Veilige industriële netwerk oplossingen in de praktijk

Jaap Westeneng

Endress+Hauser

16 maart 2017 ••• Hart van Holland Nijkerk

Industrial Ethernet

Veilige industriële netwerk oplossingen in de praktijk

De industrie wordt met de ***opkomst van industriële netwerken en IoT*** meer en meer uitgedaagd om door en ***over de verschillende domein lagen*** heen transparant ***informatie te ontsluiten*** om zodoende invulling te geven aan de toenemende vraag naar ***BIG DATA*** en ***connectiviteit***.
In de praktijk kan de invulling en realisatie van ***transparantie en connectiviteit*** complex worden als ***verschillende infrastructuren***, ***industriële communicatie componenten en protocollen*** naast elkaar worden gebruikt en met elkaar verbonden worden.

Jaap Westeneng, Product Manager Asset Management, Endress+Hauser

BIG MINING is like gold mining…

…It is team work…

…pays off well…

London Good Delivery Bar
weights around 12.5 kilo
(400 troy ounces)

1 gram = € 40,00

London Good Delivery Bar = € 500.000,00

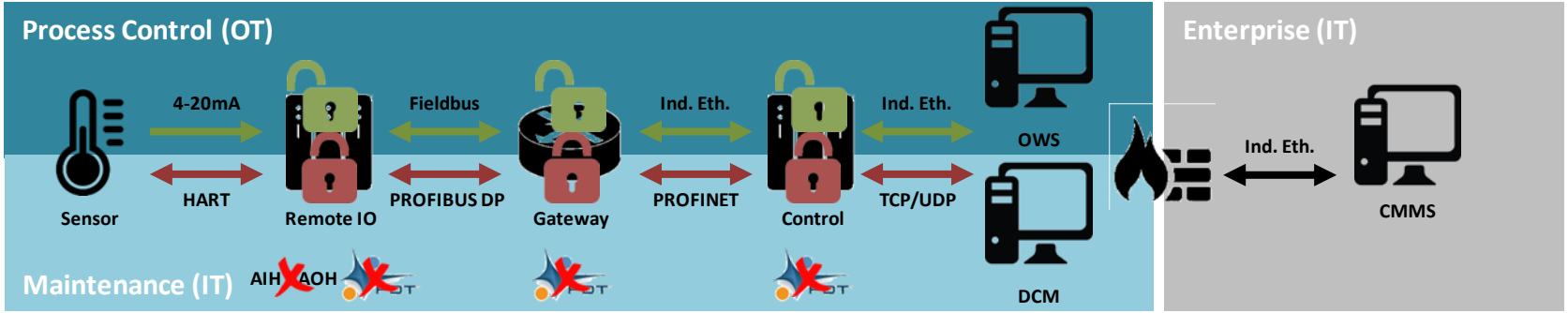
1 troy ounce = 31,1035 gram

…and needs to be secured

…some DATA is really hard to get

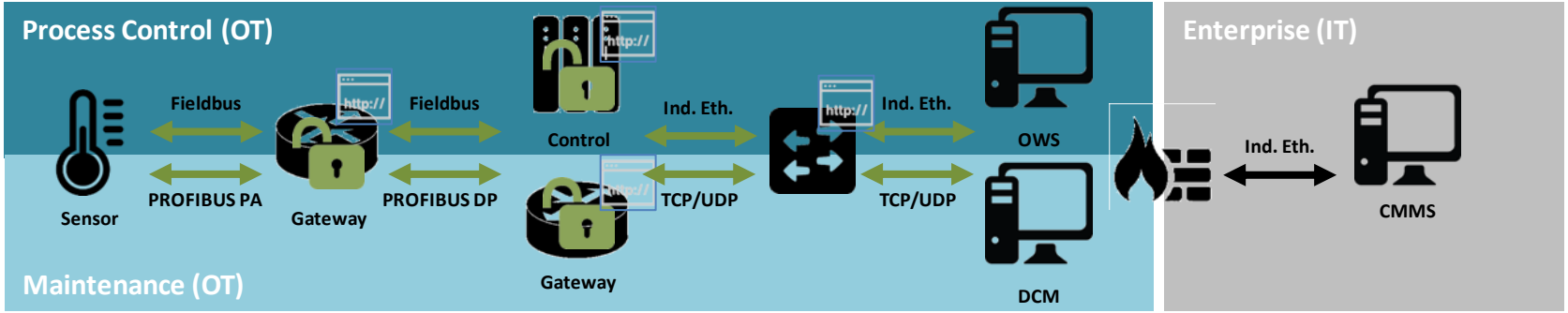
The Challenge #1

- From process control domain smart device (e.g. HART) can't be managed and maintained centrally because OT components doesn't provide a smart pass-through channel (e.g. FDT/DTM).



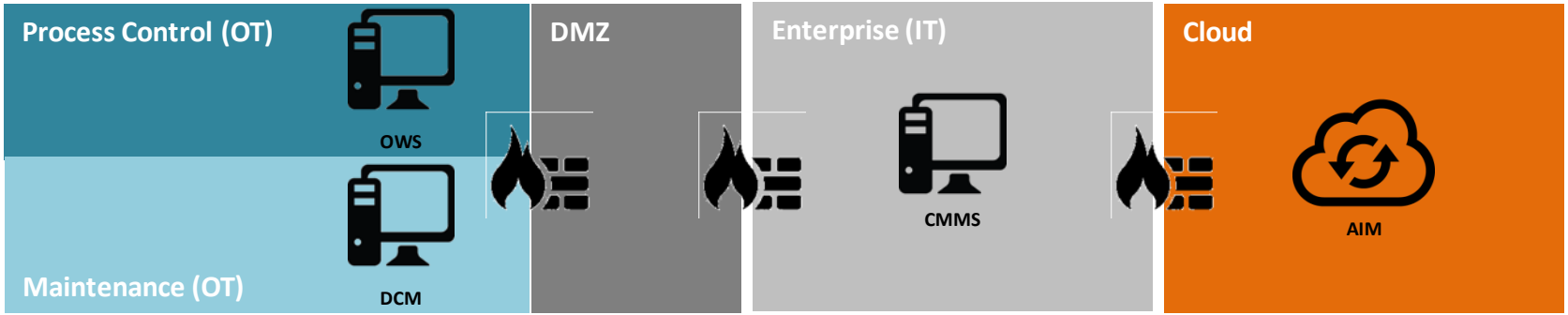
The Challenge #2

- If all OT components will become smart there will be a proliferation of unstructured data publishers!



The Challenge #3

- Direct secure connection between OT and cloud applications are technically feasible but not allowed by corporate policies (e.g. no Internet connection in OT)



From phone to smart phone

From switch to managed (smart) switch

Embedded OPC UA server

Switch

Event logging

Digital communication protocols
(IGMP, SNMP, DHCP, SMTP, HTTP, Telnet, Syslog, SNMP, LLDP,…)

Firmware updates

Virtual Local Area Network (VLAN)

Embedded webserver

Network Address Translation (NAT)

From gateway to smart gateway

Embedded OPC UA server

Communication protocol gateway

Event logging

Communication protocol transparency

Firmware updates

Mail notification

Embedded webserver

Device diagnostics

From device to smart device

OPC UA

Embedded OPC UA server

4-20 mA

Process value

Heartbeat Technology

Embedded device verification

Monitoring + Optimization

Digital communication protocols
(HART, Modbus, PROFIBUS, PROFINET, EtherNet/IP,...)

Embedded Device Driver

AI TOT
DI DO

Multiple digital process variables

Embedded webserver

Device diagnostics

IIoT Vision

- The promise of ***connecting everything*** within an ***industrial environment*** to get ***complete visibility into its operations*** and ***allow the best real-time decisions to be made***—with or without human intervention—will transform how we manufacture for years to come. The premise for this next industrial evolution is the **Industrial Internet of Things (IIoT).**

IIoT Benefits

Cost savings from:

- Minimized energy usage
- Integration with the supply chain
- Fewer on-site personnel
- Less time dedicated to low-level tasks

Better customer service through:

- Predictive maintenance
- Remote troubleshooting and patching
- Product improvement based on customer use

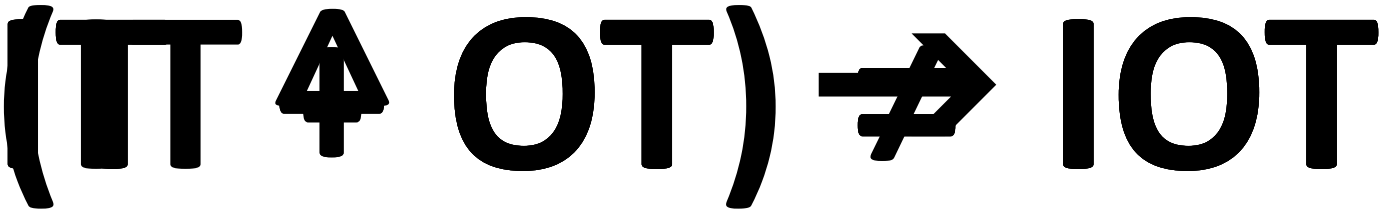
Smarter automation, providing:

- Auto-tuning and optimizing based on surroundings
- Notification reporting for diagnosis and resolution
- On-demand assembly driven by business systems

Visibility, any time and anywhere, enabling:

- Better decision-making
- Increased time to value
- Increased system safety and security
- Remote asset monitoring and managing

The Premise



Industrial Internet of Things
The concept of connecting all hardware and software components within an ***industrial environment*** for ***complete visibility into operations at any time of day and from any location.***

Critical capabilities for enabling IIoT Platform

- **Connectivity**
  This includes all necessary hardware and software to network within the plant and the enterprise, standards for integrating machines, clouds, applications and the technology for quickly and efficiently managing devices, moving data, and triggering events.
- **Cloud**
  Includes all of the various clouds across an enterprise to implement computing and storage capabilities wherever they are most needed—at the edge, within the plant, at the enterprise, or outside the firewall
- **Big Data Analytics**
  Includes the use of a broad set of statistical and optimization tools to cleanse, monitor, and analyze both structured and unstructured data for enabling unprecedented insights
- **Application Development**
  Includes the needed tools for quickly and easily creating new mash up software applications that leverage all other areas of the IIoT platform as well as quickly and easily moving existing legacy applications on top of the platform as well.

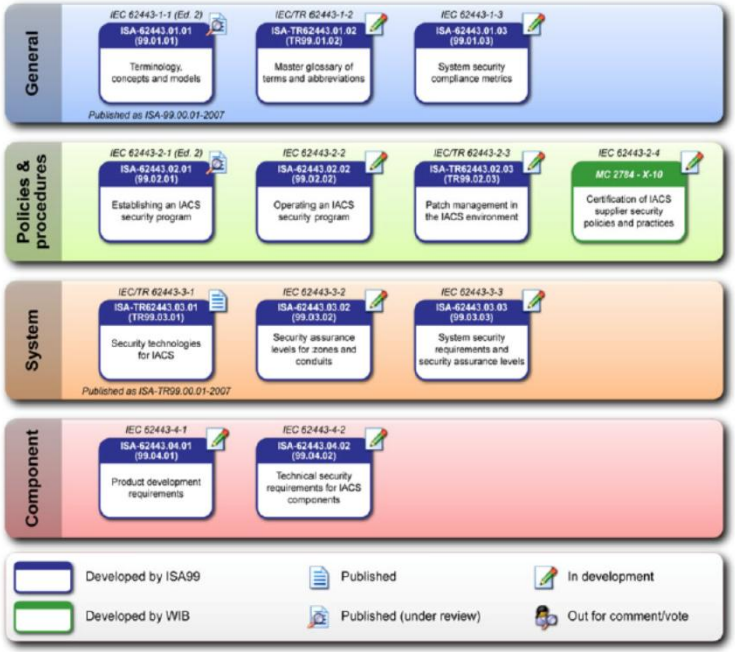
ISA/IEC-62443/ISA-99 Based Industrial Control System (ICS) Cyber security

7 Steps to Industrial Control System Security

- Assess existing systems
- Document policies and procedures
- Train personnel and contractors
- Segment the control system network
- Control access to the system
- Harden the components of the system
- Monitor and maintain system security

Source http://www.exida.com/ICS-Cybersecurity/7-Steps-to-Control-System-SCADA-System-Security

ISA/IEC-62443/ISA-99 Based Industrial Control System (ICS) Cyber security



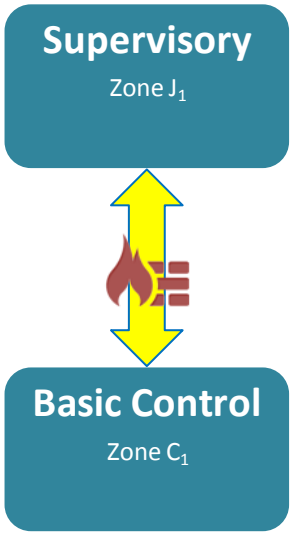
The ANSI/ISA-99 standards provide the base documents for the ISO/IEC standards in ***Industrial Control Security***, known as ***IEC-62443***.

Over the next few years, these standards are expected ***to become the core standards for Industrial Control Security worldwide.***

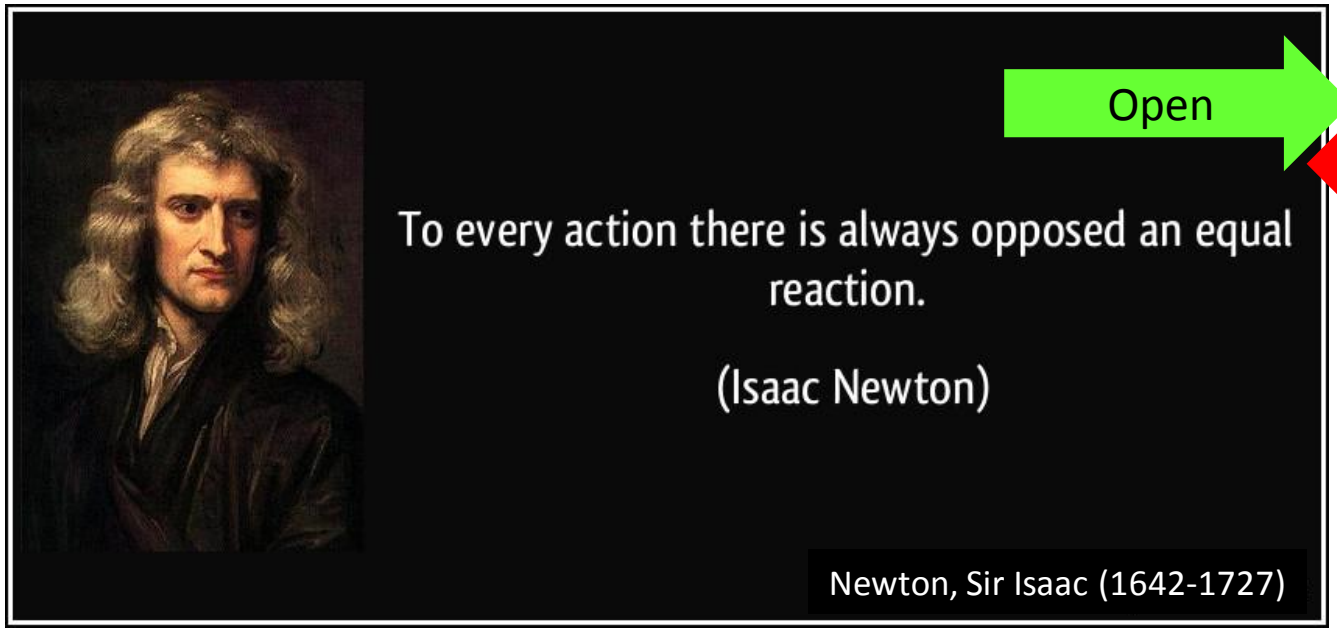
Source http://www.exida.com/ICS-Cybersecurity/7-Steps-to-Control-System-SCADA-System-Security

ISA/IEC-62443/ISA-99 Based Industrial Control System (ICS) Cyber security

- ***Zone*** is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence.
- ***Conduit*** is a path for the flow of information between two zones.
  - It can provide the security functions that allow different zones to communicate securely.
  - Any transfer of electronic data between zones must have a conduit.



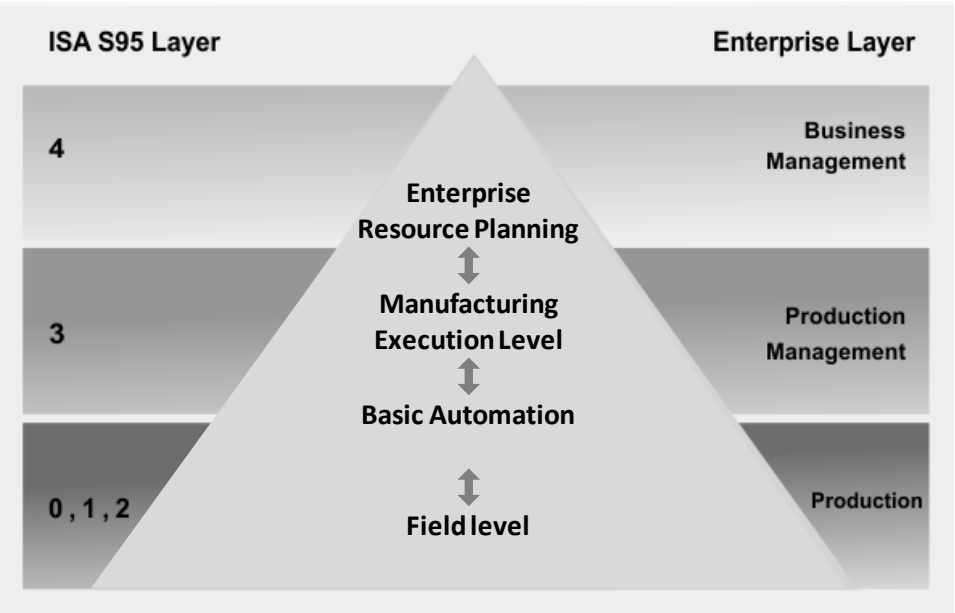
Newton's Third Law



Open

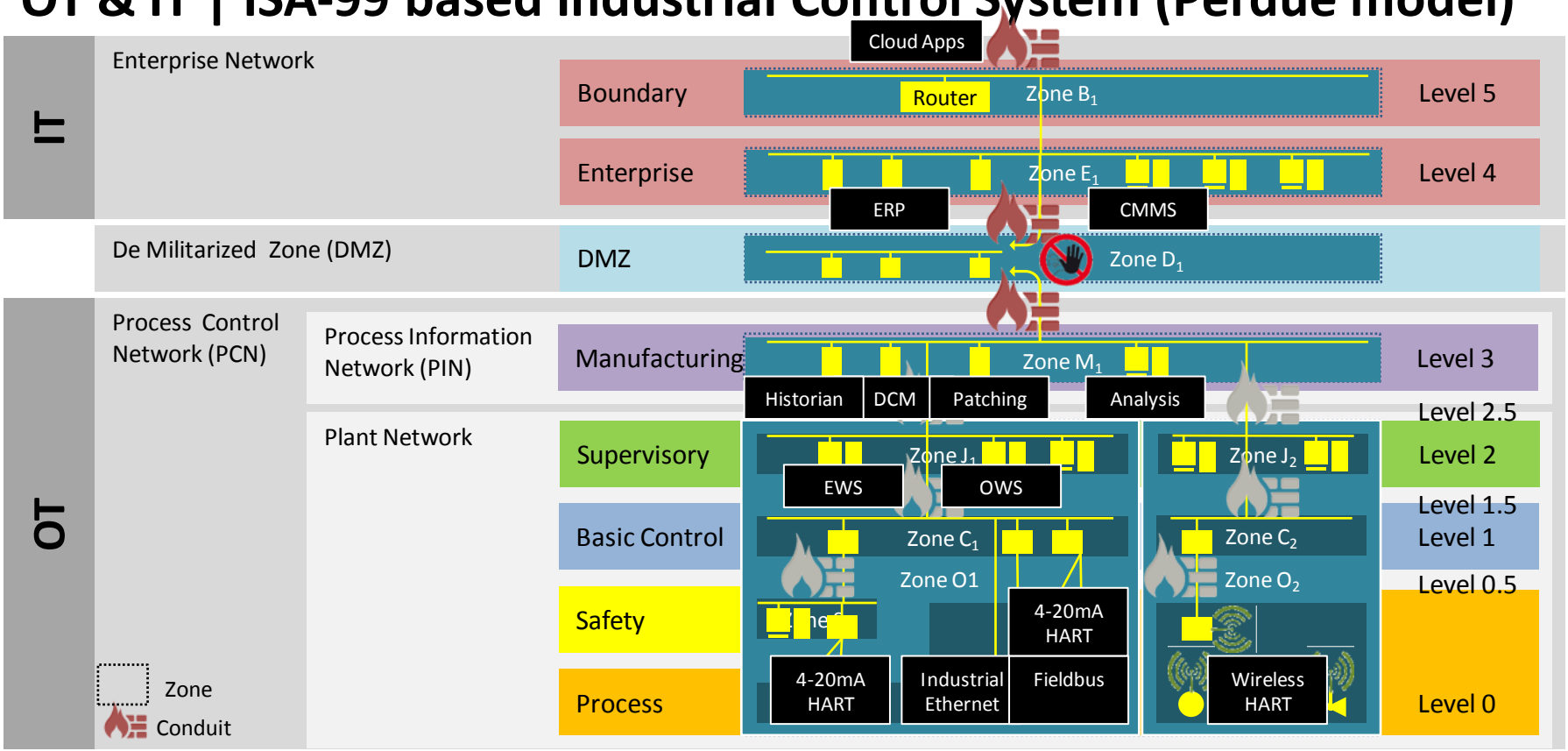
Secure

Is this the picture you have in mind for the Automation structure?

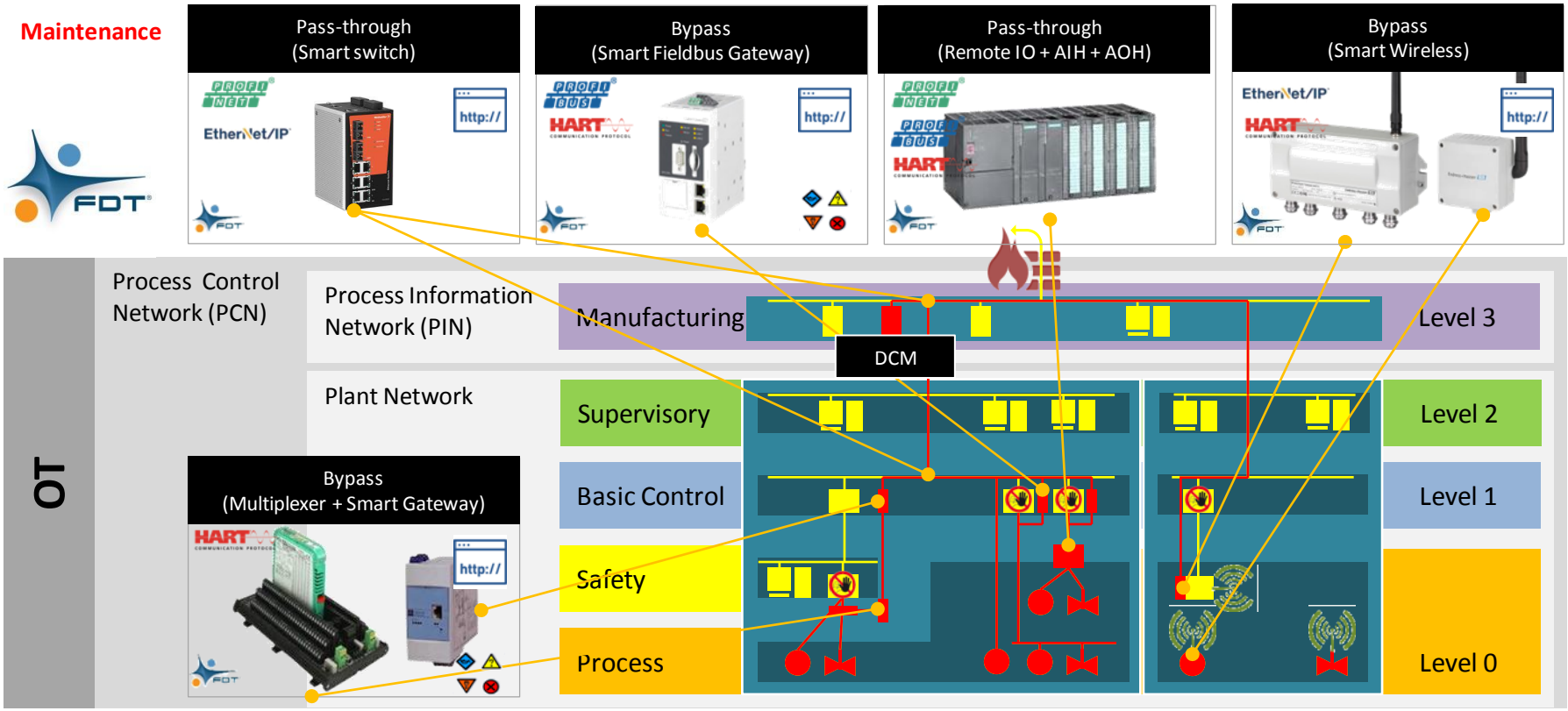


- Proven and widely accepted structure.
- Highly available and mature systems.
- Supports sustainable operations with long life cycles.

OT & IT | ISA-99 based Industrial Control System (Perdue model)



OT | Device Configuration Management (DCM) [Challenge #1]



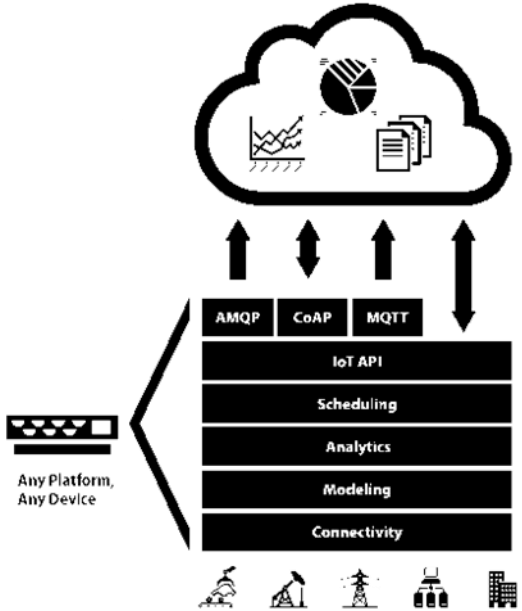
Definition

Edge

The part of the network that ***bridges the gap*** between **Information Technology** and ***Operation Technology***, where the rich resources available in the cloud are not directly available.

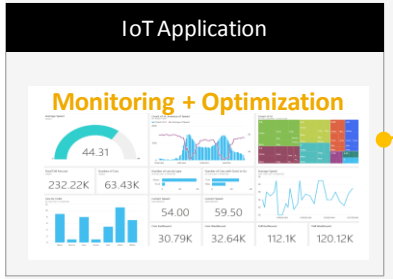
IoT Edge Solution

- In order to ***seamlessly integrate industrial data into IIoT***, a new communications platform is required.
- ***Within OT***, the platform ***must understand the various network topologies and data protocols*** that will be encountered.
- ***Within IT***, the platform ***must be able to transform the data it collects and push it into the cloud via IIoT standards***.
- With the lack of computer networking infrastructure in OT, this platform must be embeddable and run within a standalone appliance or an **edge-based device *where IT and OT converge***.



OT-IT | IoT Edge Gateway (M+O) [Challenge #2]

Monitoring
Optimization



IoT App

Boundary — Router — Level 5

Enterprise — Level 4

DMZ

IoT Edge

OT

Process Control Network (PCN)

Process Information Network (PIN)

Manufacturing — Level 3

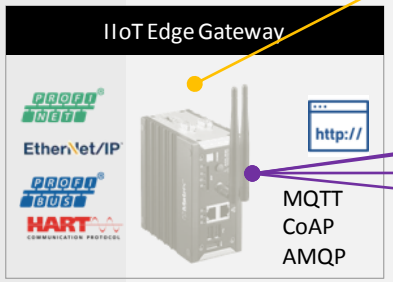
Plant Network

Supervisory — Level 2

Basic Control — Level 1

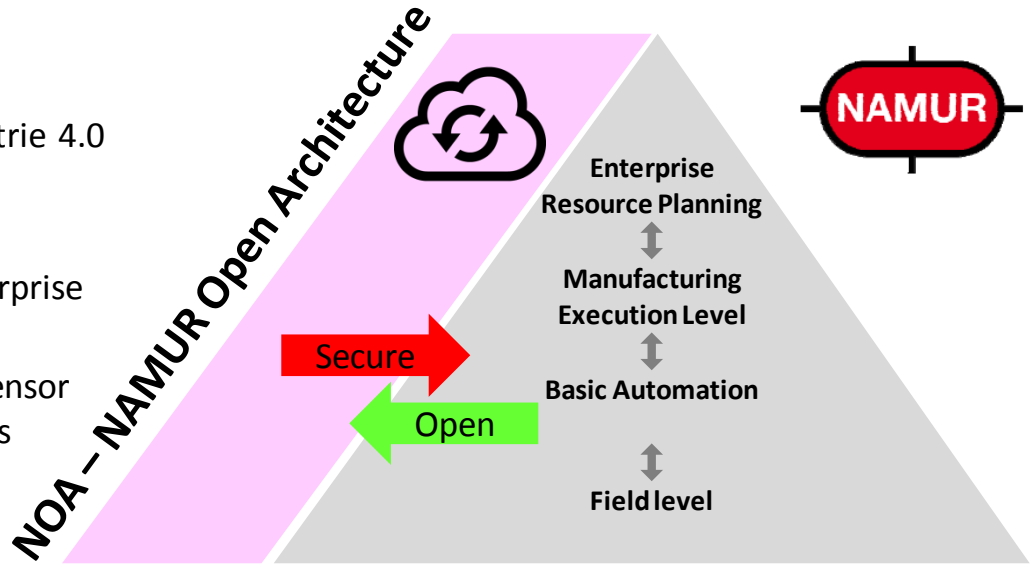
Safety

Process — Level 0



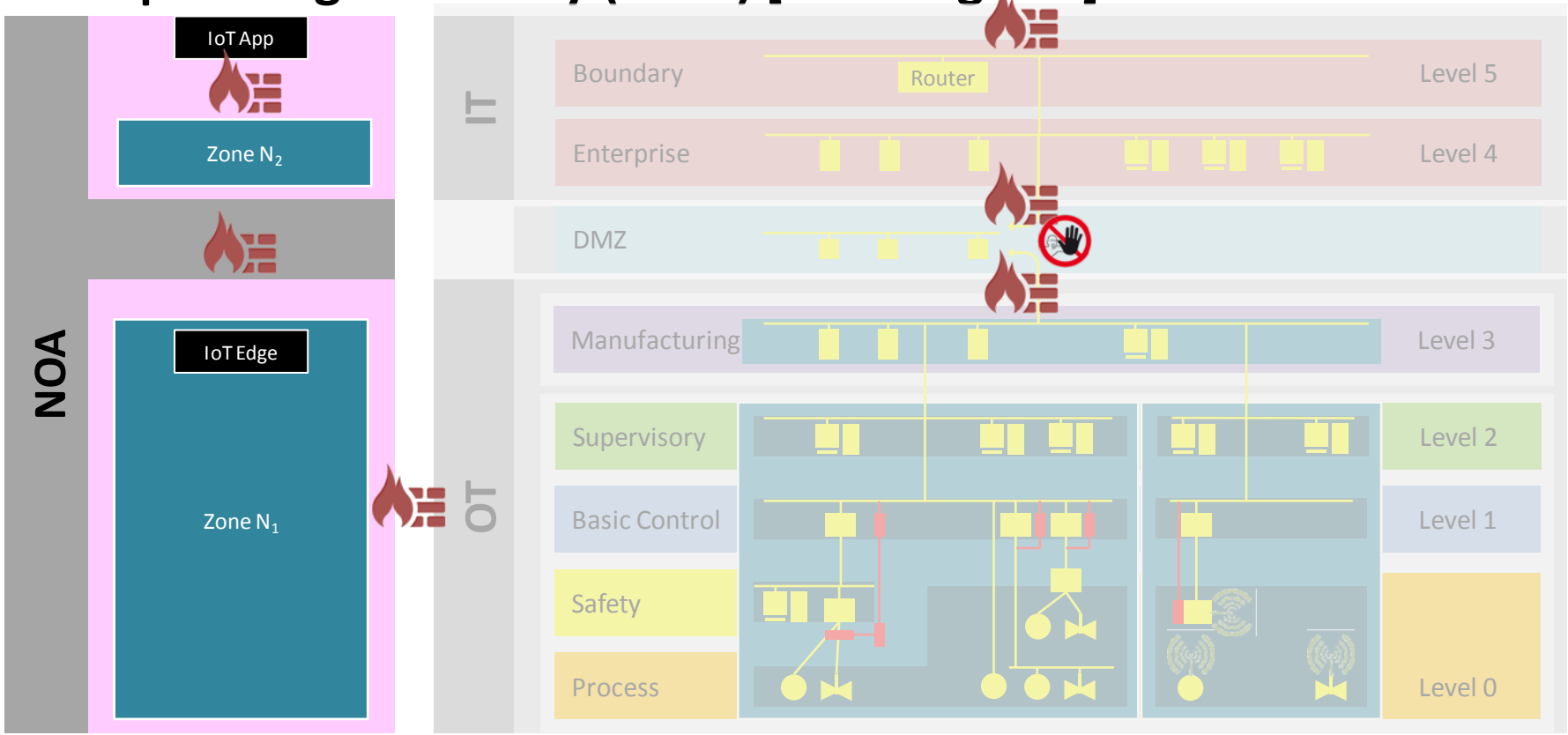
Is current Automation Structure ready for IoT?

- Additive to existing structures
- Open for new approaches within Industrie 4.0
- Based on existing standards
- Simple integration of fast changing IT components from field level up to enterprise level
- Significant improvements of cost per sensor due to open and integrative approaches
- No risk of availability and safety of installed base



Enhancement of existing approaches as a baseline for the efficient and flexible utilization of Industrie 4.0 with the process industry

NOA | IoT Edge Gateway (M+O) [Challenge #3]



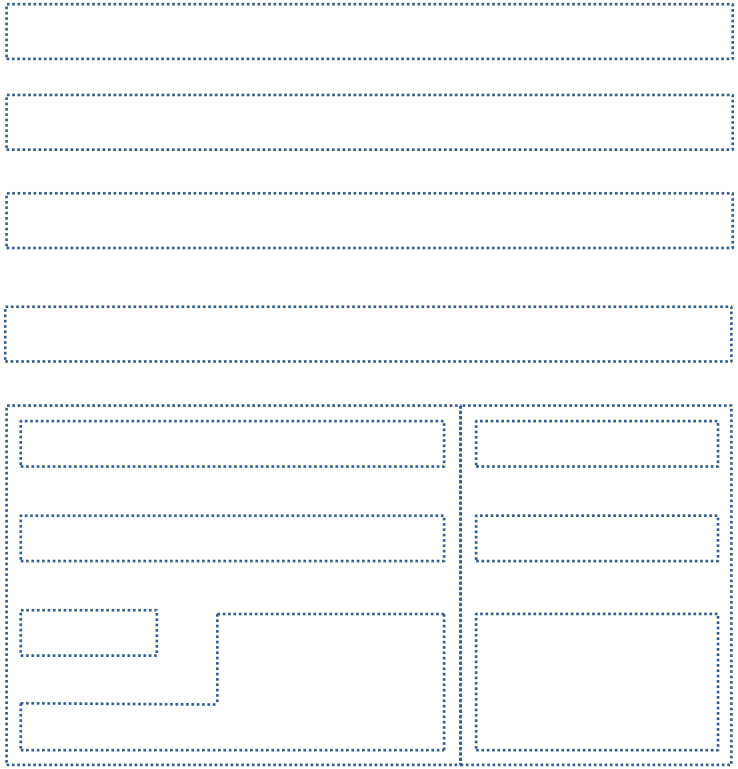
Information

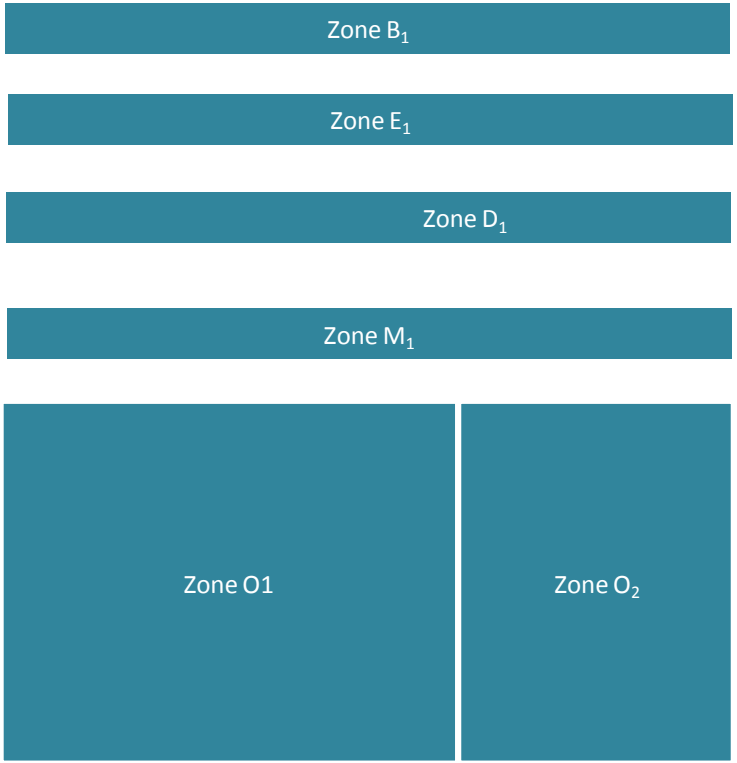
Jaap Westeneng
Business Development Manager

Endress+Hauser B.V.
Nikkelstraat 6
1411 AJ Naarden

jaap.westeneng@nl.endress.com
T 035-6958717
M 06-53729616

Plant Asset Management solutions
Industrial Communication Technologies




Zone B_1
Zone E_1
Zone D_1
Zone M_1
Zone O1
Zone O_2

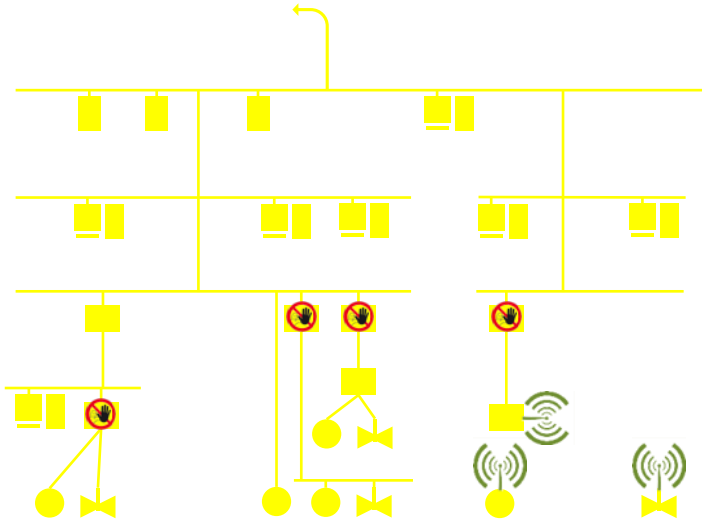

Zone J1
Zone J2
Zone C1
Zone C2
Zone S1
Zone P1
Zone W1
Zone

Level 2.5

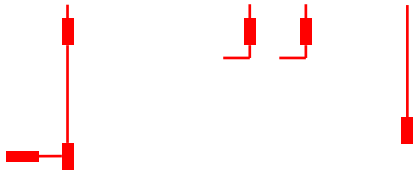
Level 1.5

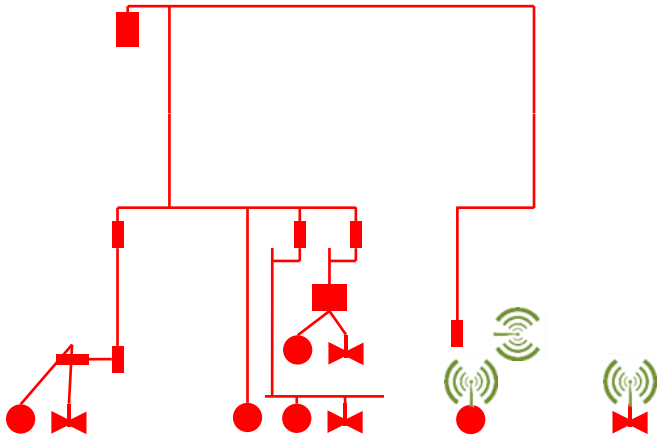
Level 0.5

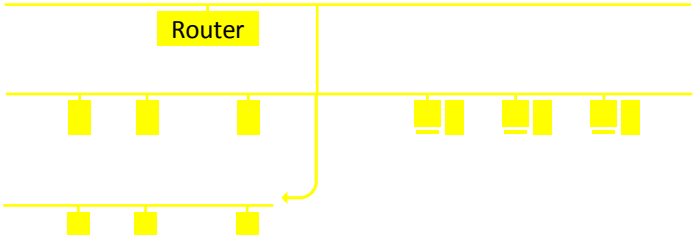
Conduit

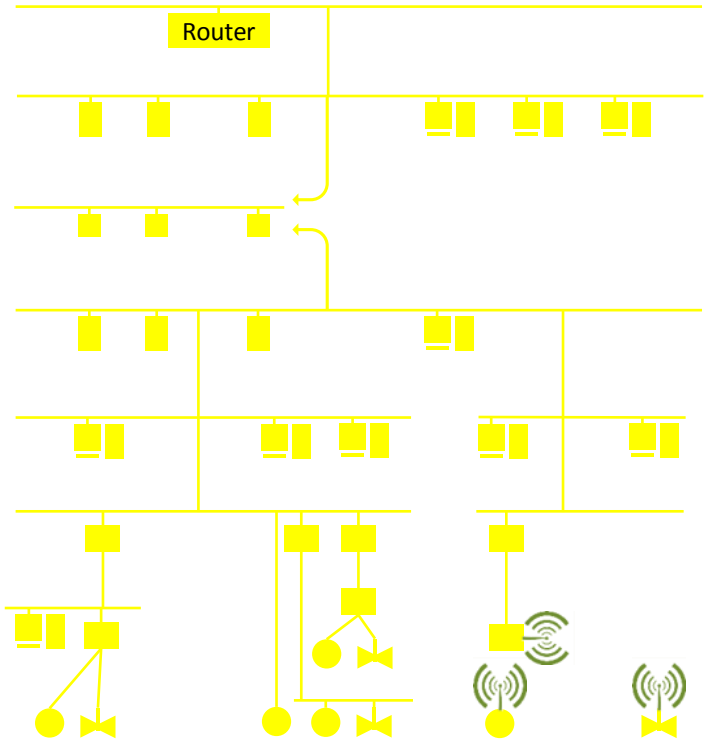


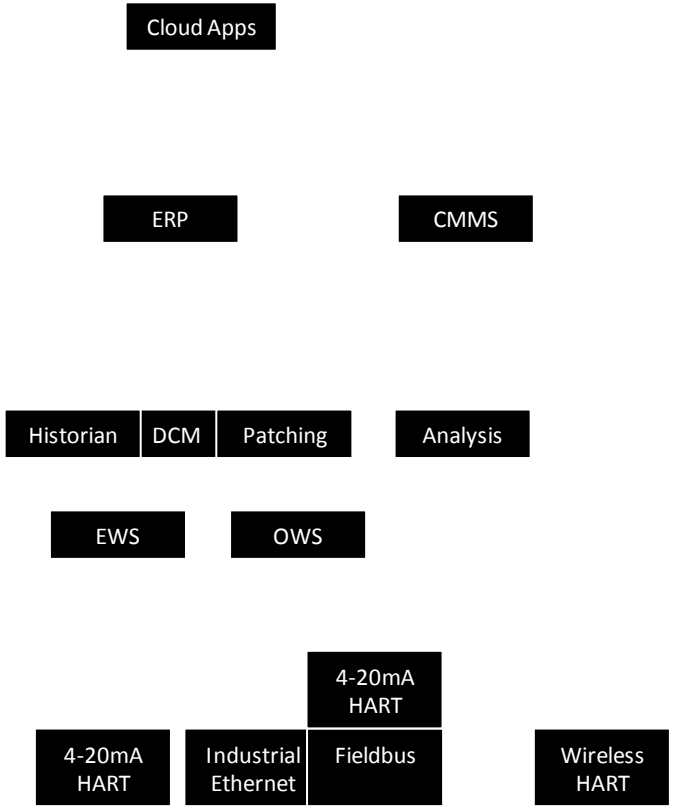
Industrial Ethernet






Router


Router


Cloud Apps
ERP
CMMS
Historian
DCM
Patching
Analysis
EWS
OWS
4-20mA HART
4-20mA HART
Industrial Ethernet
Fieldbus
Wireless HART