Industrial Systems Security

CPS and IoT Security

Alessandro Brighente

Master Degree in Cybersecurity

Università degli Studi di Padova

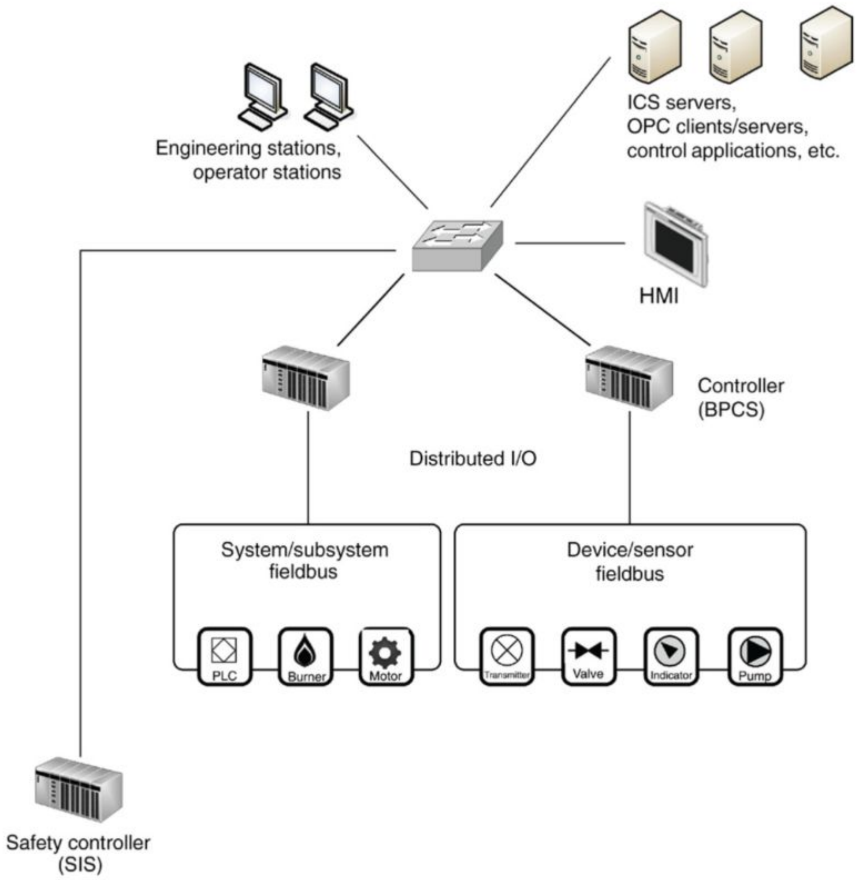
SPRITZ
Security & Privacy
Research Group

Industrial Control Systems

- An industrial control system (ICS) is a broad class of automation systems used to provide control and monitoring functionality in manufacturing and industrial facilities
- It is an aggregate of various system types:
  - Process Control Systems (PCS)
  - Distributed Control System (DCS)
  - Supervisory Control and Data Acquisition (SCADA)
  - Safety Instrumented Systems (SIS)

Industrial Control Systems

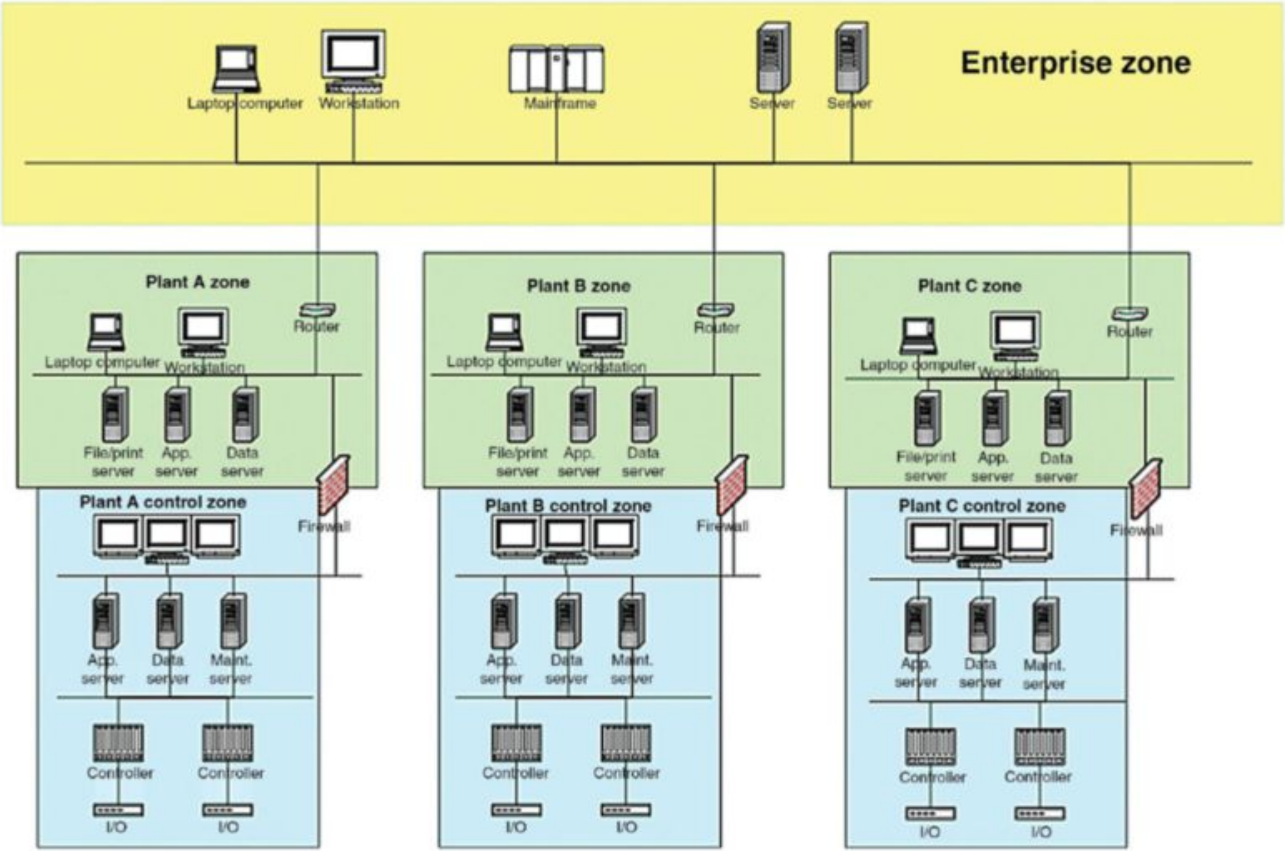
- Simplified representation with two controllers and a series of inputs and outputs
- The Human-Machine Interface (HMI) provides the operator with info on the process
- As the task are executed, results are stored in the historian


Engineering stations,
operator stations
ICS servers,
OPC clients/servers,
control applications, etc.
HMI
Controller
(BPCS)
Distributed I/O
System/subsystem
fieldbus
PLC
Burner
Motor
Device/sensor
fieldbus
Transmitter
Valve
Indicator
Pump
Safety controller
(SIS)

Zones and Enclaves

- These terms refer to closed groups of assets, or a function group of devices, services, and applications that make up a larger system
- A zone describes a special network that is created to expose a subset of resources to a larger, untrusted network
- This is often referred to as demilitarized zone
- Used when enterprises want to place external-facing services, like web servers, email servers, B2B portals on the Internet while still securing their more trusted business networks

Zones and Enclaves


Enterprise zone
Laptop computer
Workstation
Mainframe
Server
Server
Plant A zone
Plant B zone
Plant C zone
Router
Laptop computer
Workstation
File/print server
App. server
Data server
Firewall
Plant A control zone
Plant B control zone
Plant C control zone
App. server
Data server
Maint. server
Controller
I/O

Common Recommendations

- Identifying what systems need to be protected
- Separating the systems logically into functional groups
- Implementing a defense-in-depth strategy around each system or group
- Controlling access into and between each group
- Monitoring activities that occur within and between groups
- Limiting the actions that can be executed within and between groups

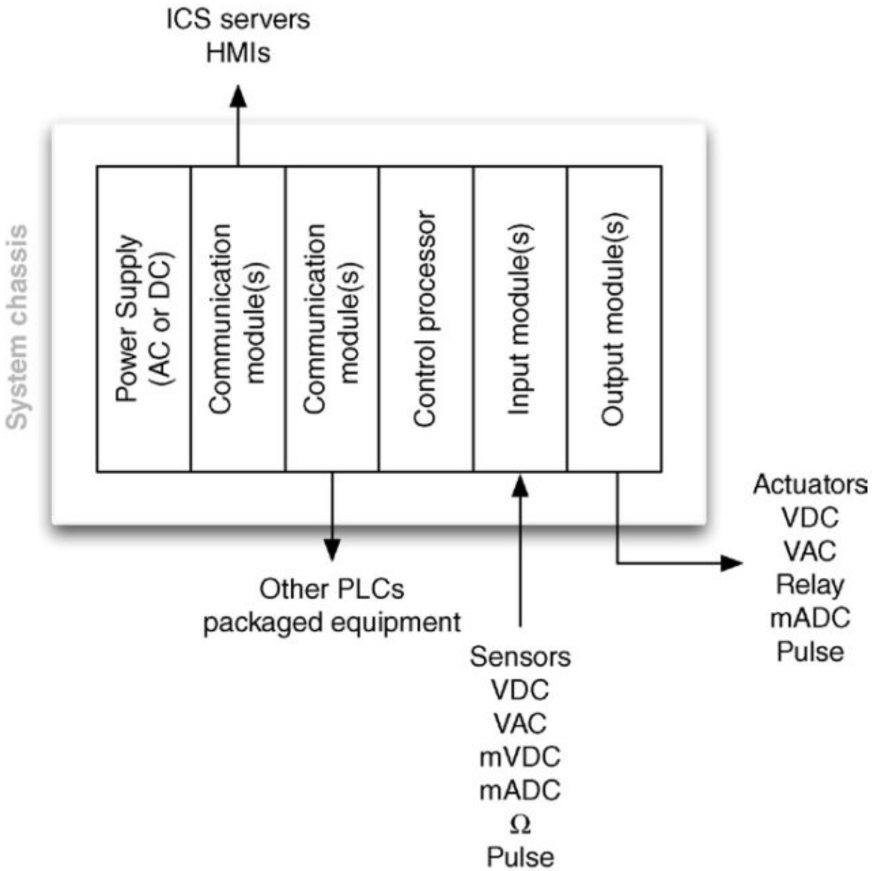
Industrial Network Assets

- Let’s see the components used in industrial networks and the role they play
- Two main groups:
    - **Field components**, such as sensors, actuators, motor drives, gauges
    - **Control system components**, such as programmable logic controllers, remote terminal units, intelligent electronic devices

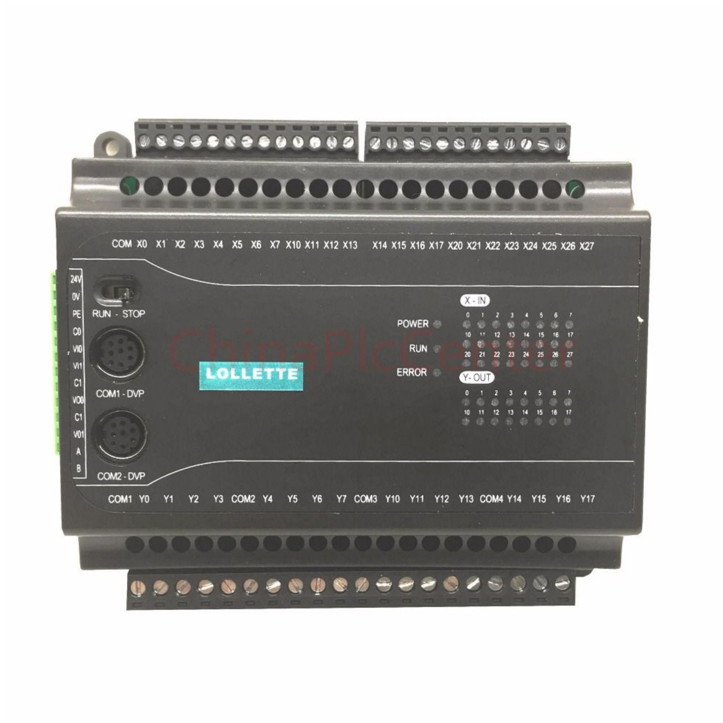
Programmable Logic Controller

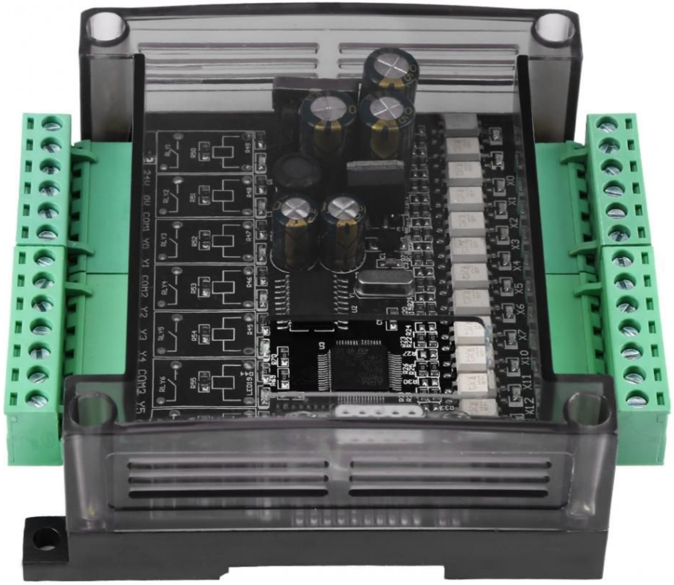
- A Programmable Logic Controller (PLC) is a specialized industrial computer used to automate functions within manufacturing facilities
- They are typically hardened, making them suitable for deployment in production environments
- May be specialized for specific industrial uses with multiple specialized inputs and outputs
- They do not use common operating systems, but rely on specific application programs that allow the PLC to function automatically generating output actions in response to specific inputs

Programmable Logic Controller


ICS servers
HMIs
System chassis
Power Supply (AC or DC)
Communication module(s)
Communication module(s)
Control processor
Input module(s)
Output module(s)
Other PLCs
packaged equipment
Sensors
VDC
VAC
mVDC
mADC
Ω
Pulse
Actuators
VDC
VAC
Relay
mADC
Pulse

Programmable Logic Controller


COM X0 X1 X2 X3 X4 X5 X6 X7 X10 X11 X12 X13 X14 X15 X16 X17 X20 X21 X22 X23 X24 X25 X26 X27
24V
0V
PE
RUN - STOP
COM1 - DVP
COM2 - DVP
LOLLETTE
POWER
RUN
ERROR
X - IN
Y - OUT
COM1 Y0 Y1 Y2 Y3 COM2 Y4 Y5 Y6 Y7 COM3 Y10 Y11 Y12 Y13 COM4 Y14 Y15 Y16 Y17



Programmable Logic Controller

- They usually control real time processes, so they are designed for simple efficiency
- Processing overhead and delay in the execution of the PLC functioning may impair a whole production process
- The logic of PLCs is implemented via a standardized set of languages given by IEC-61131-3
- Among them, we find Ladder Logics/Ladder Diagrams

Ladder Logic

- Gets its name from the legacy methods of implementing discrete logic via electromechanical relays
- Can be thought of as a set of connections between inputs (relay contacts) and outputs (relay coils)
- It defines a path consisting of logic steps that need to be fulfilled to allow for reaching the end
- If one of the conditions is false, then the overall path is false and hence the output remains “de-energized”

Ladder Logic

- The PLC applies this ladder logic by looking at inputs from discrete devices that are connected to the manufacturing equipment
- It uses a thresholder to decide whether the input is true or false
- Performs a desired output functions based on the state of these inputs
- The outputs are connected to manufacturing equipment, such as actuators and motor drives

Remote Terminal Units

- A Remote Terminal Unit (RTU) monitors the field parameters and send this data back to a central monitoring station (e.g., an ICS server, a centrally located PLC, or HMI)
- RTUs typically reside in substations along a pipeline or some other remote location where there may not have easy access to electricity
- They usually include communication capabilities, e.g., via modem, cellular data connections, radio or other wide area communication technology

Remote Terminal Units

- Their communication bandwidth is generally limited
- In order to maximize the information transmitted they use protocols supporting *report by exception* or other *publish-subscribe* mechanism

ADVANTECH
ADAM-3600
ADAM-3656
ADAM-3656
ADAM-3656
ADAM-3656

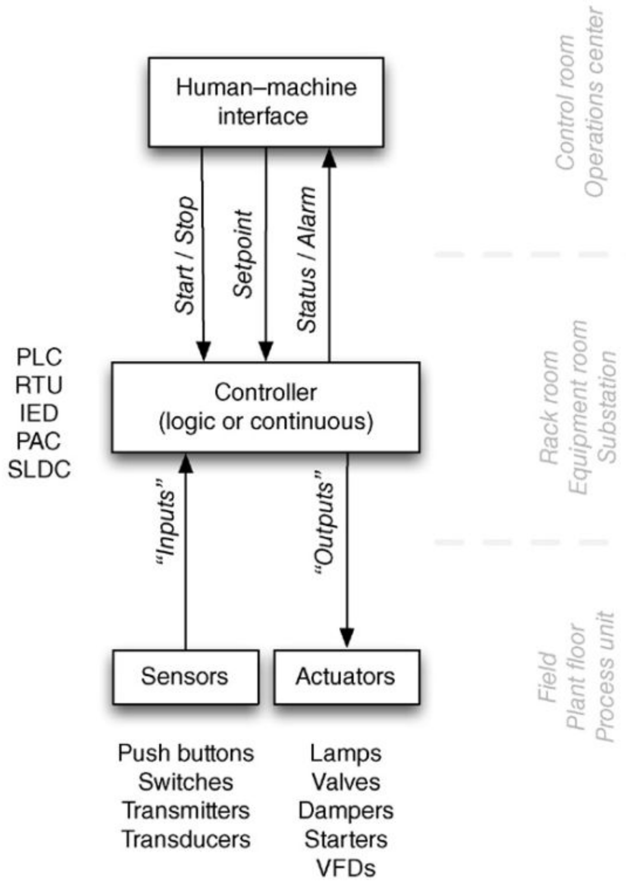
SIEMENS
SICAM A8000 CP-8000
I/O MODULE 1
DI-8100
IN D00
IN D01
IN D02
IN D03
IN D04
IN D05
IN D06
IN D07
IN D10
IN D11
IN D12
IN D13
ESC
F1
F2
F3
F4
SIEMENS

Human-Machine Interface

- They provide the means for operators to interact with PLCs, RTUs, and IEDs
- They replace manually activated switches, dials, and other electrical controls with graphical representations of the digital controls used to sense and influence the process
- They allow the operator to start and stop cycles, adjust set points and perform other functions to adjust and interact with the control process

Human-Machine Interface

- The HMI is at the top level near the human operator
- The figure shows how it is integrated in the overall (up to now) system
- The human interact with the HMI via a console, which however does not require authentication
- They are hence deployed in physically strong security areas

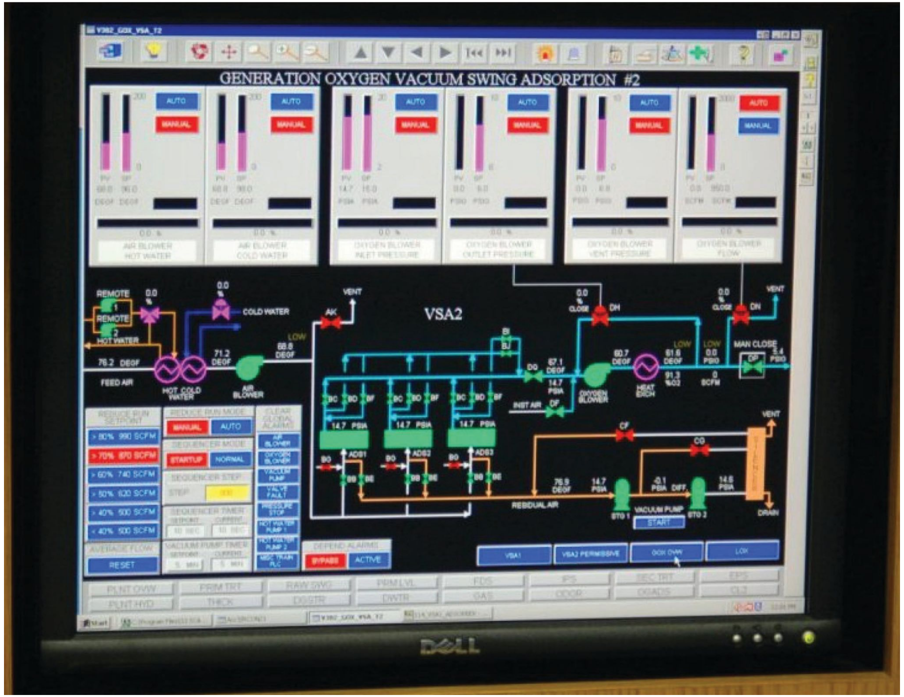

Human–machine interface
Start / Stop
Setpoint
Status / Alarm
PLC
RTU
IED
PAC
SLDC
Controller (logic or continuous)
"Inputs"
"Outputs"
Sensors
Actuators
Push buttons
Switches
Transmitters
Transducers
Lamps
Valves
Dampers
Starters
VFDs
Control room
Operations center
Rack room
Equipment room
Substation
Field
Plant floor
Process unit

Human-Machine Interface

- The HMI uses software that may come in two forms
- The first runs on operating systems such as Windows 11 and are capable of performing a variety of functions
- The other form combines an industrial hardened computer, local touch panel, and typically utilize embedded operating systems
- In this case, they are usually programmed with a separate computed and associated engineering software

Human-Machine Interface

- The HMI shows the process instead of the logic behind it
- Since they provide supervisory data as well as control, user access control should be part of the ICS
- The HMI interacts with an ICS and hence with one or more controllers


GENERATION OXYGEN VACUUM SWING ADSORPTION #2
VSA2
AUTO
MANUAL
COLD WATER
FEED AIR
HOT COLD WATER
AIR BLOWER
OXYGEN BLOWER
HEAT EXCH
VACUUM PUMP
START
RESET
DELL

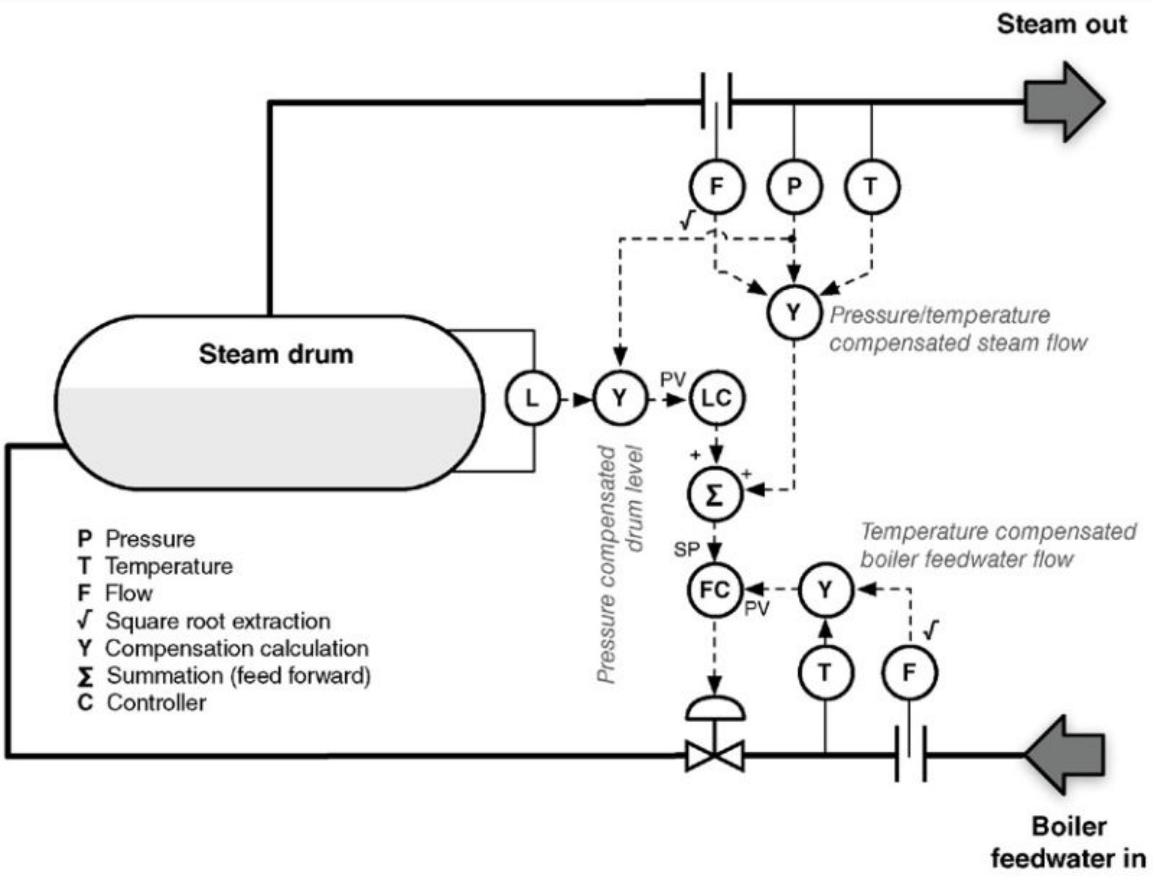
Data Historian

- It is a specialized software system that collects point values, alarm events, batch records, and other information from industrial devices and systems and stores them in a purpose-built database
- Data that are historized and stored is referred to as *tags*, and car represent almost anything
- Information used by both industrial operations and business management is often replicated across industrial and business networks and stored in data historians → security risk due to zones

Control Processes

- Control process is a general terms used to define large automated process within an industrial operation
- To manufacture a product or generate electricity, it might be necessary to use many control processes, each comprising one or more control loops
- Examples: one process might be to inject an ingredient into a mixer utilizing a control loop that opens a valve in response to volume measurements within the mixer, temperature, and other conditions

Control Processes


Steam out
F
P
T
√
Y
Pressure/temperature compensated steam flow
Steam drum
L
Y
PV
LC
+
+
Σ
Pressure compensated drum level
SP
FC
PV
Y
Temperature compensated boiler feedwater flow
√
T
F
Boiler feedwater in
P Pressure
T Temperature
F Flow
√ Square root extraction
Y Compensation calculation
Σ Summation (feed forward)
C Controller

Safety Instrumented Systems

- A risk management strategy should include different layers of protection to prevent a manufacturing environment to reach an unsafe operating condition
- Safety Instrumented Systems (SIS) are deployed as part of a comprehensive risk management strategy
- The basic process control systems is responsible for discrete and continuous control necessary for normal operations
- In the event of an abnormal situation, the SIS takes over the control

Risks of SISs

- There are risks originating within the SIS relating to cyber incidents
- The prevention of the SIS from properly performing its control functions can allow the plant to transition into a dangerous state
- Since the SIS operationally overrides the BPCS and its ability to control the plant, the SIS can also be used maliciously to cause unintentional equipment or plant shutdowns
- To prevent this situations, we need to isolate the SIS to the greatest possible extent from other basic control assets

SIS Isolation

- SIS programming is not usually allowed in operational mode
- Highly authorized applications like SIS programming tools and SIS engineering workstations can be removed from ICS networks until they are required
- SIS systems must be periodically tested to guarantee their functionality
- This also includes cyber security assessments

Industrial Networking

- An industrial network is any network that supports the interconnectivity of and communication between devices that make up or support an ICS
- They may be local-area switched networks as common with Distributed Control Systems
- They may be wide-area routed networks more typical of SCADA architectures
- Most are Ethernet and IP-based and consist of both wired and wireless connectivity

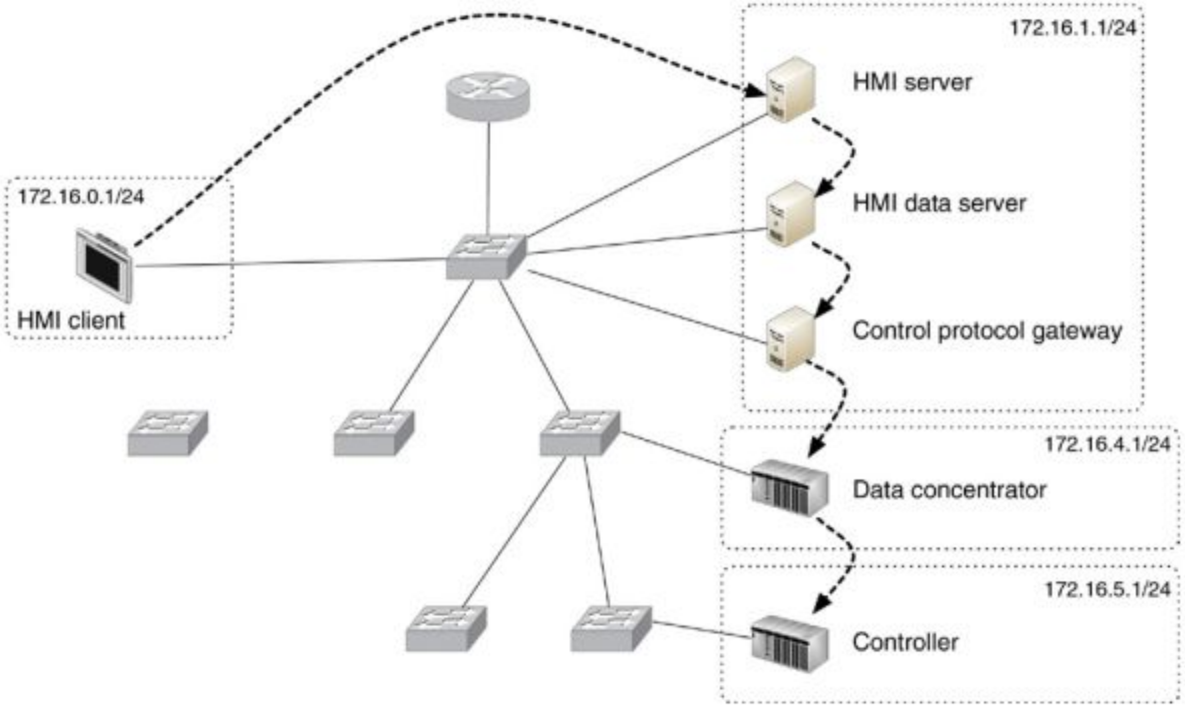
Industrial Networking

- Availability is prioritized over data integrity and confidentiality
- Therefore, there is a great use of real-time protocols, UDP transport, and fault-tolerant networks interconnecting endpoints and servers
- Bandwidth and latency are extremely important, because the applications and protocols in use support real-time operations that depend on deterministic communication often with precise timing requirements
- Ubiquitous connectivity might not be something we want to achieve

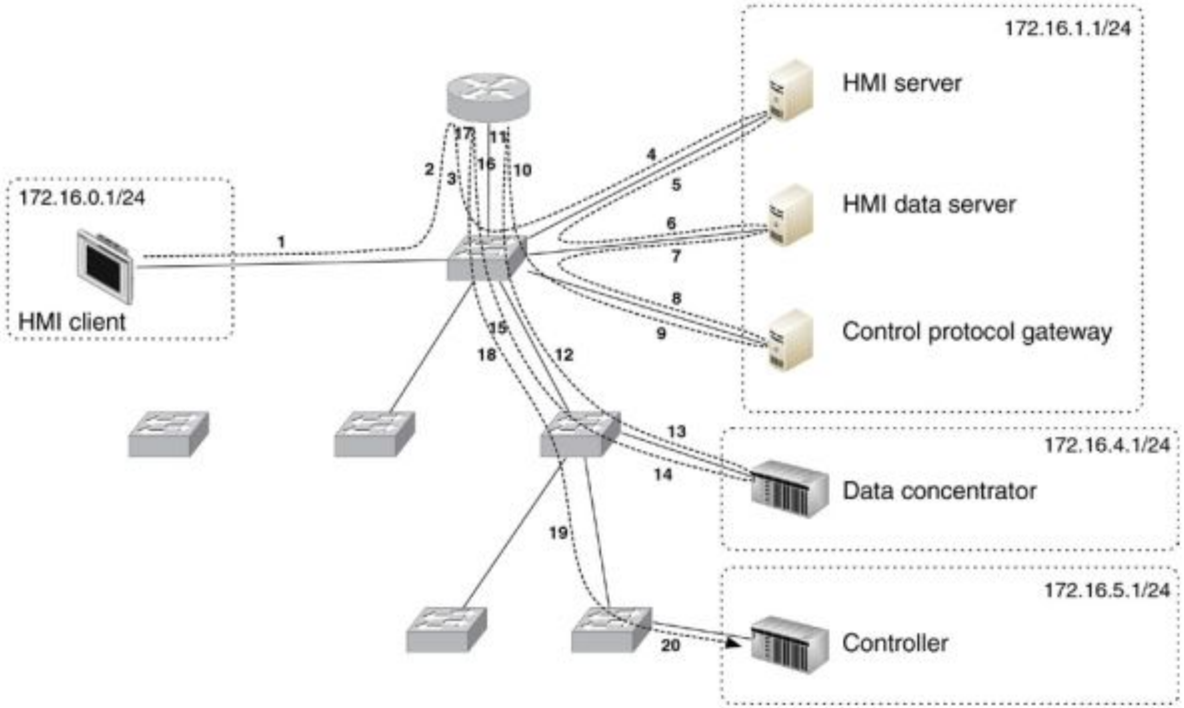
Industrial Networking

- The ICS requirements dictate the topology of the networks
- High reliability and resiliency dictates the use of ring or mesh network topologies
- Real-time operations and low latency require the minimization of switching and routing hops

Industrial Networking


172.16.1.1/24
HMI server
HMI data server
Control protocol gateway
172.16.0.1/24
HMI client
172.16.4.1/24
Data concentrator
172.16.5.1/24
Controller

Industrial Networking

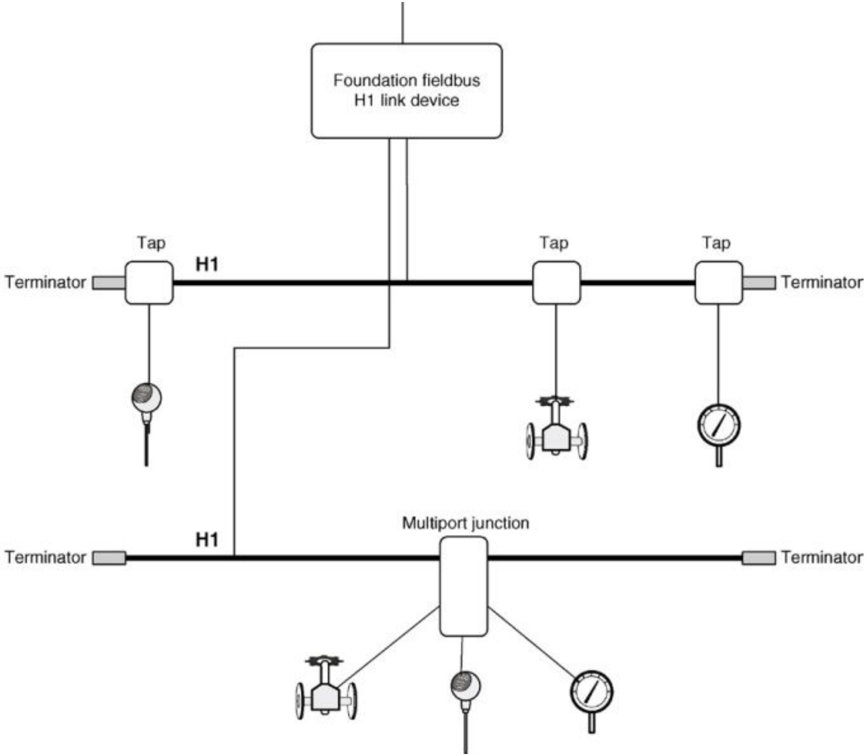

172.16.1.1/24
HMI server
HMI data server
Control protocol gateway
172.16.0.1/24
HMI client
172.16.4.1/24
Data concentrator
172.16.5.1/24
Controller
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Industrial Networking

- Five sessions require 20 paths to be traversed
- It is therefore necessary to minimize latency wherever possible to maintain real-time and deterministic communications
- Therefore, we need to use switching unless traversing a functional boundary
- We also need to use low level (Ethernet) firewalls and prefer a bridged mode, i.e., avoid relying on IP routing

Industrial Networking

- As we go lower into the control environment, functionality becomes more specialized
- Introduction of open and/or proprietary protocols in either their native form or adapted to work over Ethernet
- Figure: Fieldbus


Foundation fieldbus
H1 link device
Tap
H1
Tap
Tap
Terminator
Terminator
H1
Multiport junction
Terminator
Terminator

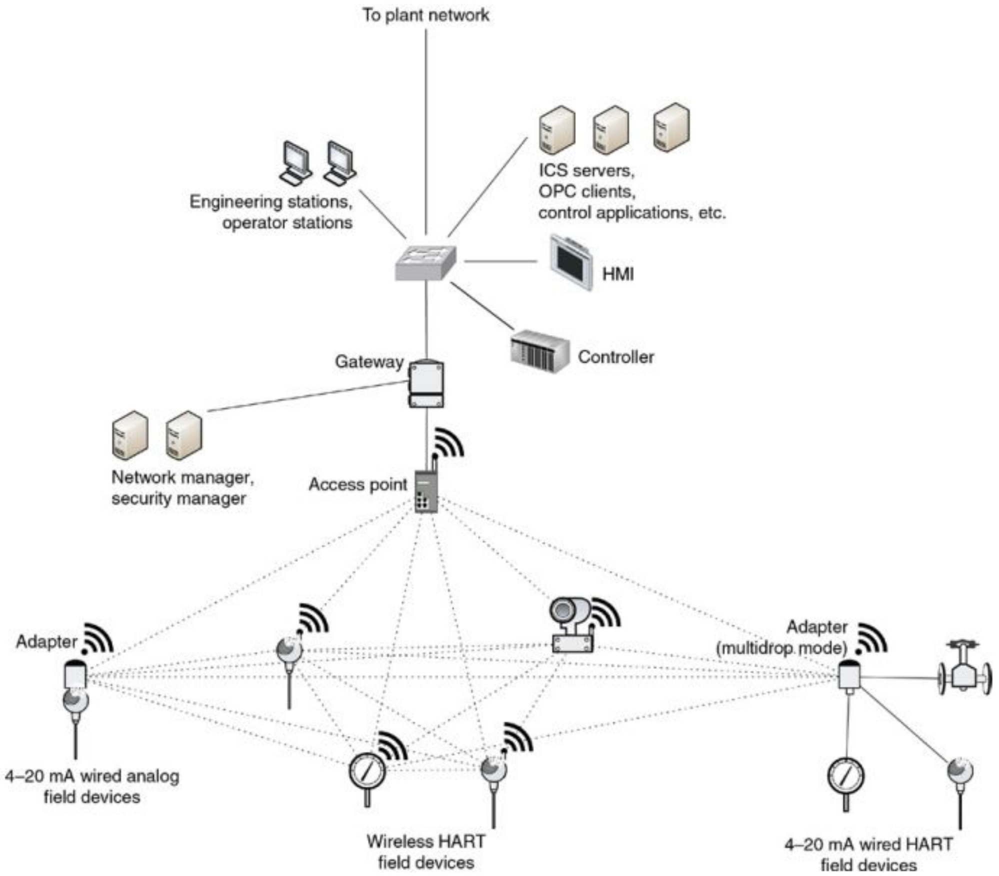
Wireless Networks

- Wireless networks are bound by the same design principles as wired networks
- However, they are more difficult to physically contain because they are bound by the range of the radio wave propagation from an access point rather than by physical cables and network interfaces
- Any device that is equipped with an appropriate receiver and is within the range of a wireless access point can physically receive wireless signals

Wireless Networks

- There is no sure way to prevent this physical (wireless) access
- While it is possible to block transmissions by using jammers or signal-absorbing materials, these measures are costly and rarely implemented
- Typically conduct thorough radio frequency surveys in order to not only place antennas in optimal locations, but also prevent unnecessary transmission of signals into untrusted and unrestricted areas

Wireless Networks


To plant network
Engineering stations,
operator stations
ICS servers,
OPC clients,
control applications, etc.
HMI
Controller
Gateway
Network manager,
security manager
Access point
Adapter
Adapter
(multidrop mode)
4–20 mA wired analog
field devices
Wireless HART
field devices
4–20 mA wired HART
field devices

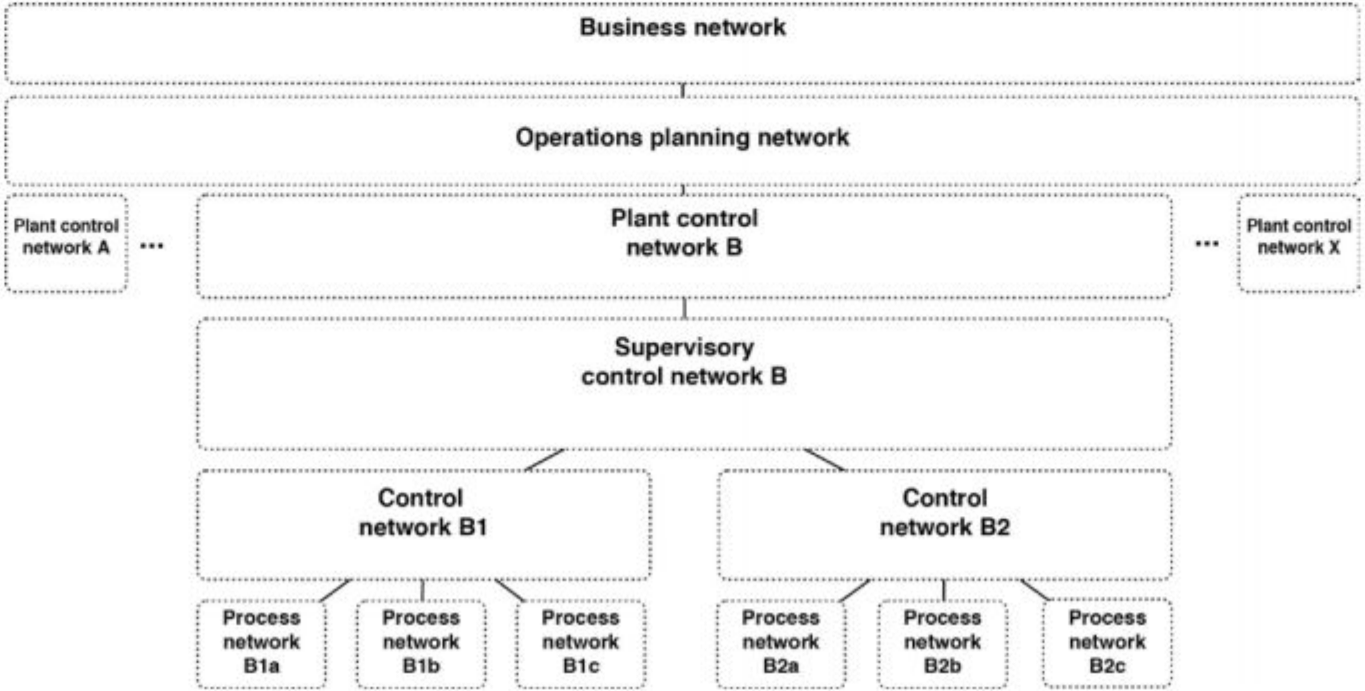
Network Segmentation

- “Segmentation” pertains to the division of networks (network segmentation) or zones (zone segmentation) into smaller units.
- Important for many reasons, including network performance considerations and cyber security
- Segmentation typically occurs at Layer 3 (the network layer) by a network device providing routing functions
- The router blocks broadcasts, enabling a large flat Ethernet network to be broken up into discrete Ethernet segments

Network Segmentation

- Segmentation provides an inherent degree of access control at each demarcation point
- Should be used to support zone segmentation whenever possible
- Results in hierarchical networks, such that communication between two networks might require traversal of several networks
- Just because a segmented network architecture supports communication flows between segments, it does not mean that this traffic should be allowed between segments

Network Segmentation


Business network
Operations planning network
Plant control network A
...
Plant control network B
...
Plant control network X
Supervisory control network B
Control network B1
Control network B2
Process network B1a
Process network B1b
Process network B1c
Process network B2a
Process network B2b
Process network B2c

Phy. vs Logical Segmentation

- Physical segmentation refers to the use of two separate physical network devices (both passive and active components) to perform the isolation between networks
- Logical segmentation refers to the use of logical functions within a single network device to achieve essentially the same result
- Physical separation of systems (“air gap” separation) is still widely used in industrial networks when talking about the coexistence of basic process control and safety systems overseeing the same process

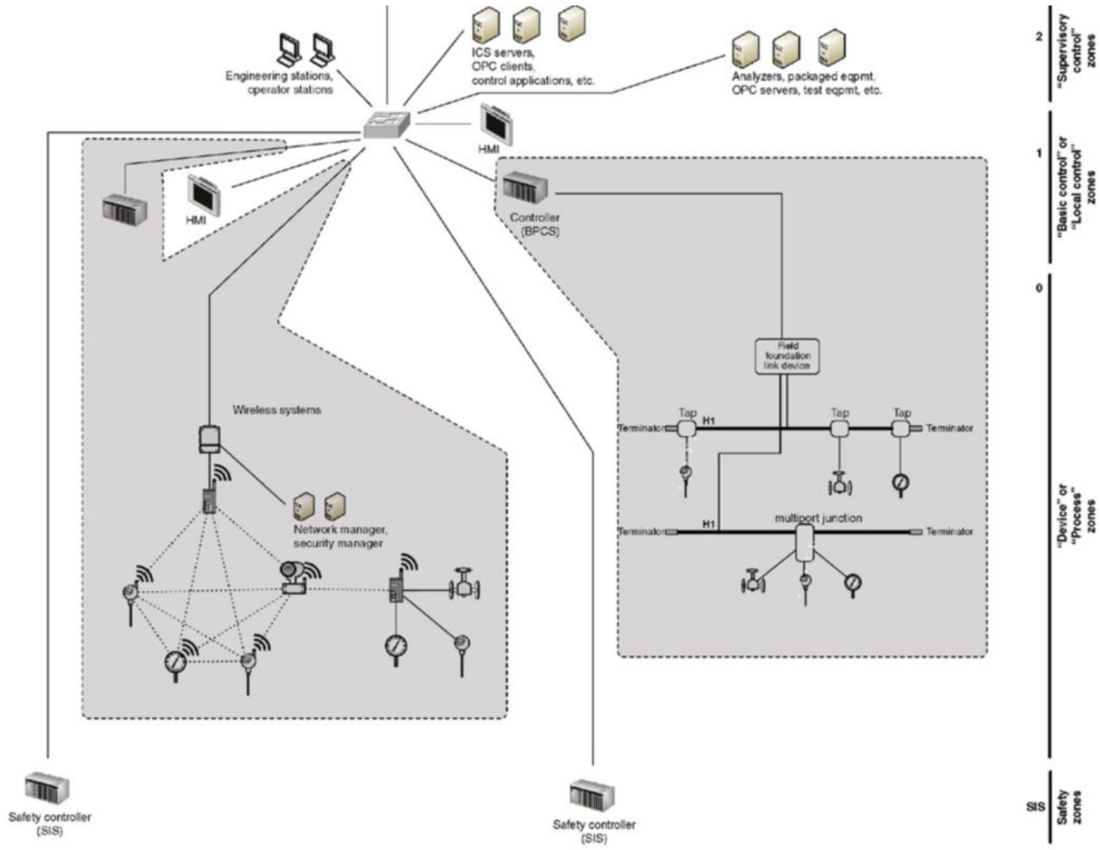
Creating Zones from Segments

- Each industrial architecture is unique, not because of the selection of equipment, but how each system is deployed in a particular environment and how each system is integrated with other ancillary systems
- A safety level applied to each system so that appropriate measures can be in place to ensure that each system performs as intended without unintentional consequences or interactions between systems
- Assets at a particular site are grouped based on their relative security requirements or security level

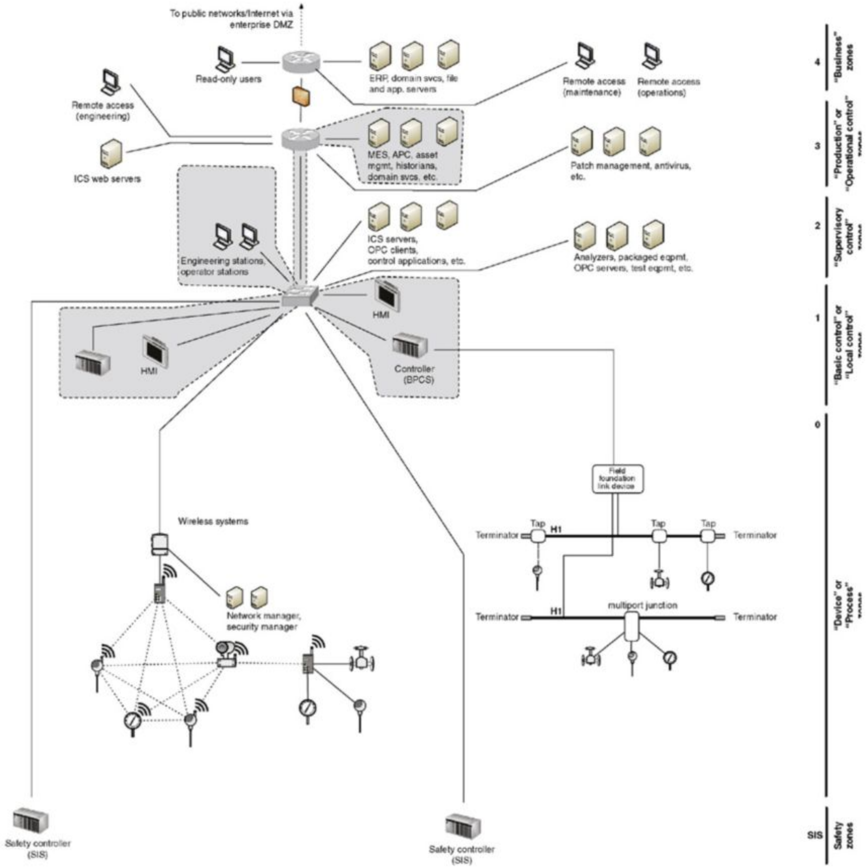
Identifying Zones

- One of the biggest challenge is the creation of a set of base requirements to determine whether a certain asset should be in a certain zone
- These goals can be broken down into categories
    - Based on communications and interactions
    - Physical access to assets
- Zones based on network connectivity are rather easy to understand

Based on Control Loops


Engineering stations, operator stations
ICS servers, OPC clients, control applications, etc.
Analyzers, packaged eqpmt, OPC servers, test eqpmt, etc.
HMI
HMI
Controller (BPCS)
Field foundation link device
Tap
H1
Tap
Tap
Terminator
Terminator
multiport junction
H1
Terminator
Terminator
Wireless systems
Network manager, security manager
Safety controller (SIS)
Safety controller (SIS)
2
"Supervisory control" zones
1
"Basic control" or "Local control" zones
0
"Device" or "Process" zones
SIS
Safety zones

Based on Plant


To public networks/Internet via enterprise DMZ
Read-only users
ERP, domain svcs, file and app. servers
Remote access (maintenance)
Remote access (operations)
Remote access (engineering)
ICS web servers
MES, APC, asset mgmt, historians, domain svcs, etc.
Patch management, antivirus, etc.
Engineering stations, operator stations
ICS servers, OPC clients, control applications, etc.
Analyzers, packaged eqpmt, OPC servers, test eqpmt, etc.
HMI
HMI
Controller (BPCS)
Field foundation link device
Wireless systems
Network manager, security manager
Terminator
Tap
H1
Tap
Tap
Terminator
Terminator
H1
multiport junction
Terminator
Safety controller (SIS)
Safety controller (SIS)
4
"Business" zones
3
"Production" or "Operational control" zones
2
"Supervisory control" zones
1
"Basic control" or "Local control" zones
0
"Device" or "Process" zones
SIS
Safety zones

Protocols and Their Use

- There are many highly specialized protocols used for industrial automation and control
- Since they are designed for efficiency, many of them usually forgo any feature or function that is not absolutely necessary
- Many of them have been adapted to run on top of Ethernet and IP
- Two categories:
    - Fieldbus: commonly found in process and control
    - Backend: commonly deployed on or above supervisory networks, and are used to provide efficient system-to-system communication

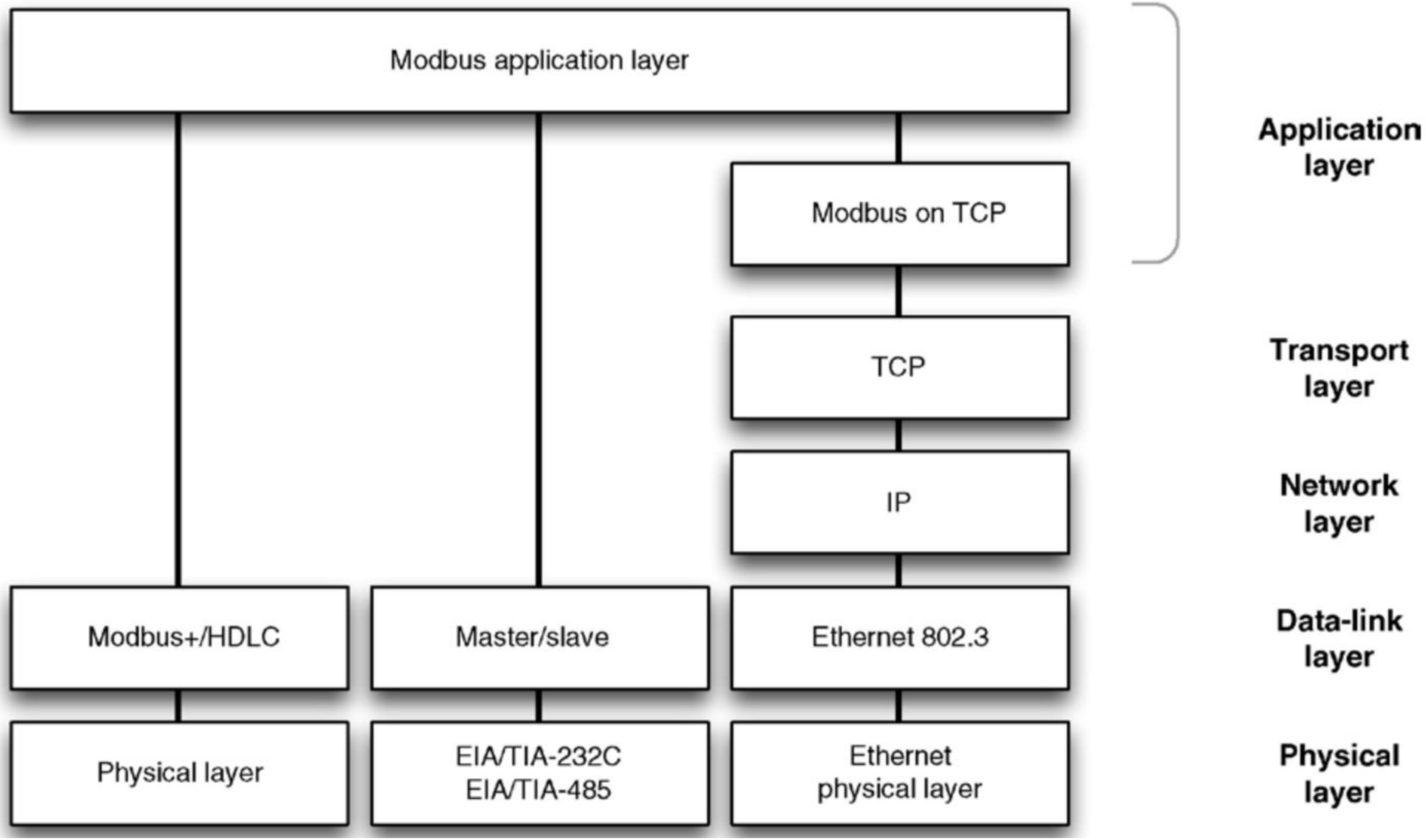
Modbus

- Modbus is an application layer messaging protocol, meaning that it operates at **Layer 7** of the OSI model
- It was designed in 1979 to enable process controllers to communicate with real-time computers
- It remains one of the most popular protocols used in ICS architectures
- It has been widely adopted as a de-facto standard, freely distributed, and well-supported by the Modbus Organization
- It has been enhanced over the years into several distinct variants

Modbus

- It is based on a request/reply methodology allowing for efficient communications between interconnected assets
- Extremely simple devices such as motors and sensors use Modbus to communicate with more complex computers
- Therefore, message generation, transmission, and receipt all require very little processing overhead
- It makes it a suitable protocol from PLCs and RTUs to communicate data to supervisory ICS

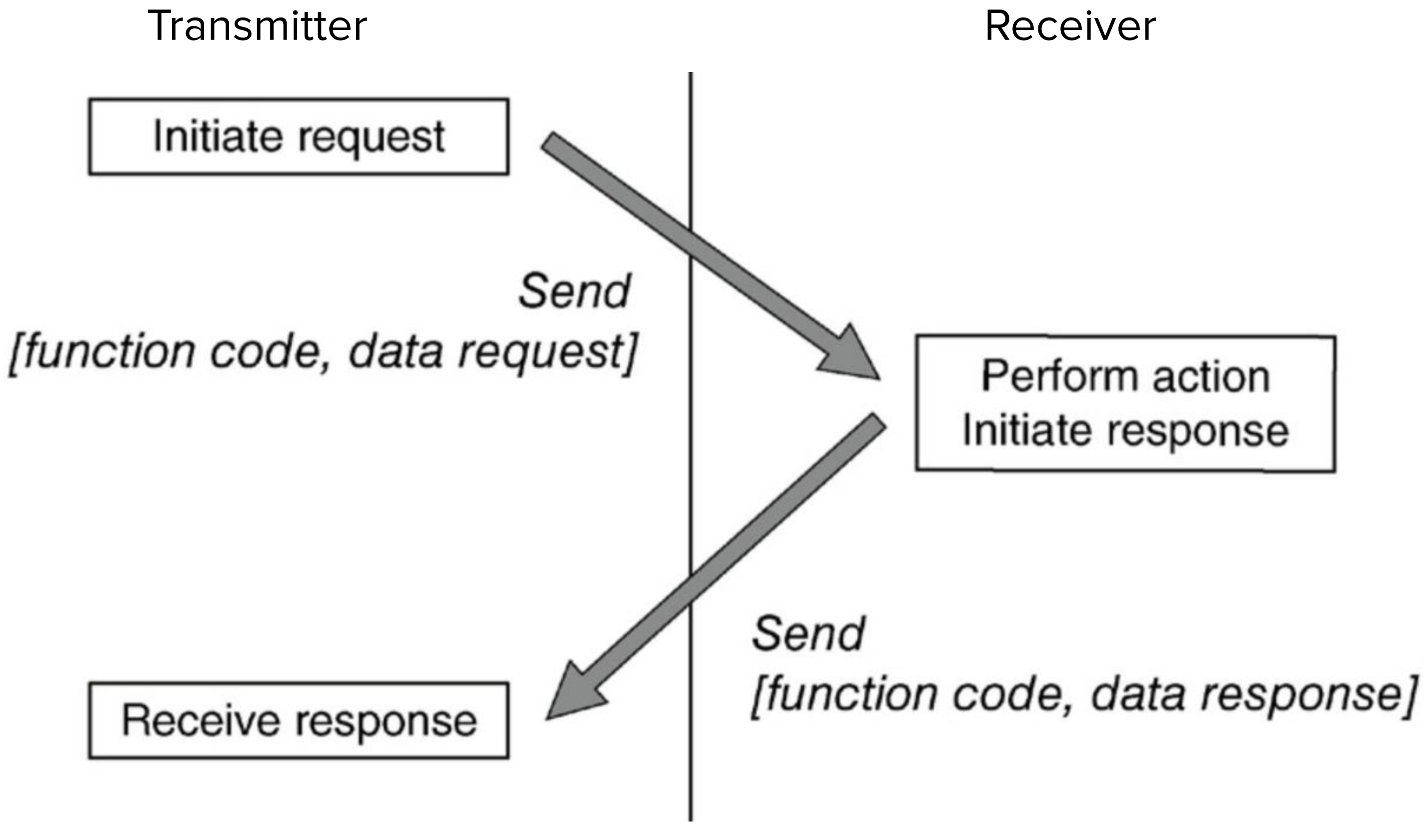
Modbus


Modbus application layer
Modbus on TCP
TCP
IP
Modbus+/HDLC
Master/slave
Ethernet 802.3
Physical layer
EIA/TIA-232C
EIA/TIA-485
Ethernet
physical layer
Application
layer
Transport
layer
Network
layer
Data-link
layer
Physical
layer

Modbus

- It is a request/response protocol using three distinct protocol data units
  - Modbus Request
  - Modbus Response
  - Modbus Exception Response
- Up to 32 devices can be connected on a single RS-485 serial link, requiring each device being assigned a unique address
- A command is addressed to a specific modbus address
- While other devices may receive the message, only the addressed device will respond

Modbus Error-Free



Transmitter

Receiver

Initiate request

Send
[function code, data request]

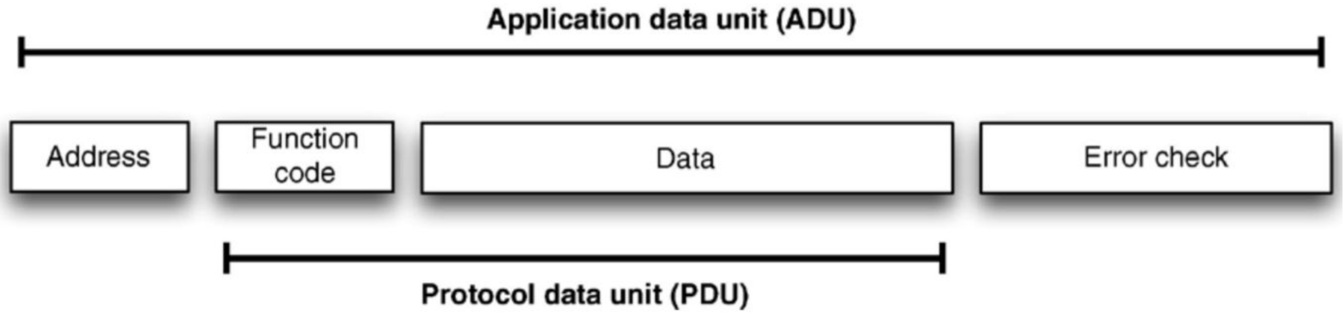
Perform action
Initiate response

Send
[function code, data response]

Receive response

Modbus

- A “transaction” begins with the transmission of an initial Function Code and a Data Request within a Request PDU
- If there are no errors, the receiver will respond with a Function Code and Data Response within a Response PDU
- If there are errors, the device will respond with an Exception Function Code and Exception Code within a Modbus Exception Response


Application data unit (ADU)
Address
Function code
Data
Error check
Protocol data unit (PDU)

Modbus

- Function Codes used in Modbus are divided into three categories and provide the device vendor with some flexibility in how they implement the protocol
- Function codes in the range of 01–64, 73–99, and 111–127 are defined as “Public” and are validated by the Modbus-IDA community and are guaranteed unique
- “User-Defined” function codes in the range 65–72 and 100–110 are provided to allow a particular vendor to implement functionality to suit their particular device and application

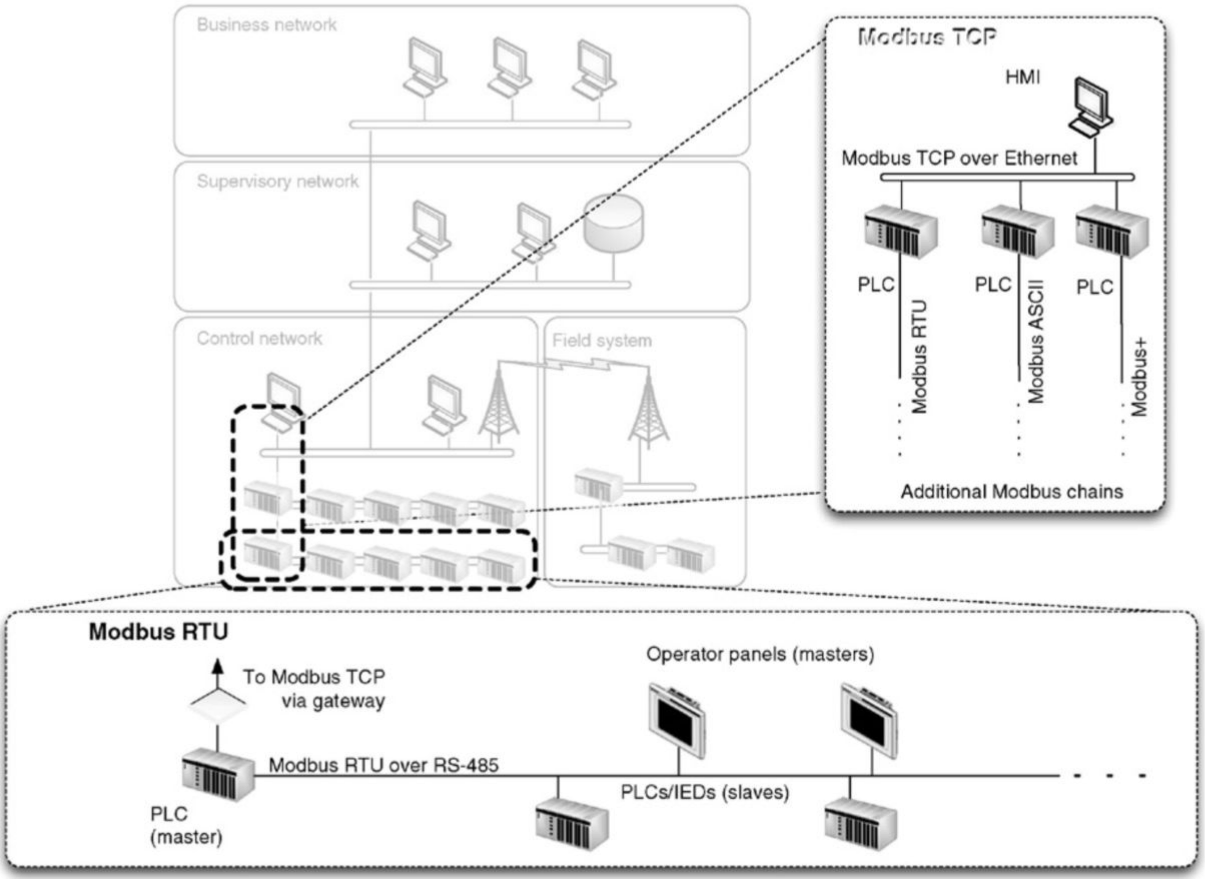
Modbus

- “User-Defined” function codes in the range 65–72 and 100–110 are provided to allow a particular vendor to implement functionality to suit their particular device and application
- Function Codes and Data Requests can be used to perform a wide range of commands
- E.g., Read the value of a single register, Write a value to a single register, Read a block of values from a group of registers, Obtain device diagnostic data

Where do We Use it

- Modbus is typically deployed between PLCs (client) and HMIs (server)
- Modbus devices may also take the role of server in some communications, while being client in other communications

Where do We Use it


Business network
Supervisory network
Control network
Field system
Modbus TCP
HMI
Modbus TCP over Ethernet
PLC
PLC
PLC
Modbus RTU
Modbus ASCII
Modbus+
Additional Modbus chains
Modbus RTU
To Modbus TCP via gateway
Operator panels (masters)
Modbus RTU over RS-485
PLCs/IEDs (slaves)
PLC (master)

Security Concerns

- Modbus presents several security issues
- It **lacks authentication**: sessions only require the use of a valid Modbus address, function code, and associated data
- The data must contain the values of legitimate registers or coils contained in the slave device, or the message will be rejected
- This requires additional information of the target in order to provide a valid message, which however can be obtained via e.g., traffic analysis
- Possibility for man-in-the-middle and replay-like attacks

Security Concerns

- It **lacks encryption:** Commands and addresses are transmitted in clear text and can therefore be easily captured and spoofed or replayed due to the lack of encryption
- Communications to/from a Modbus device can also disclose significant information pertaining to the configuration and use of the device
- It **lacks message checksum:** a command can easily be spoofed by building up the Modbus/TCP ADU with the desired parameters, as the checksum is generated at the transmission layer, not the application layer

Security Recommendations

- Should only be used to communicate between sets of known devices
- In this way it can be easily monitored by establishing clear network zones and by baselining acceptable behavior
- This baseline behavior can then be used to establish access controls on the conduit into the zone via appliances that provide protocol inspecting and filtering capabilities
- Suspicious messages: Modbus TCP packets that are of wrong size or length, function codes that force slave devices into a “listen only” mode, function codes that restart communications

Distributed Network Protocol

- Began as a serial protocol much like Modbus designed for use between “master stations” or “control stations” and slave devices called “outstations”
- Commonly used to connect RTUs configured as “master stations” to IED “outstations” in electric substations
- The primary motivation for this protocol was to provide reliable communications in environments common within the electric utility industry (high EMI and poor transmission media)

Distributed Network Protocol

- DNP3 was extended to work over IP via encapsulation in TCP or UDP packets in 1998, and is now applied in different industries
- DNP3 is very reliable, while remaining efficient and well suited for real-time data transfer
- It also utilizes several standardized data formats and supports time-stamped (and time-synchronized) data, making real-time transmissions more efficient and thus even more reliable
- A single DNP3 frame can include up to 17 CRCs
- Variations of DNP3 support link-layer authentication

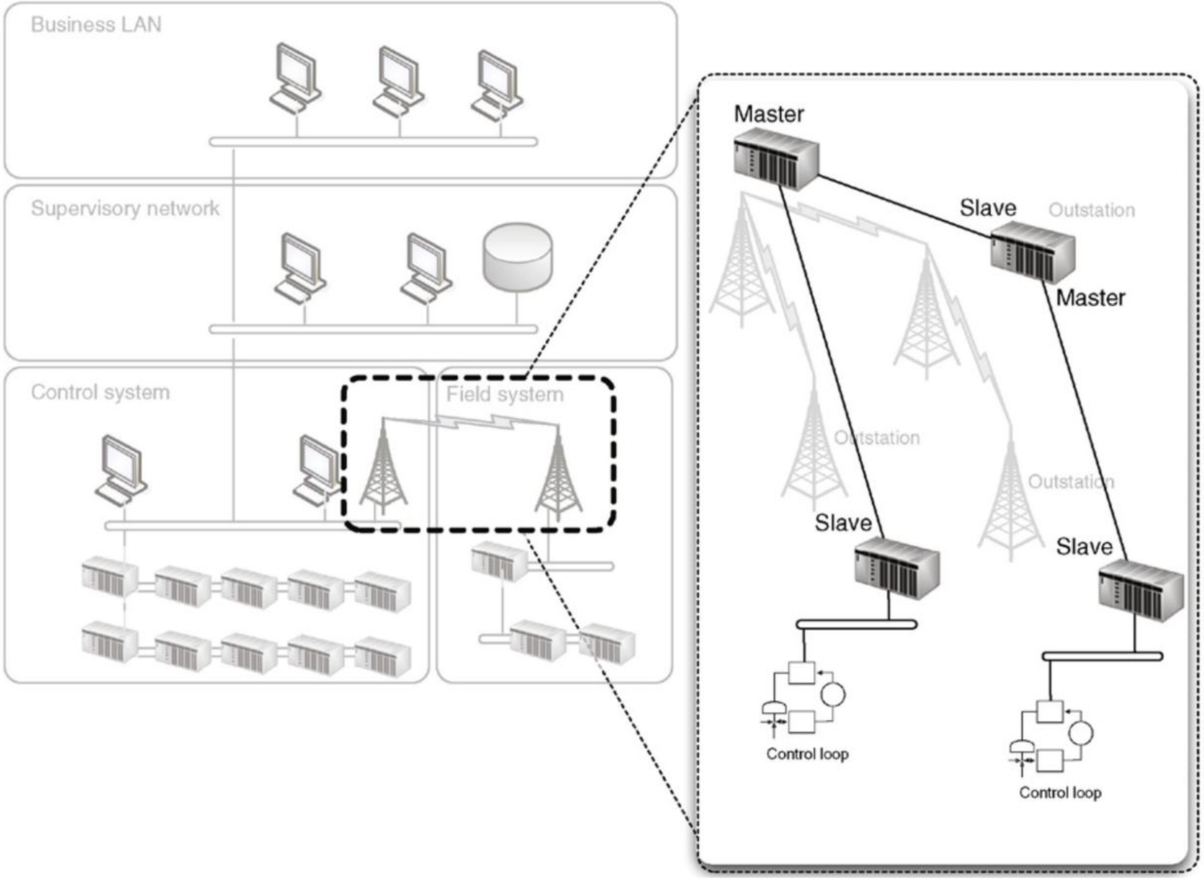
How Does it Work

- DNP3 is primarily used to send and receive messages between control system devices
- It can also be used to send control functions, or even direct binary or analog data for direct interaction with devices, such as RTUs and IEDs
- DNP3 provides a method to identify the remote device parameters and then use message buffers corresponding to event data classes 1 through 3 in order to identify incoming messages and compare them to known point data

How Does it Work

- In this way, the master station is only required to retrieve new information resulting from a point change or change event on the outstation
- Initial communications are typically a class 0 request from the master station to an outstation, used to read all point values into the master station's database
- Subsequent communications will typically either be direct poll requests for a specific data class from the master station, or control or configuration requests from the master station to an outstation

Where do We Use it


Business LAN
Supervisory network
Control system
Field system
Master
Slave
Outstation
Master
Outstation
Outstation
Slave
Slave
Control loop
Control loop

Security Concerns

- Much attention is given to the integrity of the data frame, there is no authentication or encryption inherent within DNP3
- Some examples of realistic hacks against DNP3 include the use of MitM attacks to capture addresses, which can then be used to manipulate other system components
- Examples: Turning off unsolicited reporting to suppress alarms, Spoofing unsolicited responses to the master station to falsify events, Performing a DoS attack through the injection of broadcasts

Secure DNP3

- Secure DNP3 is a DNP3 variant that adds authentication to the response/request process
- Authentication is issued as a challenge by the receiving device
- A challenge condition occurs upon session initiation, after a preset period of time, or upon a “critical” request, such as write
- Authentication occurs using a unique session key that is hashed together with message data from the sender and from the challenger
- In this way, it is very difficult to perform data manipulation or code injection, or to spoof or otherwise hijack the protocol