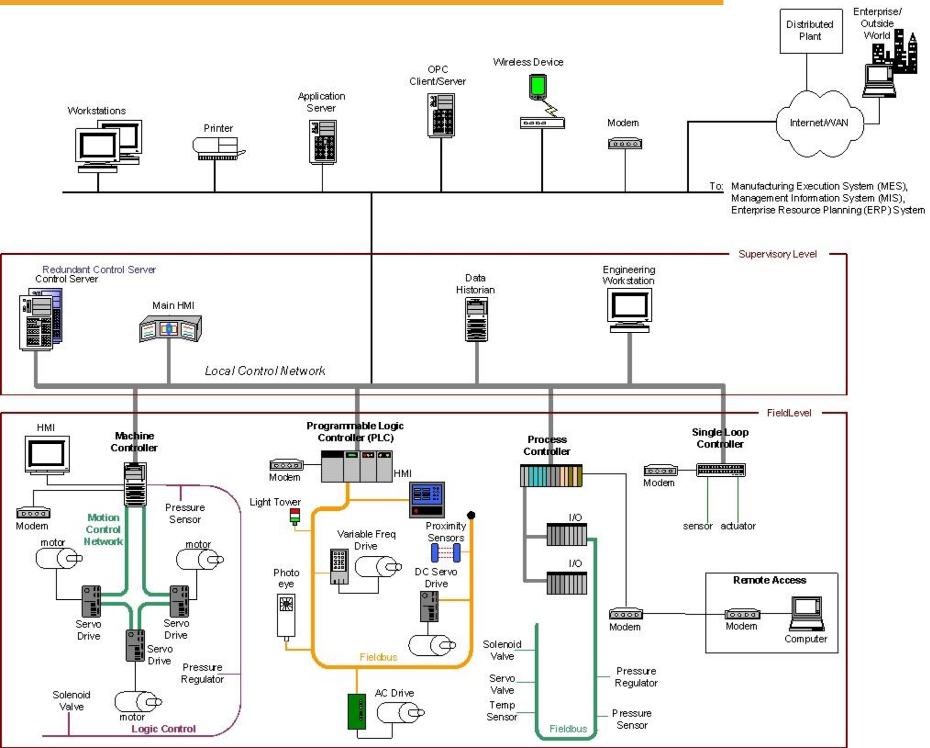
# Industrial Control System (ICS)

# Learning Outcome for ICS

- Describe industrial control system
- List common industrial networking protocols/standards
- Describe various functions of Human Machine Interface (HMI)
- Describe a typical SCADA application
- Explain OPC-UA principle and benefits
- Describe the functionality of Digital Twin

# Industrial Control Systems (ICS)

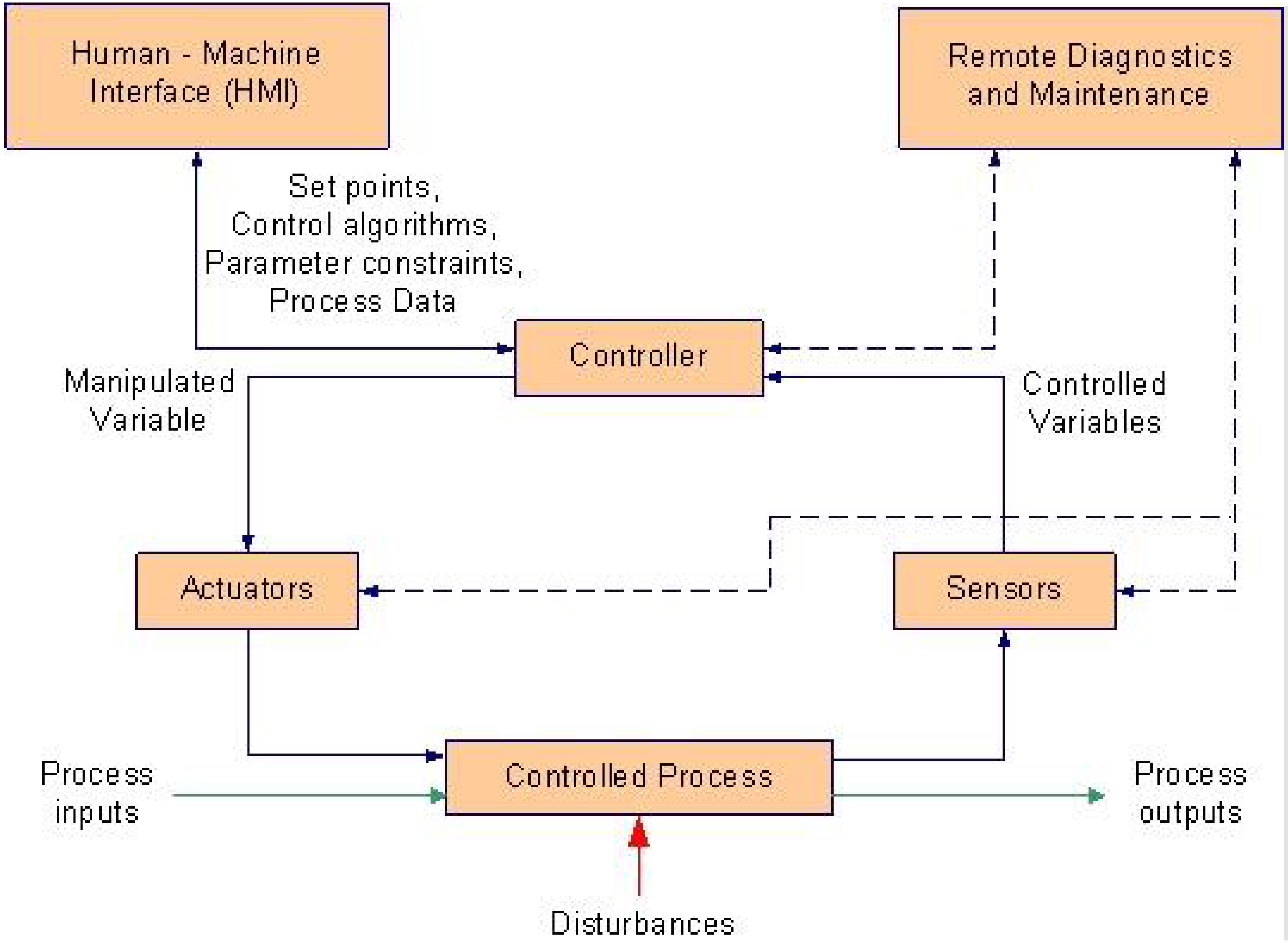



- A general term comprising of various control systems
  - Supervisory Control & Data Acquisition (SCADA)
  - Distributed Control System (DCS)
  - Other control system typically deploying Programmable Logic Controllers (PLC)
  - Etc
- Ranging from small standalone system, manufacturing plant to critical infrastructure

Source: NIST special publication 800-82, Guide to ICS Security

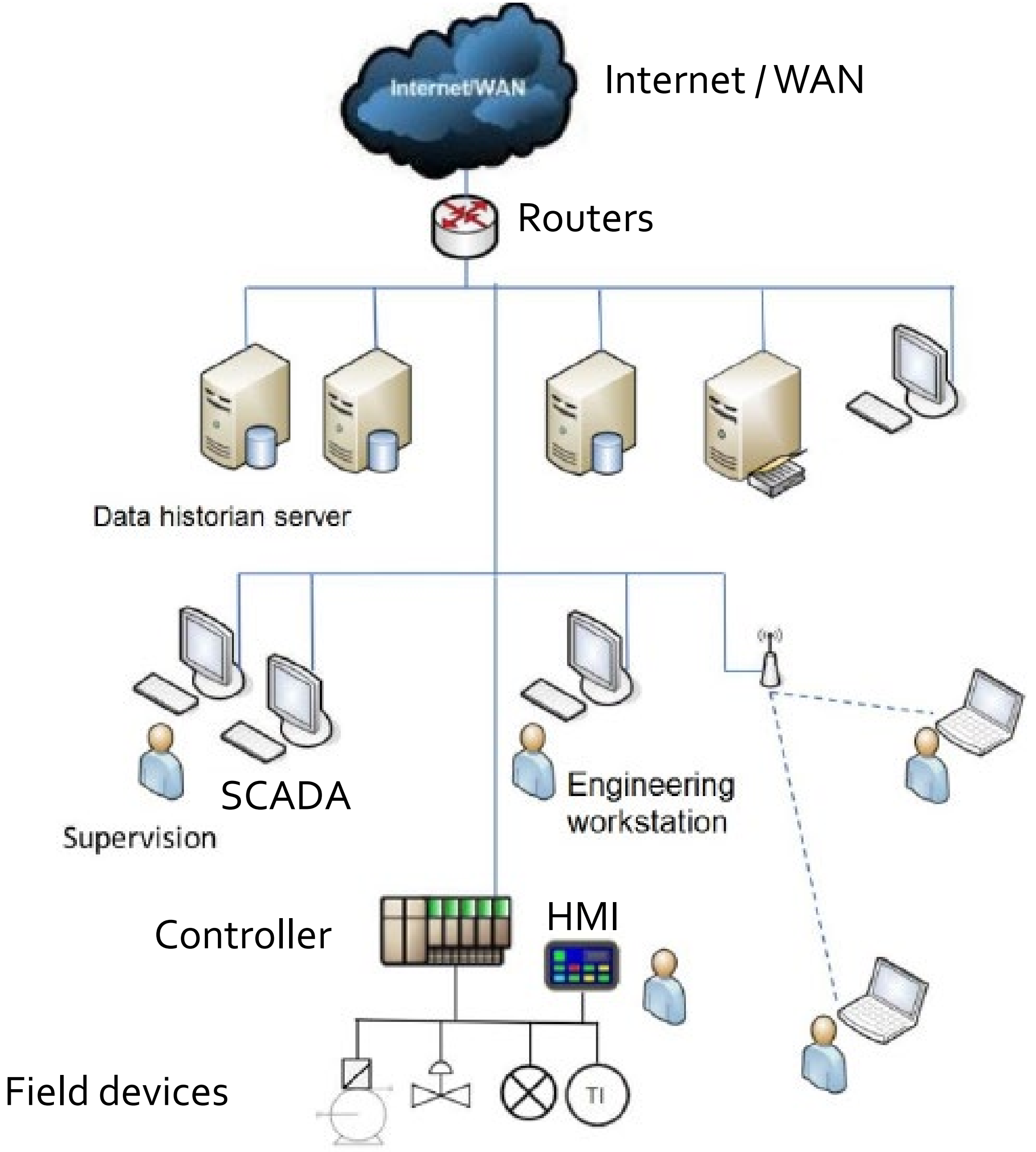
# ICS Operation

Typical ICS contains many control loops, human machine interfaces, remote diagnostics and maintenance tools. Sensors would make measurements and feedback physical property to the controller for decision making. Controller actuates control valves, contactors etc to get the process to produce desired end results. Diagnostics provides insight to prevent and identify  abnormal operations or failures.




Source: NIST special publication 800-82, Guide to ICS Security

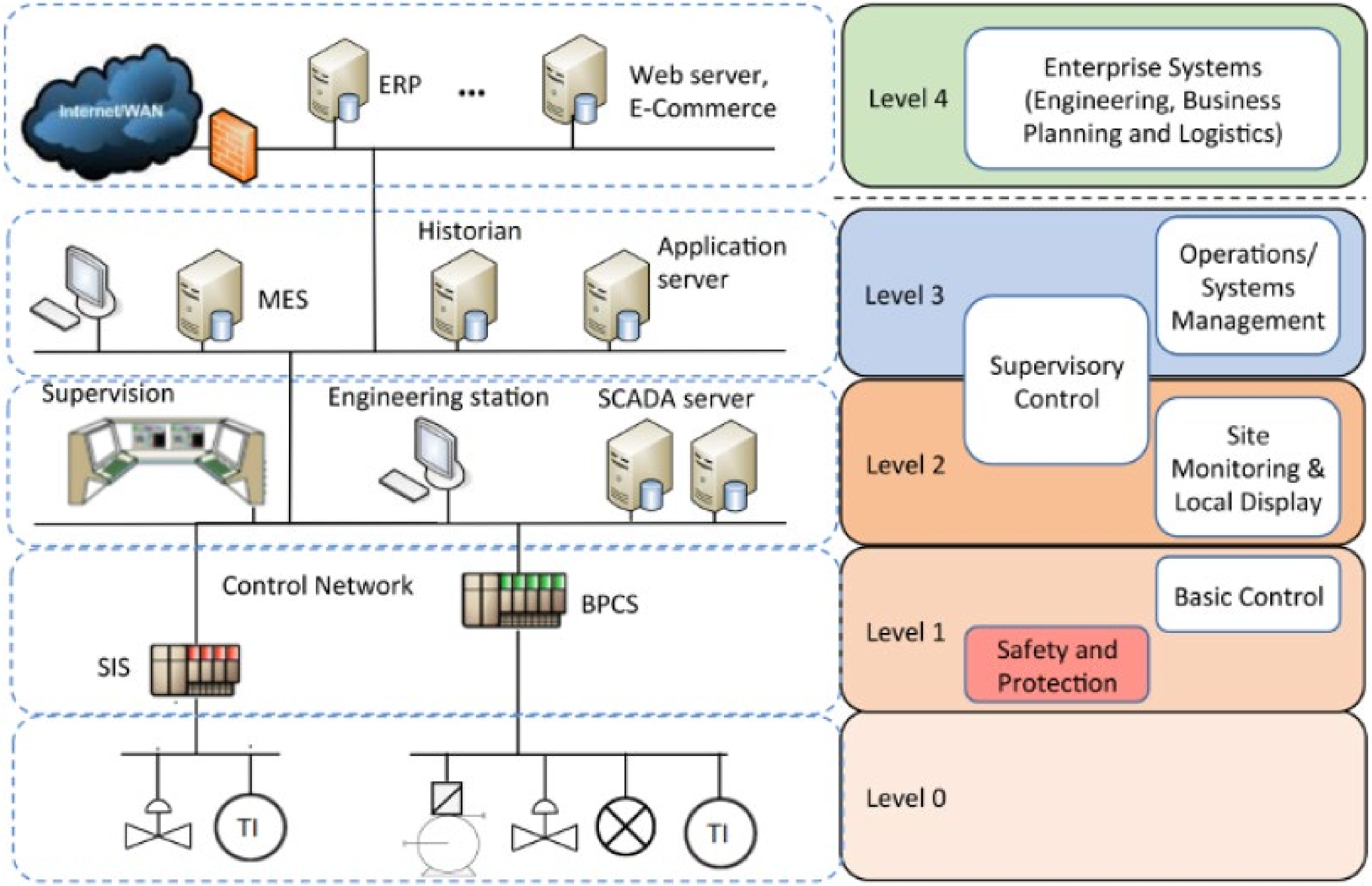
# Typical ICS Architecture




Source: Cybersecurity of Industrial Systems, Jean-Marie Flaus, WILEY

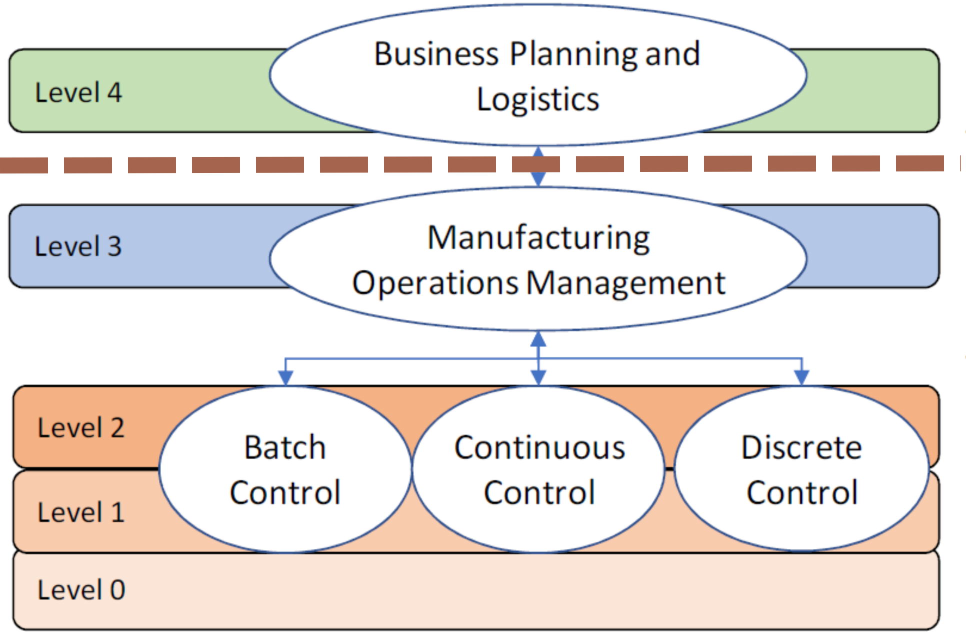
# Purdue Model

Provides a reference model for hierarchical representation of control system




Source: Cybersecurity of Industrial Systems, Jean-Marie Flaus, WILEY

# Purdue Model




- Level 0 (Physical Process)
  - Sensors and Actuators
- Level 1 (Basic Control)
  - Functions involved in detection, observation and control pf physical system
  - PLC, Remote Terminal Unit (RTU)
- Level 2 (Supervision Control) – Typically associated with production
  - Monitoring and controlling of physical processes
  - HMI, Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS)
- Level 3 (Operations Management)
  - Flow management to achieve production requirement
  - Manufacturing Enterprise System (MES) and historical databases
- Level 4 (Enterprise business system)
  - Management of manufacturing and processing operation
  - Enterprise Resource Planning (ERP)

Demilitarized zone (DMZ) between level 3 and 4 to separate the company's industrial (Operation Technology) and IT networks

# Overview of Industry 4.0


Smart factory?

Advance manufacturing?

Digital factory?

Mainly it is a combination of **cyber-physical systems** and would encompass one or more of the following:

- Integration of Manufacturing to Enterprise Systems
- Intelligent robots, Smart Machines
- IoT devices
- Smart sensors
- Data analytics
- Autonomous systems – Autonomous guided vehicles
- Artificial Intelligence

Source: https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#1ddf3e1b9788

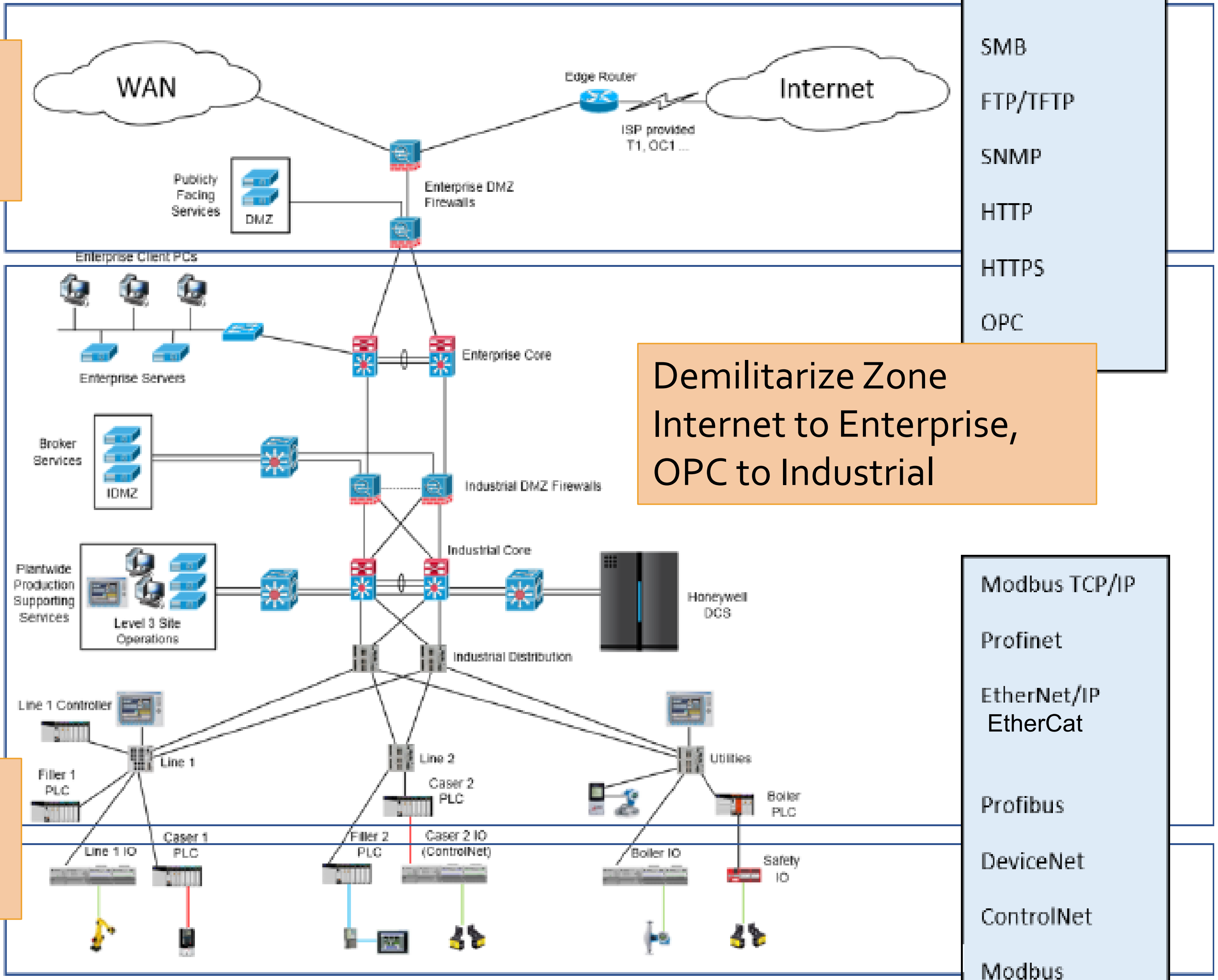

https://youtu.be/yKPrJJSv94M

# How does ICS communicate?

Enterprise Zone
Communicates
with Internet

Demilitarize Zone
Internet to Enterprise,
OPC to Industrial

Industrial Zone
Various types of
Industrial Network




SMTP

SMB

FTP/TFTP

SNMP

HTTP

HTTPS

OPC

Modbus TCP/IP

Profinet

EtherNet/IP
EtherCat

Profibus

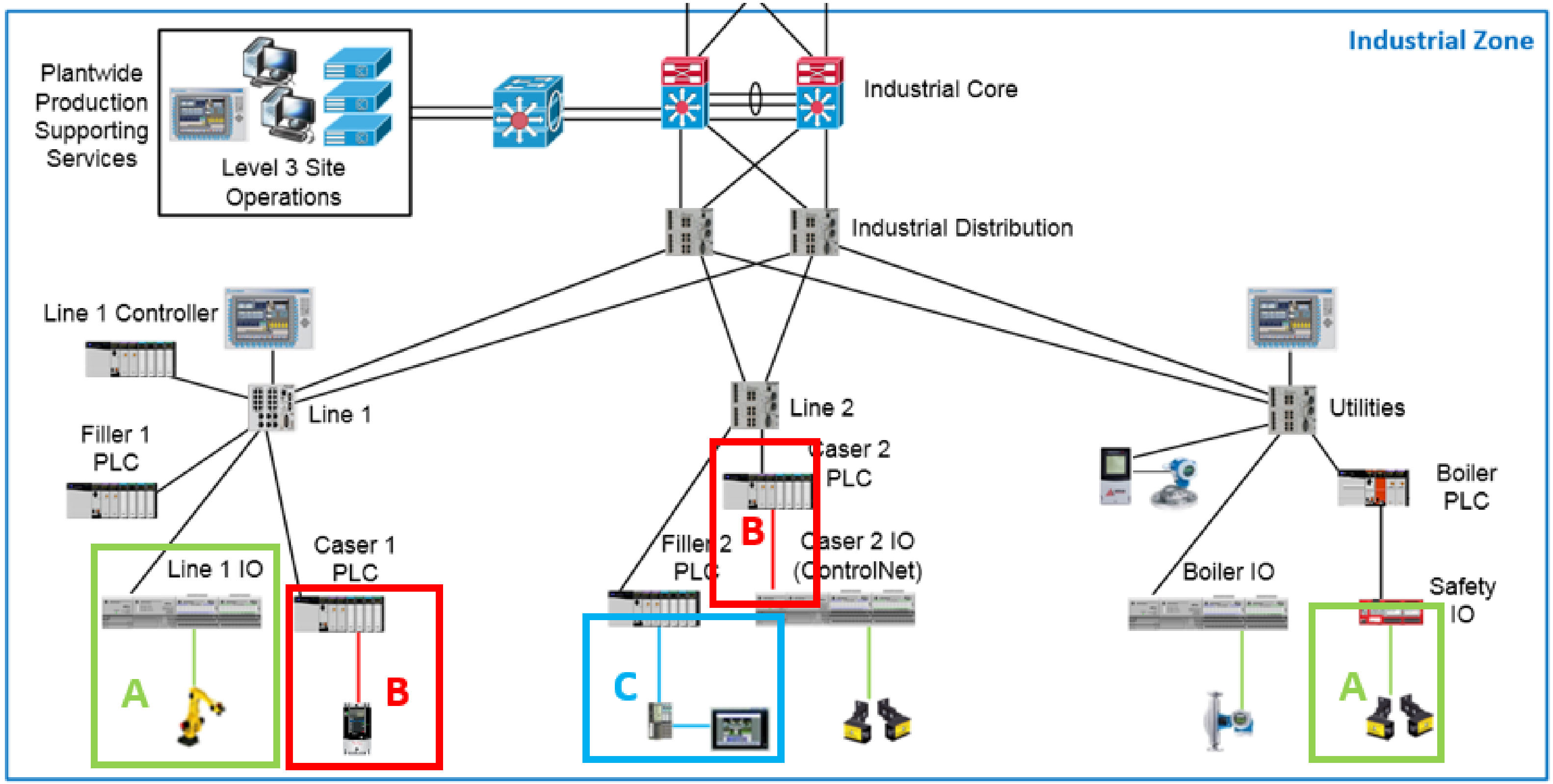
DeviceNet

ControlNet

Modbus

Source: Industrial Cybersecurity, Pascal Ackerman

# Industrial Zone



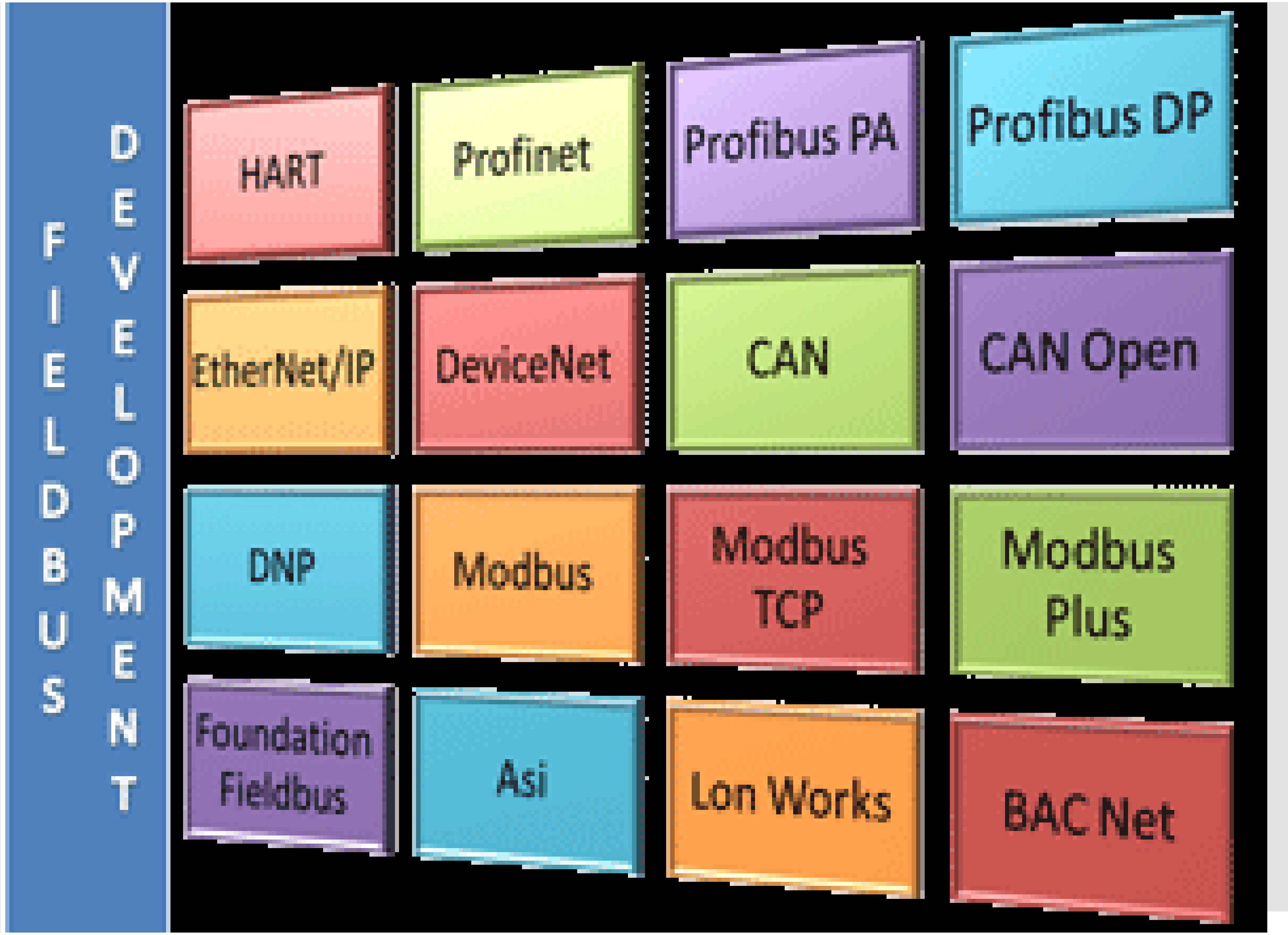

Source: Industrial Cybersecurity, Pascal Ackerman

- A – Hardwired devices with discrete signals or analog signals directly to PLC or remote IO
- B – Fieldbus protocols such as ProfiNet, Profibus & Modbus, enabling field devices connect to PLC directly without IO module
- C – Nested Ethernet is the connection to specific hardware without being visible to the entire network

# Fieldbus

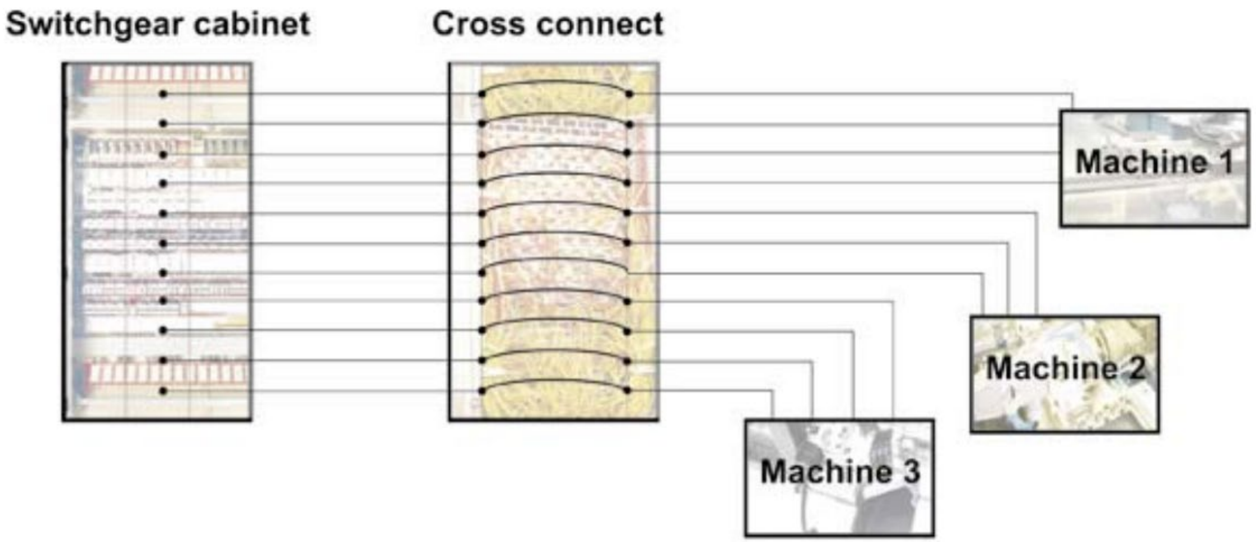
Fieldbus is non-proprietary (open) communication protocol that define how devices communicate with other devices or controllers

Variety of fieldbus mostly found in Industrial Zone

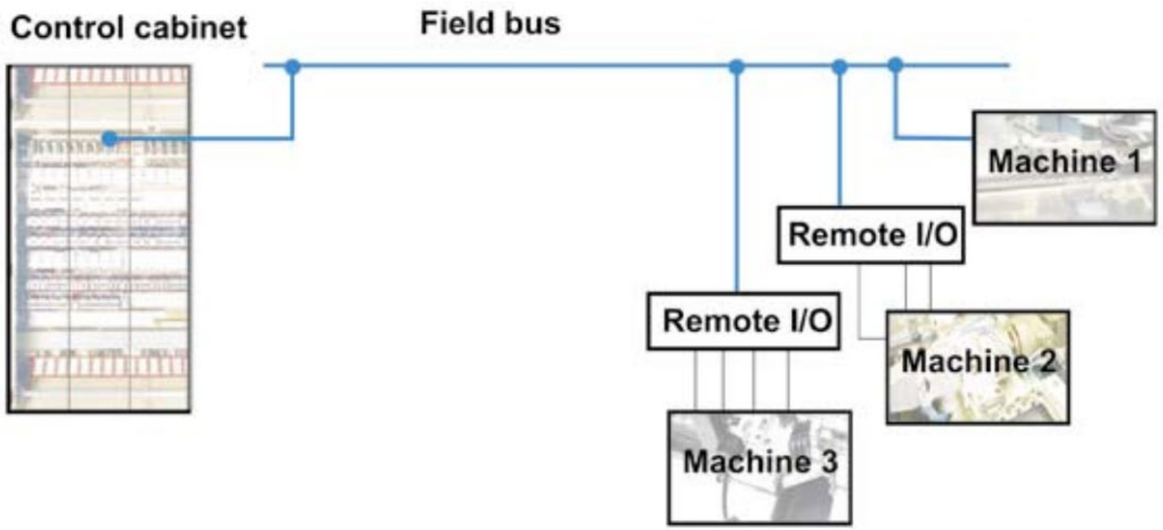


# Fieldbus Reduce Wiring

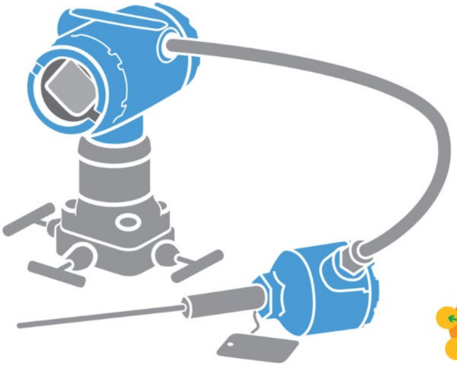
## Cable installation - Conventional




## Cable installation based on fieldbus



# Fieldbus = More Data



WirelessHART

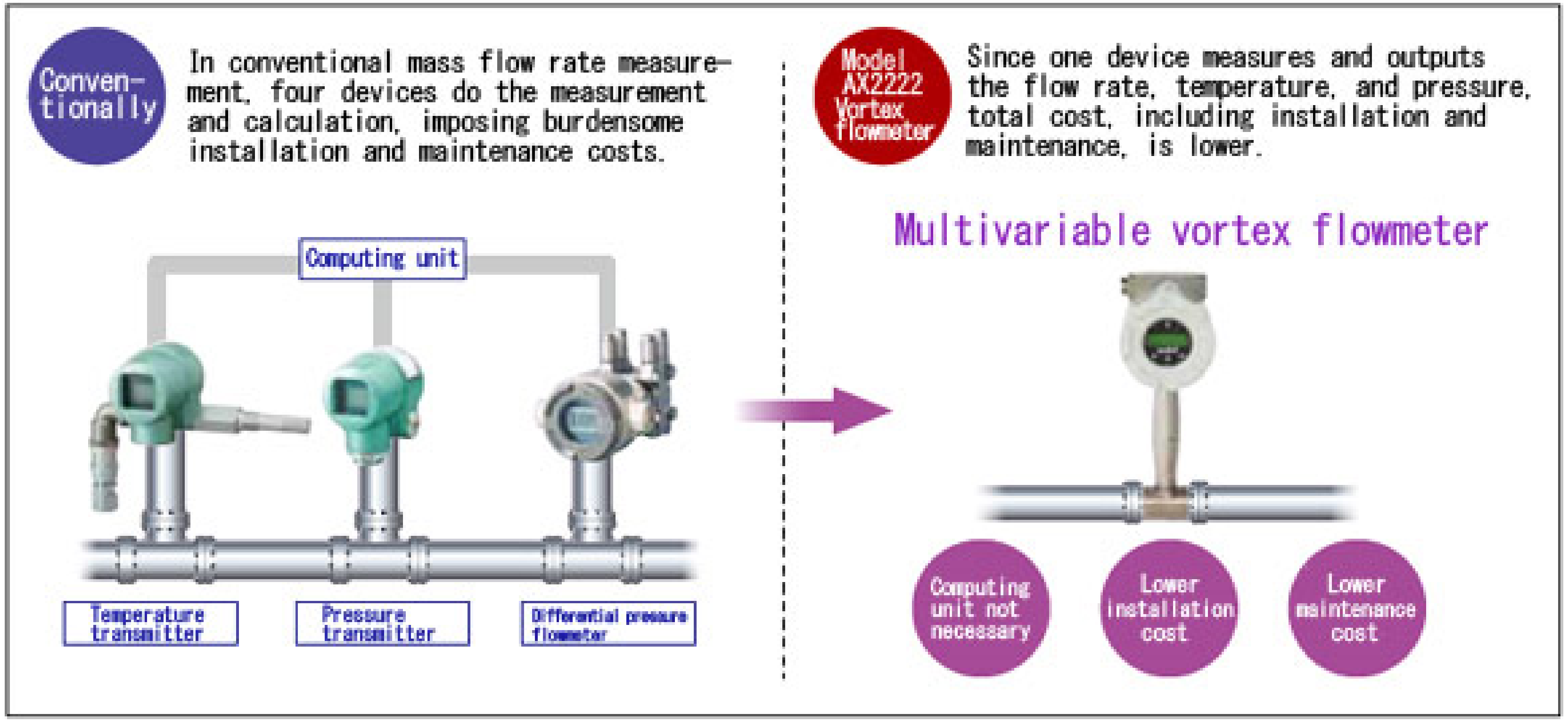
HART COMMUNICATION PROTOCOL

FOUNDATION

Modbus

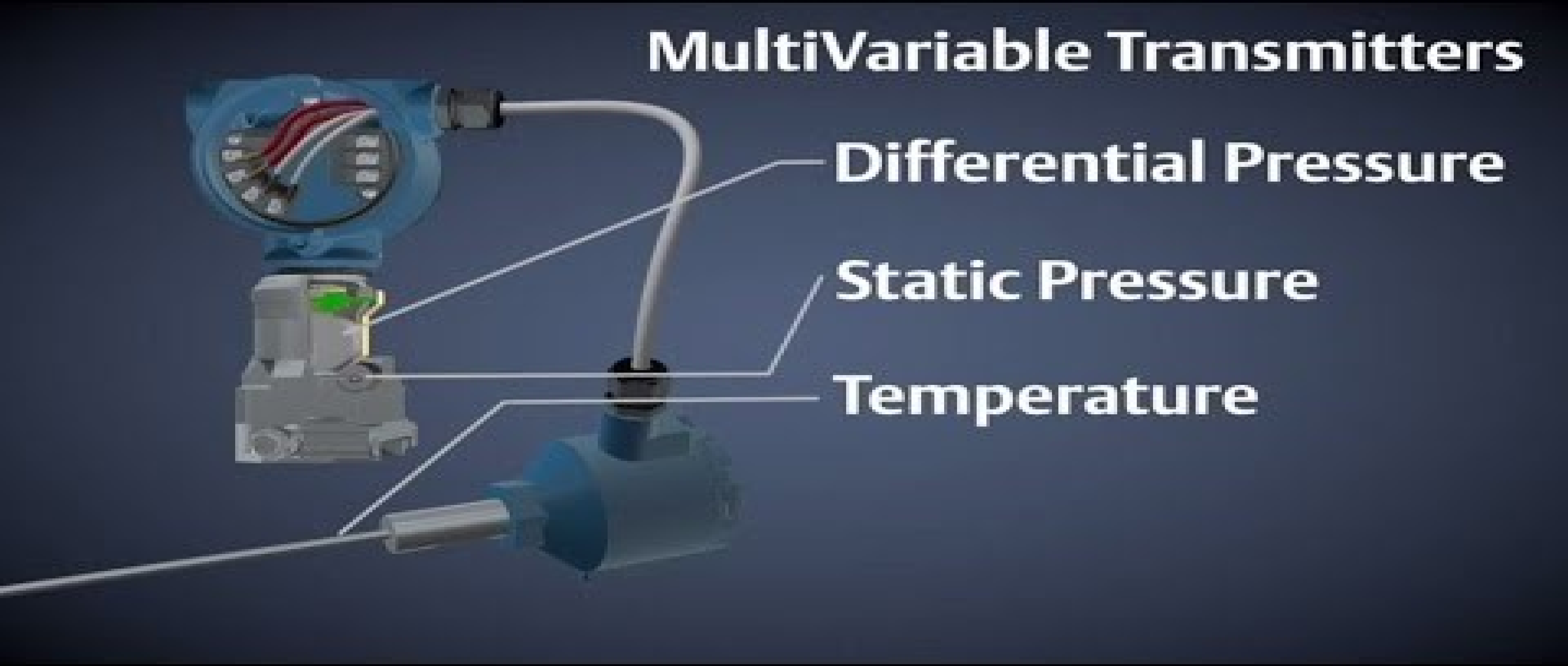
https://www.emerson.com/en-sg/automation/measurement-instrumentation/pressure-measurement/about-multivariable-measurement

## Not just 1 Process Variable data




https://www.azbil.com/products/factory/factory-product/flowmeter/vortex-flowmeter/ax2000/index.html

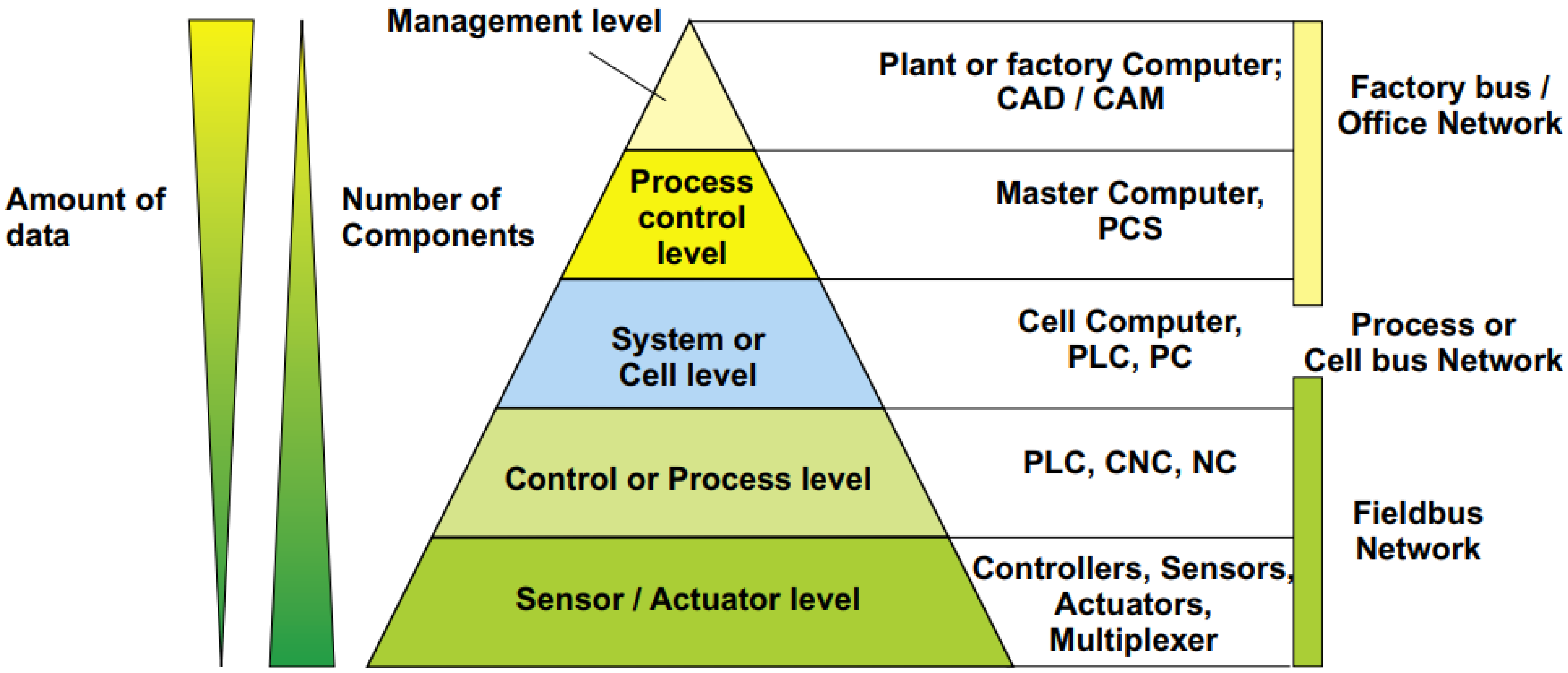
- Instead of installing 3 instruments with 3 x 4-20mA signals
- 1 instrument with fieldbus that returns flowrate, temperature and pressure
- And Diagnostics information for maintenance or alarm of the instrument




https://youtu.be/cCpojIE3oLQ

# Automation Pyramid

Source: Industrial Ethernet, Ronald Dietrich

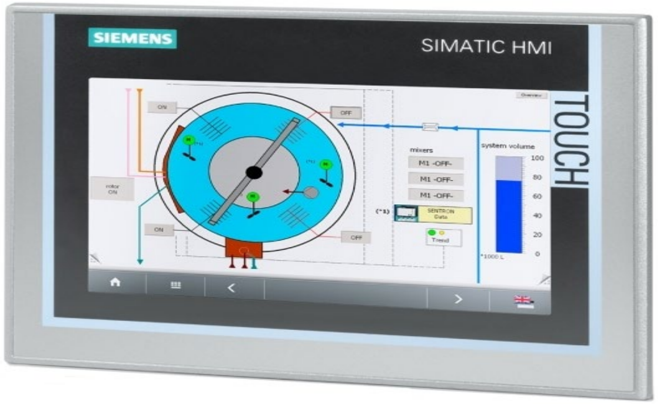



- There is resemblance to Purdue Model, but this is the automation pyramid
- Illustrates that bottom layer of automation where the field devices such as sensors and actuators are mainly communicating fieldbus to controllers such as PLC
- As the level goes higher, there would be more data transfer, Ethernet was adopted

# Human Machine Interface (HMI)

HMI is the interface between human (operator) and the process (machine/plant)

- Visualize the running process
- Controller has the actual control over the process
- Enable inspection and manipulation of process values (enter setpoint or start/stop motor)
- Displays alarms and process values trends (data log)
- Supports a variety of communication interfaces

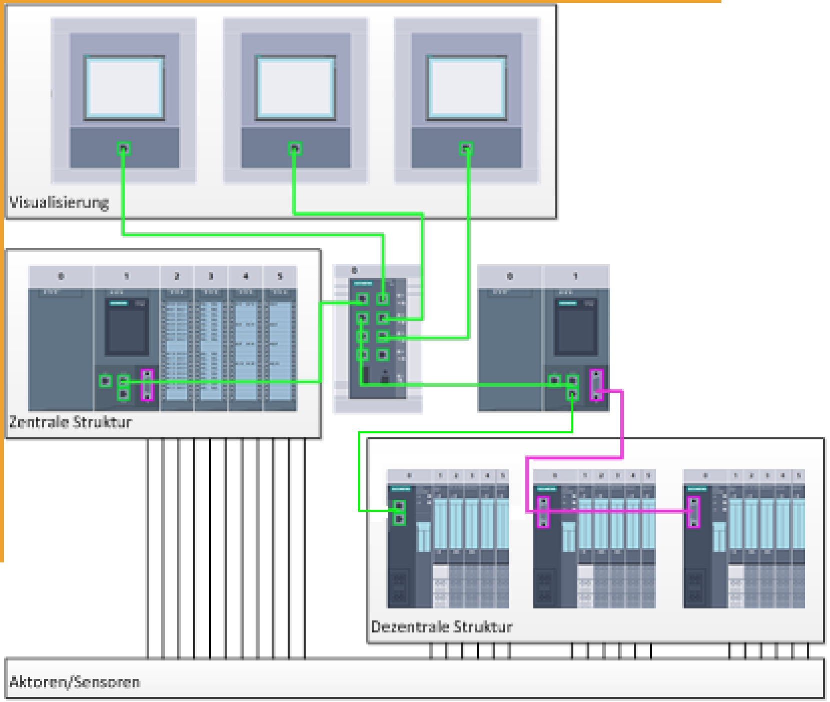


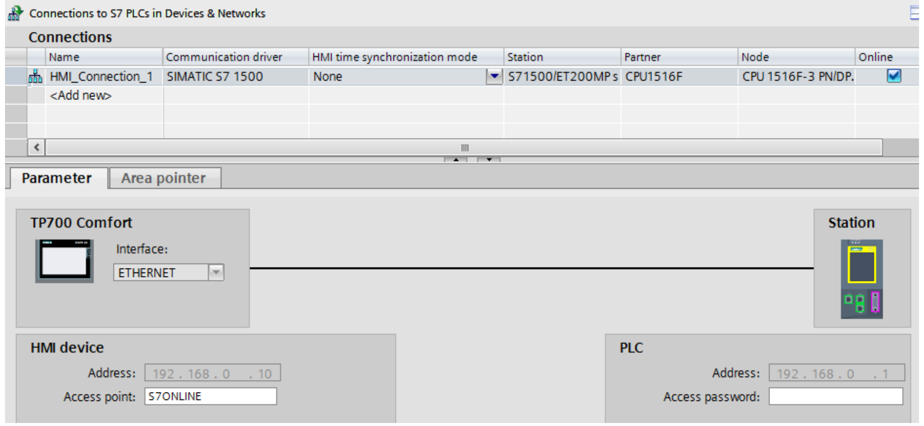

Credits to Siemens SCE

# Human Machine Interface (HMI)

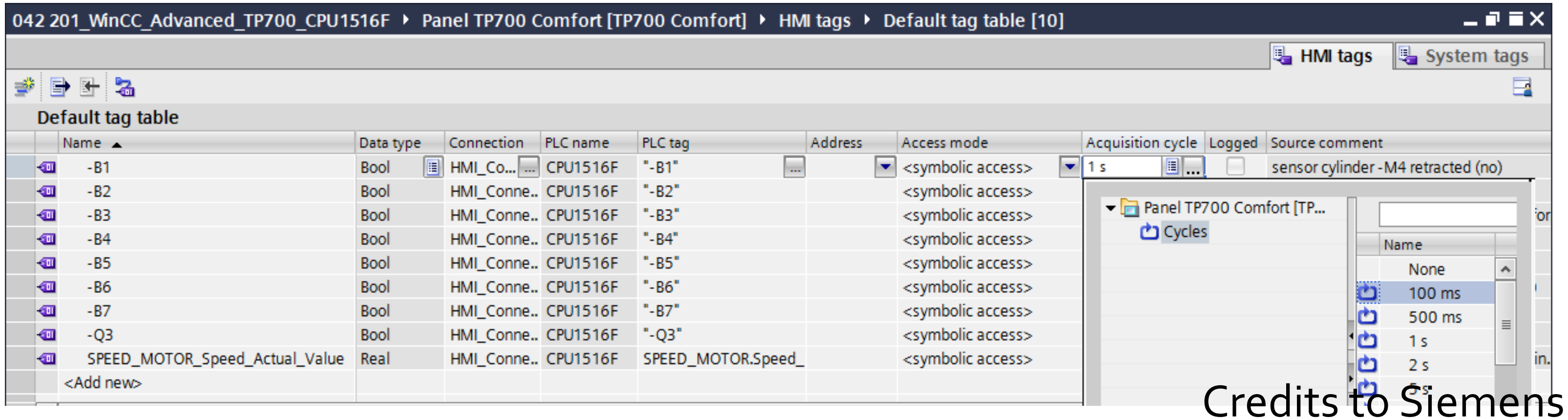
A control system could accommodate multiple HMIs

- Information exchange would be between controller and HMI
- HMI connection has to be clearly established and credentials (password) provided if required
- HMI tags need to be clearly specified based on connection(s)



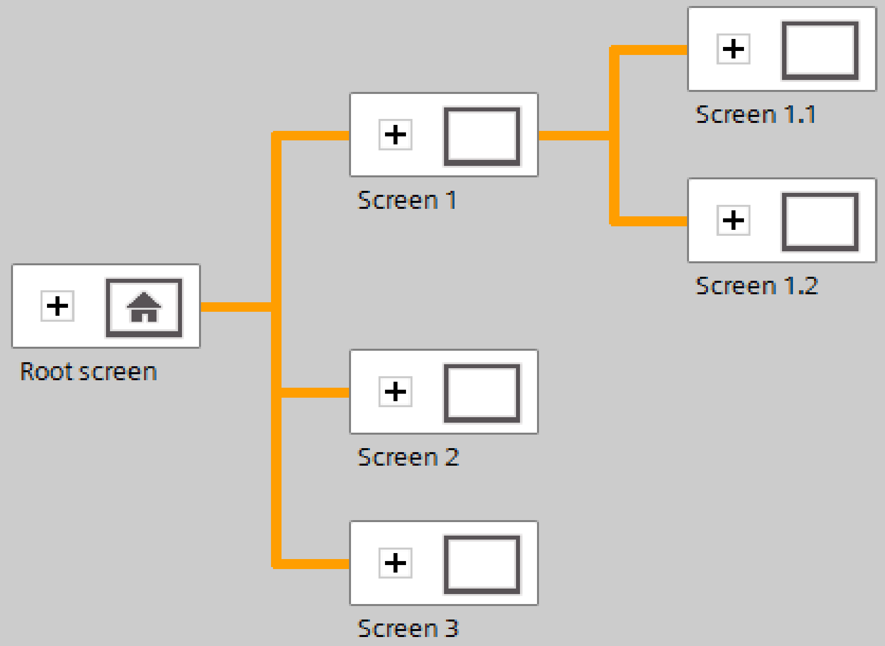

| Name | Communication driver | HMI time synchronization mode | Station | Partner | Node | Online |
|---|---|---|---|---|---|---|
| HMI_Connection_1 | SIMATIC S7 1500 | None | S71500/ET200MP s | CPU1516F | CPU 1516F-3 PN/DP. | ☑ |
| <Add new> | | | | | | |




| Name | Data type | Connection | PLC name | PLC tag | Address | Access mode | Acquisition cycle | Logged | Source comment |
|---|---|---|---|---|---|---|---|---|---|
| -B1 | Bool | HMI_Co... | CPU1516F | "-B1" | | <symbolic access> | 1 s | | sensor cylinder -M4 retracted (no) |
| -B2 | Bool | HMI_Conne.. | CPU1516F | "-B2" | | <symbolic access> | | | |
| -B3 | Bool | HMI_Conne.. | CPU1516F | "-B3" | | <symbolic access> | | | |
| -B4 | Bool | HMI_Conne.. | CPU1516F | "-B4" | | <symbolic access> | | | |
| -B5 | Bool | HMI_Conne.. | CPU1516F | "-B5" | | <symbolic access> | | | |
| -B6 | Bool | HMI_Conne.. | CPU1516F | "-B6" | | <symbolic access> | | | |
| -B7 | Bool | HMI_Conne.. | CPU1516F | "-B7" | | <symbolic access> | | | |
| -Q3 | Bool | HMI_Conne.. | CPU1516F | "-Q3" | | <symbolic access> | | | |
| SPEED_MOTOR_Speed_Actual_Value | Real | HMI_Conne.. | CPU1516F | SPEED_MOTOR.Speed_ | | <symbolic access> | | | |
| <Add new> | | | | | | | | | |

Credits to Siemens SCE

# HMI Screen Structure




## Planning of screen structure

- Collect, Group & Structure the information to display
- Optimal navigation by user for operation and monitoring of process

The following questions can aid you in this:

- *Which mental model of the process should be observed for the information display?*
- *Which data belong together?*
- *Which data belong in which order?*
- *Which data belong to which actions/processes?*
- *Is there cross-action data and the like?*
- *Which data are key data, which are supplementary data?*

Credits to Siemens SCE

# HMI Screen Structure

## Planning of screen structure

- Every screen need to be planned
- For the information display, its use by people must also be considered
- It is helpful to observe design principles such as:
  - Law of Proximity
  - Law of Similarity
  - Law of Symmetry

# HMI Screen Structure

The following rules of thumb derived from the design principles can aid in structuring screens:

- Form groups of data blocks
- Uniform division of the overall screen into work information, status or system information and controller information
- Observe the average distribution of attention on the screen as a function of reading direction.

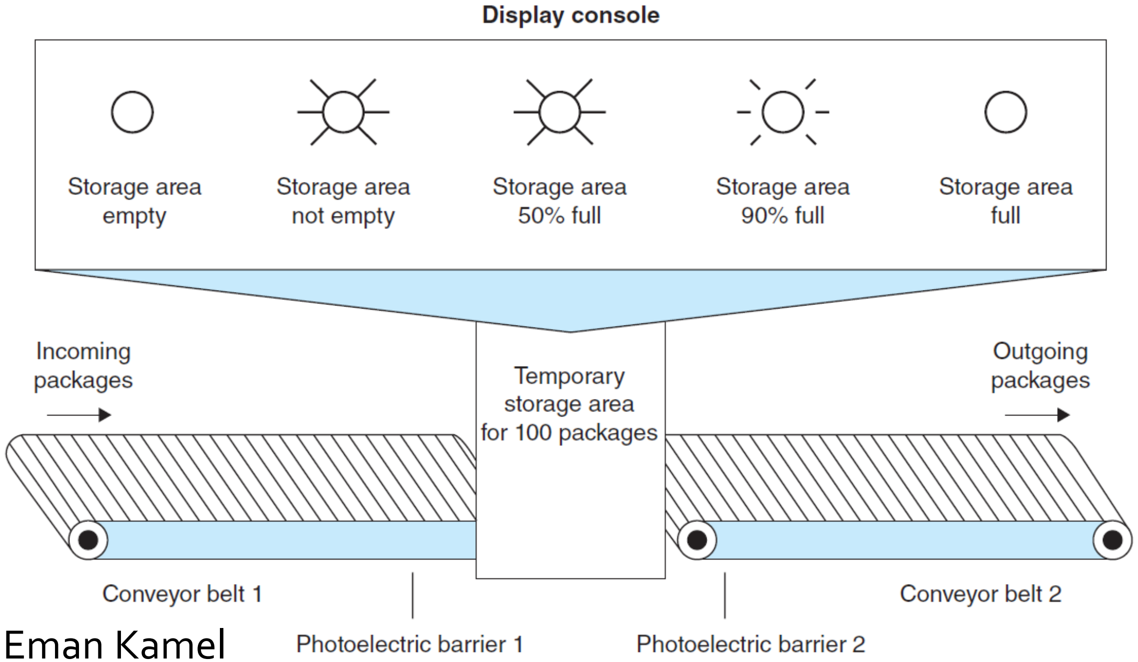
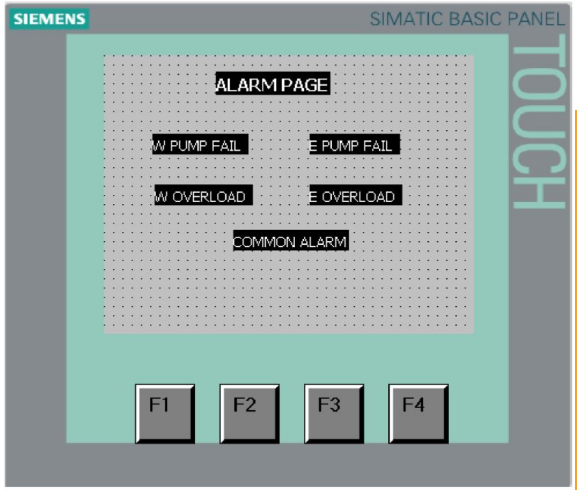
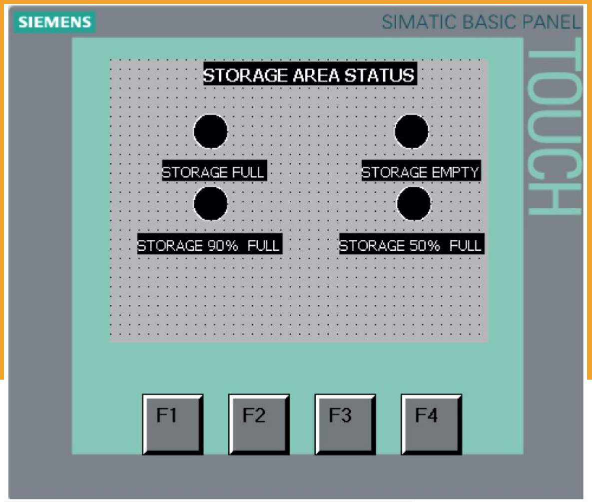



Image Source: PLC Industrial Control, Khaled Kamel & Eman Kamel




# HMI Screen Structure




The following rules of thumb derived from the design principles can aid in structuring screens:

- Use alignment as a design principle (align numbers, column headings same as column content)
- Make effective use of a maximum of 30 – 40% of the available space: place as little information as possible and as much as necessary
- Use coding sparingly (for example, color, bold text, brightness, shape, outline, pattern, flashing)
- Subdivide numbers: Subdivide numbers with more than 4 digits in groups of 2, 3 or 4 (for example, 66 234)
- Select numbers preferentially when listing objects, properties, etc.
- Use and position designations uniformly, use short words if possible

Image Source: PLC Industrial Control, Khaled Kamel & Eman Kamel