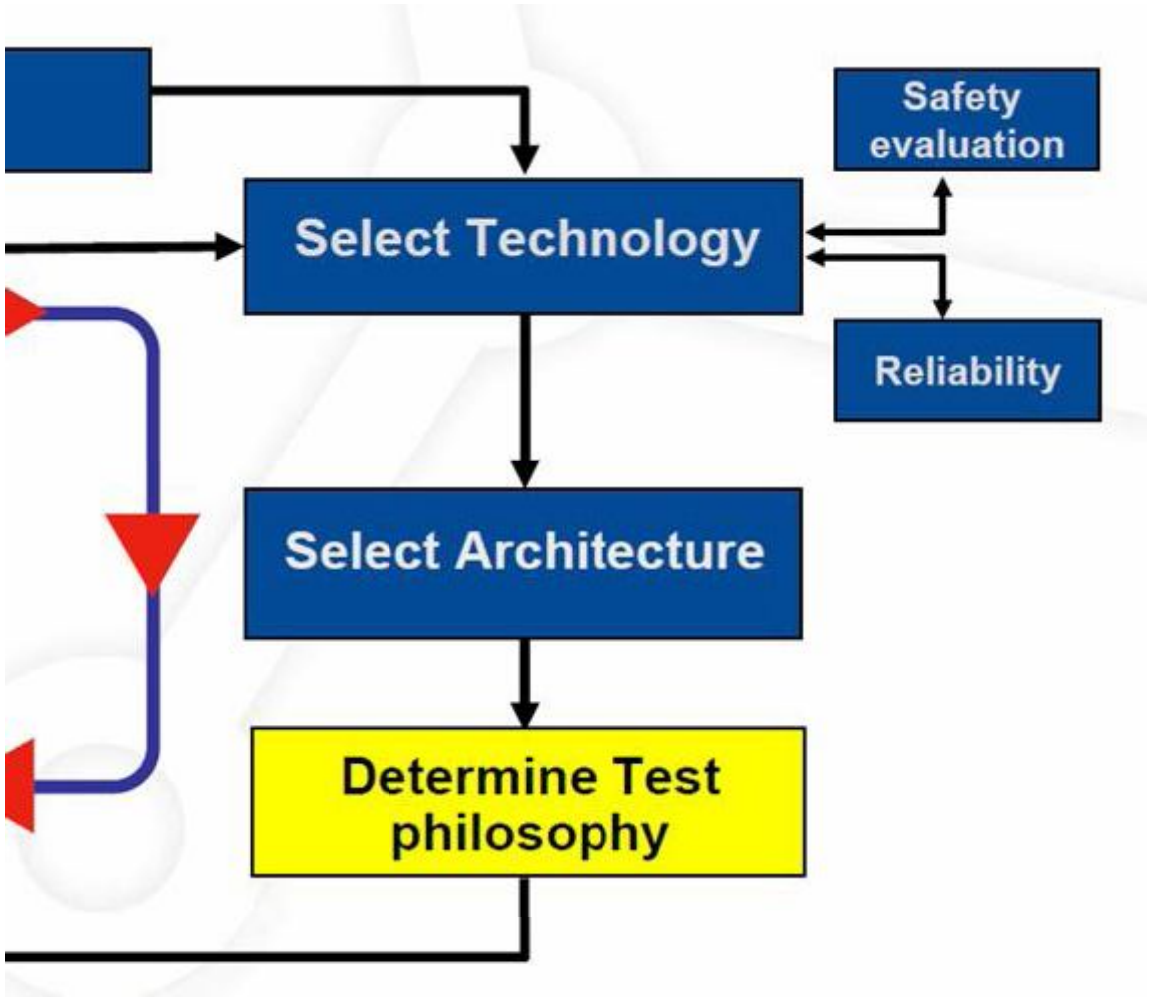
Caution
If any potential exists for dangerous failure due to plugging, freezing, gas permeation etc, Fault Tolerance must again be increased by 1



Interface

Endress+Hauser

Proof Test



Proof Test Coverage

Endress+Hauser

Functional Safety Manual

Deltabar S
PMD70, PMD75, FMD76, FMD77, FMD78

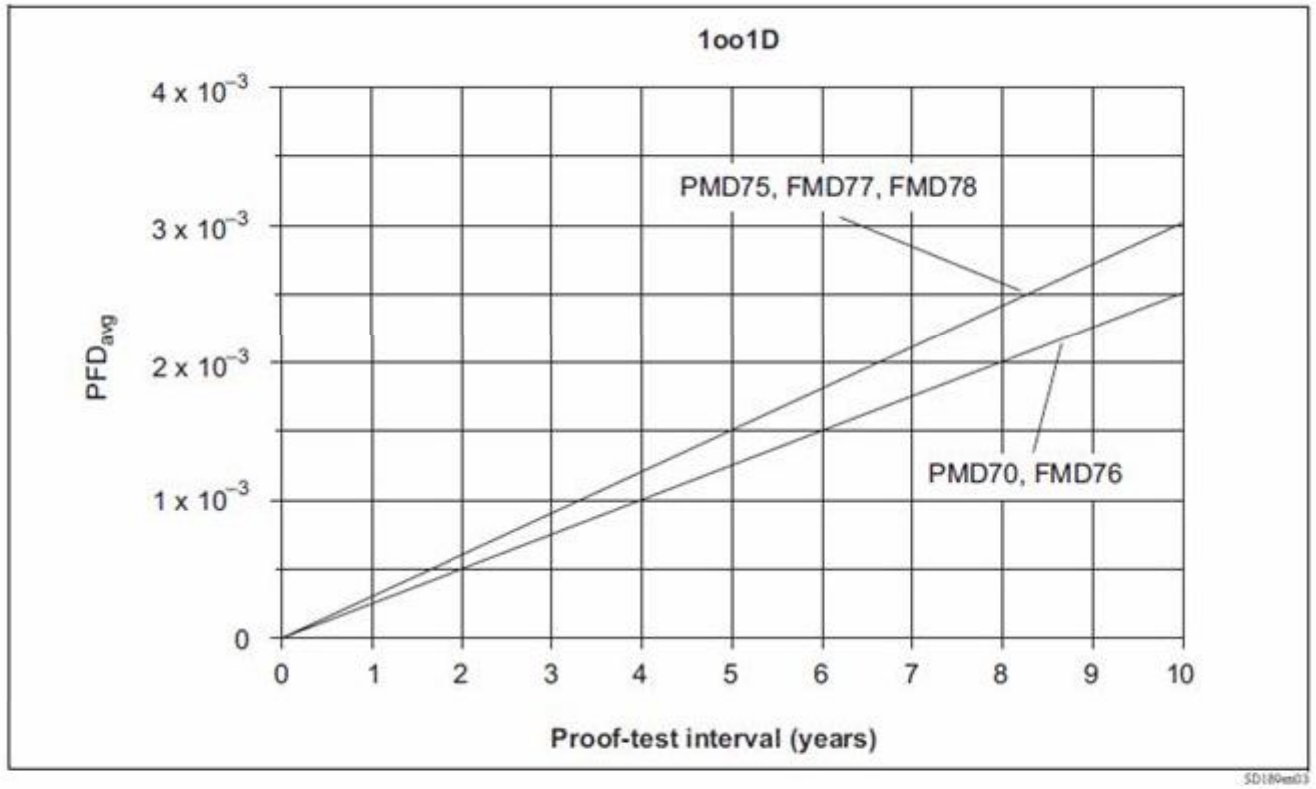
Proof-test 2:

This test detects approx. 99 % of the possible dangerous undetected device failures.

1. Perform steps 1 to 4 outlined under recurrent test 1.
2. Compare the pressure measured value displayed to the pressure present and check the current output. During this test, suitable processes, measuring resources and references must be used.
   - For the lower-range value (4 mA value) and the upper-range value (20 mA value), compare the pressure present to the measured pressure.
   - If the measured pressure deviates from the pressure present at the device, the reference pressure present must be reassigned to the 4 mA value and the 20 mA value.
     FFor the 4 mA value, → Operating Instructions BA274P, parameter descriptions for SET LRV (245) and GET LRV (309) for pressure measurement, SET LRV (013) for level measurement (LEVEL SELECTION "Level Easy Pressure") and SET LRV (637) for flow measurement.
     For the 20 mA value, → Operating Instructions BA274P, parameter descriptions for SET URV (246) and GET URV (310) for pressure measurement, SET URV (012) for level measurement (LEVEL SELECTION "Level Easy Pressure") and SET URV (638) for flow measurement.
3. Perform steps 5 to 7 outlined under proof-test 1.

Endress+Hauser

Proof Test Interval



Proof-test interval

Low Demand Mode
Demand Interval is greater then 2X Proof test interval

Endress+Hauser

Common Cause / Systematic failures consideration

- Common cause are defined as failures that impact two or more channels of redundant systems. e.g. sensors in a 2oo3 voting scheme affected by electromagnetic disturbance

- Other examples of common cause – temperature transients, thermal or physical shocks, vibration, design errors, maintenance errors.

- Common cause is represented as beta %

- Total PFD = (beta%XPFD$_{red\ sys}$) + Loop PFD

Sensor Diversity
Different vendors
Different Technology

Lower beta factor

Endress+Hauser

Common Cause

Common Cause Factor Estimator - Sensor/Final Element					
Item	**Sensors and final**		**Technique**		
	X_{SF}	Y_{SF}	**Applied?**		
Separation/segregation					
Are all signal cables for the channels routed separately at all positions?	1	2	0	0	0
Environmental control					
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	1	0.5	2.5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3	1	1	3	1
Are all signal and power cables separate at all positions?	2	1	0	0	0
Environmental testing					
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognised standards?	10	10	1	10	10
Results					
Sensors and final elements	*23.5*	*33.5*			
Beta	**57**	**5%**			

Source Kenexis

Endress+Hauser

Other Considerations

- Sensor Capabilities & Limitations
  - Of Products
  - Of Maintenance & Operations
- Safety Response Time
  - Sensor response time + time to run the diagnostics (typ 1-5s)
- Safety Accuracy
  - Comparison of Analog & Digital value
- Use of SMART transmitter with Diagnostics
- Proper design & installation of sensor to prevent process related affects like plugging, corrosion, gas permeation etc.

Endress+Hauser

Other Considerations

Restrictions for use in safety-related applications

- Device warmup time: after device warmup, the safety functions are available after a 30-second initialization period.
- In the case of local operation of the Deltabar S without a display and without an operating tool or without a HART communicator, the device cannot be safely configured because the user cannot perform a visual check. In both these situations, communication via HART alone is not sufficient.
- The device must be locked following configuration.
- When using the device as a subsystem of a safety function, the "Hold meas. value" setting may not be selected as this option does not provide failsafe alarming.
- During commissioning, a complete function test of the safety-related functions must be performed.
- The maximum interval for recurrent testing (Proof Test Interval) is 5 years.
- Faulty devices must be replaced as soon as possible to minimize the possibility of multiple errors occurring. The failure probabilities indicated in this Safety Manual are based on a medium time to repair (MTTR) of 8 hours.

The transmitter output is not safety-oriented during the following activities:

- Changes to the configuration
- Multidrop
- Simulation
- Proof-test

Endress+Hauser SIL offerings

Radars
Gamma ray
Servos

Liquid
&
Solid
Switches

Temperature
transmitters

Coriolis
Magnetic
Vortex
Flowmeters

DPT & PT
Transmitters

Active & Passive
Barriers

pH analysers

GSM/GPRS Modems

Endress+Hauser

Thank You for your Attention!

commtel NETWORKS

Let's reach the next level

PIPELINE INTRUSION DETECTION USING C-OTDR

Upendra H. Manyam

Commtel Networks, Mumbai

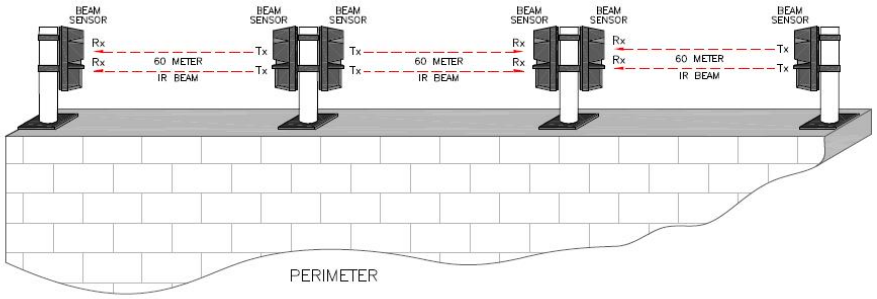
September 26, 2011

ISA (D) - PNID, New Delhi

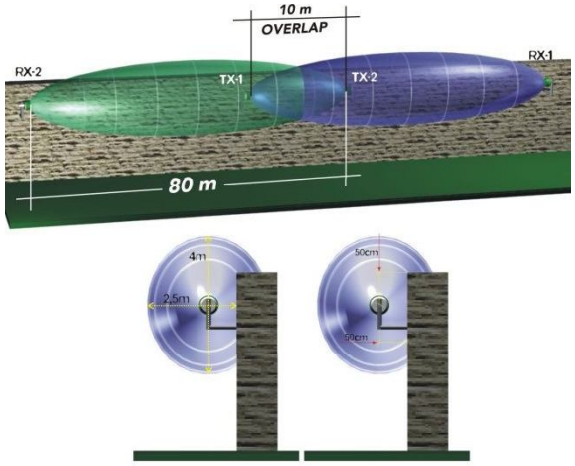
Why PIDS?

Common Intrusion Detection Techniques

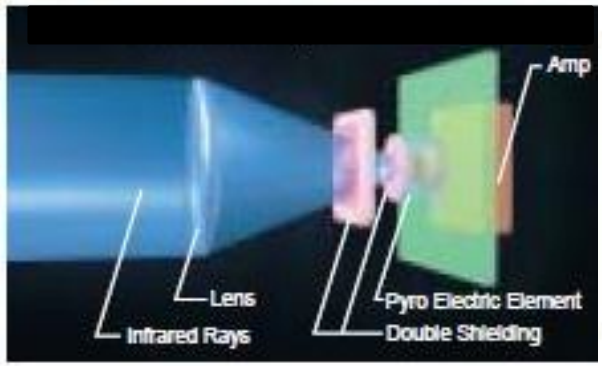
Infra-Red Beam

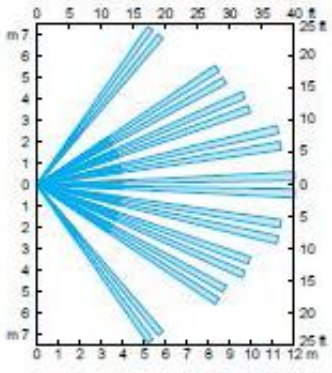


Microwave Barrier



Passive Infra-Red/Ultrasound





CCTV Analytics

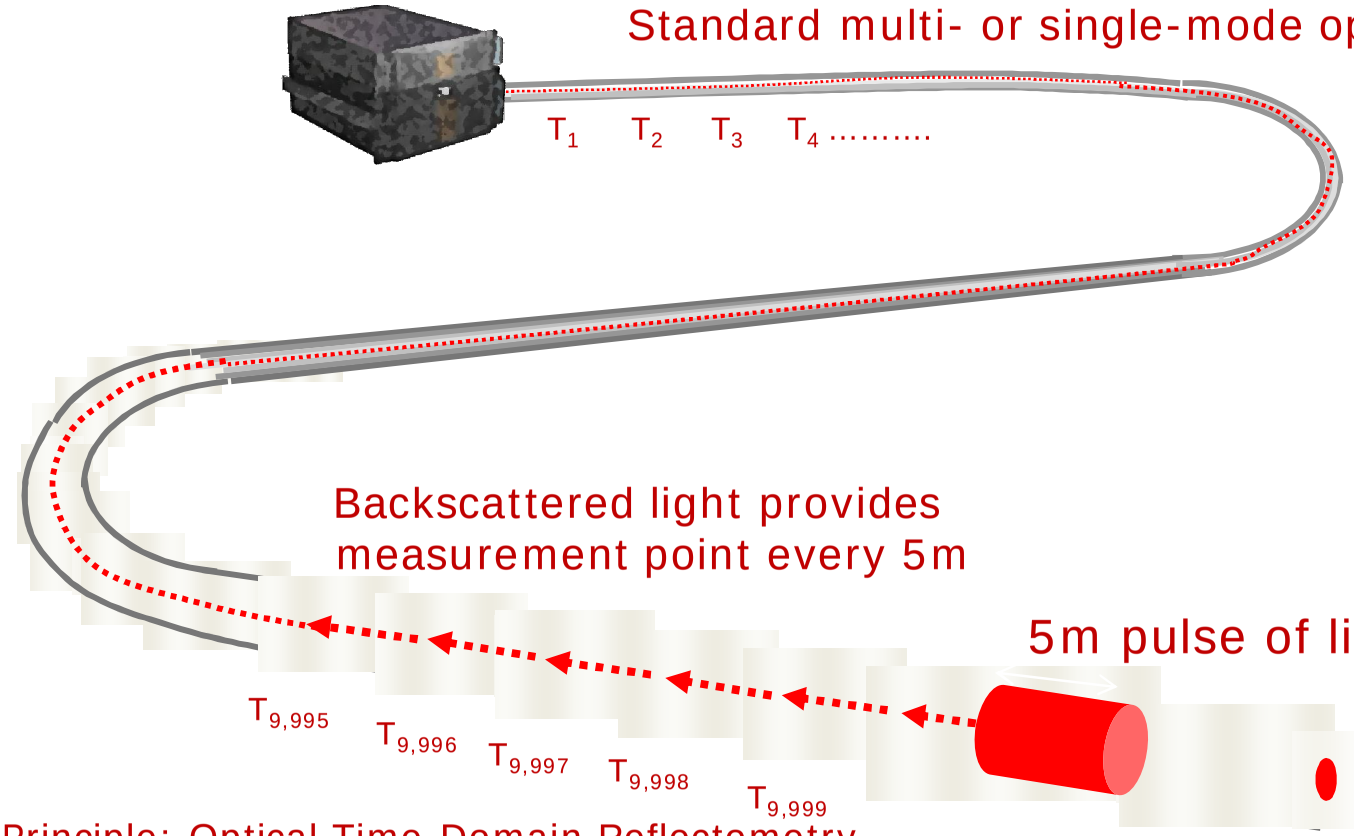
commtel NETWORKS
Let's reach the next level

Essential Requirements for Pipeline Intrusion Detection

- Long sensing range (>20km continuous distributed sensing, preferably longer)
- High sensitivity along entire range without linear variation
- Clear discrimination and accurate location of intrusion
- Invulnerable to defeating by jamming or bypassing
- Unobtrusive installation without power or special infrastructure requirements outside the instrumentation room
- Integration of Alarms with rapid response system
- Long maintenance-free life-span

Acousto-optic Distributed Sensing

The fibre is the sensor
Measurements all along a 20km fibre = 4,000 sensors!!



$$w = \frac{c}{n} . \Delta\tau$$

Pulse Width (ns)	Spatial Resolution (m)
10	1
50	5
100	10

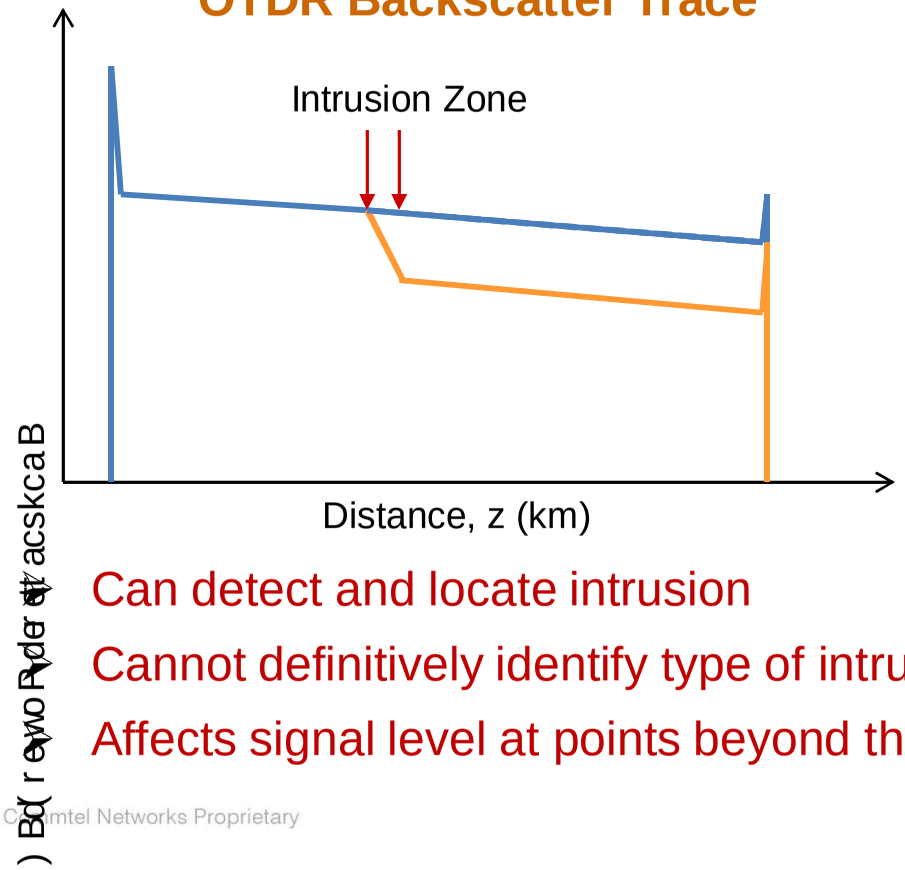
Principle: Optical Time-Domain Reflectometry

commtel NETWORKS
Let's reach the next level

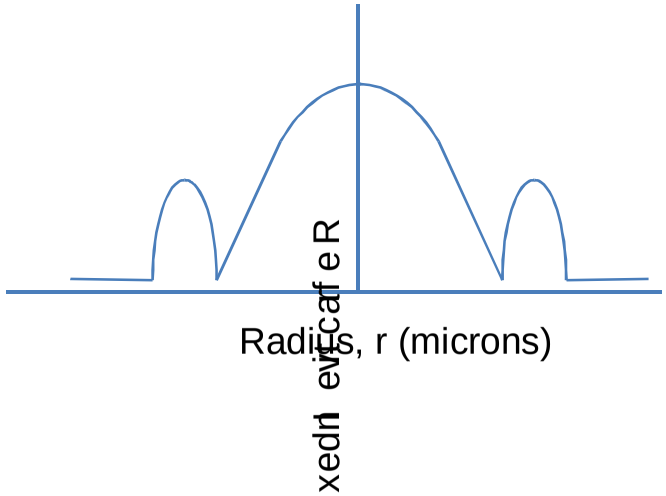
Direct OTDR Intensity Measurement

$$P_s(z) = S.\alpha_s.P_{0.}\int_0^w \exp(-2\alpha\left(z+\frac{x}{2}\right)dx$$

OTDR Backscatter Trace



Bend-Sensitive Fiber Core



Can detect and locate intrusion

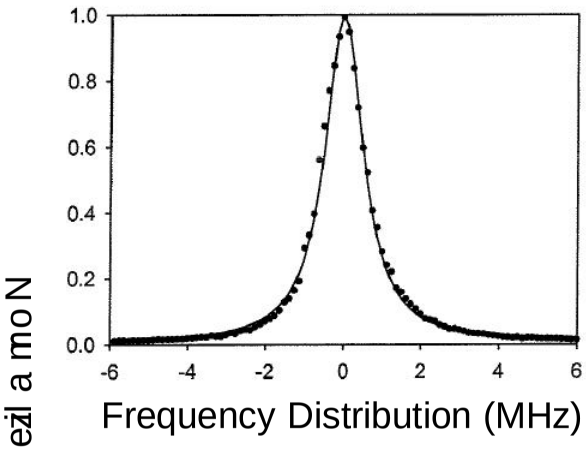
Cannot definitively identify type of intrusion

Affects signal level at points beyond the intrusion zone

commtel NETWORKS
Let's reach the next level

Coherent Signal Detection

Laser Spectral Linewidth

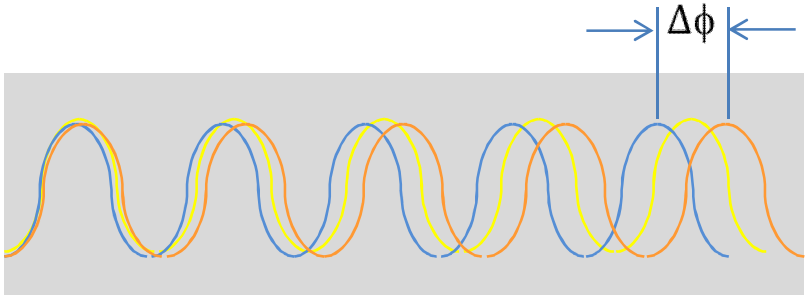


Coherence Length

$$L_C = \frac{\lambda^2}{n\Delta\lambda}$$

$\Delta\lambda$ (nm)	$\Delta\nu$	L_c
2	250GHz	0.8 mm
0.2	25GHz	8mm
0.00004	5MHz	40m
0.000004	500KHz	400m

Manifestation of Phase Difference



Effect on Backreflected Power

$$P_S = C.\langle \overrightarrow{E_1}.\overrightarrow{E_2} \rangle = C.[E_1^2 + E_2^2 + 2E_1E_2cos\phi]$$

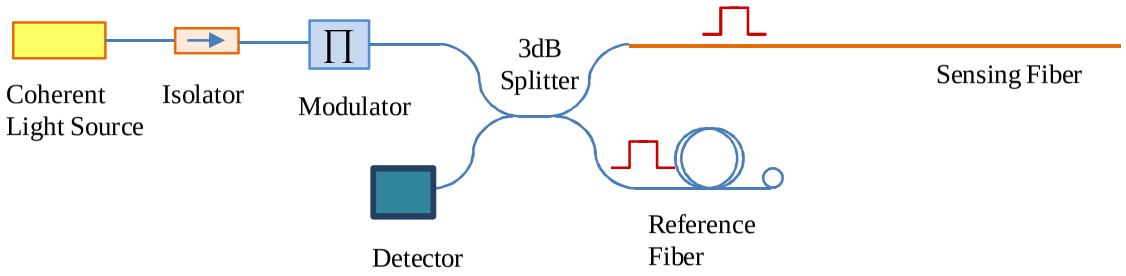
Localized Phase Change from Perturbations

$$\Delta\phi = \frac{4\pi|\Delta nl|}{\lambda}$$

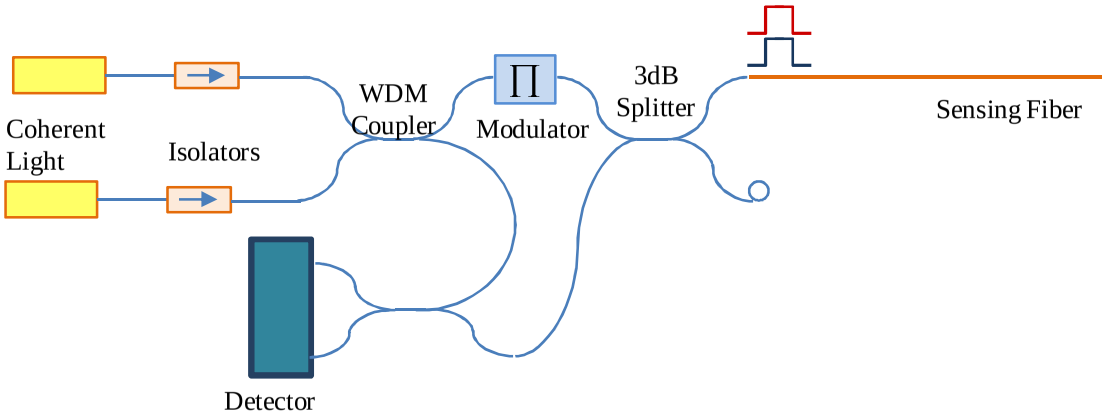
commtel NETWORKS
Let's reach the next level

Homodyne and Heterodyne Detection

Homodyne Detection $P_S = C.\langle \overrightarrow{E_1}.\overrightarrow{E_2} \rangle = C.[E_1^2 + E_2^2 + 2E_1E_2cos\phi]$

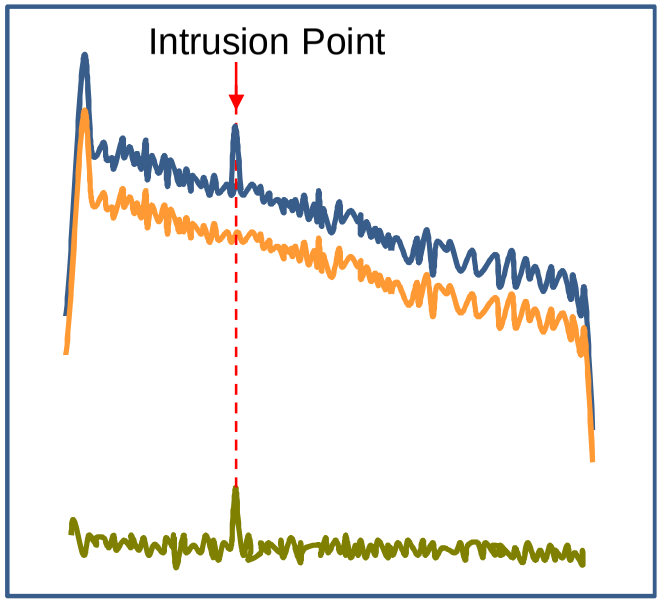


Heterodyne Detection $P_S = C[E_1^2 + E_2^2 + 2E_1E_2\cos(2\pi\Delta vt + \phi)]$

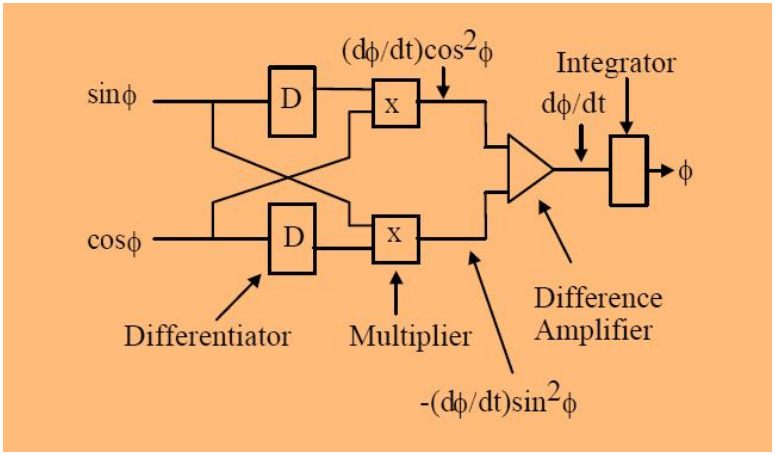


commtel NETWORKS
Let's reach the next level

Acoustic Signal Extraction

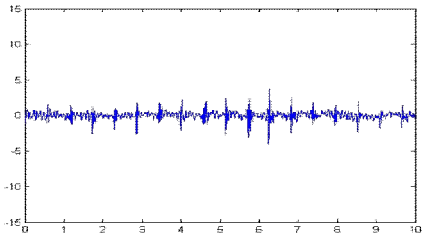


Demodulation Electronic Block

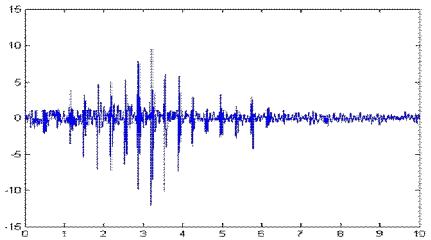


- Quadrature demodulation through sin-cosine local oscillators
- Acoustic frequency range depends on
  - Carrier Frequency (5-20MHz)
  - ADC Sampling Rate
  - Sweep Rate (constrained by round-trip time)
- Practical sensor construction must consider laser drift, temperature and polarization effects

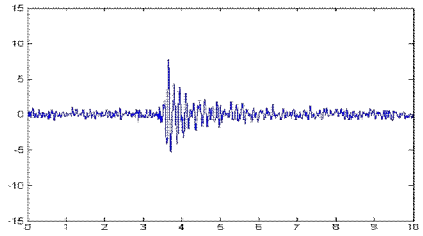
Acoustic Signal Extraction



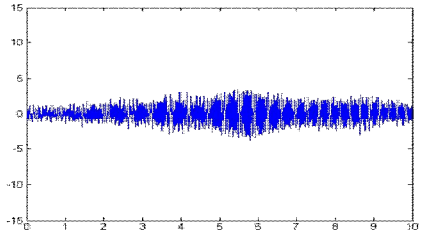
Man walking



Man running



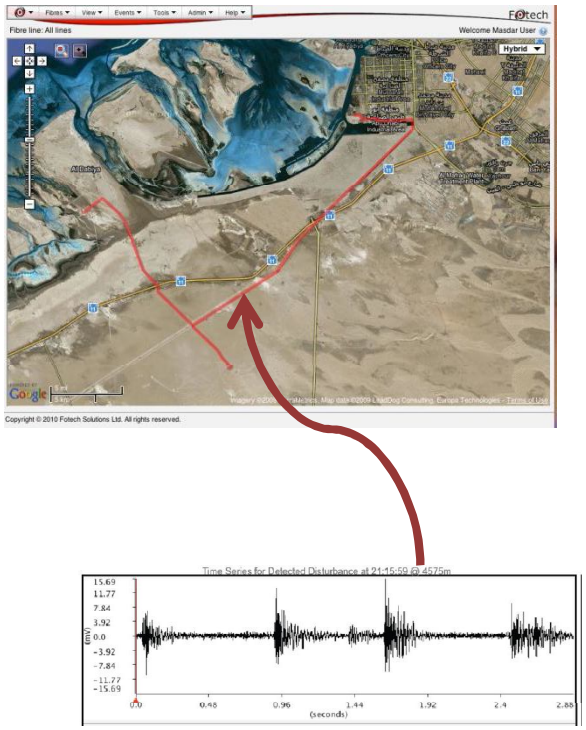
Heavy gunfire
(6km range)



Helicopter at altitude

- Identifies type and location of event (within 1-10 m)
- Range of 50 km using a single instrument
- No linear variation of sensitivity
- Uses standard communication fiber
- No electronics at sensing locations – tamper proof

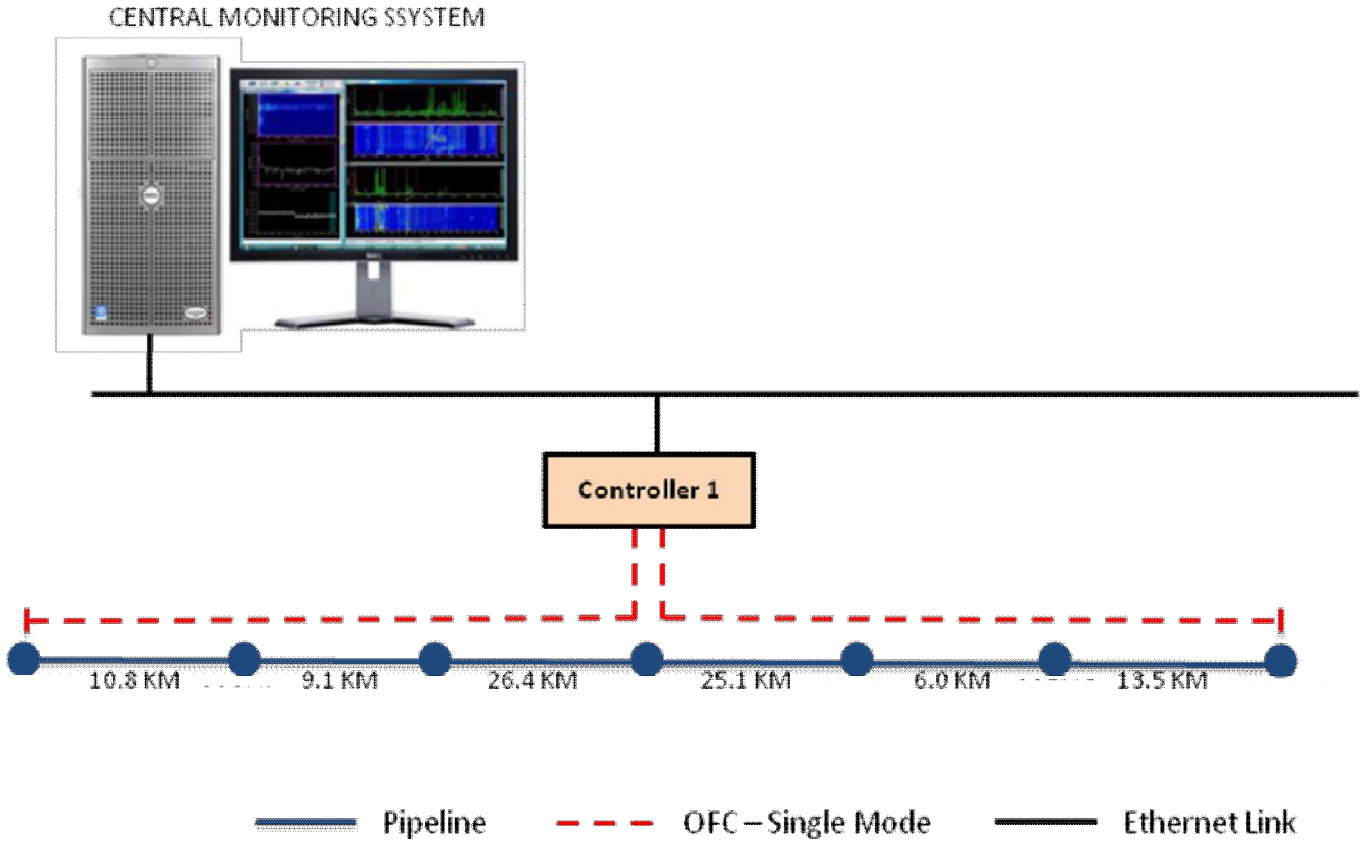
Additional Requirements for Pipeline Instrusion Detection



- Automated alertion and logging of activities such as digging, walking, vehicle movement at specified distances, pig-tracking and fiber-break
- Map of pipeline on GIS database with visualization of acoustic information in each segment (channel)
- Acoustic analysis with audio play-back
- Ability to discriminate between false alarms (acoustic cross-talk), nuisance alarms and background noise by setting thresholds and confidence levels
- Communication interface with adequate bandwidth to transfer real-time data from remotely located sensors to monitoring stations

commtel NETWORKS
Let's reach the next level

PIDS Design Example



commtel NETWORKS
Let's reach the next level

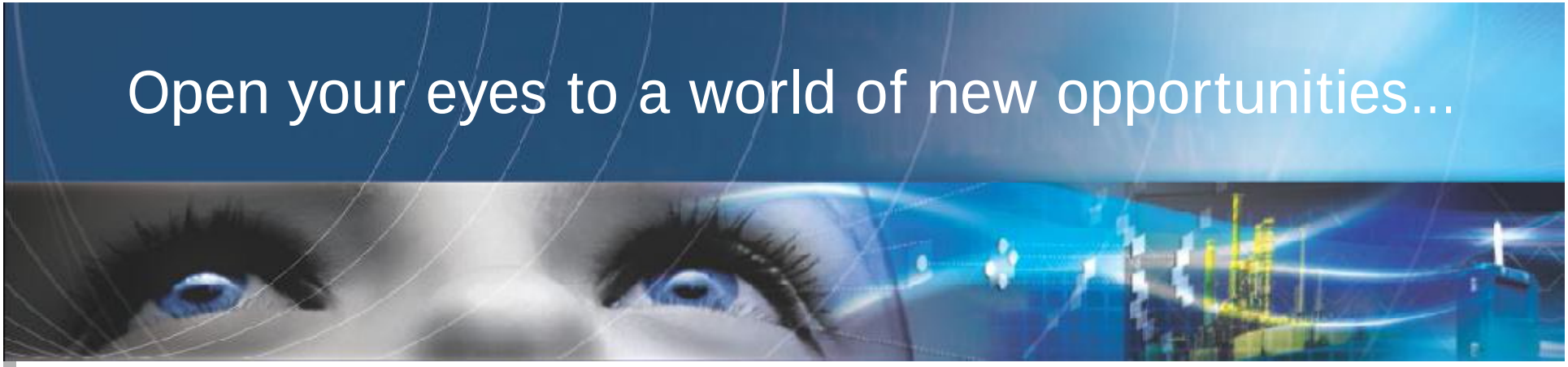
Summary

- Reliable PIDS is important for asset protection, public safety and environmental safety
- Pipeline intrusion detection has unique requirements which cannot be met by many short-range perimeter intrusion detectors
- Fiber Optics using OTDR are well suited for real-time long-range distributed sensing
- C-OTDR with fine linewidth lasers enable phase/frequency measurement with high sensitivity to acoustic frequencies
- It is possible to detect, locate and identify intrusions by distributed acoustic sensing
- By adding user-friendly interface and alarm integration, fiber optic distributed acoustic sensing is well suited for pipeline intrusion detection

Questions & Answers

uhmanyam@commtelnetworks.com

commtel NETWORKS
Let's reach the next level



ISA100 – Field Wireless Solutions

Date : 26th September 2011

Venue : ISA Delhi Section – PNID 2011

ISA100Wireless

YOKOGAWA

The History of Radio

vigilantplant.®

- The theory of radio waves was first discovered by the physicist James Clerk Maxwell
  - Born 1831, died 1879
- Maxwell combined the separate theories of Electricity and Magnetism into one Electro-magnetic field
- “Electromagnetic waves” or RADIO
  - Travel through space at the speed of Light

The History of Radio

vigilantplant.®

- Marconi had an early interest in science, and was especially interested in the work of Hertz
- He quickly realized the potential of wireless transmission and filed a British patent
  - Awarded on 2nd July 1897, GB12039
- At 12:00pm on the 12th December 1901 Marconi send and received the first Transatlantic radio transmission

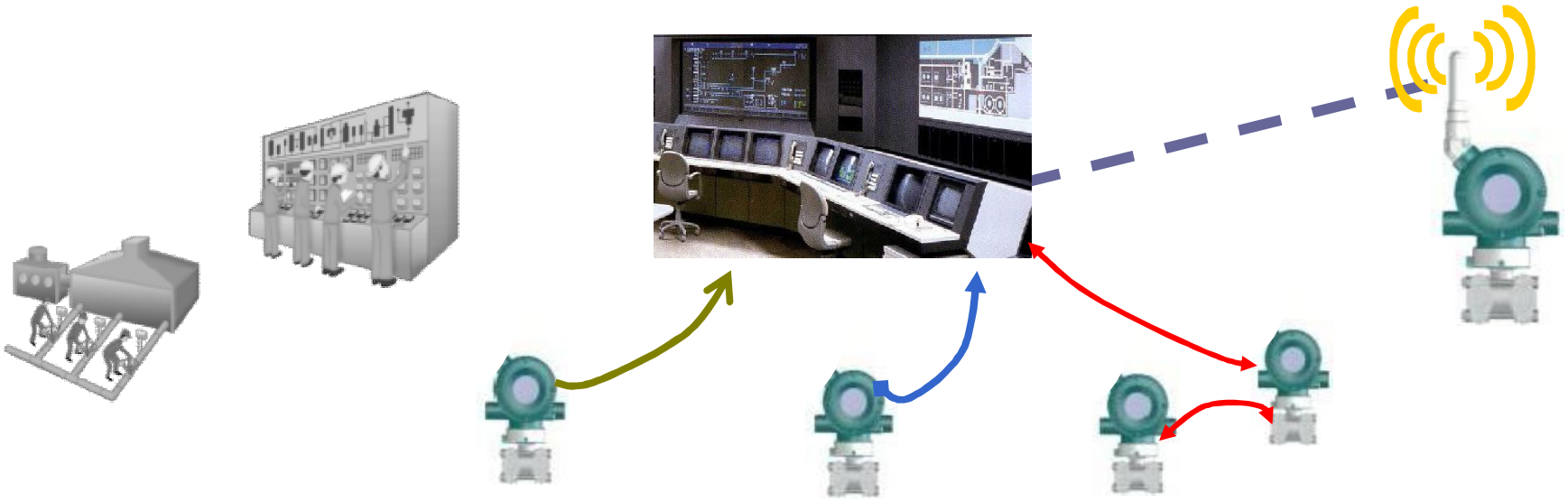
The History of Radio

vigilantplant.®

- On Sunday evening 14th April 1912 the largest passenger ship in the world, Titanic struck an iceberg
- The radio operators onboard were employed by Marconi International Marine
- They sent a distress signal alerting the world and the Carpathia
- Radio had proven it worth…

Evolution of Field digital communication

vigilantplant®



3 – 15 psi Pneumatic

4 - 20 mA Analogue

4 - 20mA Smart

Fieldbus

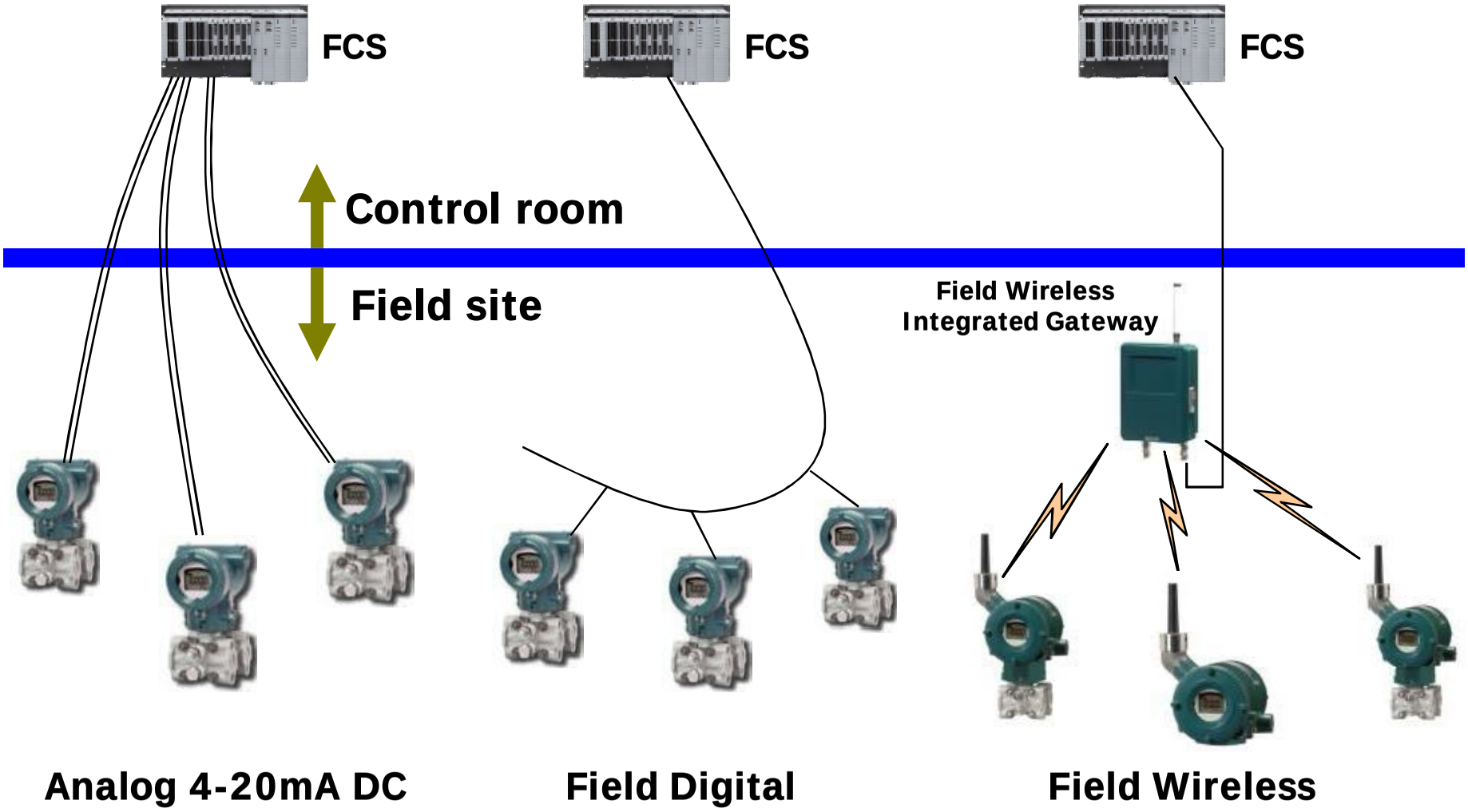
Wireless

1940 1960 1980 2000 2010 2020

Interpreted from ARC report – Pressure transmitter worldwide outlook 2009

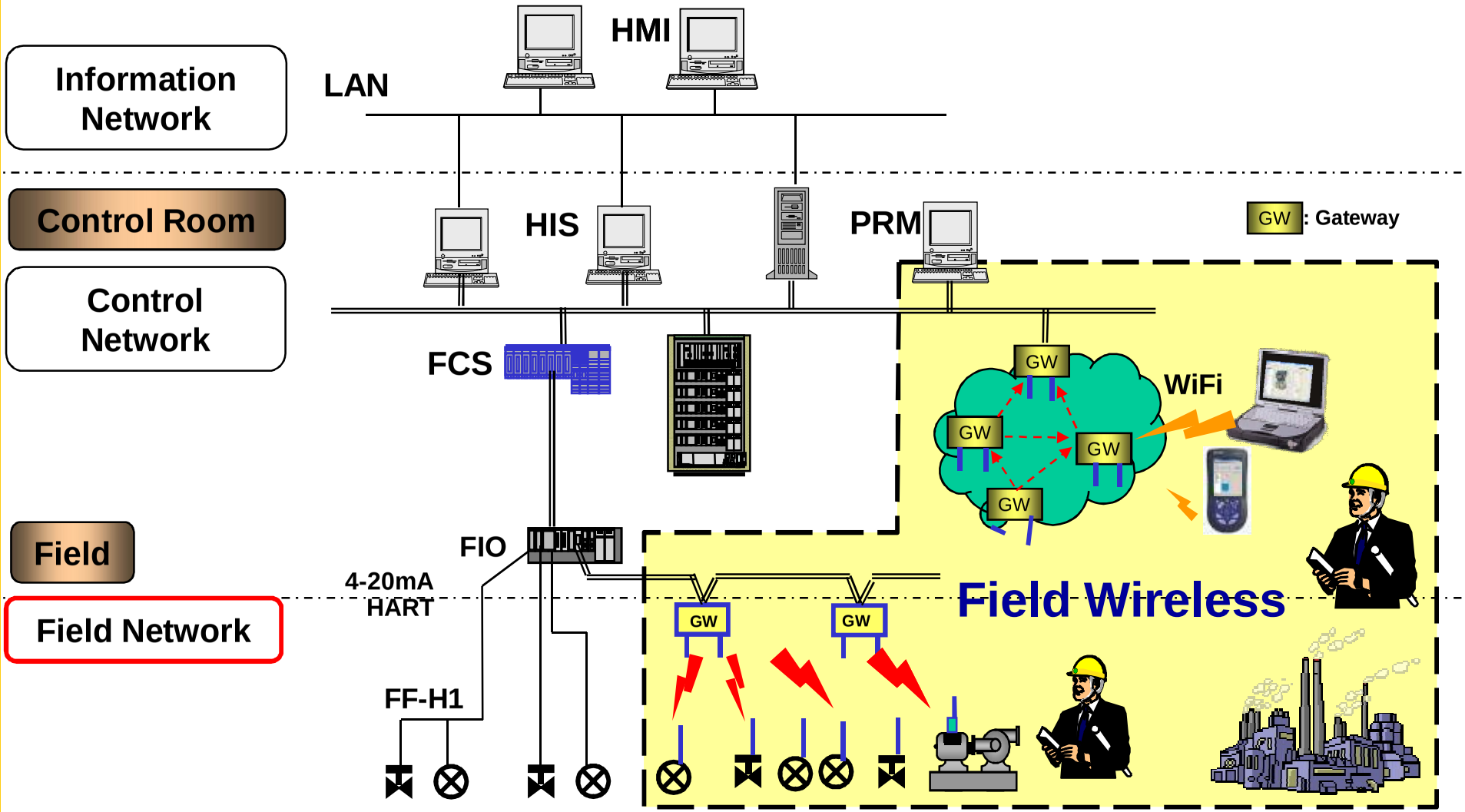
What is Field wireless system ?

vigilantplant®



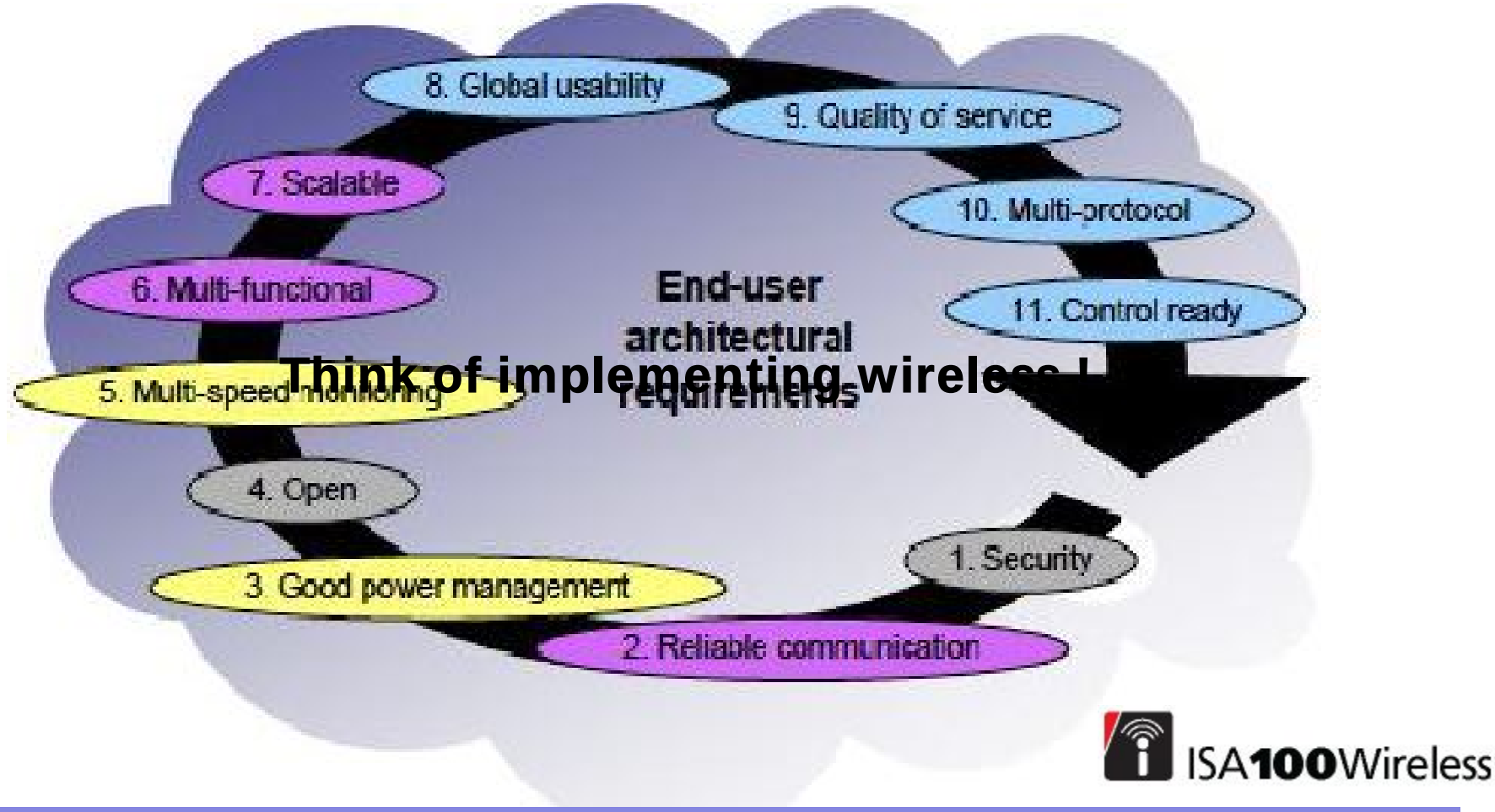
Positioning of Field Wireless Solutions

vigilantplant®



For use in Industrial application

vigilantplant®



ISA100 solutions address these …

What is ISA100 ?

vigilantplant®

- **ISA: The International Society of Automation**
  - Founded in 1945, a leading, global, nonprofit organization that is setting the standard for automation
- **ISA100: Wireless Systems for Industrial Automation**
  - Developing a Reliable, Universal family of Wireless Standards
  - Cover many different applications
- **ISA100.11a:**
  - Addresses wireless sensor networks in the operating plant environment
  - The first standard to provide reliable and secure operation on various applications
  - IEC approval as Publically Available Specification (PAC)

ISA100 standard committee?

vigilantplant®

End User driven standard…

The ISA100 standard

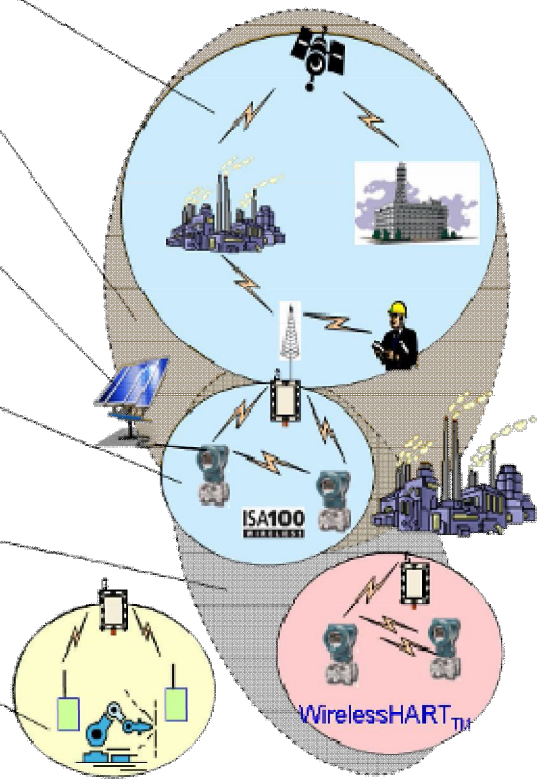
vigilantplant®

Plant-wide needs today and into the future

ISA100 Family of Standards

- Working Group 15 Backhaul Network
- Working Group 14 Trustworthy Wireless
- Power Sources Study Group
- Working Group 3 100.3 Shared documents
- ISA100.12 WirelessHART Convergence
- Working Group 16 Factory Automation
- Working Group 21 People and Asset Tracking

ISA100Wireless



ISA100 has advanced technologies to prevent from data falsification, information leakage and spoofing

- Advanced Encryption Standard (AES)128 Bit Codified
- Atomic International Time (TAI)
- The Join Key Management

Reliable Communication

vigilantplant®

- Channel Hopping to avoid radio interference
- Channel Black listing for coexistence with WiFi