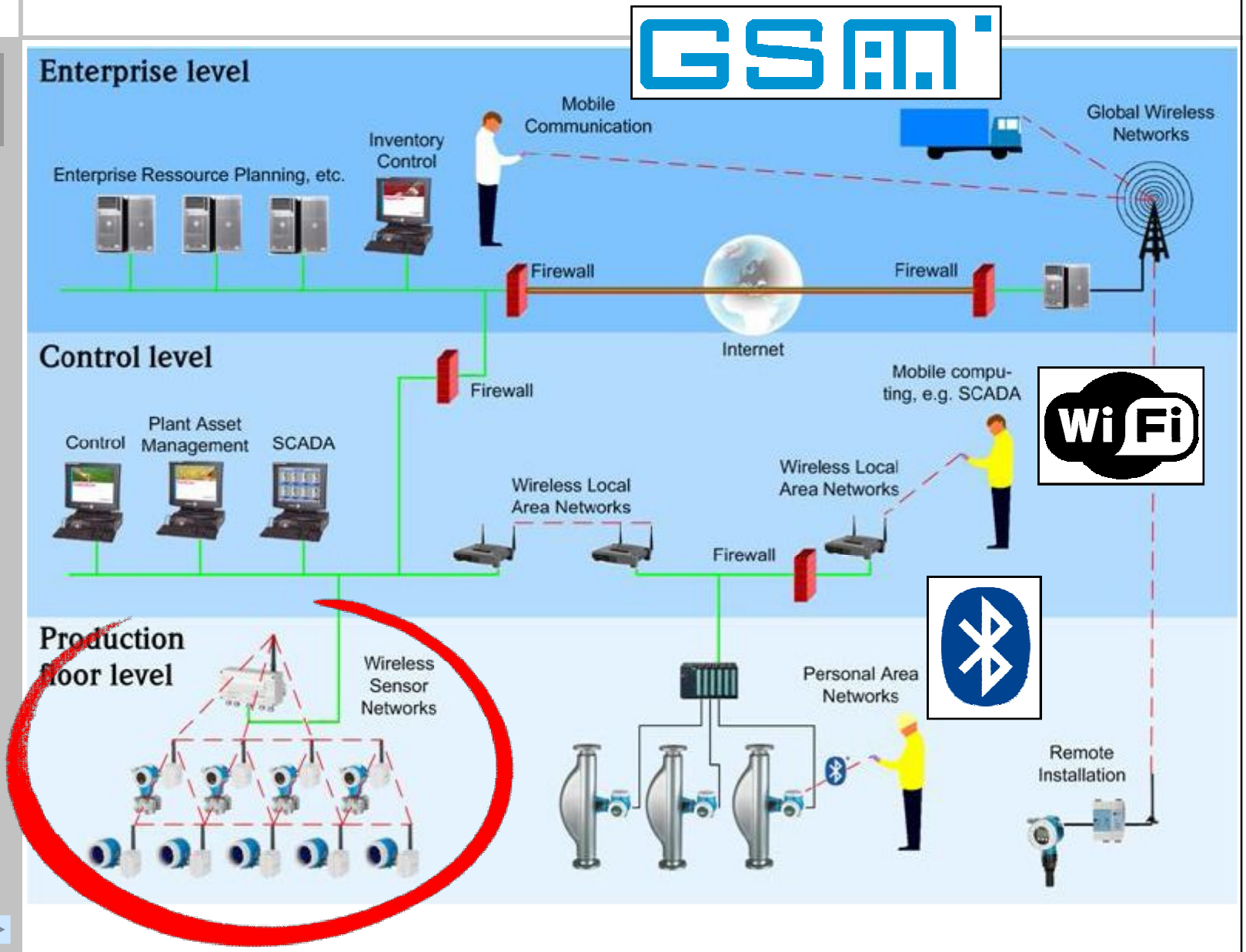
Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economics
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

Wireless is used in process automation in many ways



Each application requires its own wireless technology

Wireless Local Area Networks (WLAN)

Global wireless networks (WAN)

Personal Area Networks (PAN)

Local Wireless Sensor Networks

Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

WirelessHART – IEC 62591 Standard

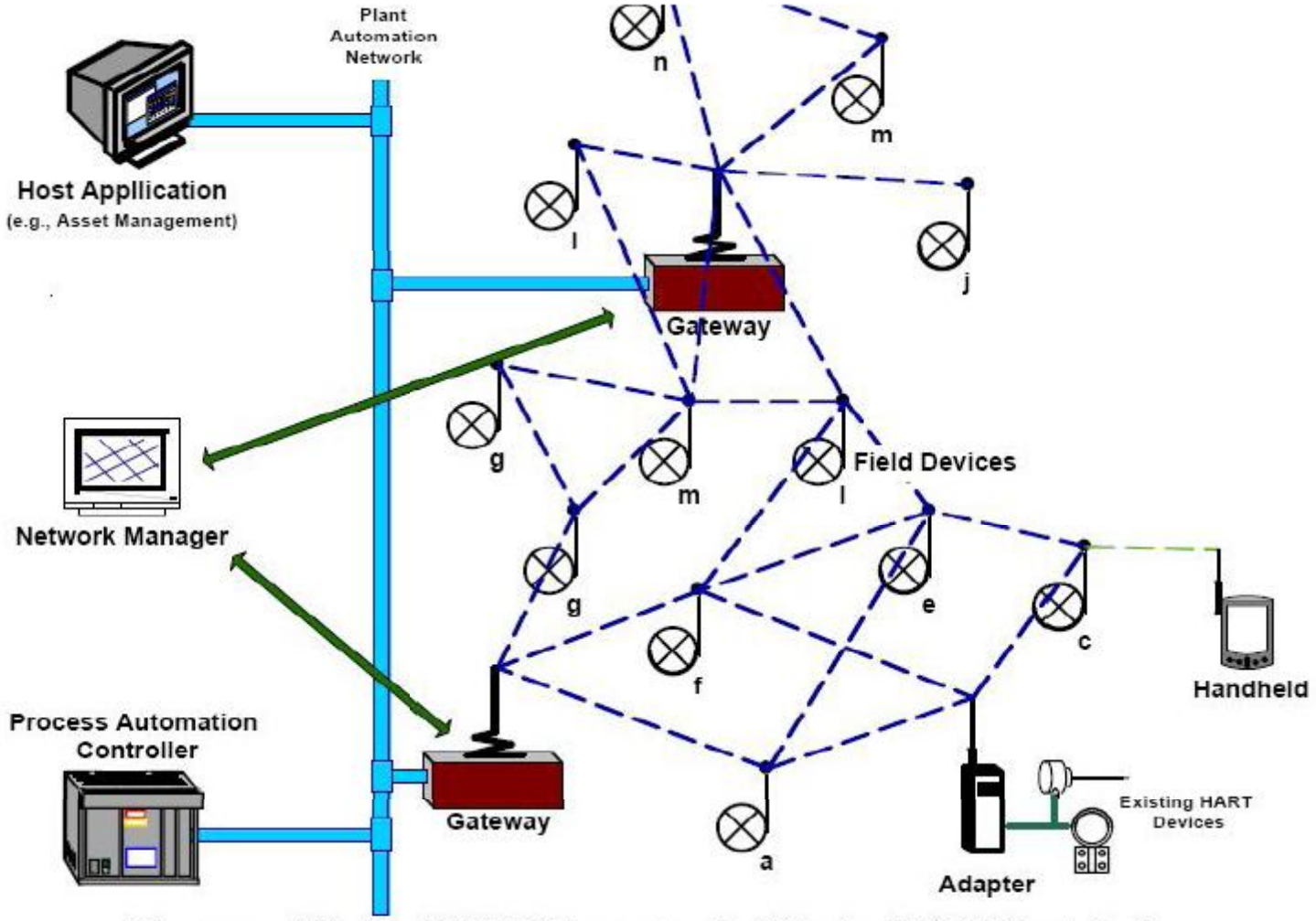


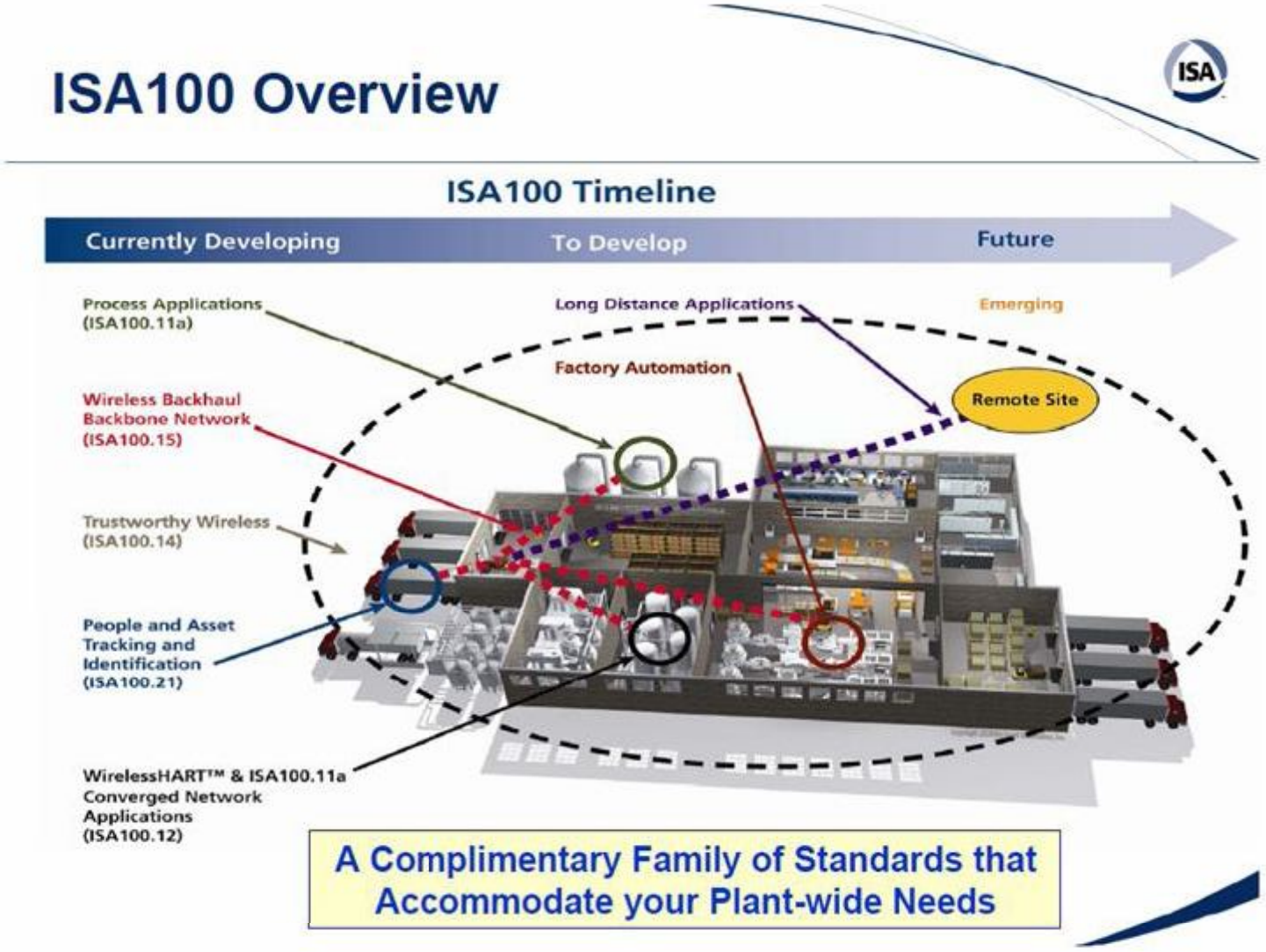
Figure. WirelessHART Elements of a WirelessHART Installation.

Source : HART® Communication Foundation

WirelessHART – Key benefits

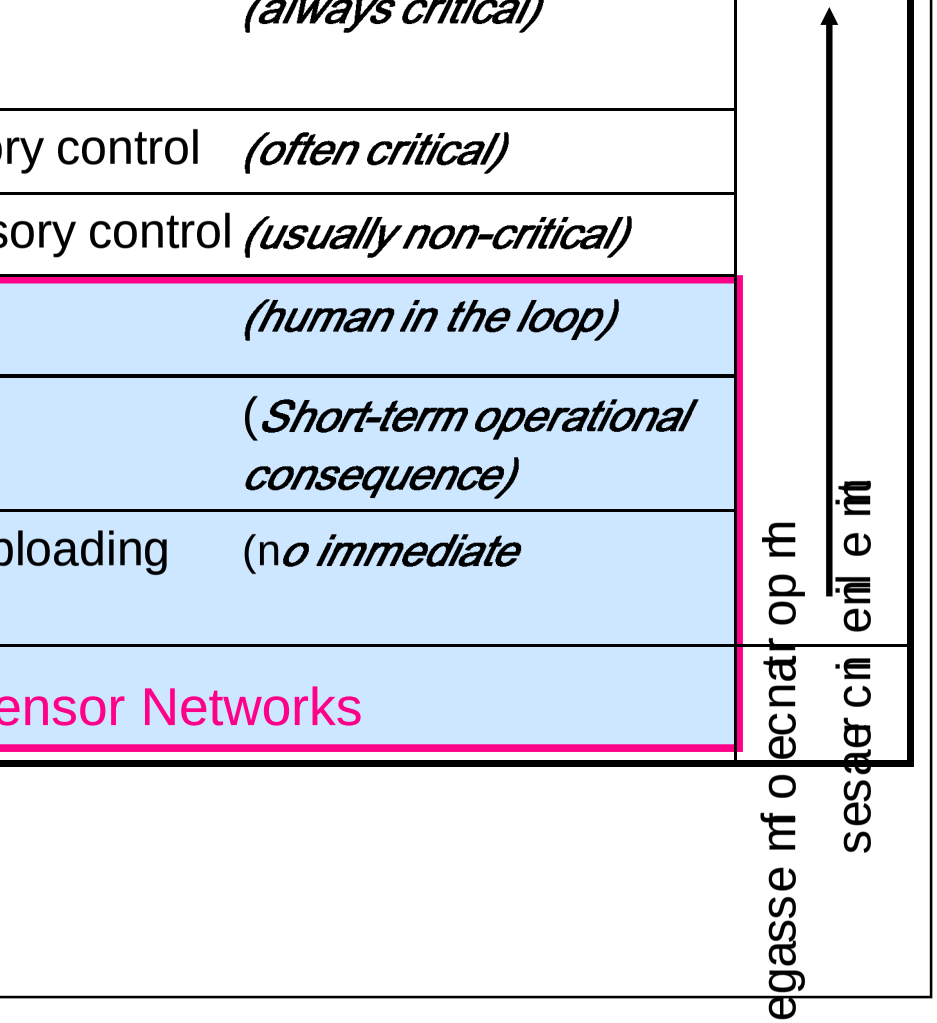
- HART technology has been serving the process automation industry for the last 20 years.
- The HART communication protocol is an open standard, master-slave token passing network protocol, where devices are connected over 4-20 mA analog loop.
- *Wireless*HART is a key part of the HART field communications protocol revision 7.1.
- It adds *Wireless* capability with existing HART devices, commands and tools.
- It is compatible with existing HART devices and applications
- It is a secure and robust mesh networking technology operating in the 2.4 GHz ISM radio band.
- It uses IEEE 802.15.4 compatible DSSS radios with channel hopping on a packet by packet basis.
- It uses TDMA technology to arbitrate and co-ordinate communications between the network devices.
- It is designed to be simple, reliable and useful.
- All *Wireless*HART devices shall support Device Description Language (DDL).

ISA 100 - PAS

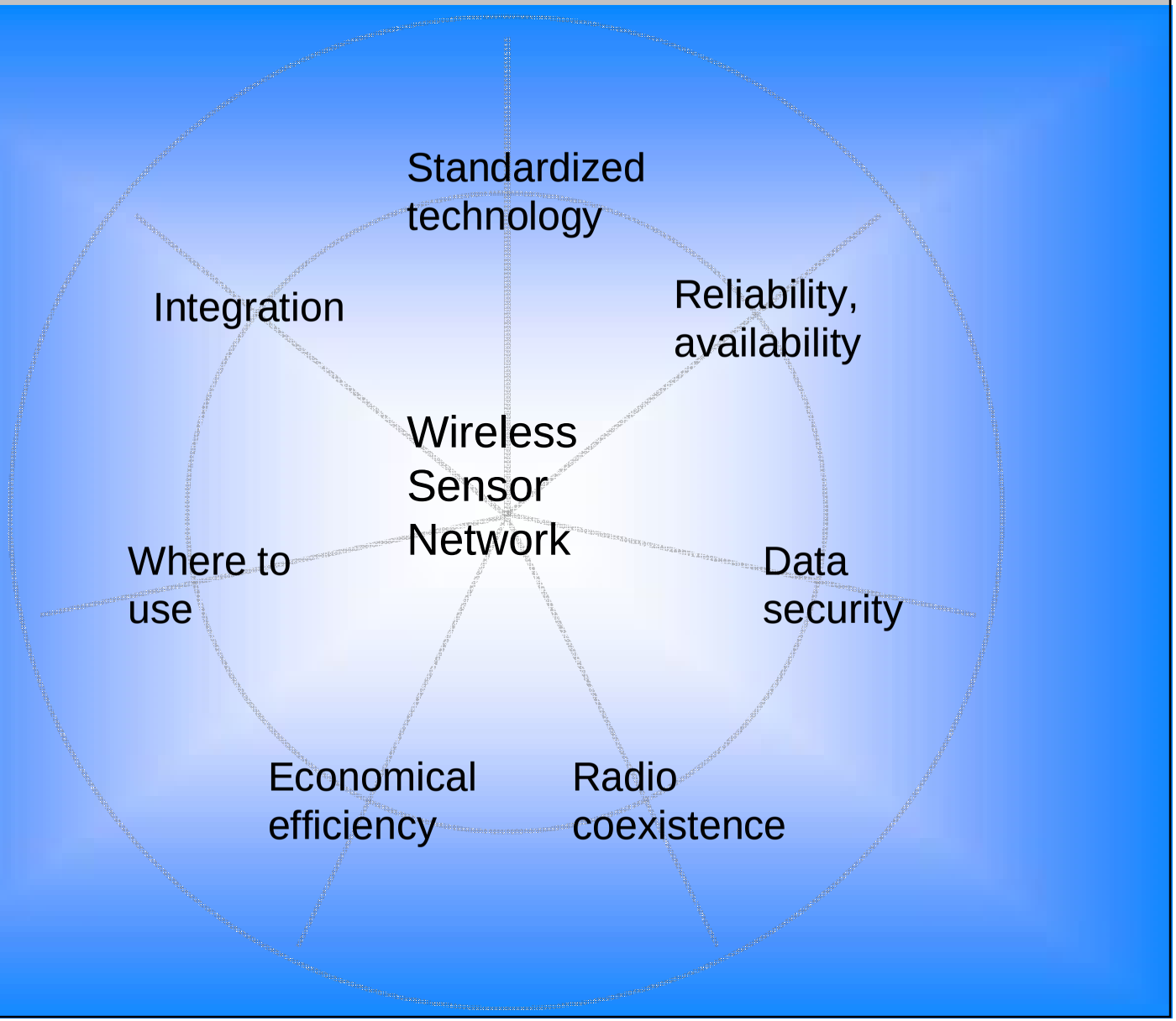

ISA100 Overview
ISA
ISA100 Timeline
Currently Developing
To Develop
Future
Process Applications (ISA100.11a)
Long Distance Applications
Emerging
Factory Automation
Remote Site
Wireless Backhaul Backbone Network (ISA100.15)
Trustworthy Wireless (ISA100.14)
People and Asset Tracking and Identification (ISA100.21)
WirelessHART™ & ISA100.11a Converged Network Applications (ISA100.12)
A Complimentary Family of Standards that Accommodate your Plant-wide Needs

Wireless Technology Use

NAMUR Class	*ISA* (Comprehensive Concept Usage classes of wireless data networks.)	
A – Safety	Class 0: Emergency action	*(always critical)*
B – Control	Class 1: Closed loop regulatory control	*(often critical)*
	Class 2: Closed loop supervisory control	*(usually non-critical)*
	Class 3: Open loop control	*(human in the loop)*
C – Monitoring	Class 4: Alerting	(*Short-term operational consequence)*
	Class 5: Logging, down- or uploading	(n*o immediate operational consequence)*
	Wireless Sensor Networks	



WSN user requirements



Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

WirelessHART typically consists of 3 components

WirelessHART Fieldgate

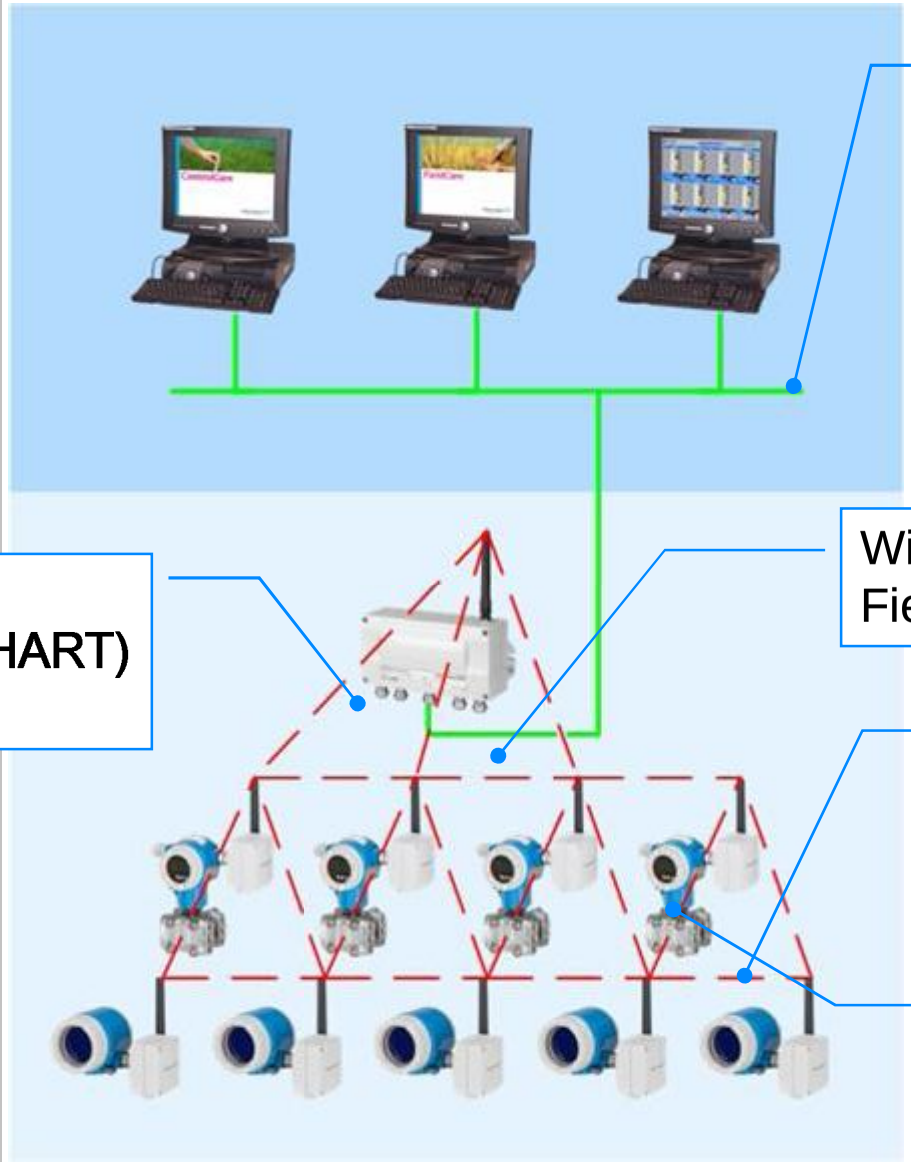
WirelessHART Adapter

DTM/DD/OPC

+

+

WirelessHART is interoperable



HTTP

IEC62591 *(Wireless*HART) Network

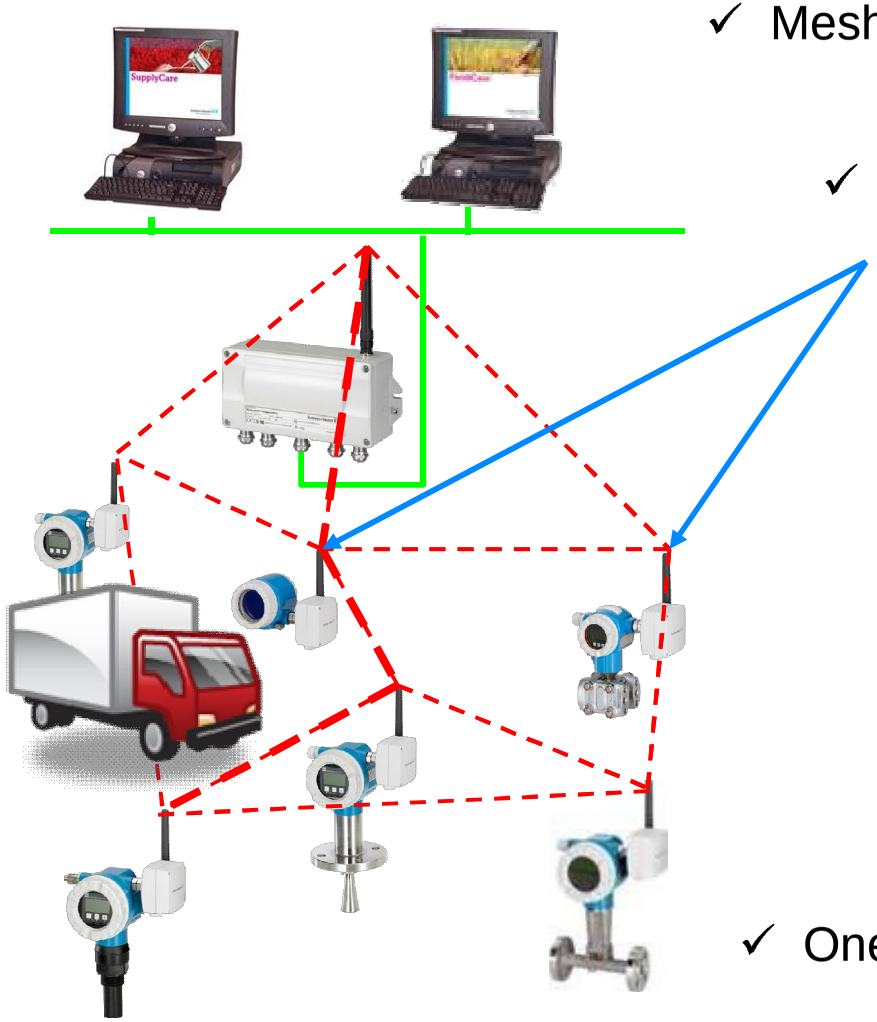
WirelessHART Fieldgate

WirelessHART Adapter

Any HART or 4-20 mA field device

Unique Features of WirelessHART

No expert knowledge required to setup the network



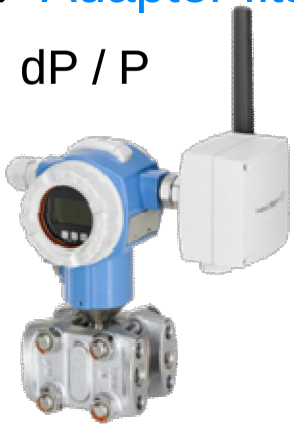
- ✓ Mesh technology: self-organizing and self-healing → easy-to-deploy
- ✓ Range from antenna to antenna up to 250 m
- ✓ Data encryption for privacy and authentication
- ✓ Highest energy efficiency by using state-of-the-art communication technology
- ✓ License-free 2.4 GHz with frequency hopping for coexistence w/ WLAN, etc
- ✓ One Gateway supports 250 devices

WirelessHART Adapters - Fits to all HART & 4-20ma devices

Wired interface of adapter talks HART and measures 4-20 mA.

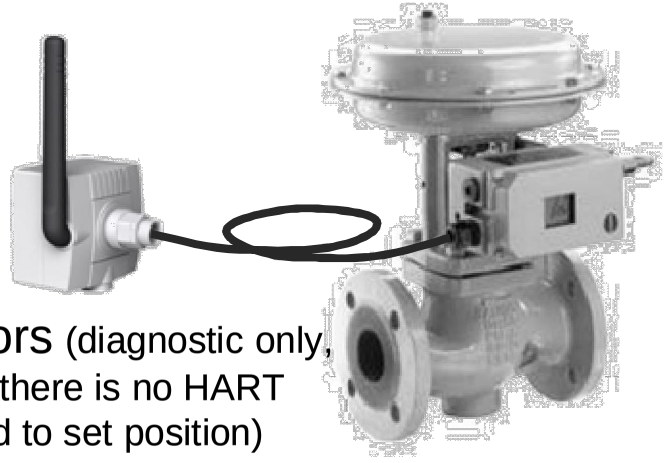
→ Adapter fits to ALL HART and 4-20 mA devices

dP / P



T

L



Actuators (diagnostic only, because there is no HART command to set position)

Repeater to support network

WirelessHART Gateway

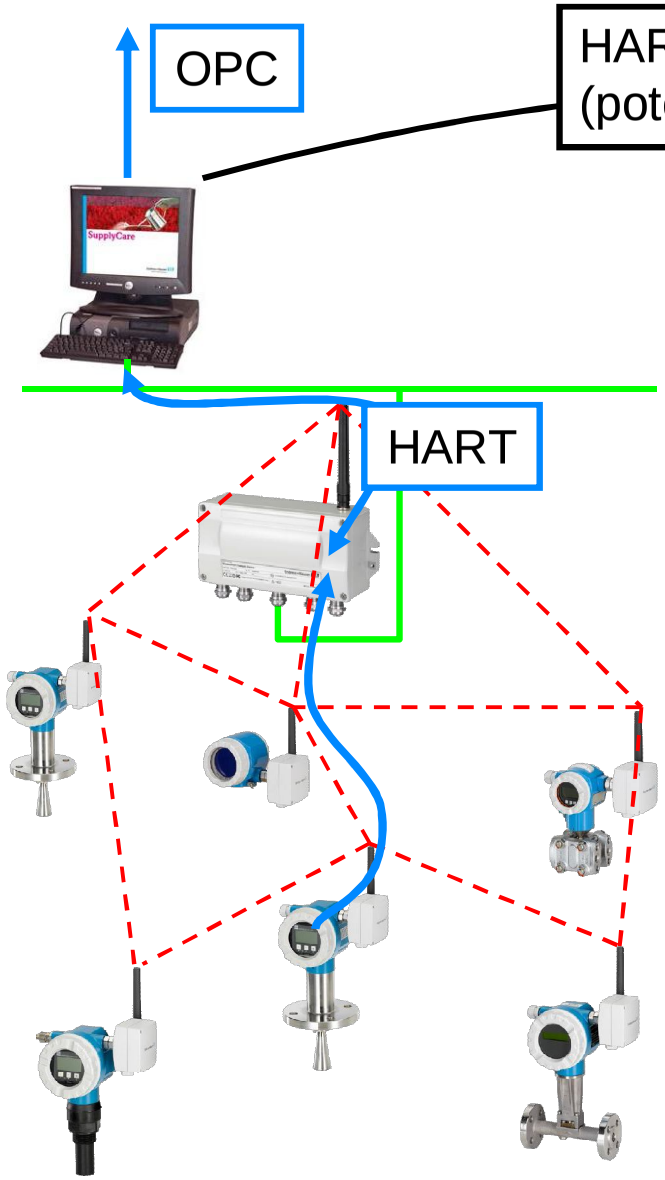
- WirelessHART Network
  - Includes software for network management and security management
  - up to 250 participants
- Protocols
  - HART over RS485 and HART over Ethernet; both are used for the OPC connectivity
  - Modbus/RTU over RS485 and Modbus/TCP over Ethernet
  - HTTPS over Ethernet, i.e. HTML pages for configuration
  - DHCP, NTP client for automatic configuration of IP-address and system clock

WirelessHART Gateway

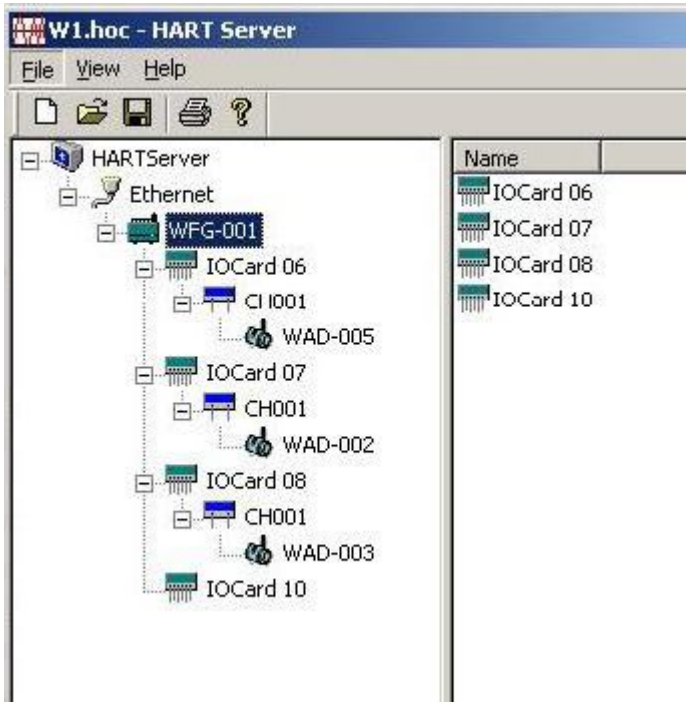
- Enclosure
  - Polyester IP65, IP66 NEMA 4
  - Aluminum IP67 NEMA 4X

- Energy supply
  - 24 VDC (5W, typical)
  - Full galvanic isolation & redundant, i.e. if one fails the second power input is used
  - Voltage monitoring
- Hazardous area
  - Optional version which can be mounted it Zone 2 (ATEX)

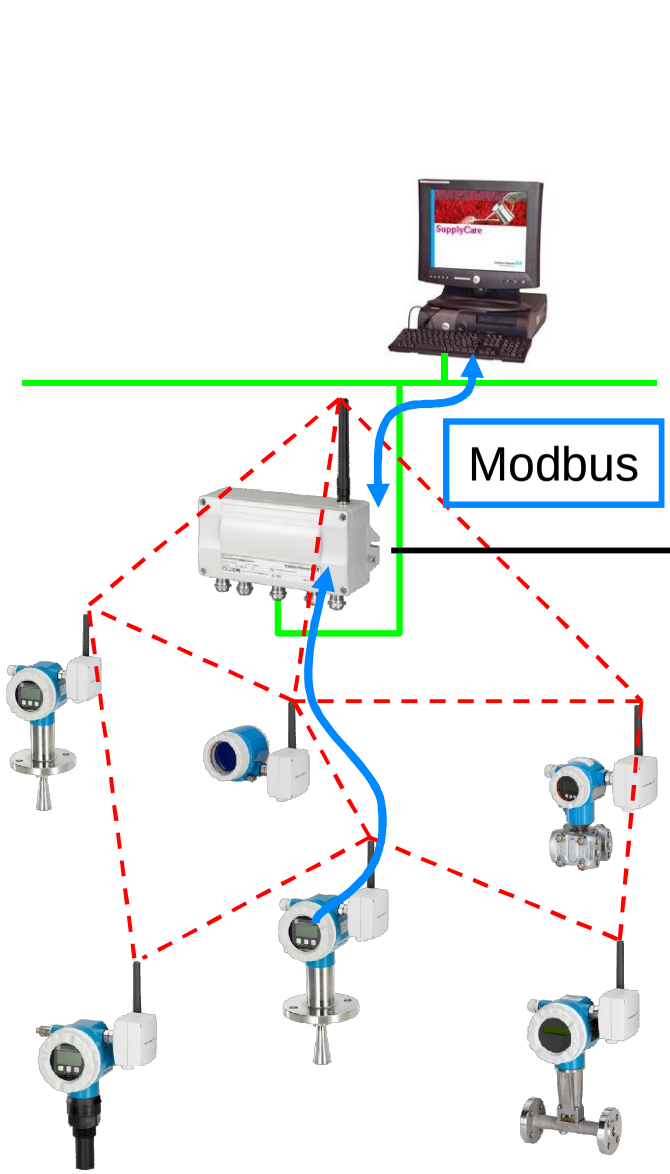
Integration via OPC Server to DCS or SCADA (HART over Ethernet)

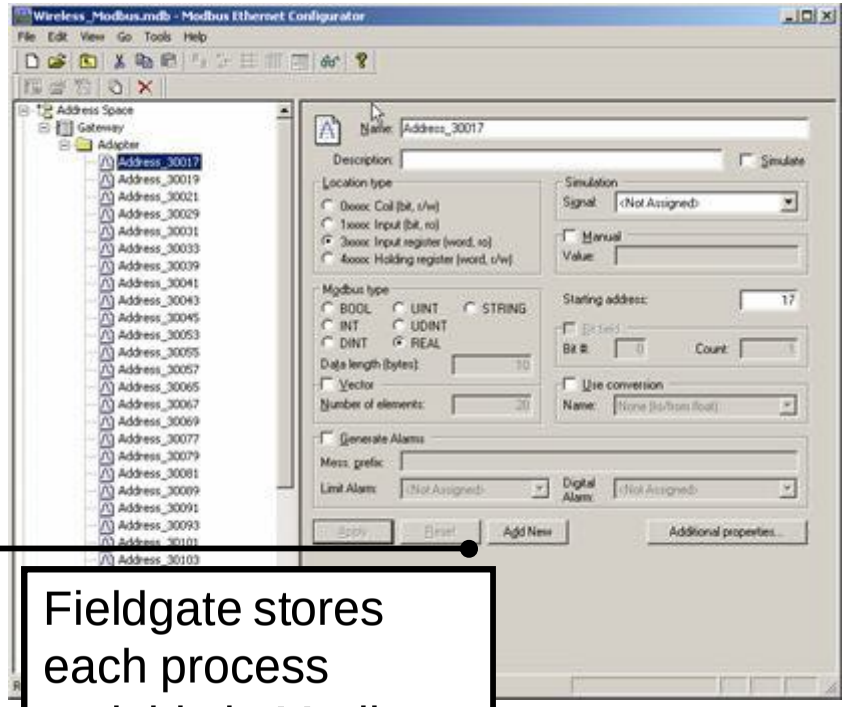


HART-OPC-Server runs one PC
(potentially on the same PC as OPC client)



Integration via Modbus to DCS & PLC





Fieldgate stores each process variable in Modbus register

Explosion protection

Adapter

- ATEX II 2G Ex ia IIC T4
- ATEX II 2G Ex ia IIC T4,
  ATEX II 2D Ex tD A21
- CSA IS Cl.I,II,III Div.1 Gr.A-G,
  Cl.I Div.2 Gr.A-D, Ex ia
  for US and Canada
- IEC Ex Gb Ex ia IIC T4 Zone 1
- IEC Ex Gb Ex ia IIC T4 Zone 1,
  Ex dB tD (iaD) IIIC A21 Zone 21

Fieldgate

- ATEX II 3 G Ex nA II T4

- Battery exchangeable within
  hazardous area

Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

Security Threats in Wireless Networks

- Eavesdropping within & outside network
- Intrusion by rogue devices
- Frequency Jamming
- Denial of service attack using Trojan

Security Management

- Security cannot be disabled. Security is part of the Protocol
- Wireless security management can be broken down into
  - Data Protection (Privacy & Integrity of data)
  - Network Protection (Availability of network)

Data protection

- Data Protection, or Confidentiality, deals with maintaining the Privacy and Integrity of the information being passed over the network
- Prevent eavesdropping by Rogue devices present within or outside the network
  - Communication network encryption key
  - Individual sessions key
  - AES 128 bit encryption
  - Automatic key rotation
- Separate 128 bit joining encryption key
- Message integrity check with each packet
- Authentication of sender & receiver with information in each packet.

Network protection

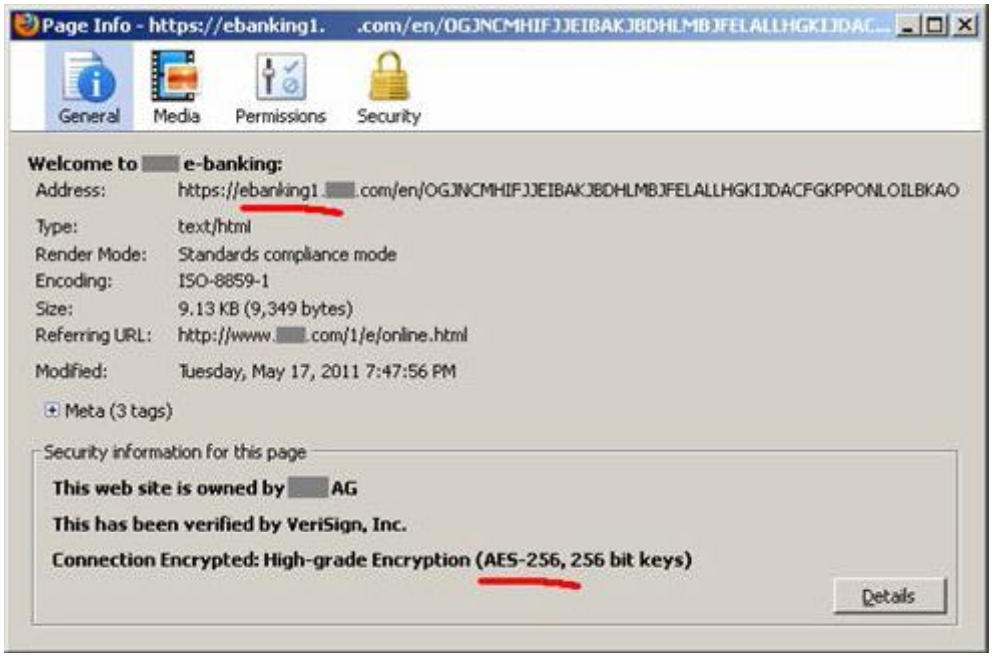
- Network Protection, or Availability, deals with maintaining the functionality of the network in the face of internal and/or external attacks (intentional or unintentional). Like Jamming & Denial of Service attacks
- The Gateway controls the secured authentication during the join process to allow only legitimate devices to join the network. The negotiation during the process is encrypted end-to end
- Channel hopping
- WirelessHART devices can report anomalous conditions that might signal a denial of service attack, such as traffic counters, retransmissions, etc. Other attacks may be indicated by failed access attempts, message integrity check failures, authentication failures, etc.

WirelessHART networks are secure

All data are encrypted using the currently best algorithms

- AES128 officially validated by NIST for privacy
- CCM mode for authentication

which are also used for online banking as well



For comparison

- 10^9 computers trying 10^9 keys in a second would need approximately 10.8 trillion years to crack the AES with a 128-bit key length.
- The age of the universe is about 13.7 billion years!

AES128 = Advanced Encryption Standard with 128-bit keys, protection against eavesdropping
CCM = Mode describing the packaging of the message, protection against tampering, forgery

HART v7 support

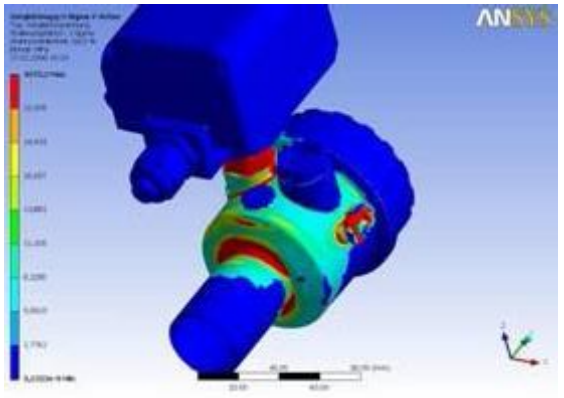
*Wireless*HART

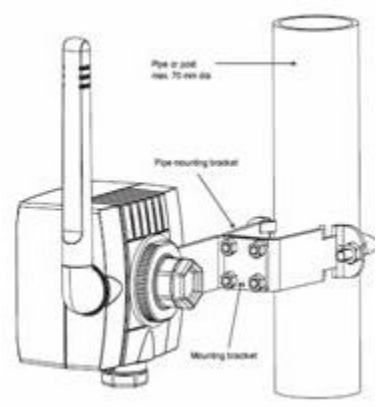
- Based on HART and thus it is straight forward to use
- facilitates the rich diagnose information of HART
- is fully compatible with all HART field devices and all HART host systems

	Protocol Revision		
Feature	**7**	**6**	**5**
Analog Loop Check	✓	✓	✓
Broadcast messaging	✓	✓	✓
Device Calibration	✓	✓	✓
Device Configuration	✓	✓	✓
Device Status	✓	✓	✓
Multi-variable reads	✓	✓	✓
PV with status	✓	✓	✓
32 Character TAG	✓	✓	
All variables with status	✓	✓	
Digital Loop Check	✓	✓	
Enhanced Multi-variable Support	✓	✓	
Local Interface Lock	✓	✓	
Manual ID of device by host	✓	✓	
Peer to peer messages	✓	✓	
Visual ID of device	✓	✓	
Time or Conditions based Alerts	✓		
Report of exceptions	✓		
Synchronized sampling	✓		
Time stamp	✓		
Trends	✓		
Wireless Co-existence	✓		
Wireless Diagnostics	✓		
Wireless mesh & star topology	✓		
Wireless message routing	✓		
Wireless Security	✓		

WirelessHART Adapter enables flexible mounting

- Integral to the instrument
- Remote mount
  - Pipe mounting
  - Wall mounting





Interoperability Test at BASF under NAMUR

- Test under the banner of NAMUR hosted by BASF
- 16 WirelessHART Adapters from Endress+Hauser; other equipmer from ABB, Emerson, MACTek, Pepperl+Fuchs, Siemens
- 4 different applications / sites on BASF's plant in Ludwigshafen
- Process values are incorporated into control systems from ABB and Emerson using Modbus for visualization

WSN user requirements addressed by

WirelessHART

FDT, DD, OPC, Modbus

Standardized technology

Self-organized mesh network

Integration

Reliability, availability

Wireless Sensor Network

Where to use?

Data security

Monitoring

Encryption w/ AES128 & CCM

Economical efficiency

Radio coexistence

Retrofit adapter w/ long battery lifetime

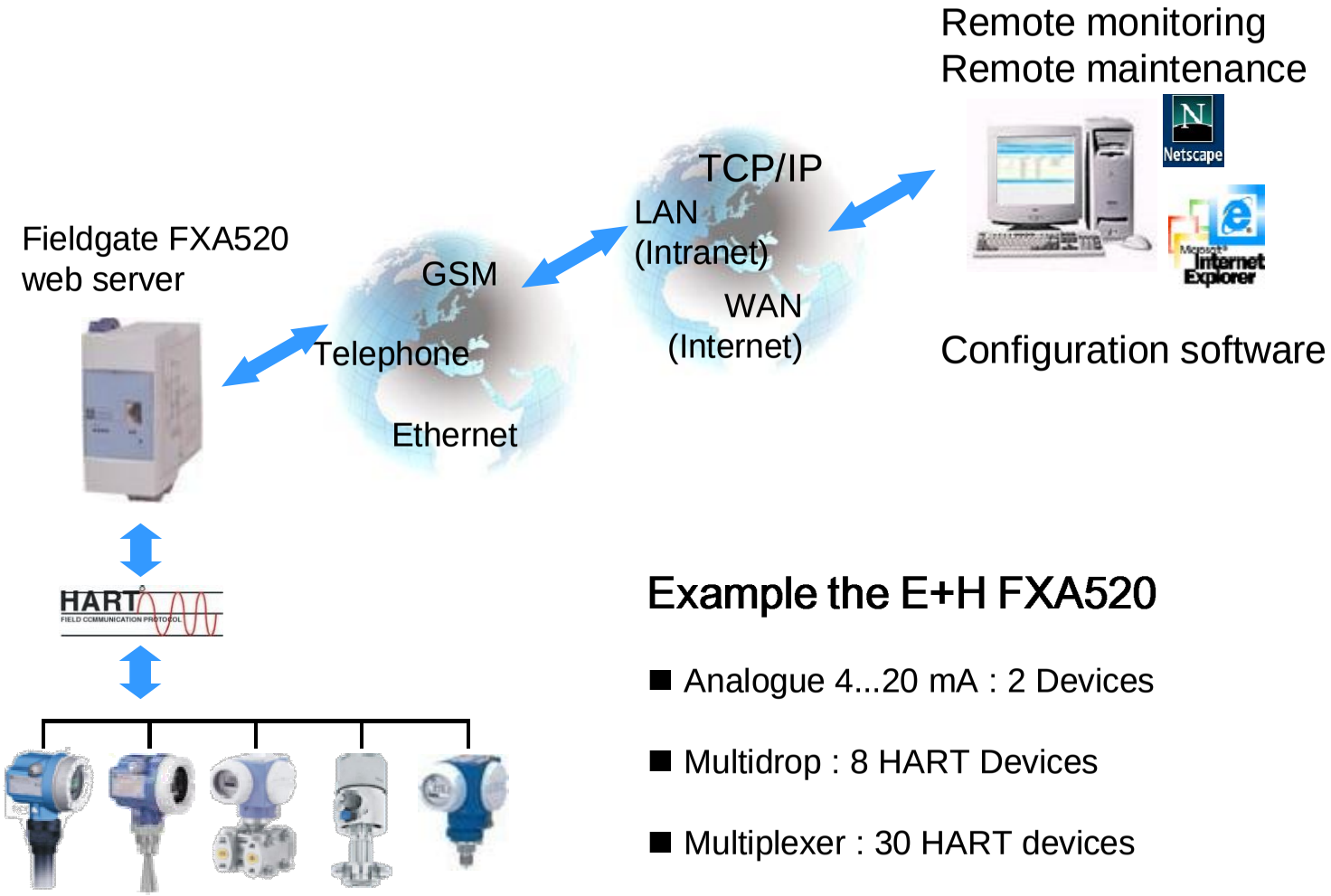
TDMA, FHSS, DSSS, CCA, blacklisting

Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

Remote Wireless Monitoring Inventory & Utilities

Remote Wireless Monitoring Inventory & Utilities



Example the E+H FXA520

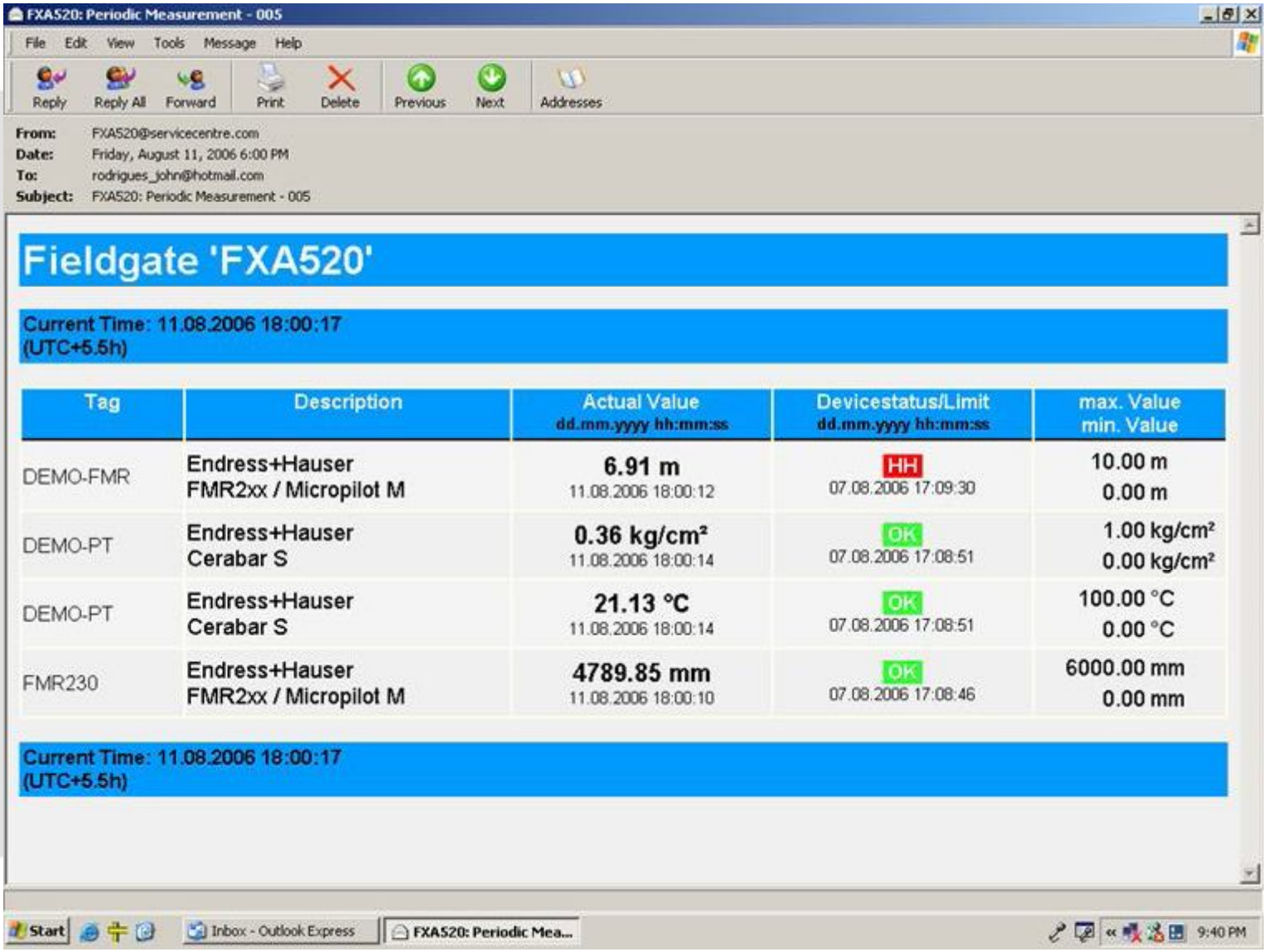
- Analogue 4...20 mA : 2 Devices
- Multidrop : 8 HART Devices
- Multiplexer : 30 HART devices
- Digital Switches support : Yes

Solutions

Wireless Technology in Oil & Gas

Endress+Hauser

Remote Wireless Monitoring Inventory & Utilities



Agenda

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

Wireless Applications in Oil & Gas

- Introduction to Wireless Technologies
- International Wireless Standards for Process Industries
- WirelessHART
  - Standardization
  - Reliability
  - Safety Issues & Security Threats
  - Coexistence
  - Economy
  - Integration
- Remote Wireless Monitoring
- Case Studies Oil & Gas Application Examples

Solutions

Wireless Technology in Oil & Gas

Endress+Hauser

Wireless Applications in Oil & Gas

Process Monitoring

- Crude oil flow measurement
- Gas plant monitoring
- Crude separator pressure monitoring
- Tank Inventory Management
- Offshore gas monitoring
- Oil production monitoring
- Oil well monitoring
- Onshore well head monitoring
- Pipe pressure monitoring
- Relief valve monitoring
- Remote vessel pressure monitoring
- Tank level monitoring
- Environmental surveys

Asset management

- Bearing temperature monitoring
- Pump pressure monitoring
- Vibration monitoring
- Corrosion monitoring

Safety & Mobility

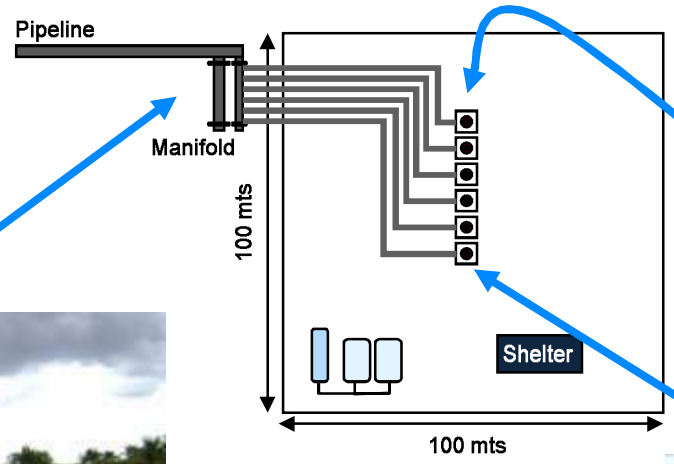
- Local monitoring
- Mustering solution
- Mobile operator & maintenance

Well head monitoring in Oil & Natural Gas

- Application: Monitoring of pressure and temperature at several well heads as well as flow and pressure at corresponding manifold
- Current Wireless Network
  - Each site spread over an area of about 100 × 100 m²
  - 800 Oil well are covered with WirelessHART
  - There are 75 sites
  - Sites are spread in area of 250 sq Kms
- Installation: December 2010
- 20 new wells being drilled every month

Endress+Hauser

Well head monitoring



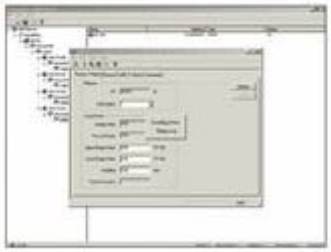
Benefits to the customer

- Compliance with local regulations
- Previously in clipboard rounds monitored values
- Cost-efficient installation in a rapidly changing location
- Improved process operation increases product yield

Tank farm Storage in Refinery Mexico

Endress+Hauser provided:

- Development of the mesh network design to ensure proper communication of all participants
- Support for the proper installation of the equipment
- HMI development for tank level display
- Service implementation of the WirelessHART network
- 16 Levelflex Transmitters FMP40
- 16 WirelessHART Adapters SWA70
- 1 WirelessHART Gateway SWG70
- 1 P View HMI Software SPV200



Fast, Flexible and Economic solution

Refinery

Client : Refinery at Mumbai

Plant : Tank Farm

Scope : Wireless ATFMS

21 Tanks Phase 1

Radars

Wireless Hardware

Tank Vision HW & SW -

Engineering, Design, Manufacturing, Supervision & Startup

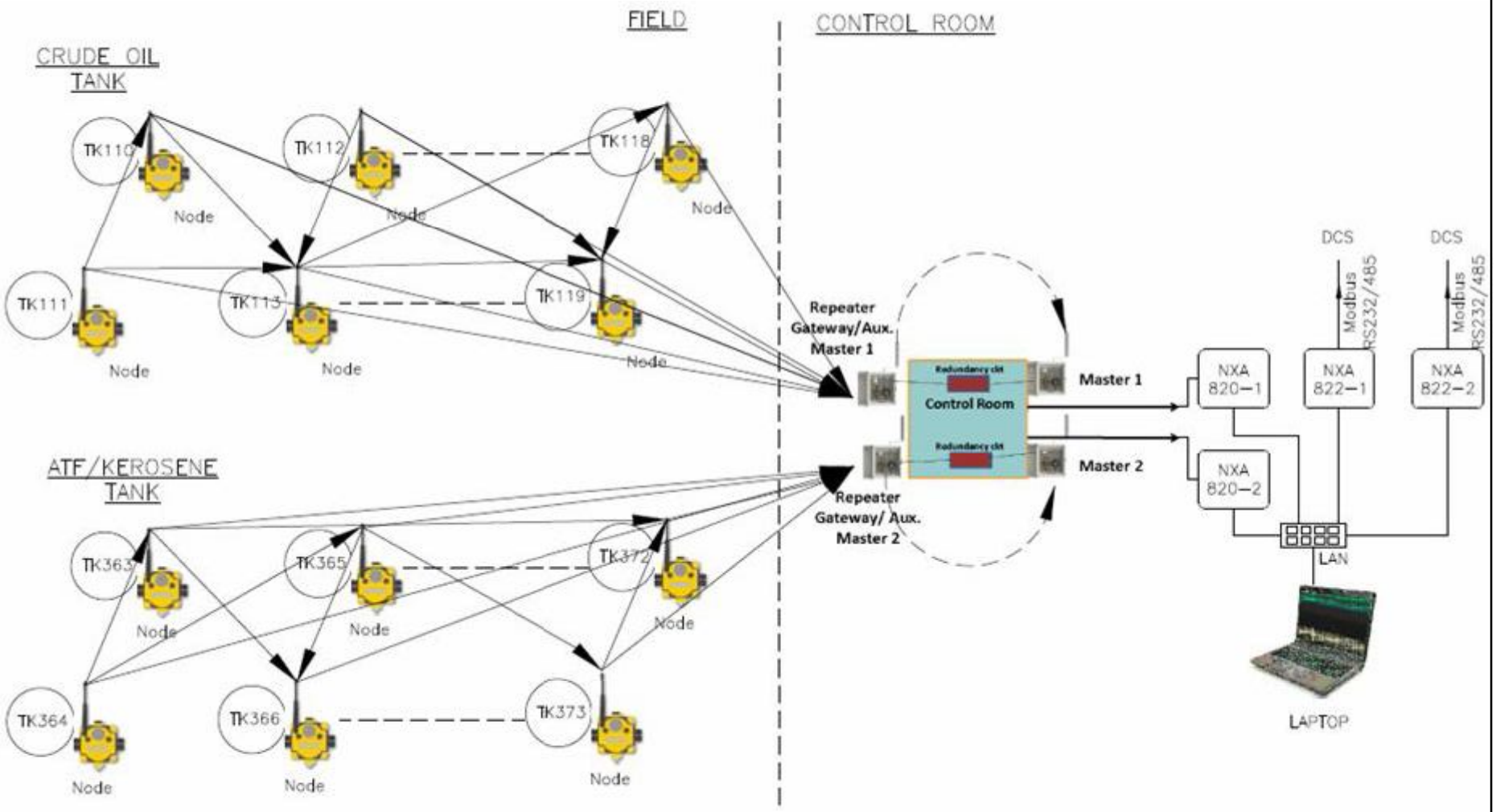
Date : From Sept 2010 as per availability of tanks

Solutions

Wireless Technology in Oil & Gas

Refinery at Mumbai

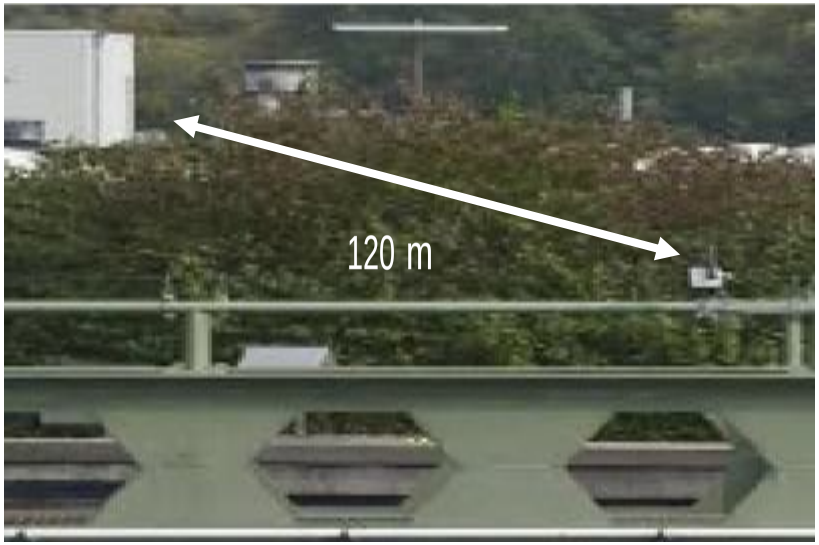
Endress+Hauser



Endress+Hauser

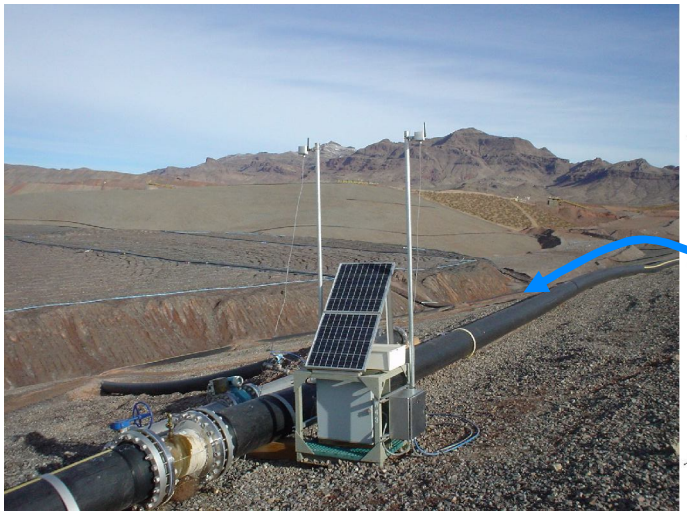
Effluent Treatment Plant

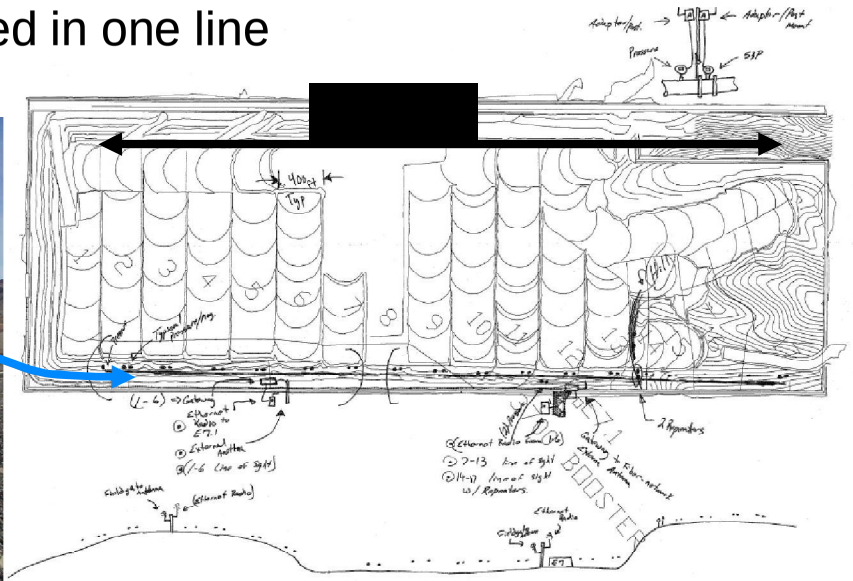
- Application “Waste water treatment plant”



Wireless Network Monitors Mobile Mining Operations

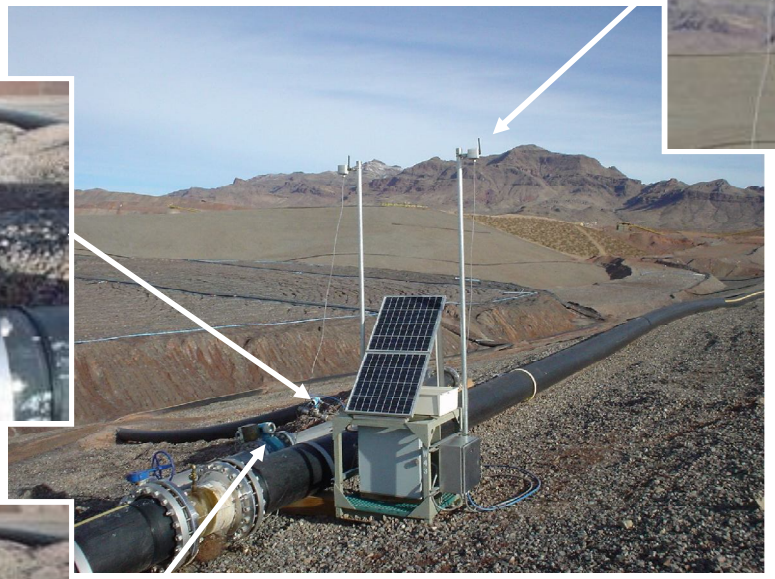
- Application: Monitoring of pressure and flow of a leaching fluid in a mining field
- Wireless network (4/2009)
  - 44 Adapters SWA70 non-Ex and 2 Fieldgates SWG70, i.e. 2 networks with about 22 adapters each
  - All adapters are arranged in one line





Endress+Hauser

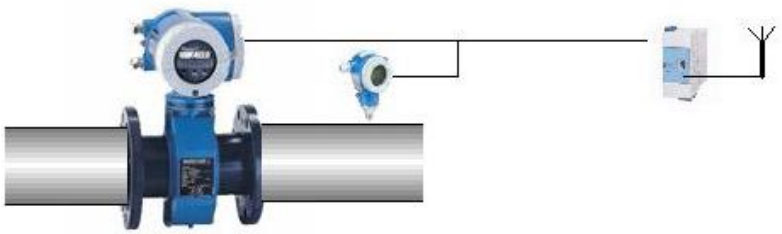
Wireless Monitors Mobile Operations



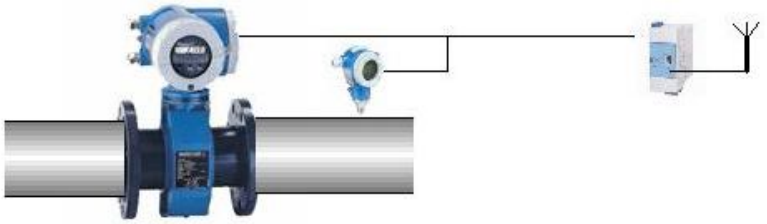
Benefits to the customer

- The use of robust wireless field network reduces costs in implementation and relocation
- The availability of reliable flow and pressure information allows leach field operators to optimize operation resulting in a ROI of about 2 months

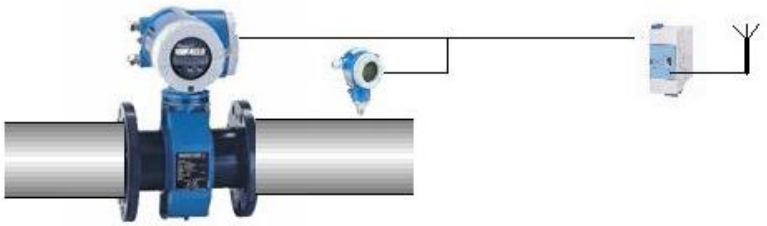
Continous data via GPRS



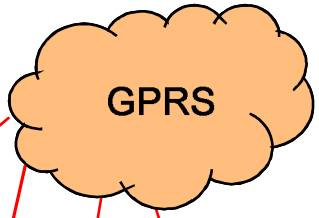
Location -1



Location - 2



Location - 3



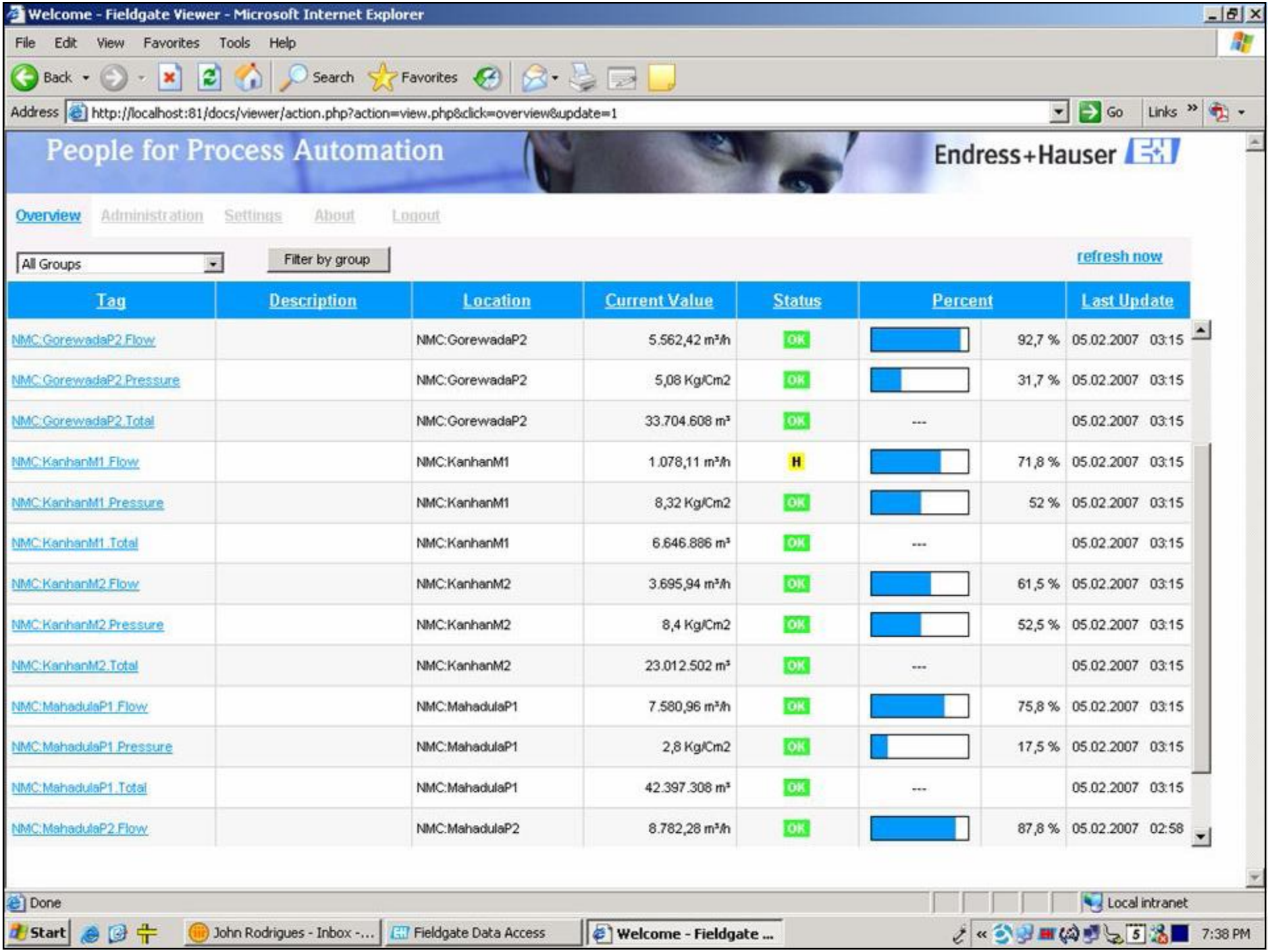
Alarm SMS
+ SMS On demand

Monitoring software

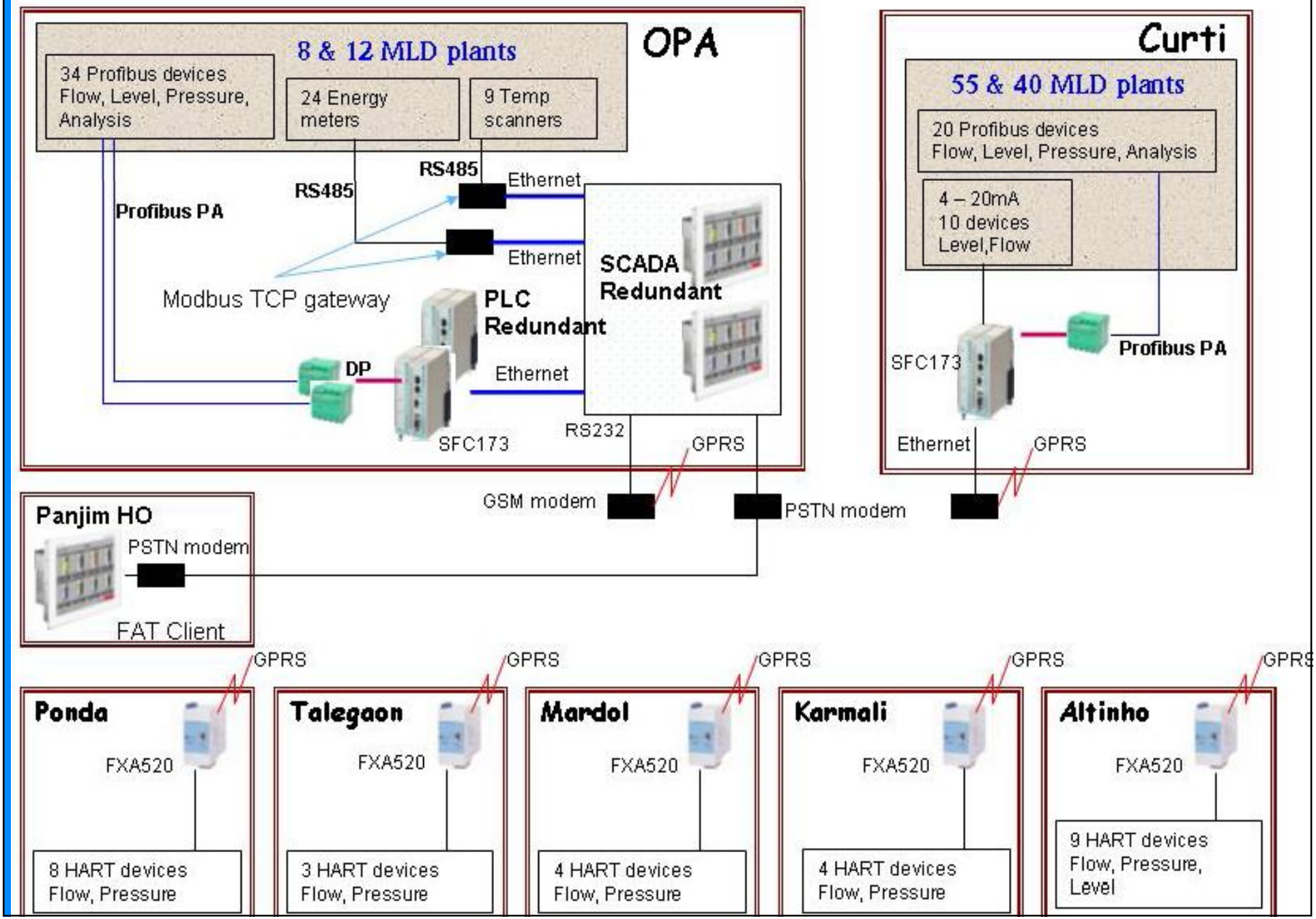
Locations across 100 sq Kms

Endress+Hauser

People for Process Automation


Welcome - Fieldgate Viewer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:81/docs/viewer/action.php?action=view.php&click=overview&update=1
Go Links
People for Process Automation
Endress+Hauser
Overview Administration Settings About Logout
All Groups
Filter by group
refresh now
Tag | Description | Location | Current Value | Status | Percent | Last Update
NMC:GorewadaP2.Flow | NMC:GorewadaP2 | 5.562,42 m³/h | OK | 92,7 % | 05.02.2007 03:15
NMC:GorewadaP2.Pressure | NMC:GorewadaP2 | 5,08 Kg/Cm2 | OK | 31,7 % | 05.02.2007 03:15
NMC:GorewadaP2.Total | NMC:GorewadaP2 | 33.704.608 m³ | OK | --- | 05.02.2007 03:15
NMC:KanhanM1.Flow | NMC:KanhanM1 | 1.078,11 m³/h | H | 71,8 % | 05.02.2007 03:15
NMC:KanhanM1.Pressure | NMC:KanhanM1 | 8,32 Kg/Cm2 | OK | 52 % | 05.02.2007 03:15
NMC:KanhanM1.Total | NMC:KanhanM1 | 6.646.886 m³ | OK | --- | 05.02.2007 03:15
NMC:KanhanM2.Flow | NMC:KanhanM2 | 3.695,94 m³/h | OK | 61,5 % | 05.02.2007 03:15
NMC:KanhanM2.Pressure | NMC:KanhanM2 | 8,4 Kg/Cm2 | OK | 52,5 % | 05.02.2007 03:15
NMC:KanhanM2.Total | NMC:KanhanM2 | 23.012.502 m³ | OK | --- | 05.02.2007 03:15
NMC:MahadulaP1.Flow | NMC:MahadulaP1 | 7.580,96 m³/h | OK | 75,8 % | 05.02.2007 03:15
NMC:MahadulaP1.Pressure | NMC:MahadulaP1 | 2,8 Kg/Cm2 | OK | 17,5 % | 05.02.2007 03:15
NMC:MahadulaP1.Total | NMC:MahadulaP1 | 42.397.308 m³ | OK | --- | 05.02.2007 03:15
NMC:MahadulaP2.Flow | NMC:MahadulaP2 | 8.782,28 m³/h | OK | 87,8 % | 05.02.2007 02:58
Done
Local intranet
Start
John Rodrigues - Inbox -...
Fieldgate Data Access
Welcome - Fieldgate ...
7:38 PM

Automation Project of WTP , Filteration Plant and Distribution network.



Level | Pressure | Flow | Temperature | Liquid Analysis | Registration | Systems Components | Services | Solutions

Thank you for your time!

Endress+Hauser
People for Process Automation


Safety & Availability – Voting Schemes Comparison
5th Oct 2012

Safety & Availability – Voting Schemes Comparison

Contents:

Introduction

- *Safety is of paramount concern for any industrial processes such as refineries, oil and gas, petrochemical plants, power plants and so on.*

- *Reasons of safe guarding measures are protection of personnel and environment from harm, conformance to laws and regulations, increase productivity and reduce damage to equipments and so on and so forth.*

- *As phrased in ISA TR 84.00.02 " Process start up and shutdown are periods where chances of hazardous events are high and hence the reduction of spurious trips will increase the safety of the process.*

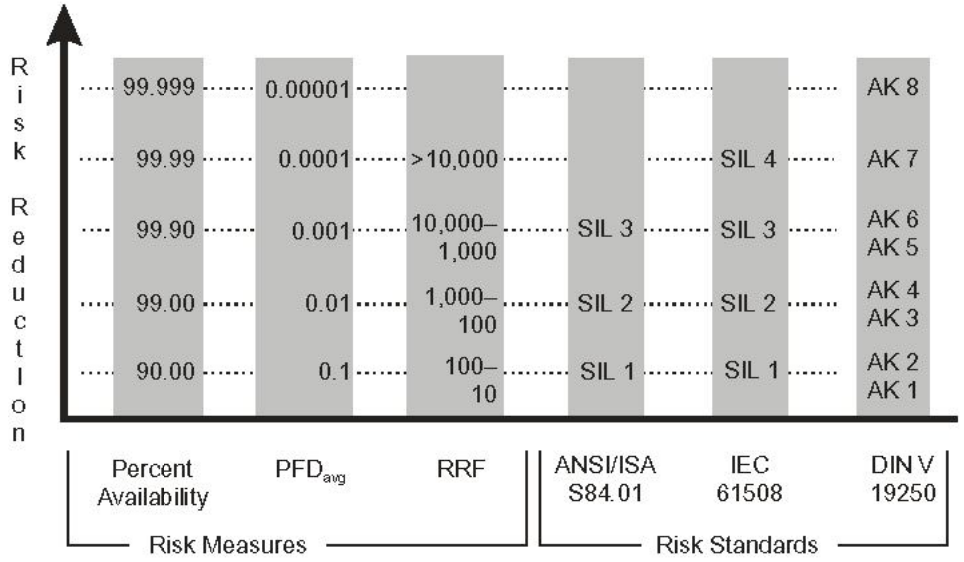
- *Well designed Safety system balance both safety and availability.*

- *Here is an attempt to compare frequently applied voting schemes in terms of safety availability (PFD), nuisance trips (PFS) and Fault tolerance.*

Safety Integrity Level (SIL)

SIL are categories of Probability of Failure on Demand (PFD) for a particular safety instrumented function.

These categories ranges from one to three, as defined by ISA 84.01, or one to four as defined by IEC 61508 and IEC 61511.



Failure Modes

- *DANGEROUS FAILURES*

  Faults or failures that immediately disable the capability of the SIS to respond to a demand .These are measured in terms of Probability of failure on demand (PFD).

  Example: Stuck-on or stuck off of an output

- *SAFE FAILURES*

  Faults or failures that initiates a safe response of the SIS without a demand. These are measured in terms of Probability of safe failure (PFS).

  Example: Opening of contact due to some component fault.

  Failures are further classified as Overt failures and Covert failures.

  Overt – Revealed failures (Can be detected by diagnostics)

  Covert – Un revealed failures (Only during demand, can be detected by off-line proof testing)

Probability of Failure on Demand (PFD)

PFD calculations take into account

1. *Random failures (can be assessed from the reliability data provided by manufacturers and are likely to affect only one channel at a time.*
2. *Common cause failures*
3. *Systematic failures*

   (2 and 3 could affect all the channels of a system in exactly same way. Depends on the system design of various vendors)

Note: For the sake of computations, the failure rates of a hypothetical single safety controller are used for all voting schemes throughout this paper.
λDU(Dangerous undetected) = 22 FITS,
λSD(Safe detected) = 1872 FITS,
λSU(Safe undetected) = 93 FITS,
λDD(Dangerous detected) = 1034 FITS
Mission Time (T) = 8760 hrs (1 year) ,
Mean Repair Time (MRT) = 8 hrs (Typically 1 Shift) and
Time required to restart the process after shutdown (RS) = 16 hrs (2 shifts).

Definitions

FAULT TOLERANCE:

Fault-tolerance or graceful degradation is the property that enables a system to continue operating properly in the event of the failure of (one or more faults within) some of its components.

VOTING:

ANSI/ISA 84.01 defines NooM voting as : System made up of M independent channels, which are so connected that at least "n" of the "m" channels to be in agreement before the SIS can take action.

DIAGNOSTICS:

One important feature of any safety system is its ability to detect a failure and to manage the failures. This feature can be used to reduce the repair times and to control operation of several fault tolerant architectures. The measure of this ability is known as diagnostic coverage factor, which is calculated by adding failure rates of detected failures and dividing by the total failure rates. Detected failures are expected to be repaired within few hours; dangerous undetected failures are called covert failures and detected only by a periodic offline proof test. Diagnostic can only raise the level of detection of faults; it cannot increase the life span of component.

1oo2D Architecture

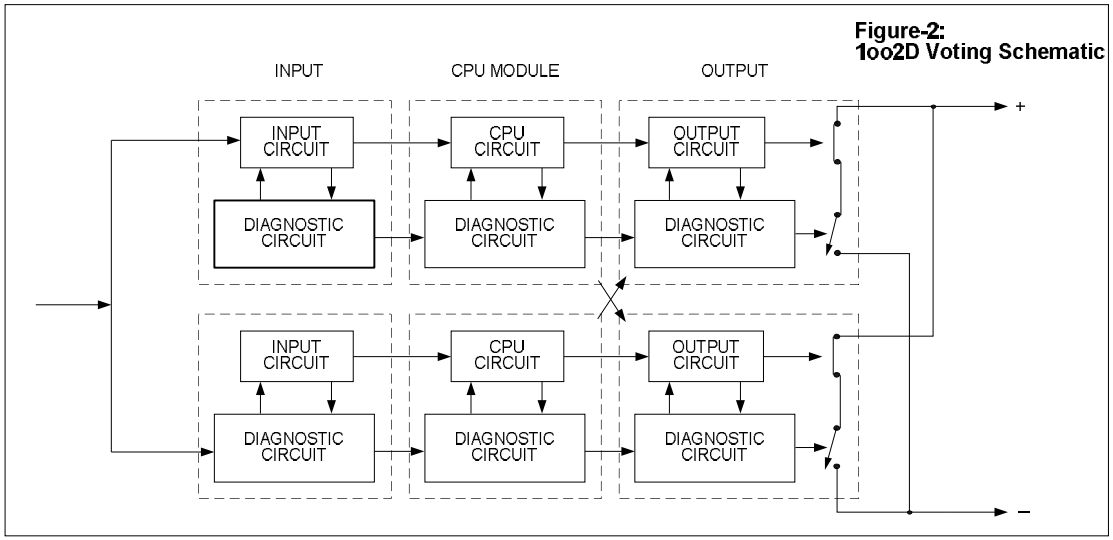


Figure-2:
1oo2D Voting Schematic

1oo2D differs from 1oo2 by the way the contacts are wired. This architecture consists of two channels connected in parallel. During normal operation, both channels need to agree to execute shutdown.

The diagnostics information signals are shared between two channels and this information is used to control the diagnostic switches of both channels. If the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by other channel.

.

1oo2D Architecture (Markov Model)

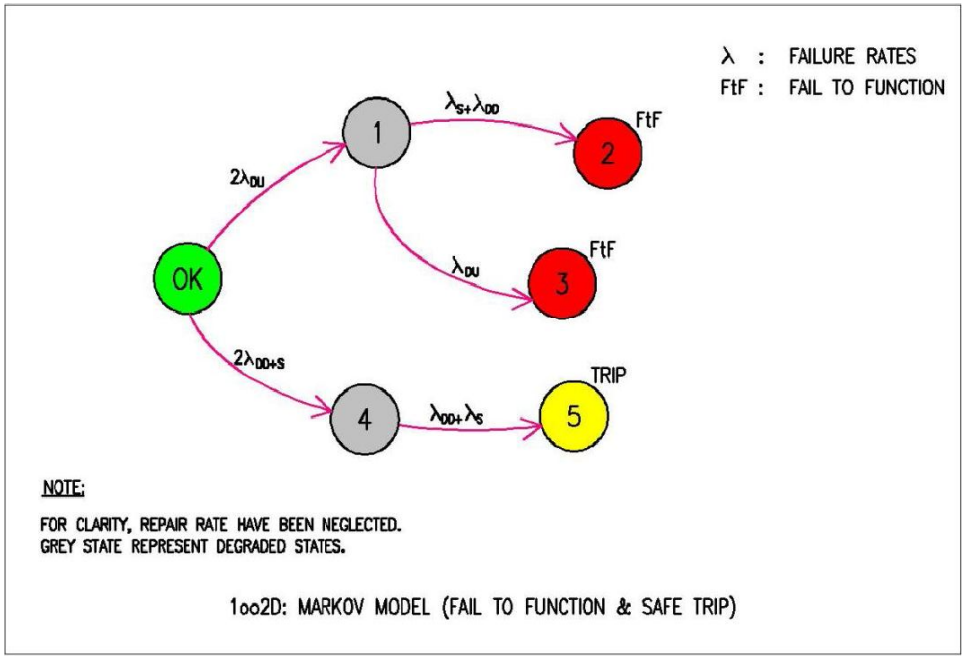


Table-1 : 1oo2 D Truth Table

S. No.	Voting	Channel-1	Channel-2	Channel-3	Channel-4	System Status
1	1oo2D	DU	DU	not press.	not press.	Fail to function
2	1oo2D	S or DD	DU	not press.	not press.	Fail to function
3	1oo2D	DU	S or DD	not press.	not press.	Fail to function
4	1oo2D	SD or DD	Healthy	not press.	not press.	Safe Operating
5	1oo2D	Healthy	SD or DD	not press.	not press.	Safe Operating
6	1oo2D	SU or DU	Healthy	not press.	not press.	Safe Operating
7	1oo2D	Healthy	SU or DU	not press.	not press.	Safe Operating
8	1oo2D	S or DD	S or DD	not press.	not press.	Trip

Note : Diagnostic testing will report the faults and would change any output states or change the output voting.

From the Markov Model and voting truth table of 1oo2D,

- *There is a combination of two failures that leads the system FtF. It is therefore concluded that 1oo2D is one fault tolerant*
- *Also one failure does not lead to spurious trips.*

1oo2D Architecture (Contd….)

Table-1 : 1oo2 D Truth Table

S. No.	Voting	Channel-1	Channel-2	Channel-3	Channel-4	System Status
1	**1oo2D**	DU	DU	not press.	not press.	Fail to function
2	**1oo2D**	S or DD	DU	not press.	not press.	Fail to function
3	**1oo2D**	DU	S or DD	not press.	not press.	Fail to function
4	**1oo2D**	SD or DD	Healthy	not press.	not press.	Safe Operating
5	**1oo2D**	Healthy	SD or DD	not press.	not press.	Safe Operating
6	**1oo2D**	SU or DU	Healthy	not press.	not press.	Safe Operating
7	**1oo2D**	Healthy	SU or DU	not press.	not press.	Safe Operating
8	**1oo2D**	S or DD	S or DD	not press.	not press.	Trip

Note : Diagnostic testing will report the faults and would change any output states or change the output voting.

Table-1 : 1oo2 Truth Table

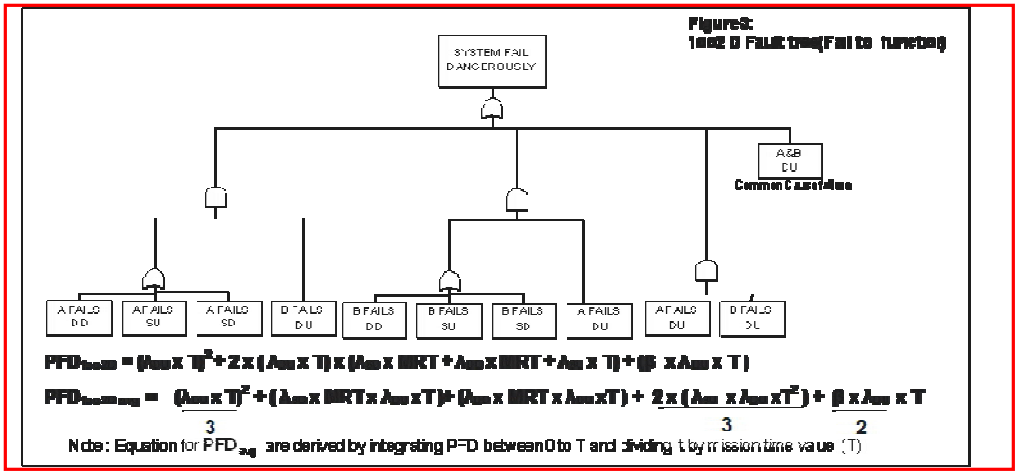
S. No.	Voting	Fail leg-1	Fail leg-2	Safety system
1	1oo2	**DD or DU**	**DD or DU**	**Fail to function**
2	1oo2	**SD**	**Healthy**	**Trip**
3	1oo2	**SU**	**Healthy**	**Trip**
4	1oo2	**Healthy**	**SD**	**Trip**
5	1oo2	**Healthy**	**SU**	**Trip**
6	1oo2	**DD or DU**	**Healthy**	**Safe Operating**
7	1oo2	**Healthy**	**DD or DU**	**Safe Operating**

How does 1oo2D has advantages of both 1oo2 and 2oo2?

- *1oo2D system fails to function when there is a DU failure in one channel combined with any failure in other channel. This is similar to 1oo2 system in exception to an additional safe failure in 1oo2D resulting in FtF. (However as it will be clear from the subsequent slides, the contribution to the PFD by this additional failure is very negligible.)*
- *Unlike 1oo2 (which trips the plant if there is a safe failure in any one of the channel), 1oo2D trips only when there is a combination of Safe or DD failure in both channels. This is similar to 2oo2.*

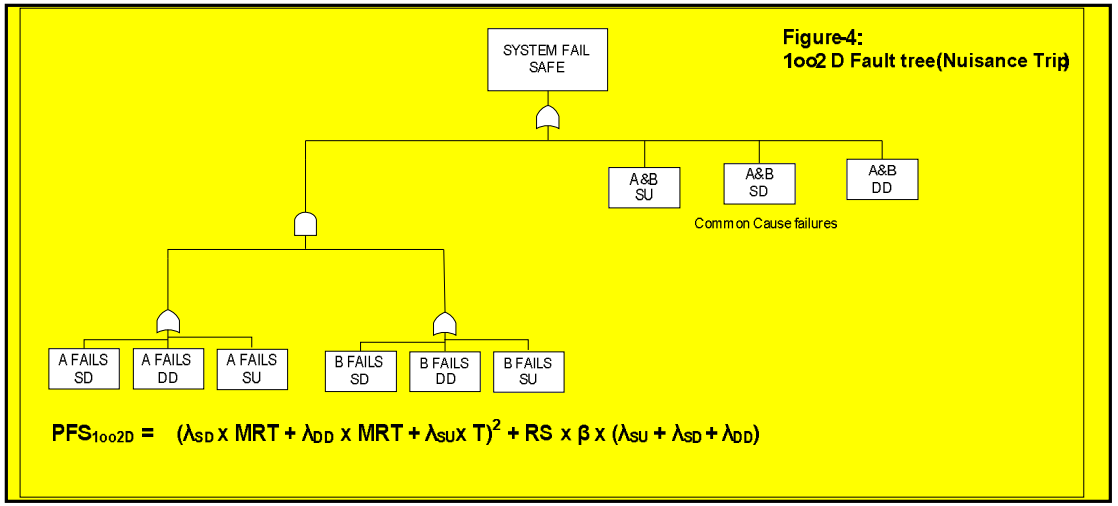
  Thus 1oo2D has advantage of 1oo2 in terms of safety and 2oo2 in terms of availability

1oo2D Architecture (Fault Tree)



PFD Fault Tree

PFS Fault Tree



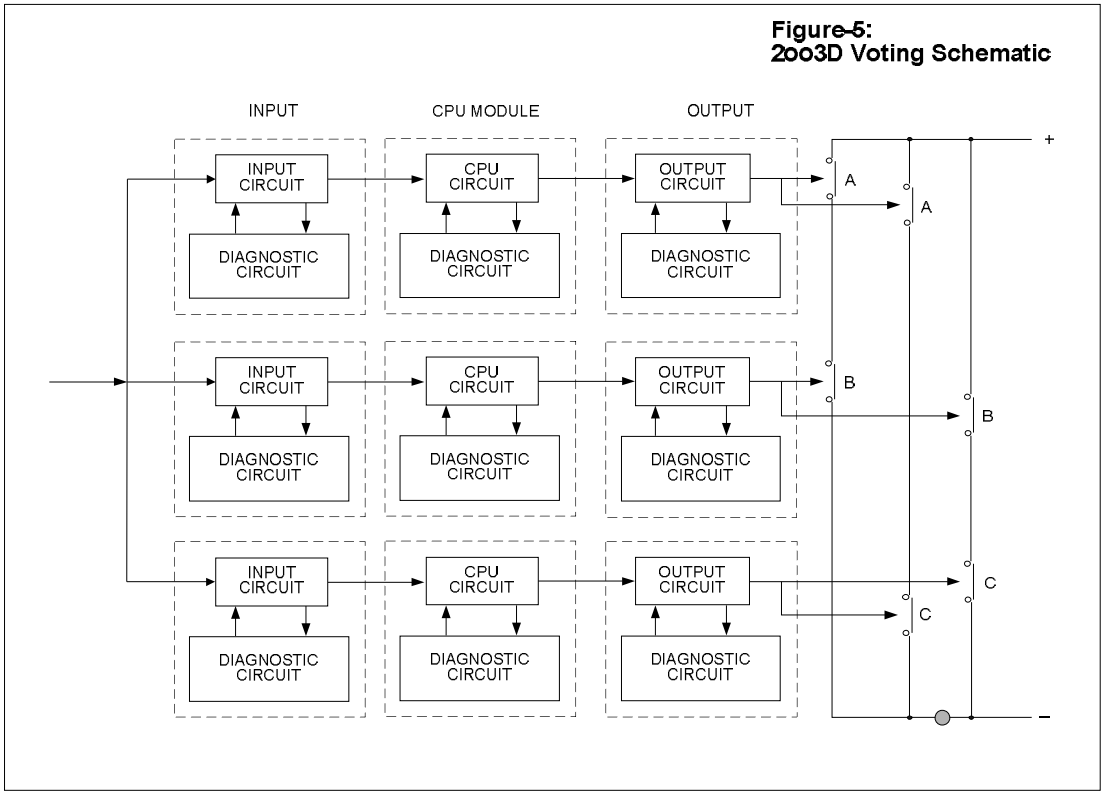
1oo2D Architecture (Calculations)

$$PFD_{1oo2D\ avg} = \frac{(\lambda_{DU} \times T)^2}{3} + (\lambda_{SD} \times MRT \times \lambda_{DU} \times T) + (\lambda_{DD} \times MRT \times \lambda_{DU} \times T) + \frac{2 \times (\lambda_{SU} \times \lambda_{DU} \times T^2)}{3} + \frac{\beta \times \lambda_{DU} \times T}{2}$$

1.23803E-08 | 2.88617E-09 | 1.59418E-09 | 1.0467E-07 | 1.9272E-06

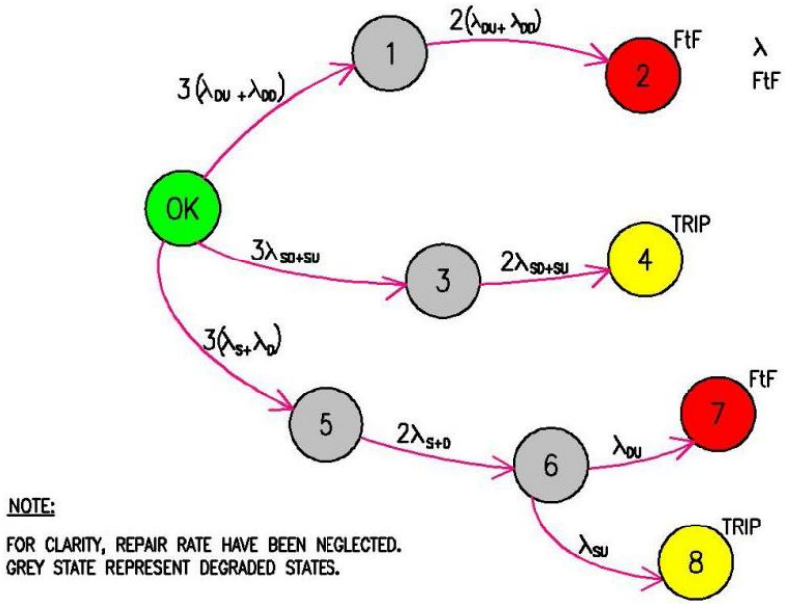
1. *The first and fourth term represents undetected failures which can be revealed during the off-line proof test intervals.*
2. *The second and the third term represents multiple failures during repairs and is typically negligible for short repair times (typically less than 8 hrs) which are magnitudes smaller than the mission time T (for instance in this study it is considered 8760 hrs ie 1 year).*
3. *The last term is the common cause term and contributes significantly for the $PFD_{avg.}$ Varies with vendor design depending on the failures related to common cause.*

2oo3D Architecture



- *This architecture consists of three channels connected in parallel with majority voting arrangement for the output signals, such that the output state is changed if two channels give a similar result. Whatever two or more channel says, that's what the system does.*
- *It is assumed that diagnostic testing would report the faults found and would not change any output states or change the output voting.*

2oo3D Architecture (Contd….)



2oo3D: MARKOV MODEL (FAIL TO FUNCTION & SAFE TRIP)

Table-2 : 2oo3 D Truth Table

S. No.	Voting	Channel-1	Channel-2	Channel-3	Channel-4	System Status
1	2oo3D	DU or DD	DU or DD	Healthy	not press.	Fail to function
2	2oo3D	Healthy	DU or DD	DU or DD	not press.	Fail to function
3	2oo3D	DU or DD	Healthy	DU or DD	not press.	Fail to function
4	2oo3D	SD or SU	SD or SU	Healthy	not press.	Trip
5	2oo3D	Healthy	SD or SU	SD or SU	not press.	Trip
6	2oo3D	SD or SU	Healthy	SD or SU	not press.	Trip
7	2oo3D	S or D	Healthy	Healthy	not press.	Safe Operating
8	2oo3D	Healthy	S or D	Healthy	not press.	Safe Operating
9	2oo3D	Healthy	Healthy	S or D	not press.	Safe Operating
10	2oo3D	S	D	Healthy	not press.	Safe Operating (Time restriction)
11	2oo3D	D	S	Healthy	not press.	Safe Operating (Time restriction)

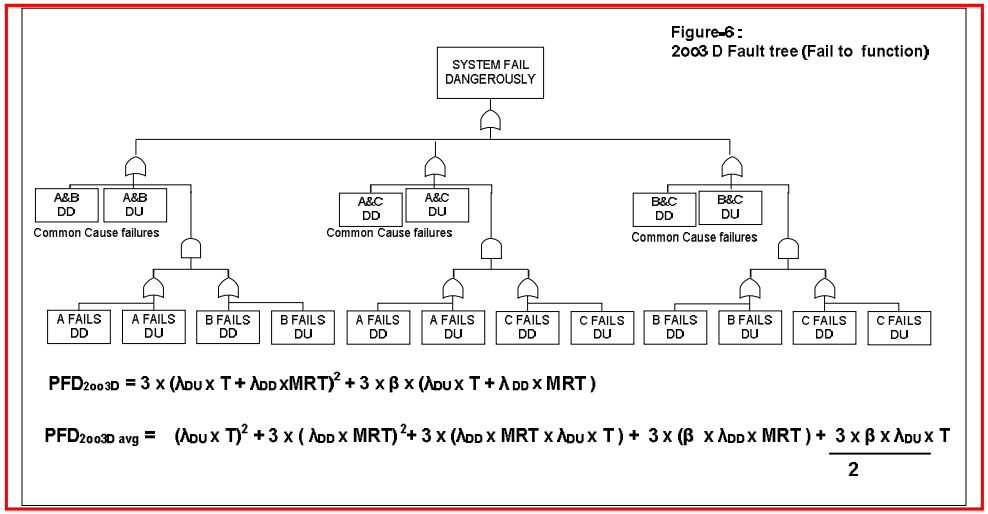
Note : Diagnostic testing will only report the faults and would not change any output states or change the output voting.

2oo3D Architecture (Contd….)

From the Markov Model and voting truth table of 2oo3D,

- *There is a combination of two failures that leads the system FtF.*
- *There is a combination of S failure in one channel and D failure in another channel which degrades the system to 1oo1D.*
- *Therefore we conclude that 2oo3D is actually partly two fault tolerant.*
- *A combination of two or three failures are required for nuisance trips.*

2oo3D Architecture (Fault Tree)

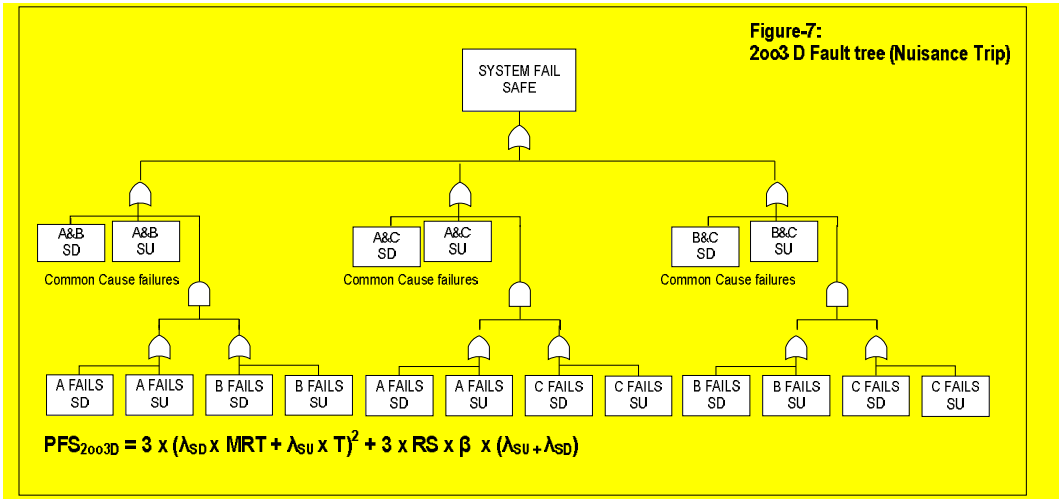


$$PFD_{2oo3D} = 3 \times (\lambda_{DU} \times T + \lambda_{DD} \times MRT)^2 + 3 \times \beta \times (\lambda_{DU} \times T + \lambda_{DD} \times MRT)$$

$$PFD_{2oo3D\ avg} = (\lambda_{DU} \times T)^2 + 3 \times (\lambda_{DD} \times MRT)^2 + 3 \times (\lambda_{DD} \times MRT \times \lambda_{DU} \times T) + 3 \times (\beta \times \lambda_{DD} \times MRT) + \frac{3 \times \beta \times \lambda_{DU} \times T}{2}$$

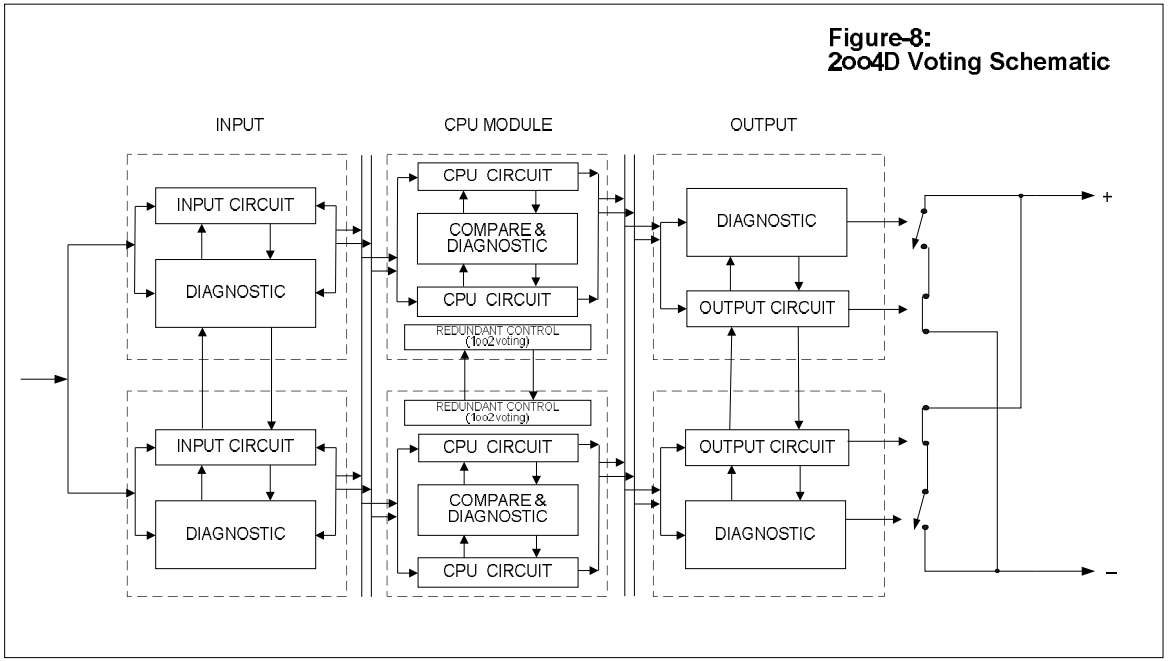
PFD Fault Tree

PFS Fault Tree



$$PFS_{2oo3D} = 3 \times (\lambda_{SD} \times MRT + \lambda_{SU} \times T)^2 + 3 \times RS \times \beta \times (\lambda_{SU} + \lambda_{SD})$$

2oo4D Architecture



- *This architecture consists of pair of redundant channels (1oo2) connected in parallel with a high level of diagnostic. Thus it provides total four (4) channels (redundant channels per leg, both legs are connected as 1oo2D).*

2oo4D Architecture (Voting Truth Table)

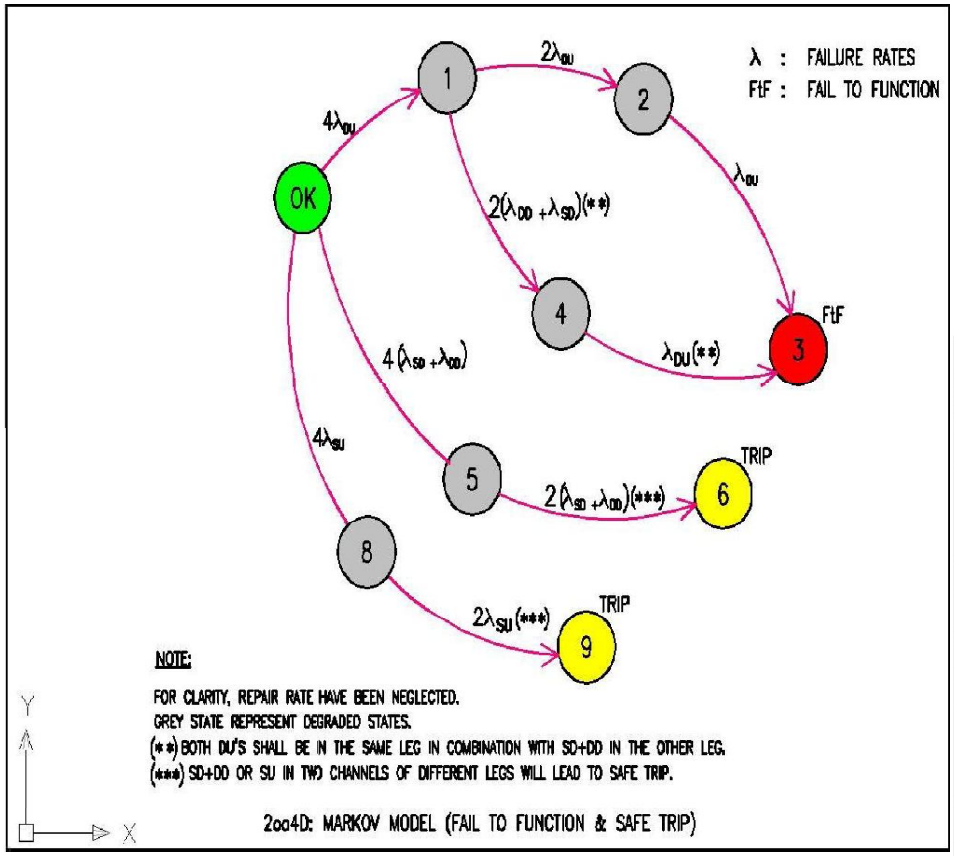


Table-3 : 2oo4 D Truth Table

		Leg-1		Leg-2		
S. No.	Voting	Channel-1	Channel-2	Channel-3	Channel-4	System Status
1	2oo4D	DU	DU	DU	Healthy	Fail to function
2	2oo4D	Healthy	DU	DU	DU	Fail to function
3	2oo4D	DU	DU	Healthy	DU	Fail to function
4	2oo4D	DU	Healthy	DU	DU	Fail to function
5	2oo4D	DD or SD	Healthy	DU	DU	Fail to function
6	2oo4D	DD or SD	Healthy	DU	DU	Fail to function
7	2oo4D	Healthy	DD or SD	DU	DU	Fail to function
8	2oo4D	Healthy	DD or SD	DU	DU	Fail to function
9	2oo4D	DU	DU	DD or SD	Healthy	Fail to function
10	2oo4D	DU	DU	DD or SD	Healthy	Fail to function
11	2oo4D	DU	DU	Healthy	DD or SD	Fail to function
12	2oo4D	DU	DU	Healthy	DD or SD	Fail to function
13	2oo4D	SD or DD	Healthy	SD or DD	Healthy	Trip
14	2oo4D	SD or DD	Healthy	Healthy	SD or DD	Trip
15	2oo4D	Healthy	SD or DD	Healthy	SD or DD	Trip
16	2oo4D	Healthy	SD or DD	SD or DD	Healthy	Trip
17	2oo4D	SU	Healthy	SU	Healthy	Trip
18	2oo4D	SU	Healthy	Healthy	SU	Trip
19	2oo4D	Healthy	SU	Healthy	SU	Trip
20	2oo4D	Healthy	SU	SU	Healthy	Trip
21	2oo4D	SD or DD	SD or DD	Healthy	Healthy	Safe Operating
22	2oo4D	Healthy	Healthy	SD or DD	SD or DD	Safe Operating
23	2oo4D	SU	SU	Healthy	Healthy	Safe Operating
24	2oo4D	Healthy	Healthy	SU	SU	Safe Operating

Note : Diagnostic testing will report the faults and would change any output states or change the output voting.

2oo4D Architecture (Contd….)

From the Markov Model and voting truth table of 2oo4D,

- *There is a combination of three failures that leads the system FtF.*

Therefore we conclude that 2oo4D is actually fully two fault tolerant .

- *A combination of two failures in different legs are required for nuisance trips.*

2oo4D Architecture (Fault Tree)

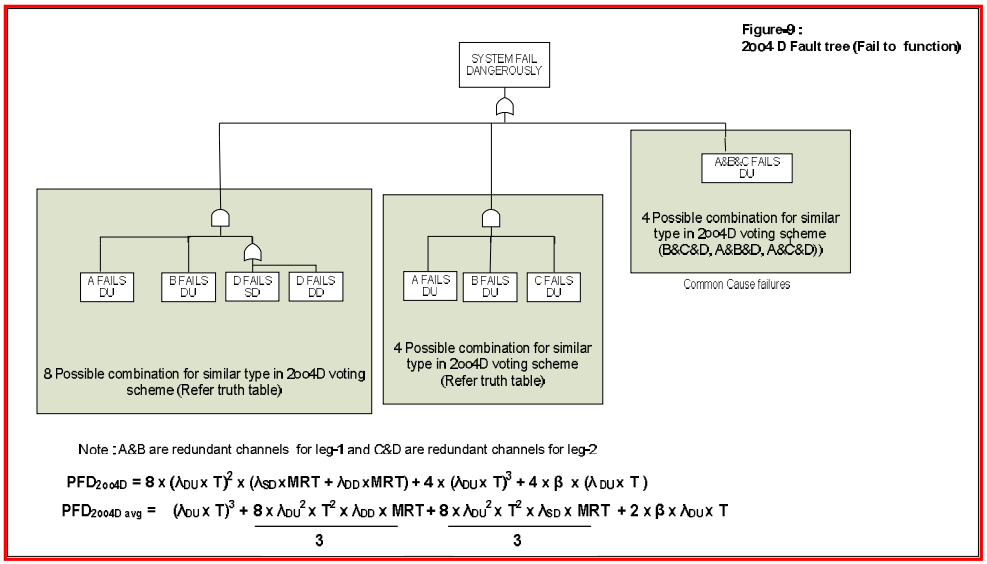


Figure-9 :
2oo4 D Fault tree (Fail to function)

$$PFD_{2oo4D} = 8 \times (\lambda_{DU} \times T)^2 \times (\lambda_{SD} \times MRT + \lambda_{DD} \times MRT) + 4 \times (\lambda_{DU} \times T)^3 + 4 \times \beta \times (\lambda_{DU} \times T)$$

$$PFD_{2oo4D\ avg} = \frac{(\lambda_{DU} \times T)^3}{3} + \frac{8 \times \lambda_{DU}^2 \times T^2 \times \lambda_{DD} \times MRT}{3} + \frac{8 \times \lambda_{DU}^2 \times T^2 \times \lambda_{SD} \times MRT}{3} + 2 \times \beta \times \lambda_{DU} \times T$$

PFD Fault Tree

PFS Fault Tree

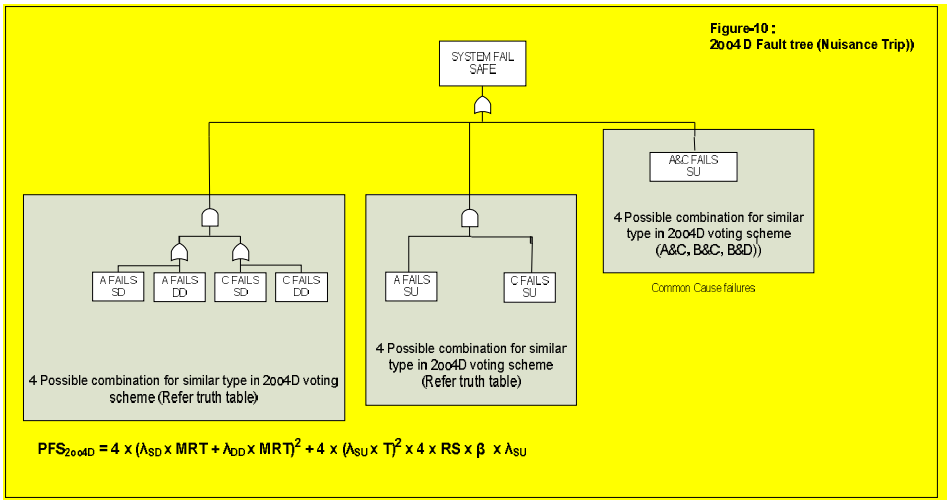


Figure-10 :
2oo4 D Fault tree (Nuisance Trip))

$$PFS_{2oo4D} = 4 \times (\lambda_{SD} \times MRT + \lambda_{DD} \times MRT)^2 + 4 \times (\lambda_{SU} \times T)^2 \times 4 \times RS \times \beta \times \lambda_{SU}$$

Voting Architecture Comparisons

- *as per the ascending order of the PFDavg (*)*
  1. *1oo2D* **2.04873E-06** *(twice in 10^6 years)*
  2. *2oo3D* **6.32005E-06** *(six times in 10^6 years)*
  3. *2oo4D* **7.70881E-06** *(seven times in 10^6 years)*

- *as per the ascending order of PFS (*) (Nuisance Trips)*
  1. *1oo2D* **1.6618E-06** *(twice in 10^6 years)*
  2. *2oo4D* **2.77602E-06** *(twice in 10^6 years)*
  3. *2oo3D* **3.95139E-06** *(thrice in 10^6 years)*

**- Based on the assumed failure rates of a hypothetical controller.*

The conclusions may be different if common cause failures are ignored or if the vendor design of system is such that common cause does not fail a group of channels which increases the PFDavg and PFS.

Degraded Mode Of Operation (TUV Report)

Fault-free system	TUV approved Operating Modes w/Restrictions	TUV Class Approval for Safety	TUV Time Requirements for Repair	Remarks
1oo2D	2-1-0	AK5	72 Hrs	For AK6 applications, operating mode is 2-0 (immediate shutdown after the system degrades to 1oo1D)
2oo3D	3-2-1-0	AK5	72 hrs	For AK6 applications, operating mode is 3-2-0 (immediate shutdown after the system degrades to 1001D)
2oo4D	4-2-0	AK5,AK6		
2oo2		Not approved		
1oo2	2-0	AK5,AK6		

Wrap Up

- *1oo2D and 2oo4D voting schemes are based on channel comparison/switch over mechanism.*

- *Even though 1oo2D systems quantitatively present better results for safety and availability, the real problem is that they are not deterministic and can't resolve a conflict in data. They can attempt to resolve the discrepancy by diagnostics. This places a huge responsibility on diagnostics to function very accurately and therefore the performance is based on the efficiency of the diagnostics circuit and switch over mechanism.*
  The essence of the above is captured in IEC-61508-6 (year 2010) which has additionally included parameter "K" for taking consideration of efficiency of inter-channel comparison/ switch mechanism in their PFDavg calculations.

- *Though 2oo4D is built with 1oo2D as its building block, both the safety and availability has not been comparable to 1oo2D and this is to be expected due to the fact that 2 channels of each leg lie in the same module and the degradation is 4-2-0 (degradation for a true 2oo4D would be 4-3-2-0) and also it has more components and hence more common cause failures.*

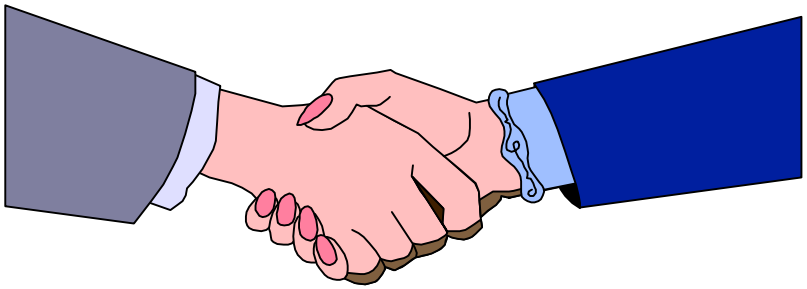
- *2oo3D scheme is based on majority voting arrangement and therefore there is no requirement of high level of comprehensive diagnostics built in the for system to perform efficiently. Traditionally this system is considered as a fault tolerant system. It surprises people to see that TMR systems have a higher nuisance trips than a dual system and greater probability to fail to function.*

Wrap Up (Contd….)

- *All offers good benefits and selecting one would be a difficult task but should be based on how well any option fits in your needs.*

- *Evaluate the entire solution and take an well educated decision. Also the TUV report and restrictions to be carefully followed.*

- *Demand the failure rates from supplier and verify quantitatively the PFD figures following ISA and IEC standards.*



Thank You

Asel-Tech

Technology for people and environment

www.asel-tech.com

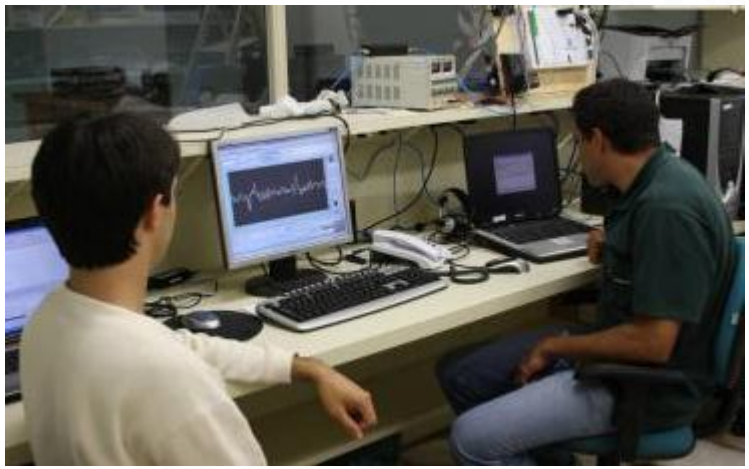
Leak Detection and Location Systems

- SLDS / ILDS / Marc One –

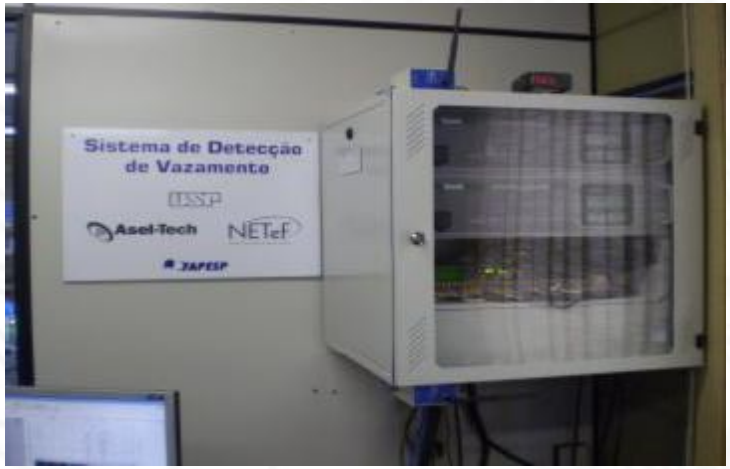
Products & Services

- Products:
- Leak Detection and Locations Systems for Pipelines:
  - Sonic System (Acoustic),
  - Integrated System (Acoustic + Mass Balance),
- Acoustic Leak Detection and Monitoring System for subsea equipment,
- Pipeline Intrusion Monitoring System,
- Pig Location System,
- Anchoring Systems for Pipelines,
- Integrity and Corrosion Monitoring Systems for Pipelines,
- Remote Methane Leak Detector,
- Remote Methane Leak Detector for Platforms (Intrinsically Safe),
- Vigilance and Protection Systems for Property by Cameras.
- Services:
  - Tank cleaning and inspection using robots,
  - Installation / Commissioning / Start-up / Maintenance / Projects / Technical Assistance / Equipment rental.

R & D - São Carlos



Test laboratory NETEF - USP

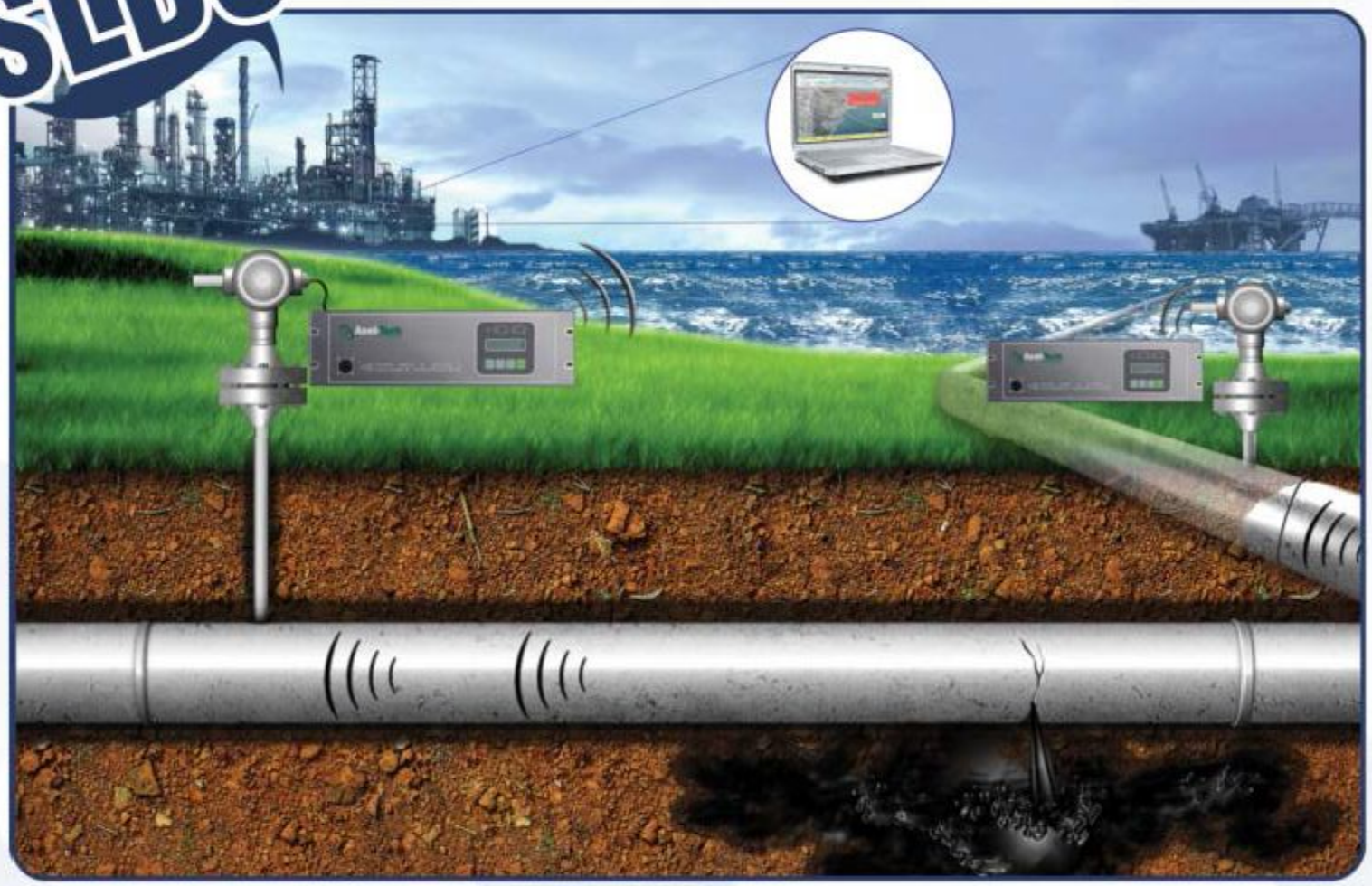


Asel-Tech

Technology for people and environment

www.asel-tech.com

SLDS



Asel-Tech

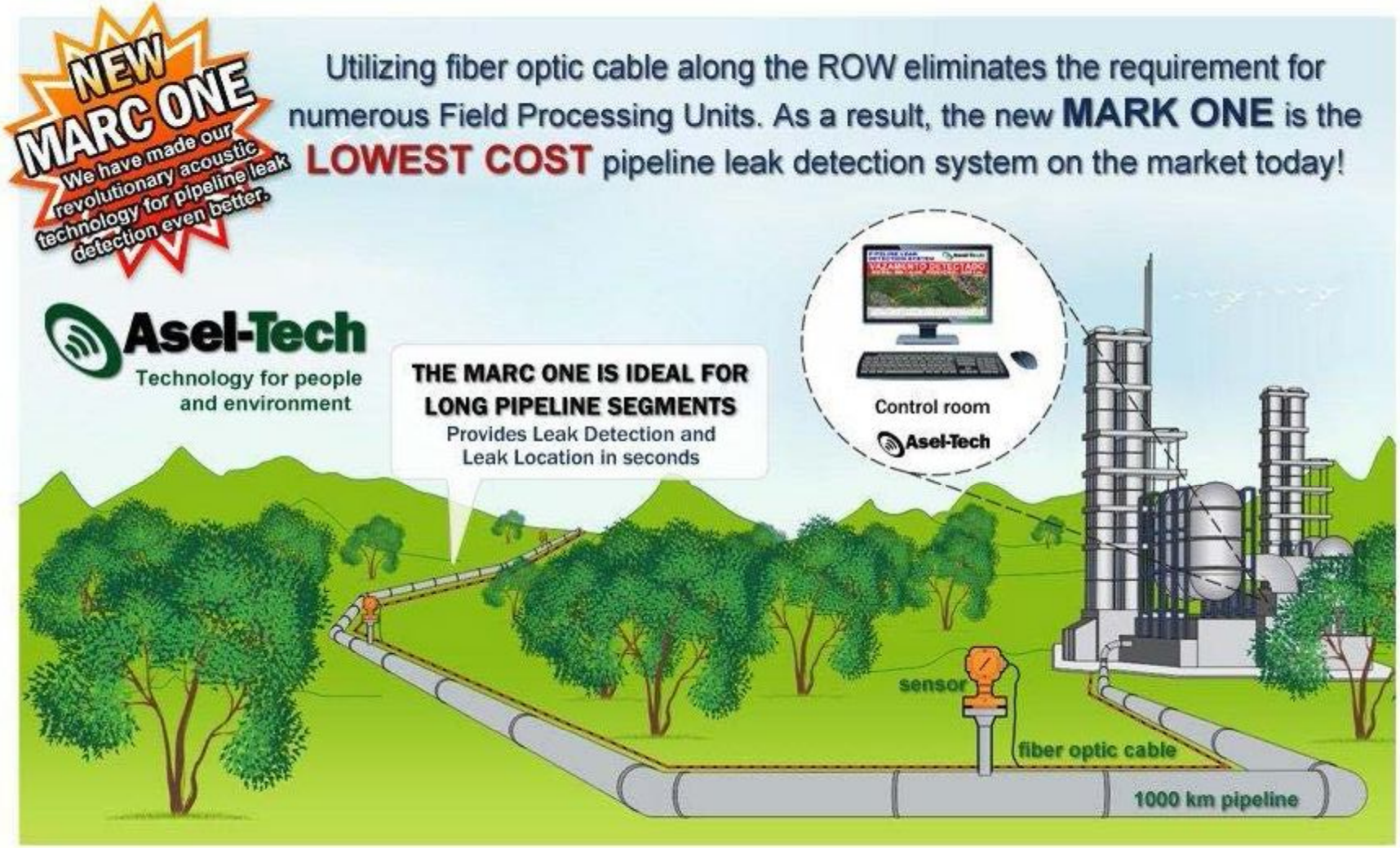
Technology for people and environment

www.asel-tech.com

Asel-Tech

Technology for people and environment

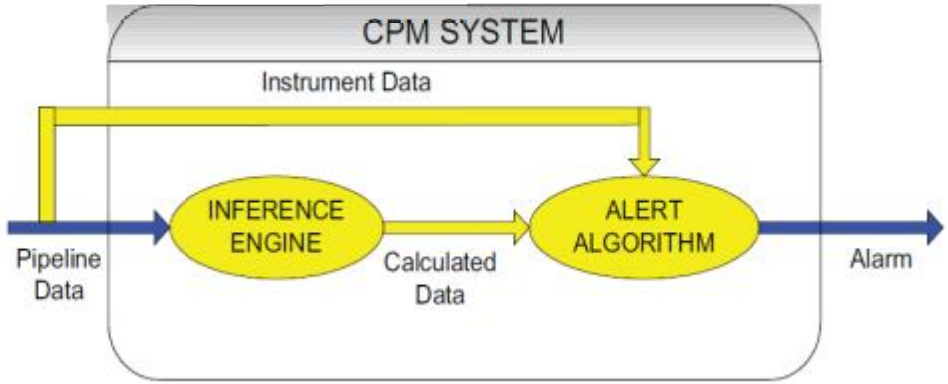
www.asel-tech.com



API – 1130

Internal Methodology

CPM Techniques



CPM is intended usually as a tool to be used by the pipeline controller in the safe operation of the pipeline. Effective operation of a pipeline requires that the pipeline controller be familiar with the pipeline and the tools at their disposal. CPM is not currently intended to replace human judgment and intervention in the shutdown of the affected pipeline segment(s) and the closure of remote control valves or directing field staff to close hand operated valves on the pipeline.

Integrated System

ILDS = Two combined Leak Detection Methodologies Avaliable on ILDS and Marc One.

ACOUSTIC TECHNOLOGY (SLDS)

- Quick leak detection
- Accurate location
- Works with liquids, gas & multiphase flow

MASS BALANCE

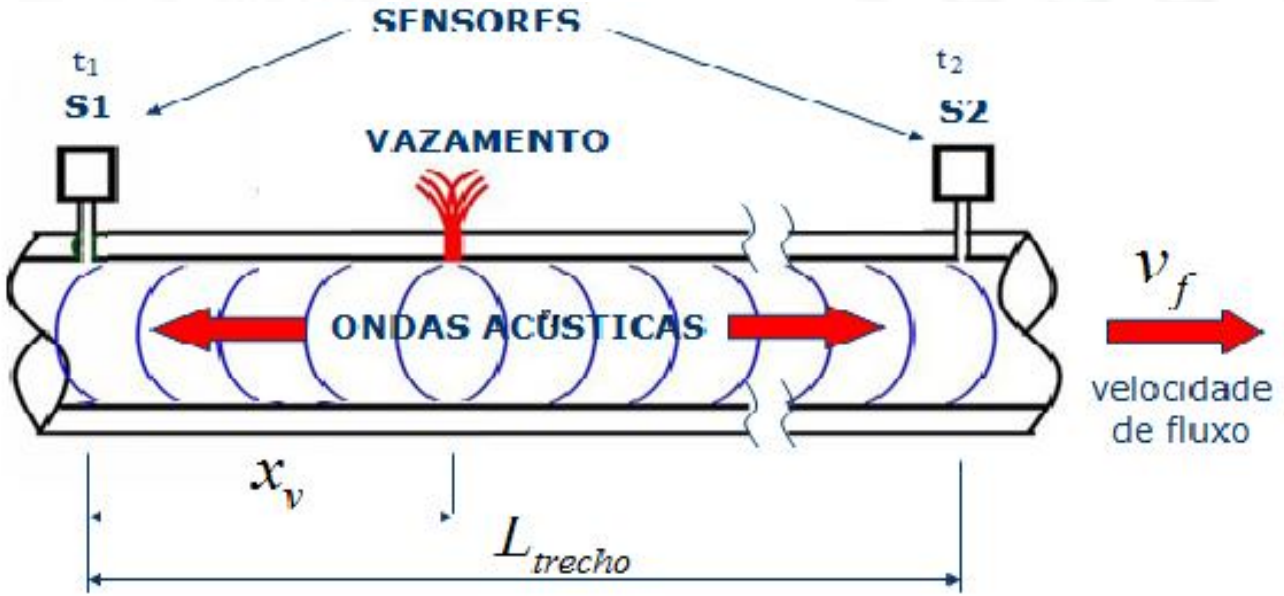
- Progressive leaks
- Direct leak rate & quantification

Complementary & mutual benefits

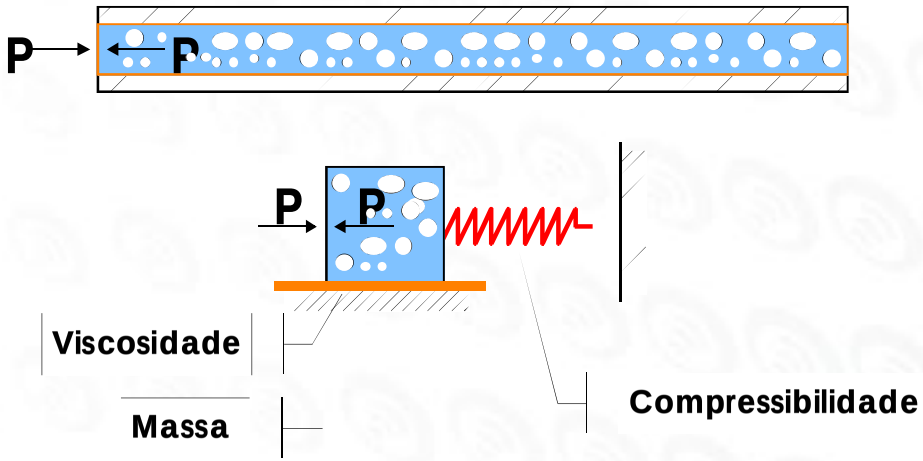
Working Principle

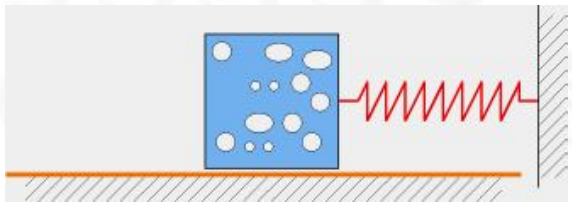
Acoustic System

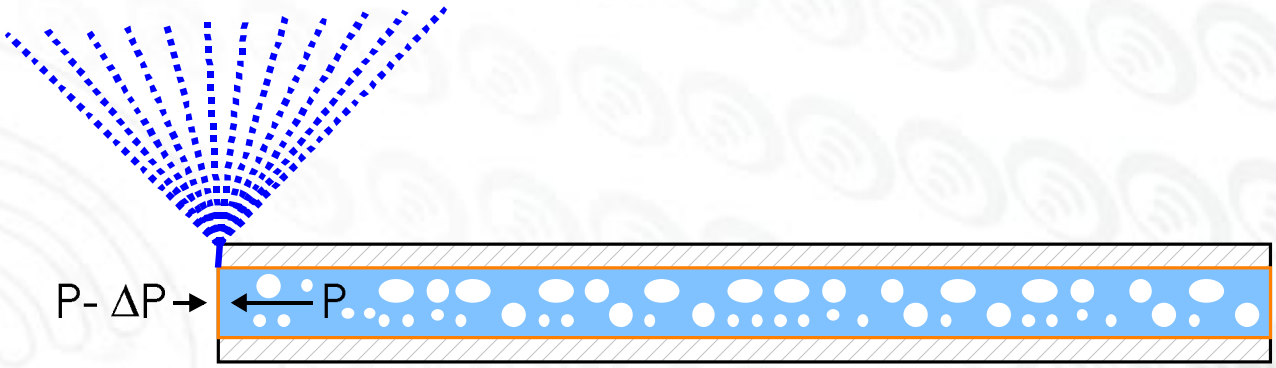
The operation is based on the detection of the negative pressure transient that is generated when a leak occurs. When a rupture occurs on the pipeline this transient is propagated as a subsonic wave throughout the pipeline and can reach long distances.



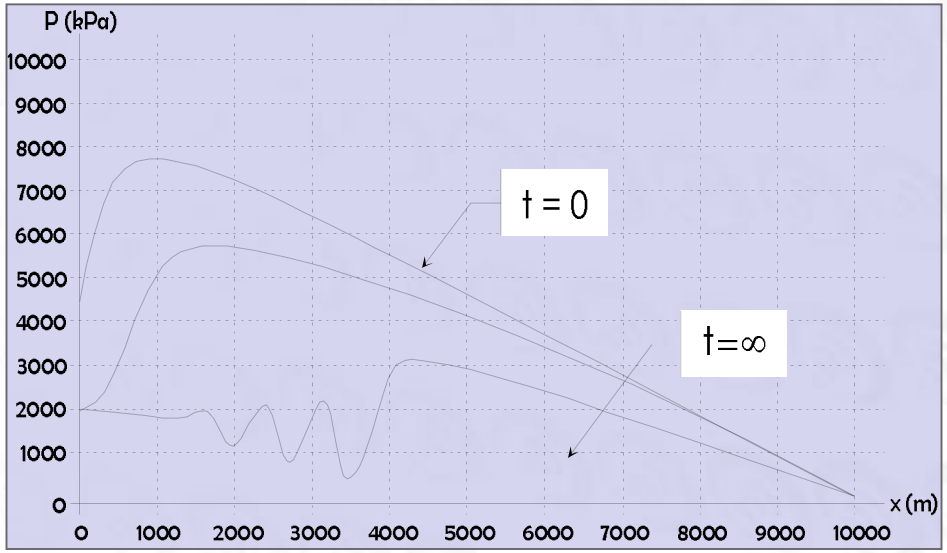
The physical Phenomenon







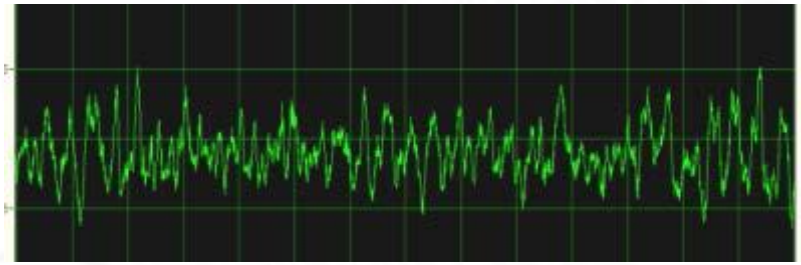
The figure shows the temporal evolution of the pressure profile thru the pipeline downstream from the leak, between the beginning of the leak until the stationary regime is reached again.



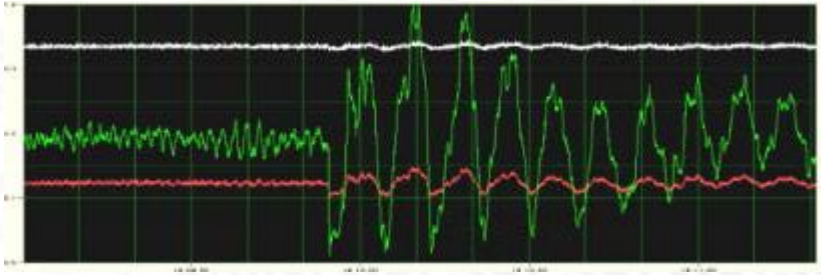
Two aspects are highlighted: 1) The fast propagation velocity of the front wave that corresponds to the pressure transient. 2) The occurrence of oscillations on the front wave. These pressure oscillations indicate the rupture of the pipeline and are monitored by the leak detection system.

Detection and Location

Acoustic sensors are placed on strategic points of the pipeline to read these signs that will allow the identification of a leak. The system calculates the travel time of this acoustic transient, since the spill location until they reach the adjacent acoustic sensors, enabling a fast location of the leak and with great precision.



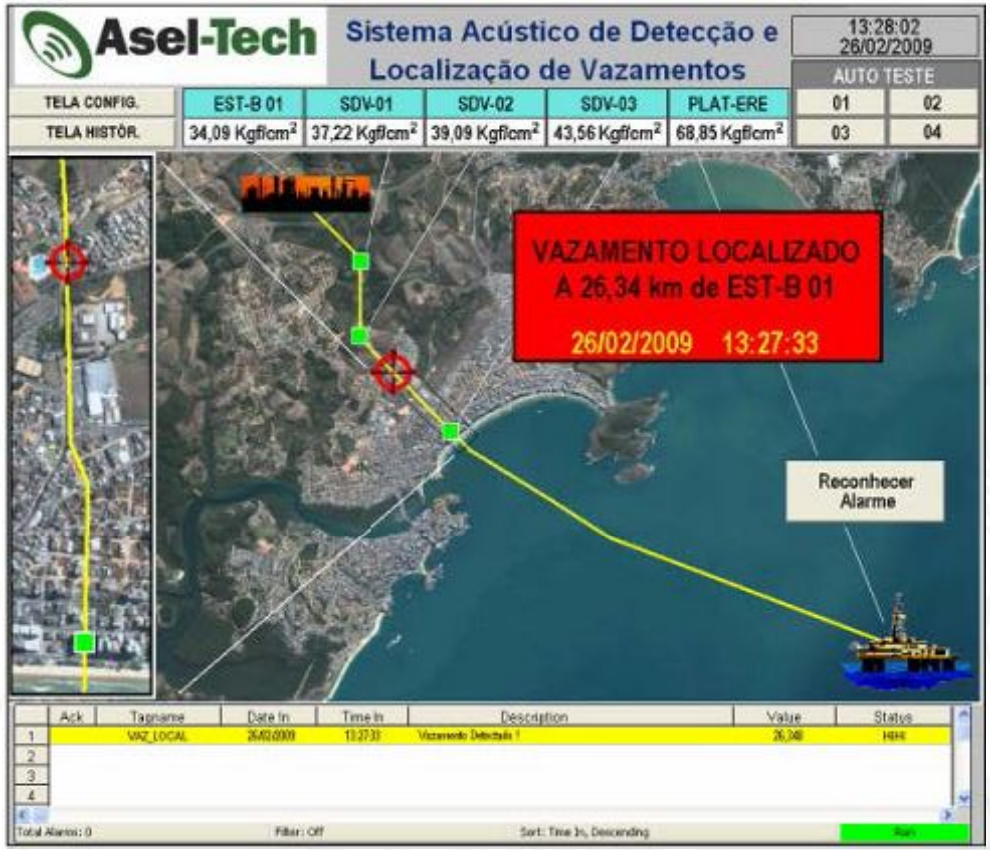
Background noise



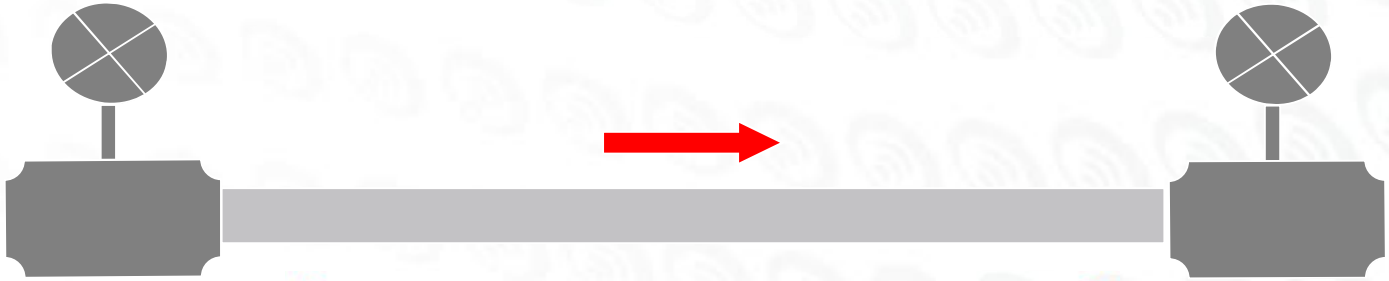
Leak signal

The system uses subsonic frequencies, below 3 Hz, region where are located the main spectral components of acoustic signals produced by the leaks.

The leak signals are analyzed and send to the supervisory system located in the control room. The leak alarm and its location are displayed one the supervisory screen.



Mass balance - Concept



Point "A"
Flow
Pressure
Temperature
Density

Computational Fluid Dynamics - CFD

Poitn "B"
Flow
Pressure
Temperature
Density

Input totalization

Line packing

Output totalization

BALANCE = INPUT – OUTPUT + LINE PACKING

Final uncertainty = function of the 3 combined uncertainties

System Components ILDS/SLDS

The system is basically composed of 03 equipment:

Acoustic Sensor FSS

Processor FPU320

Central Monitoring Station CMS

Acoustic Sensors (FSS)

The acoustic sensors are responsible for the acquisition (4-20mA) of the pressure signals. The sensor and its elements are assembled in an explosion-proof box which is connected to the pipeline via 2“ flanges. Instrumentation cables are responsible for the connections between FPU320 and sensors.

Examples of installed sensors




FPU 320

The FPU320 is assembled in a 19" standard cabinet that is installed next to the sensors. It is possible to connect until 3 pars of sensors (FSS) to a single FPU320. It main function are: process, filter and analyze all the signals received from the sensors, compare these signal with pre-established digital masks and forward the results to the supervisory system.

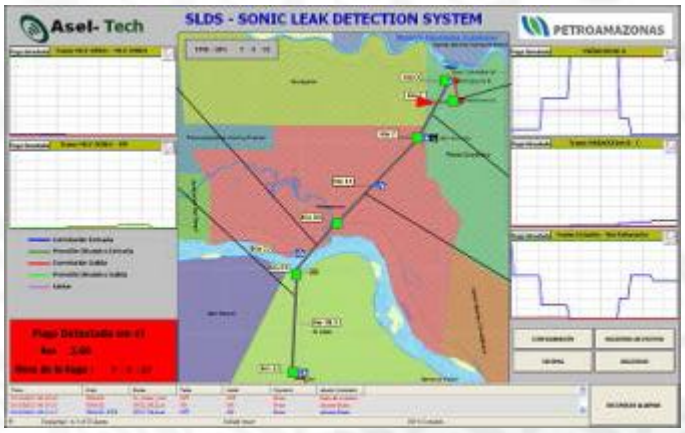
Examples of installed FPUs



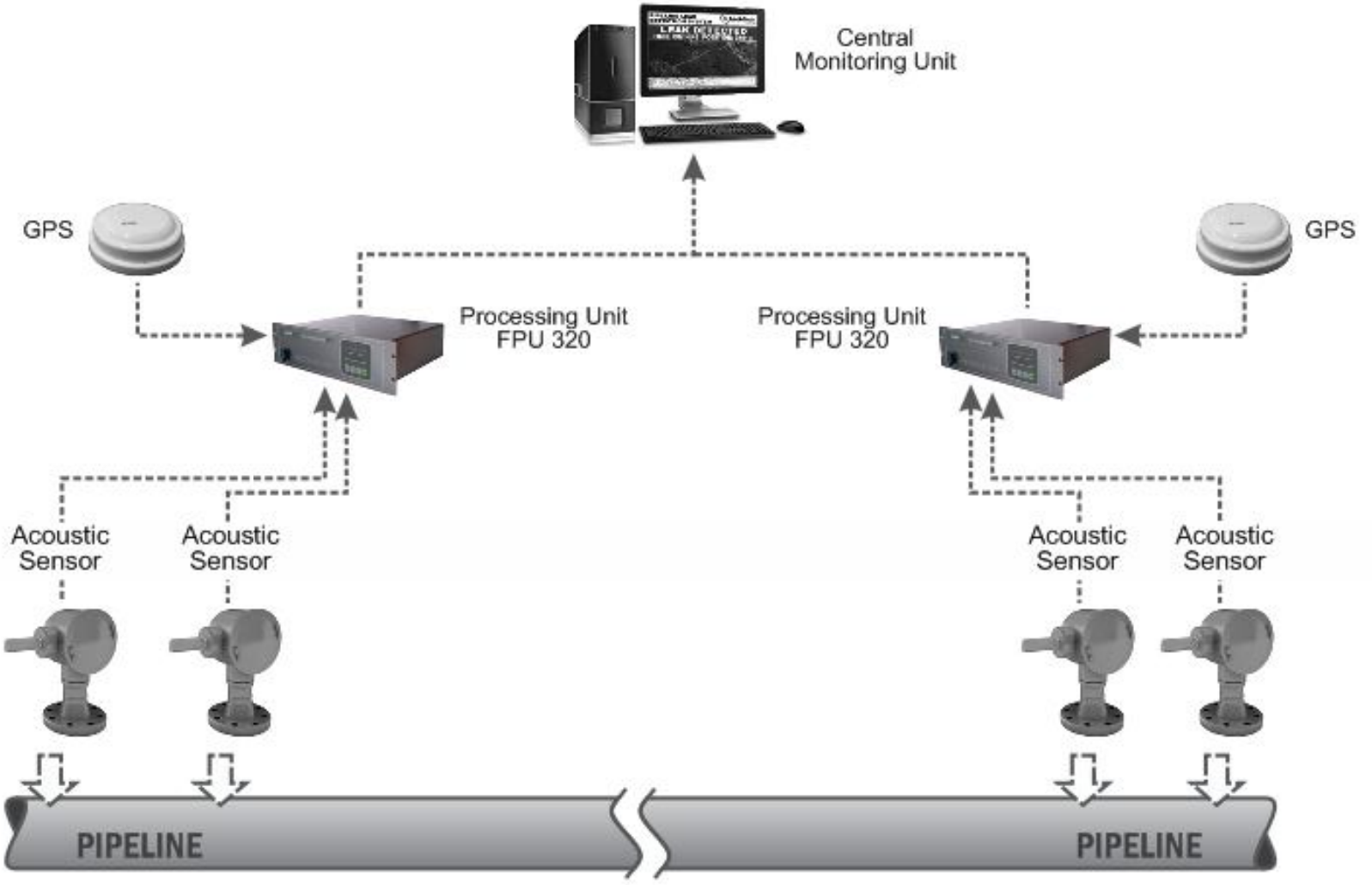
Central Monitoring Station

The supervisory is responsible for the system operation and it is normally installed in a dedicated computer that acts as an Human Machine Interface (HMI). The supervisory combines custom screens, ducts, monitoring points and all other details of the system.

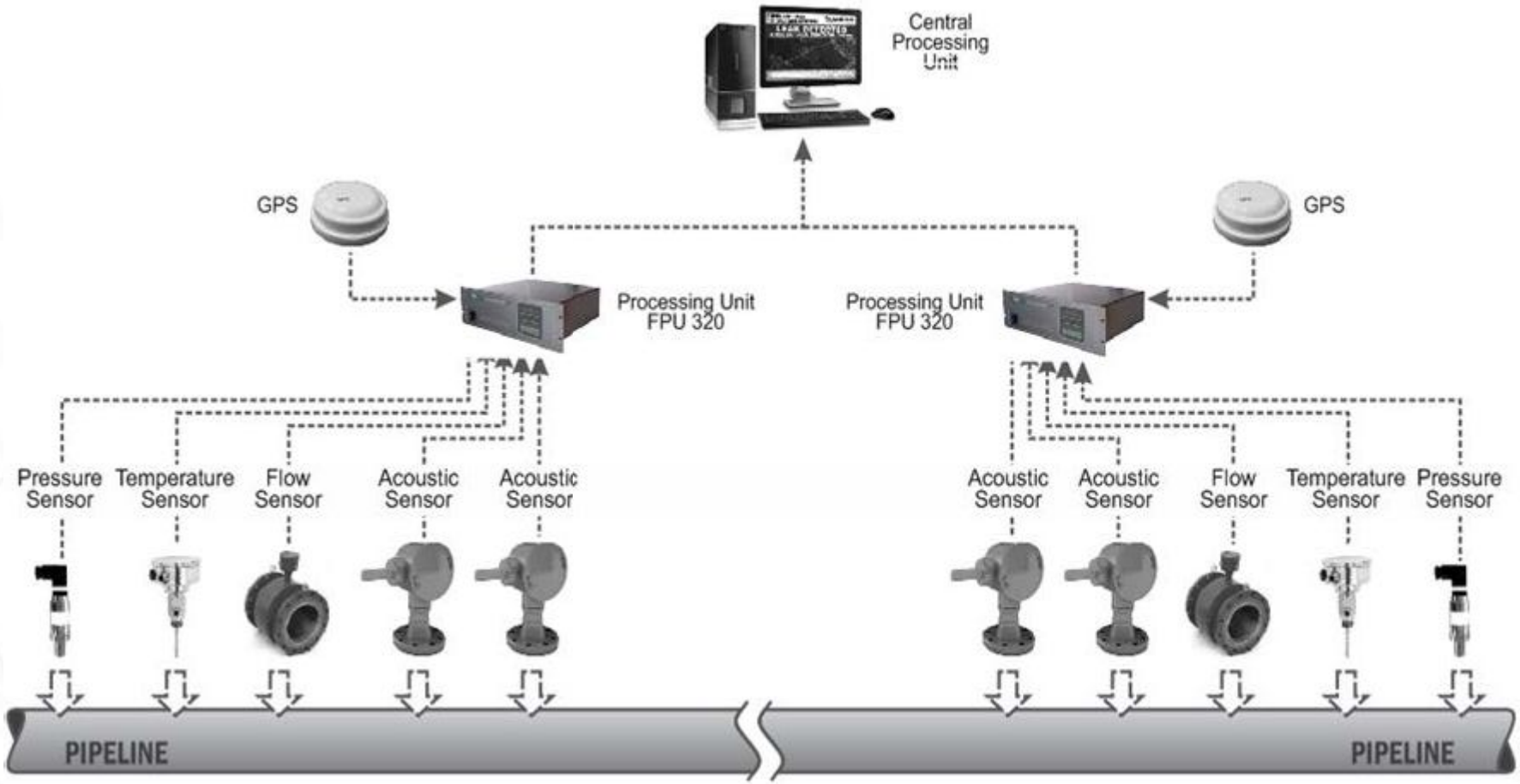
Examples of installed supervisory



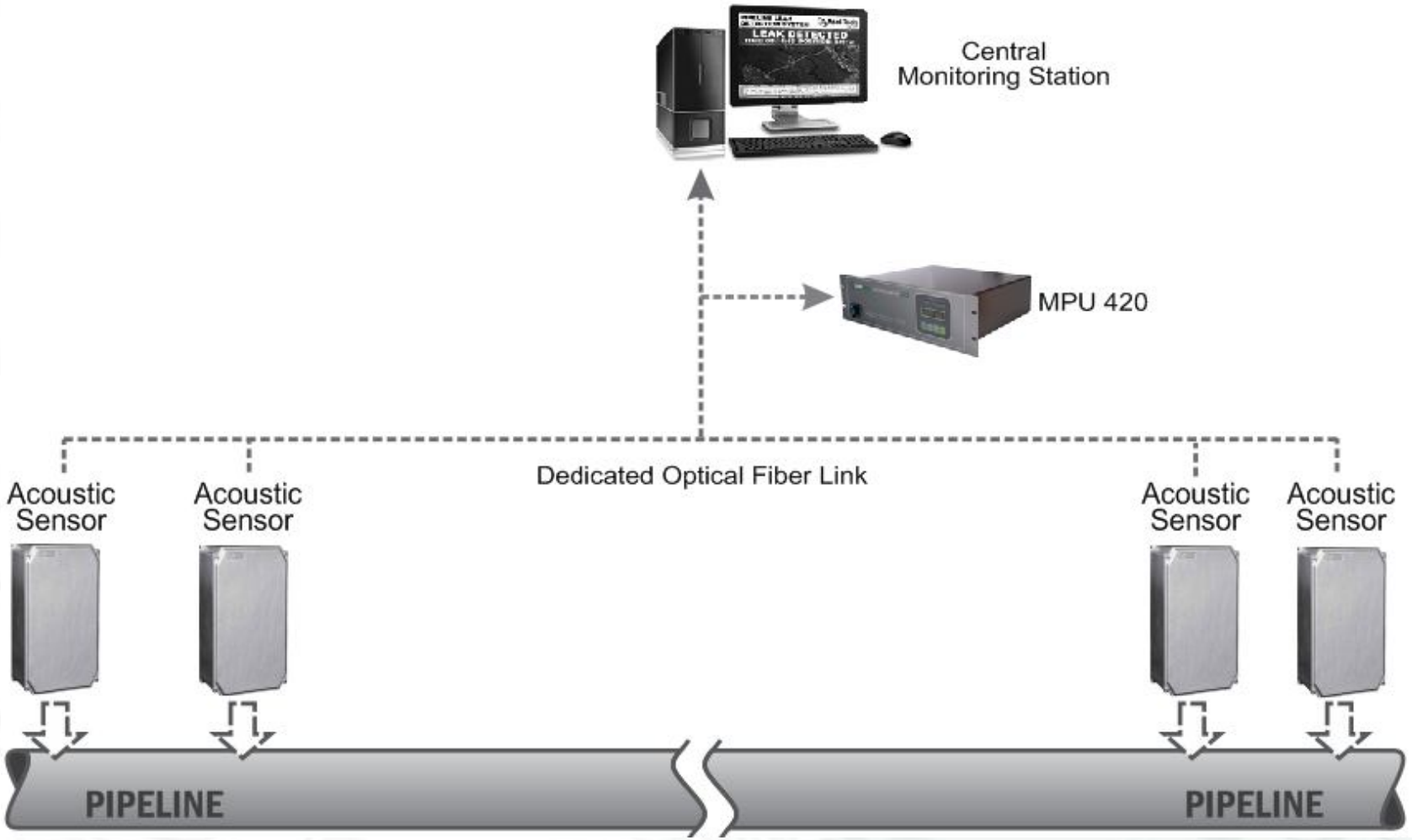
Typical SLDS Architecture



Typical ILDS Architecture



Typical Marc One Architecture



The Marc One System

The Marc One follows the same principles of the acoustic system (SLDS), with the same performance and accuracy, but with a very attractive cost benefit.

In its typical configuration, the Marc One system is composed of:

- **Dedicated acoustic sensors with a optical fiber output;**
- **Sensor power module with solar panel (optional)**
- **Optical fiber dedicated to the Leak Detection System**
- **Main Processing Unit - MPU**
- **Computer dedicated to the leak detection system**
- **Management Software and User Interface**

Main Features

- Complies with API RP 1130
- Sophisticated processing techniques including multi-layered algorithms and Artificial Neural Networks
- Easy integration with the SCADA
- High sensitivity and fast response
- Accurate locating better than 2% of the length of the section
- 100% coverage of the section between sensors with no mute zones
- Detects leaks even in a blocked line
- Report with the location and time of the leak
- Easy installation and operation
- Total customer support including remote assistance
- Low implementation cost

MPU - Main Processing Unit

The Main Processing Unit, denominated MPU, is responsible for the acquisition and processing of signals from the sensors and is installed in the control room, near the Central Monitoring Station (CMS).

The MPU continually monitors the signals collected from all the acoustic sensors and at the same time executes a complex processing of these signals, transferring the results to the CMS, which will issue the due alarm in case of a leak.

Examples of Instalations


TRANSPETRO - SE


BRASKEM - BA


PAM / EQUADOR


ARÁBIA SAUDITA


USP - SP


ENAP - CHILE