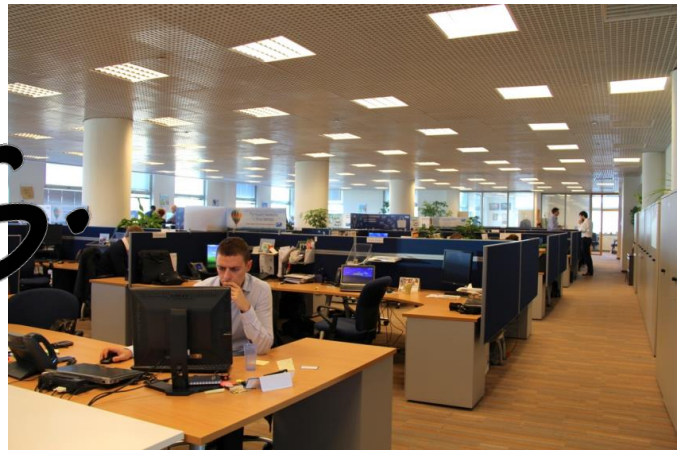
Course Outline

- ICS OVERVIEW
  - Terms & Definitions
  - Generic architectures
  - History of ICS
- Hands on: Basic PLC Programming
  - Creating a first Flowchart-based program
  - Creating visualisation
- **Commonly used ICS protocols**
  - “Industrial Ethernet” Versus “Traditional Ethernet”
  - Overview of ethernet based ICS protocols
  - Security considerations for commonly used protocols
  - Hands-on: Wireshark captures
- Introduction to ICS Security
  - Basics of a ICS security penetration test
  - Red team Excercise & Demo’s

- **Commonly used ICS protocols**
  - **"Industrial Ethernet" Versus "Traditional Ethernet"**
  - Overview of ethernet based ICS protocols
  - Security considerations for commonly used protocols
  - Hands-on: Wireshark captures

VS.



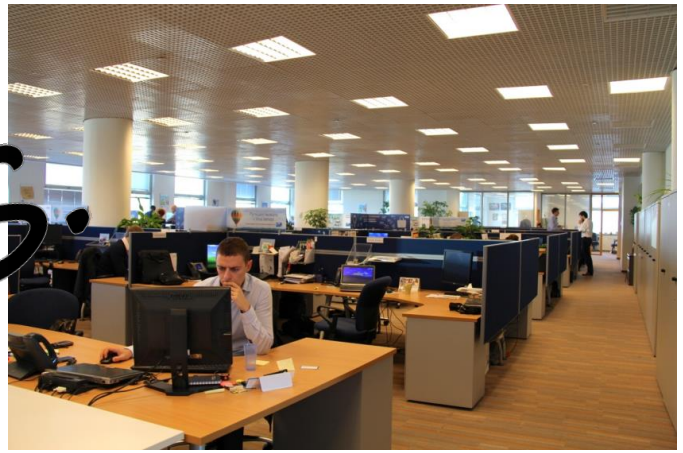
Commonly used ICS protocols: Industrial vs traditional Ethernet

“Industrial Ethernet” Versus “Traditional Ethernet”

Key differences:

- Environmental Requirements
- Installation Requirements
- Performance Requirements

VS.



Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Environmental Requirements

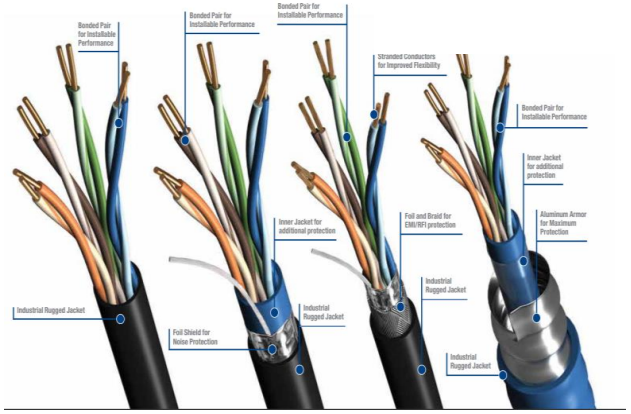
- **Industrial (ethernet) conditions:**
  - Temperature
  - Vibrations
  - EMC/noise
  - Chemicals
- **Hardware adaptions:**
  - Rugged
  - No moving parts (fans,…)
  - Low power (<=24V)

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Environmental Requirements

- **Industrial (ethernet) conditions:**
  - Temperature
  - Vibrations
  - EMC/noise
  - Chemicals
- **Hardware adaptions:**
  - Rugged
  - No moving parts (fans,…)
  - Low power (<=24V)



Commonly used ICS protocols: Industrial vs traditional Ethernet

	Office areas	**Industrial areas**
Supply voltage	230 V AC	24 V DC
Mounting	Desktop device, cabinet or wall mounted	Top-hat rail, wall mounted
Design size	Flat	Slim
Operating temperature	0 °C to +40 °C	• -40 °C to +70 °C • 0 °C to +55 °C
Shock	-	15 g
Vibration	-	2 g
Cooling	Fan	Heat sink
Degree of protection	IP 20 / IP 30	• IP 20 (with protective housing) • IP 65 / IP 67
Resistance to	Dust	Dust, oils, solvents, acids, …
Tests, safety	EN 60 950	EN 60 950
Tests, EMC	• EN 50 081-1 (residential) • EN 50 082-1 (residential)	• EN 50 081-2 (industrial) • EN 50 082-2 (industrial) • DIN EN 50 155 (railway standard)
Response time	> 100 ms	< 20 ms
Operational lifetime	> 3 years	> 6 years
Availability (spare parts)	4 years	10 years

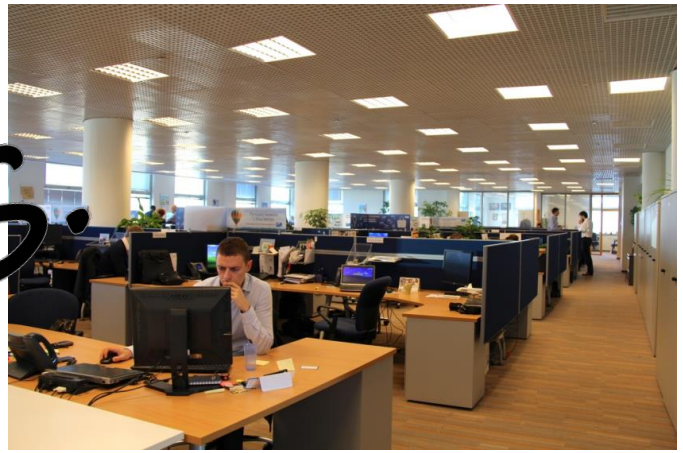
Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Key differences:

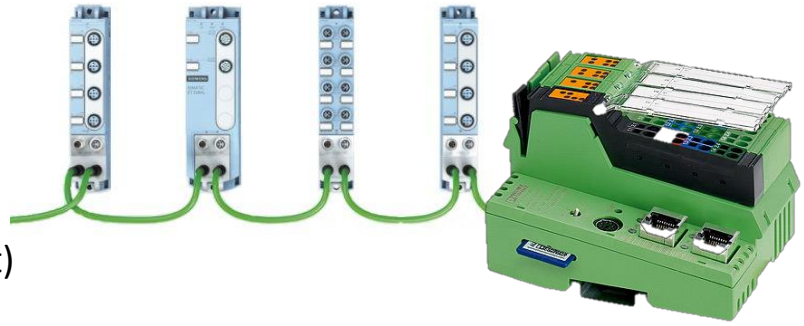
- Environmental Requirements
- **Installation Requirements**
- Performance Requirements

VS.



Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"



Installation Requirements

- **Topologies:**
  - *Office*: Tree / Star
  - *Industrial*: Bus (linear) & ring (often redundant)

- **Connections:**
  - *Office*: Pre-assembled device connection cables
    Variable workplace device connections
    Permanently installed basic installation
  - *Industrial*: System specific connection cables
    Connection points rarely altered
    Wiring very dependent on system requirements

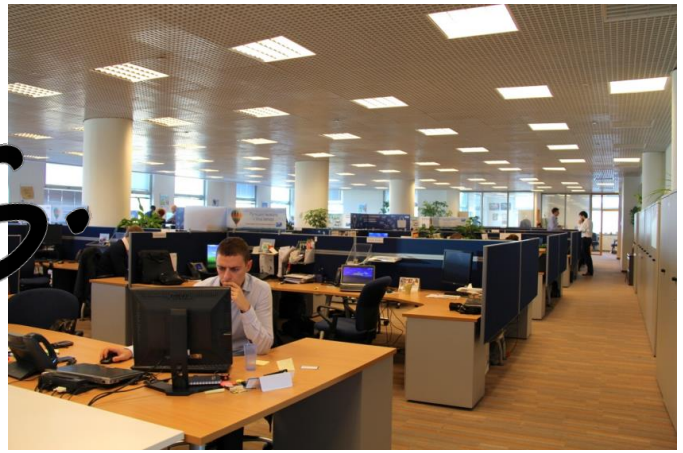
Commonly used ICS protocols: Industrial vs traditional Ethernet

“Industrial Ethernet” Versus “Traditional Ethernet”

Key differences:

- Environmental Requirements
- Installation Requirements
- **Performance Requirements**

VS.



Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance

- **Packets:**
  - *Office*: Large volume data packets
  - *Industrial*: small data packets (for example measurement data)

- **Network:**
  - *Office*: Medium network availability
    Transmissions Timed in seconds
    predominantly acyclic transfers
    No isochromism
  - *Industrial*: Very High network availability
    Transmissions timed in microseconds
    high proportion of cyclic transfers
    isochronism

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance

- **Packets:**
  - *Office*: Large volume data packets
  - *Industrial*: small data packets (for example measurement data)

- **Network:**
  - *Office*: **Medium network availability**
    Transmissions Timed in seconds
    predominantly acyclic transfers
    No isochromism
  - *Industrial*: **Very High network availability**
    Transmissions timed in microseconds
    high proportion of cyclic transfers
    isochronism

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance

- **Packets:**
  - *Office*: Large volume data packets
  - *Industrial*: small data packets (for example measurement data)

- **Network:**
  - *Office*: **Medium network availability**
    Transmissions Timed in seconds
    predominantly acyclic transfers
    No isochromism
  - *Industrial*: **Very High network availability**
    Transmissions timed in microseconds
    high proportion of cyclic transfers
    isochronism

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Availability	DPM	Downtime Per Year (24x365)		
99.000%	10000	3 Days	15 Hours	36 Minutes
99.500%	5000	1 Day	19 Hours	48 Minutes
99.900%	1000		8 Hours	46 Minutes
99.950%	500		4 Hours	23 Minutes
99.990%	100			53 Minutes
99.999%	10			5 Minutes
99.9999%	1			30 Seconds

"High Availability"

DMP—Defects per Million

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance

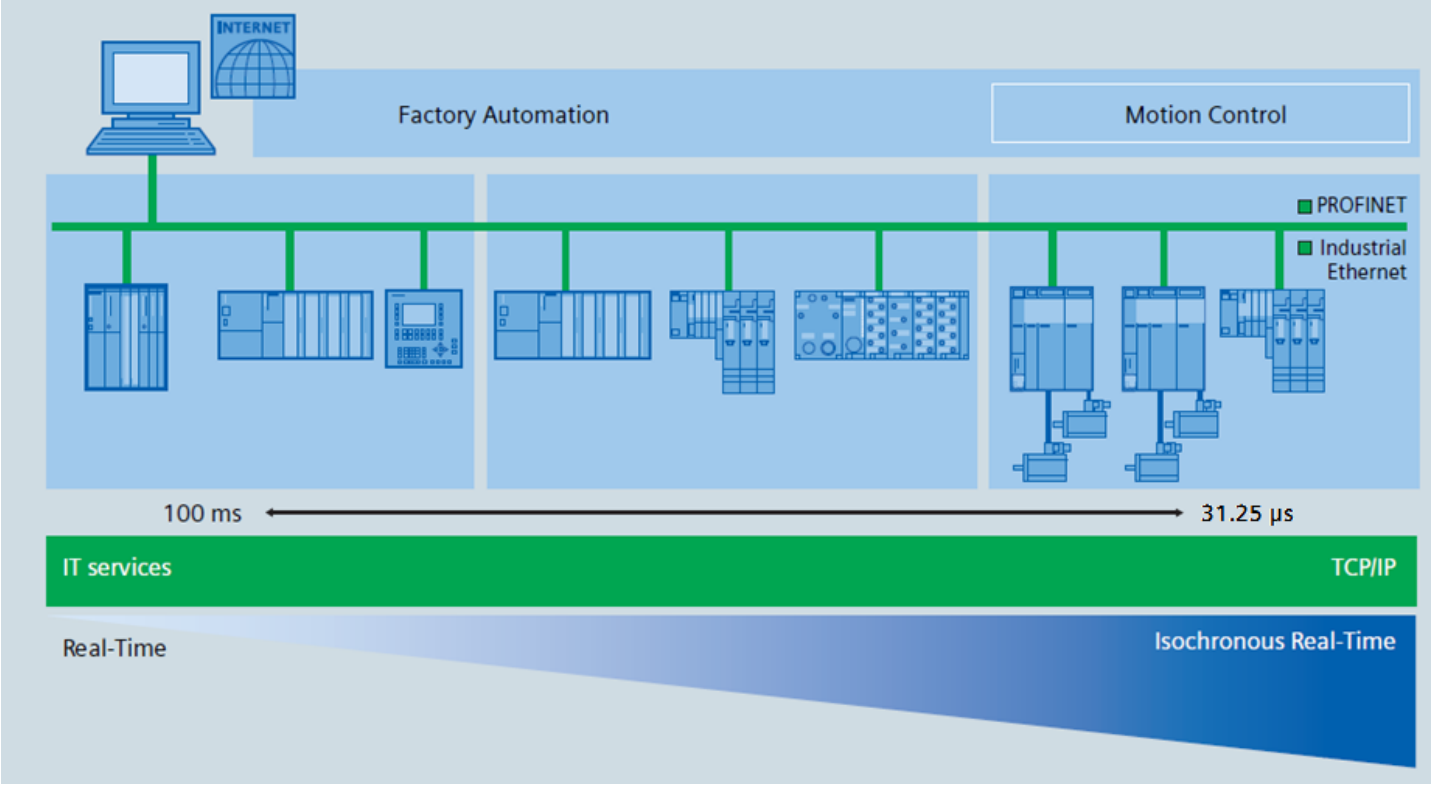
- **Packets:**
  - *Office*: Large volume data packets
  - *Industrial*: small data packets (for example measurement data)

- **Network:**
  - *Office*: Medium network availability
    Transmissions Timed in seconds
    predominantly acyclic transfers
    No isochromism
  - *Industrial*: Very High network availability
    Transmissions timed in microseconds
    high proportion of cyclic transfers
    isochronism

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance



Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance

- **Packets:**
  - *Office*: Large volume data packets
  - *Industrial*: small data packets (for example measurement data)

- **Network:**
  - *Office*: Medium network availability
    Transmissions Timed in seconds
    predominantly acyclic transfers
    No isochromism
  - *Industrial*: Very High network availability
    Transmissions timed in microseconds
    high proportion of cyclic transfers
    isochronism

Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

Transmission Performance

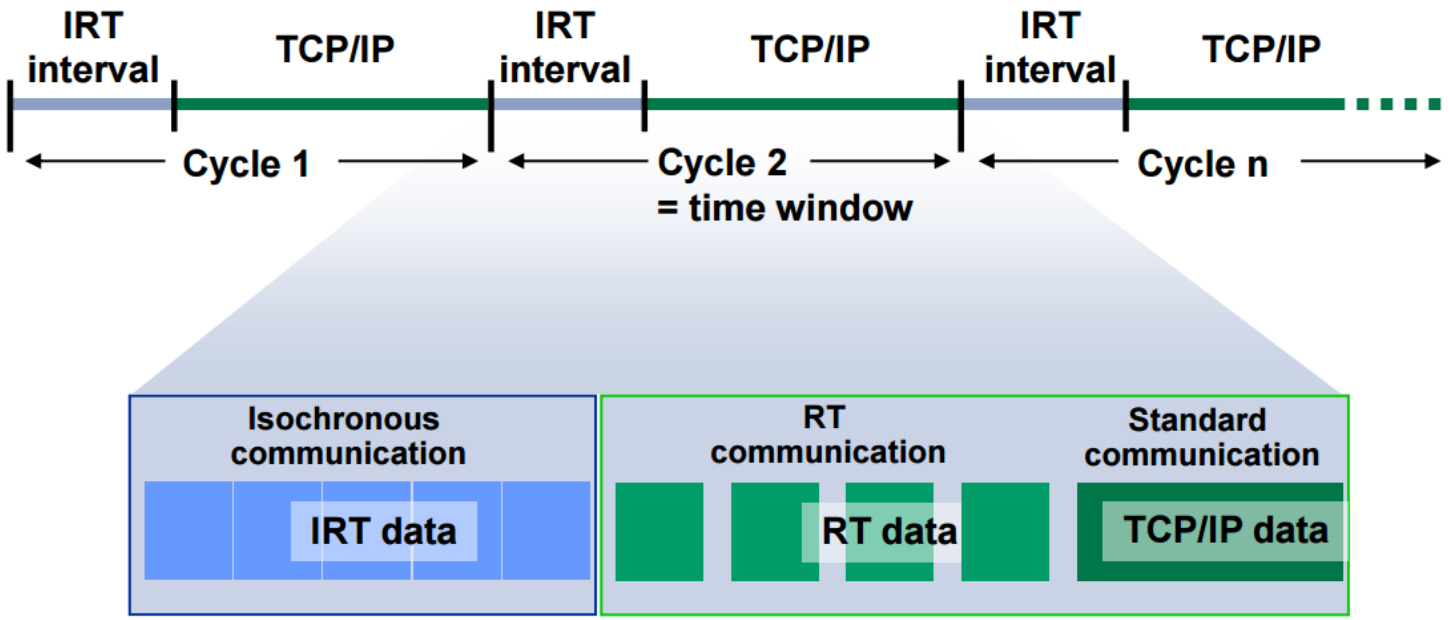
- **Packets:**
  - *Office*: Large volume data packets
  - *Industrial*: small data packets (for example measurement data)

- **Network:**
  - *Office*: Medium network availability
    Transmissions Timed in seconds
    predominantly acyclic transfers
    No isochromism

  - *Industrial*: Very High network availability
    Transmissions timed in microseconds
    high proportion of cyclic transfers
    isochronism

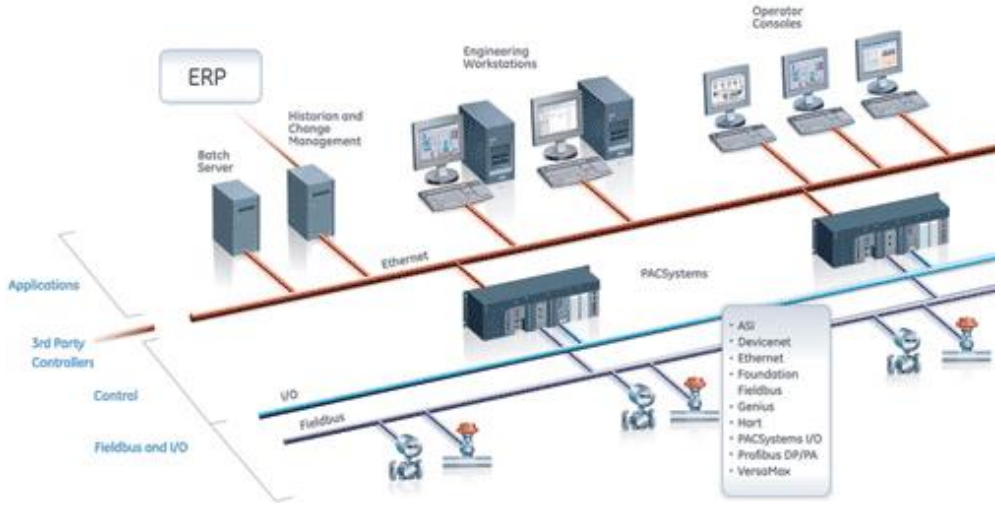
Commonly used ICS protocols: Industrial vs traditional Ethernet

"Industrial Ethernet" Versus "Traditional Ethernet"

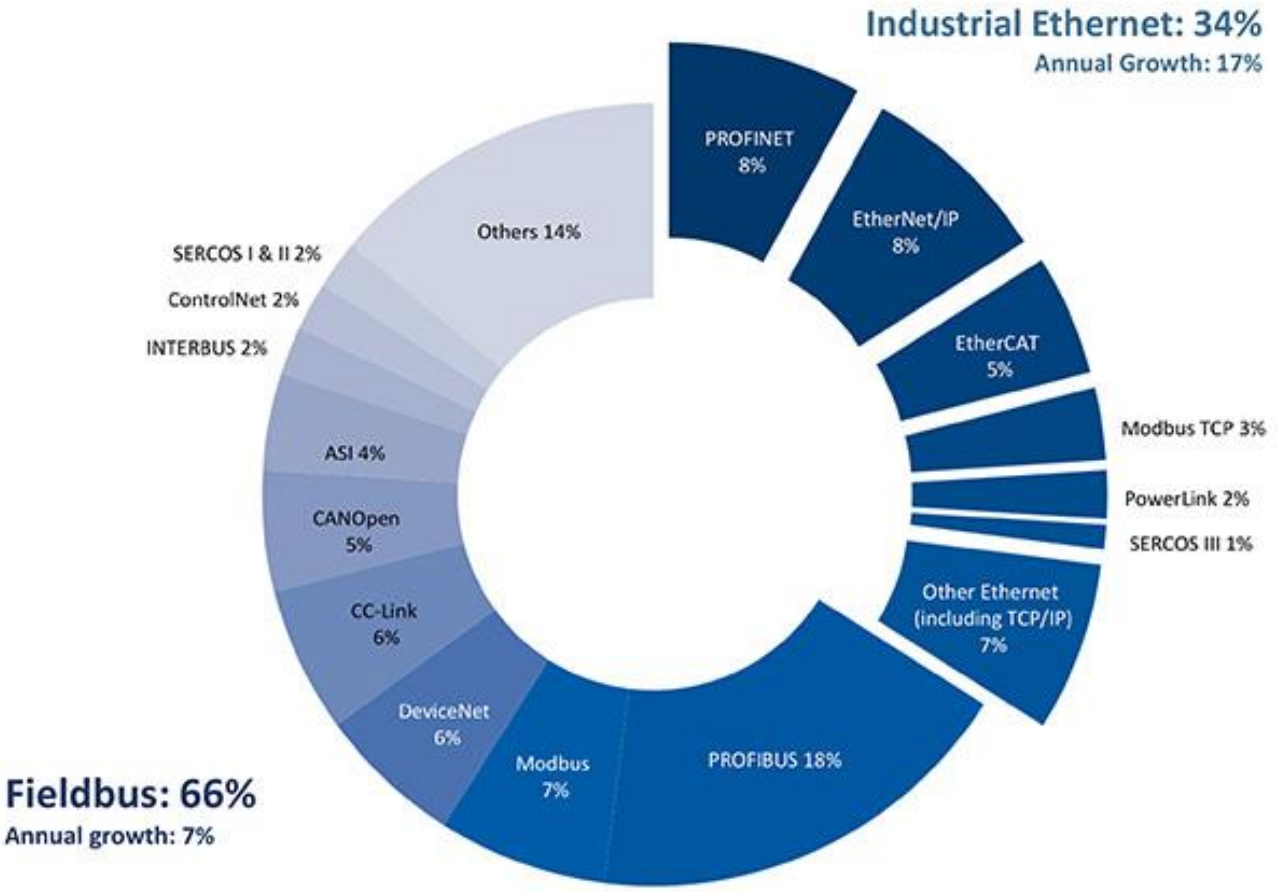


- Bandwidth reservation for isochronous communication
- IRT permits high-precision synchronization

- **Commonly used ICS protocols**
  - "Industrial Ethernet" Versus "Traditional Ethernet"
  - **Overview of ethernet based ICS protocols**
  - Security considerations for commonly used protocols
  - Hands-on: Wireshark captures

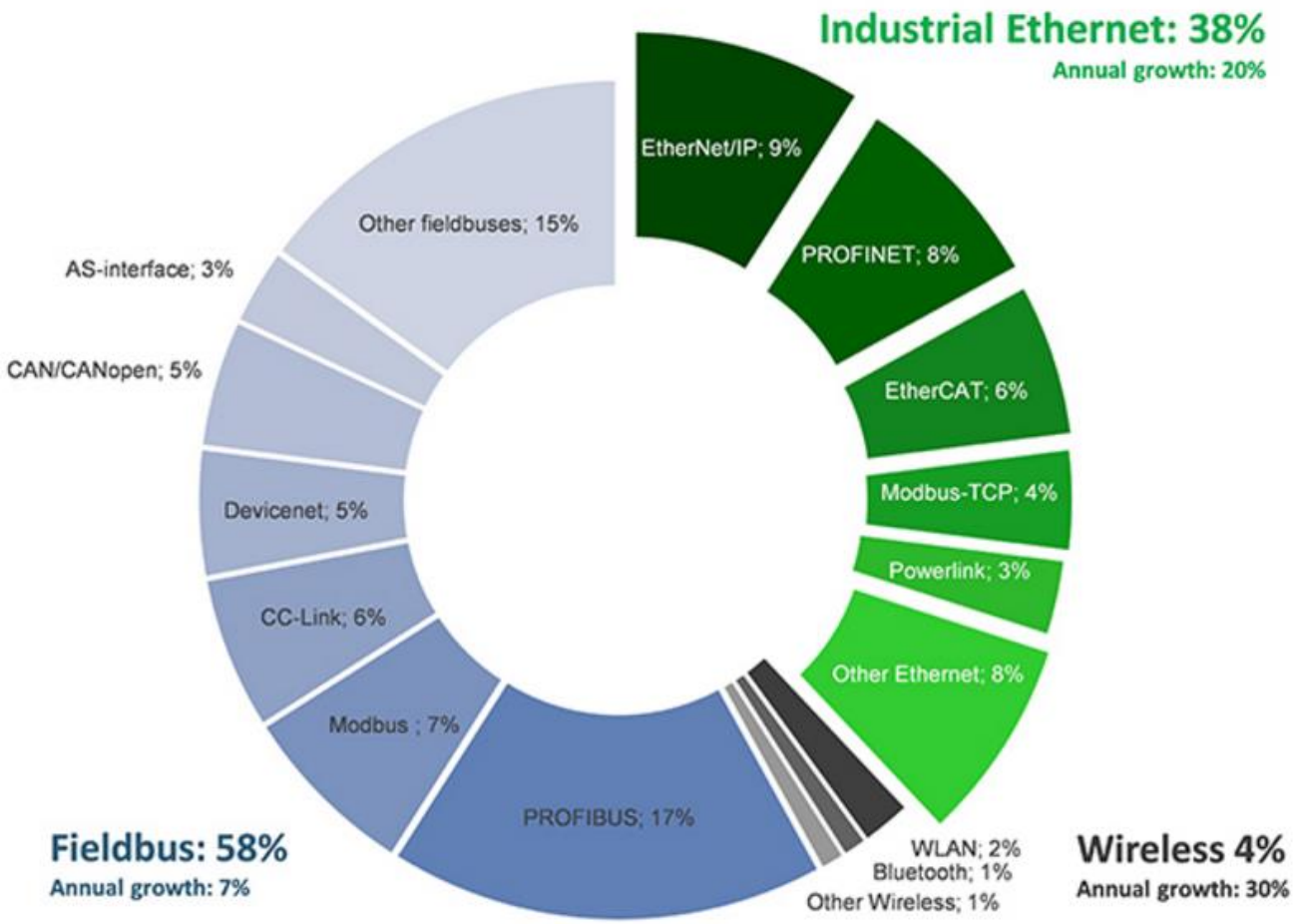


Commonly used ICS protocols: Overview



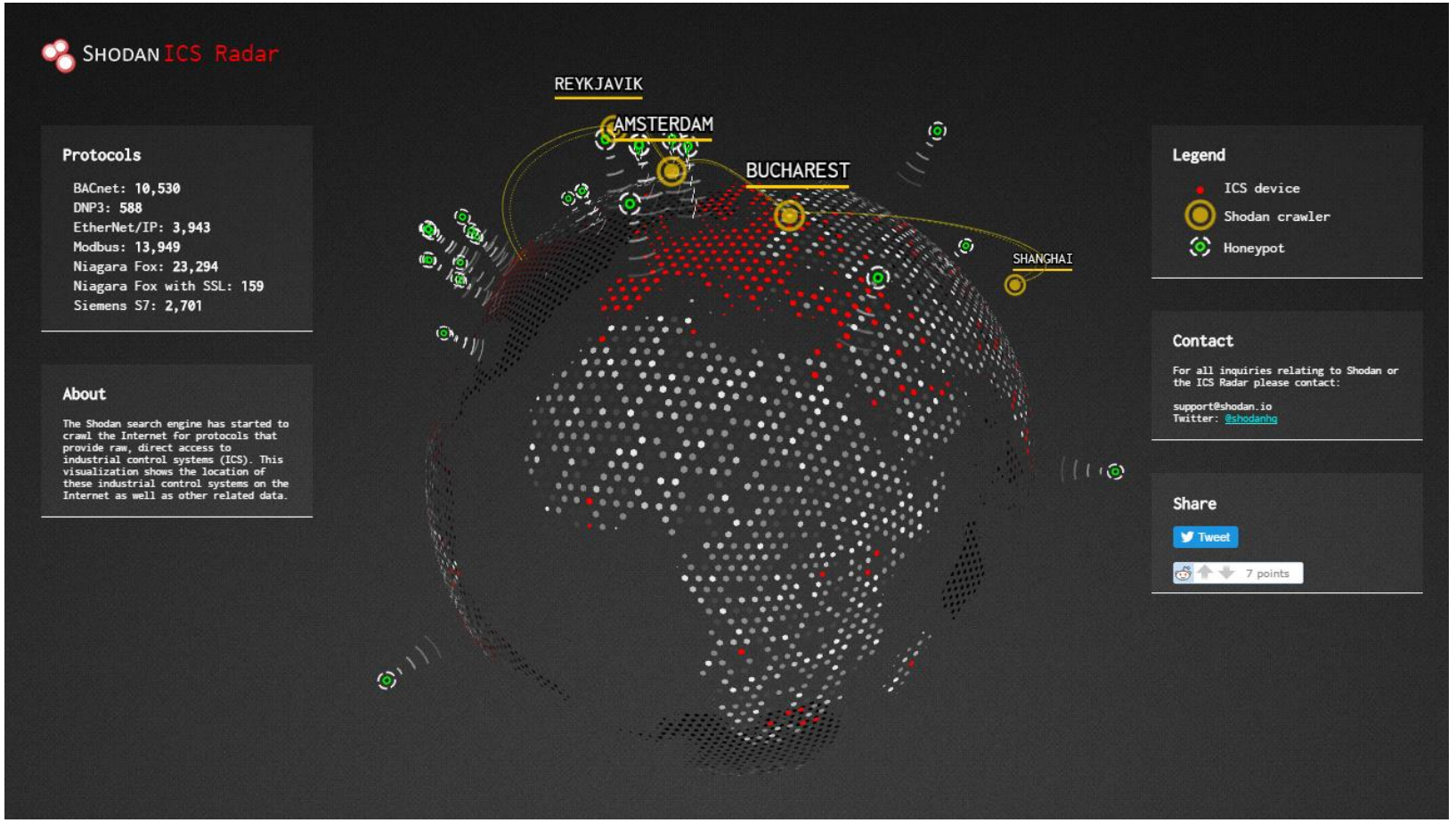
Source: HMS Industrial Networks (2015)

Commonly used ICS protocols: Overview



Source: HMS (2016)

Commonly used ICS protocols: Overview

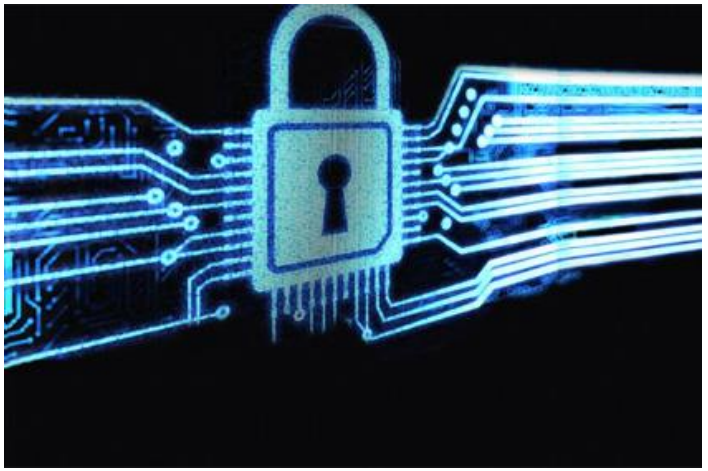


Commonly used ICS protocols: Overview

Ethernet Based Protocols

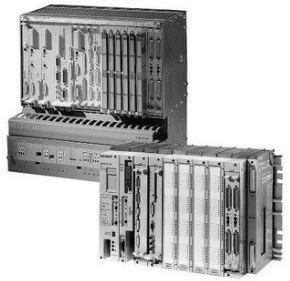
- **Universal ICS Protocols**
  - Modbus TCP: TCP/502
  - OPC UA: TCP/4840
  - OP UA XML: TCP/80, TCP/443
- **Process automation specific protocols**
  - EtherCat: UDP/34980
  - Ethernet/IP: TCP/44818, UDP/2222,44818
  - FL-net: UDP/55000 to 55003
  - Fieldbus HSE: TCP/1089-1091, UDP/1089-1091
  - HART-IP: TCP/5094, UDP/5094
  - PROFINET: TCP/34962-34964, UDP/ 34962-34964
- **Building automation Specific protocols**
  - BACnet/IP: UDP/47808
  - LonTalk: UDP/1628, UDP/1629
  - FOX (Tridium/niagara): TCP/1911
- **Energy Sector specific protocols**
  - DNP3: TCP/20000, UDP/ 20000
  - DLMS/COSEM: TCP/4059, UDP/4059
  - ICCP: TCP/102
  - IEC 104: TCP/102
  - IEE C37.118: TCP/4712, UDP/4713
  - MMS: TCP/102

- **Commonly used ICS protocols**
  - "Industrial Ethernet" Versus "Traditional Ethernet"
  - Overview of ethernet based ICS protocols
  - **Security considerations for commonly used protocols**
  - Hands-on: Wireshark captures



Commonly used ICS protocols: Modbus

Modicon communication bus: Modbus



- Designed in 1979 by Modicon (now Schneider Electric)
- Original goal: enable process controllers to communicate with real time computers (eg. MODCOMP FLIC, DEC PDP-11)
- Widely adopted protocol used in multiple industries
- Mostly used on field level (sometimes between PLC & HMI)
- Open Standard, freely distributed by the modbus organization

Variants

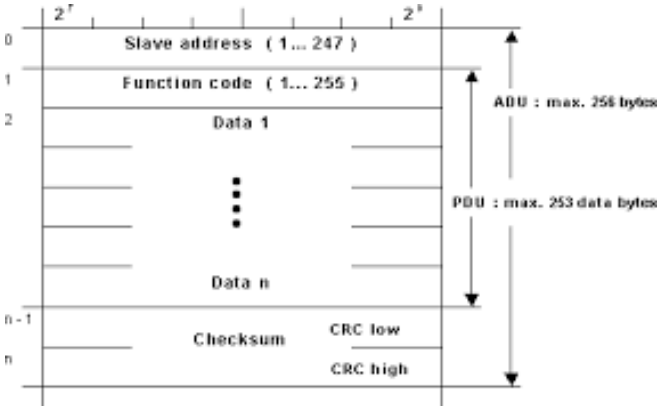
- *Modbus RTU*: Serial, compact binary representation of data
- *Modbus ASCII*: Serial, ASCII characters for protocol communication
- *Modbus TCP/IP*: modbus over TCP/IP networks
- *Modbus RTU/IP*: Checksum is included in the payload as with modbus RTU
- *Modbus over UDP*: removes overhead required for TCP
- *Modbus Plus*: Proprietary to Schneider Electric.
- *Modbus PEMEX*: extension of standard modbus for historical and flow data (not widespread adopted)
- *Enron Modbus*: extension of standard modbus for 32 bit Integers and Floatin point variables, and historical and flow data. Meets API industry standad for historical data storage.

Commonly used ICS protocols: Modbus

Modicon communication bus: Modbus

How it works

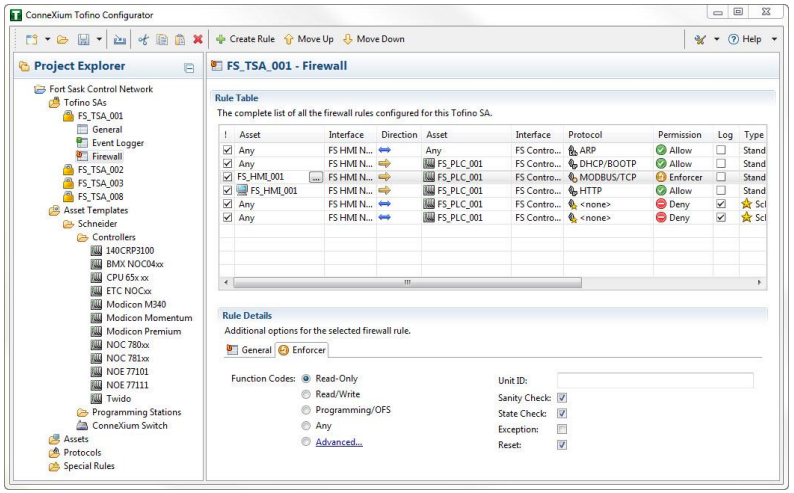
- **Master / slave** (Standard 1 master and max 247 slaves in a network)
- **Request / reply** (Only master can initialise communication)
- Each Modbus device is assigned an unique (in the network) adress.
- All devices see all the messages, only adressed device responds
- Three distinct **protocol data units** (PDU)
  - Modbus request
  - Modbus response
  - Modbus exception response
- **Function codes** used to described the action desired from device



Function Code	Action	Table Name
01 (01 hex)	Read	Discrete Output Coils
05 (05 hex)	Write single	Discrete Output Coil
15 (0F hex)	Write multiple	Discrete Output Coils
02 (02 hex)	Read	Discrete Input Contacts
04 (04 hex)	Read	Analog Input Registers
03 (03 hex)	Read	Analog Output Holding Registers
06 (06 hex)	Write single	Analog Output Holding Register
16 (10 hex)	Write multiple	Analog Output Holding Registers

Commonly used ICS protocols: Modbus

Modicon communication bus:



Security Aspect

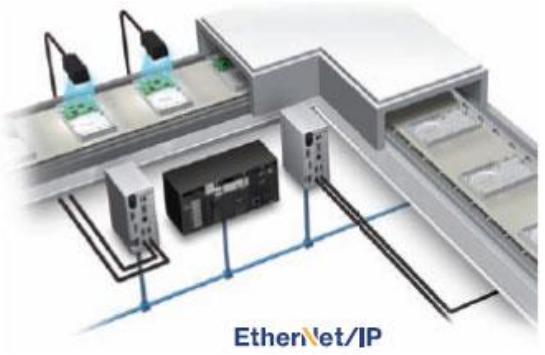
- Concerns
  - Lack of Authentication
  - Lack of Encryption
  - Lack of message Checksum
  - Lack of broadcast suppression

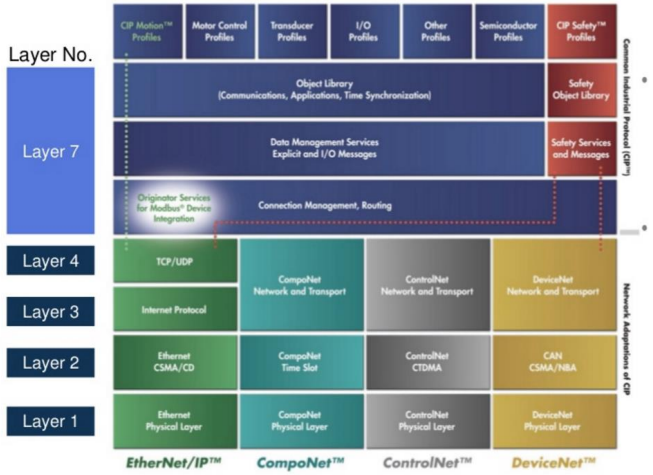
- Recommendations
  - Establishing clear network zones
  - Use baseline behavior to establish access controls on the conduits
    - E.g. industrial firewall with deep-packet inspection capabilities
  - ICS-aware intrustion protection systems configured with modbus signatures

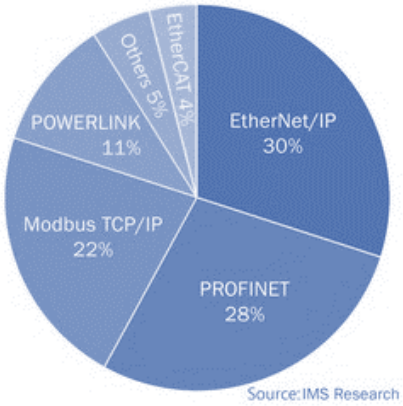
Commonly used ICS protocols: Profibus

Ethernet Industrial Protocol: EtherNet/IP

- Development began in the 1990s within a technical working group of ControlNet International
- Industrial ethernet combines standard ethernet technologies with the media-independent Common Industrial Protocol (CIP)
- CIP is an application layer protocol defining messages and services
- Widly used in a range of industries
- One of the leading industrial ethernet networks in the United States
- Commonly implemented in the field level (controller – sensor/actuators)







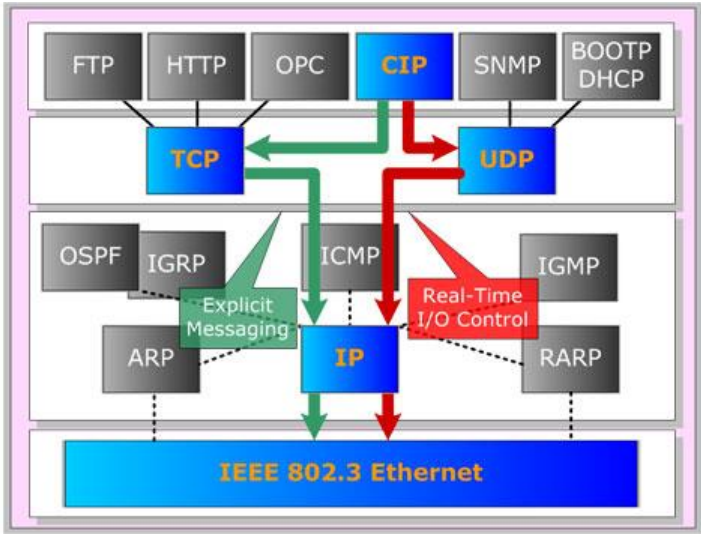
Commonly used ICS protocols: Profibus

Ethernet Industrial Protocol: EtherNet/IP

How it works

- Uses two message types
  - **Explicit Messaging**: **TCP/**44818
    - Client/server,
    - transaction executed on demand (configuration, setpoints,…)
    - with or without prior establishment of a CIP connection
  - **Real-time I/O Control**: **UDP/**2222
    - Producer/Consumer,
    - I/O data transfer done at a specific, periodic rate

- One-to-one (unicast), one-to-many (multicast), and one-to-all (broadcast) communication via IP



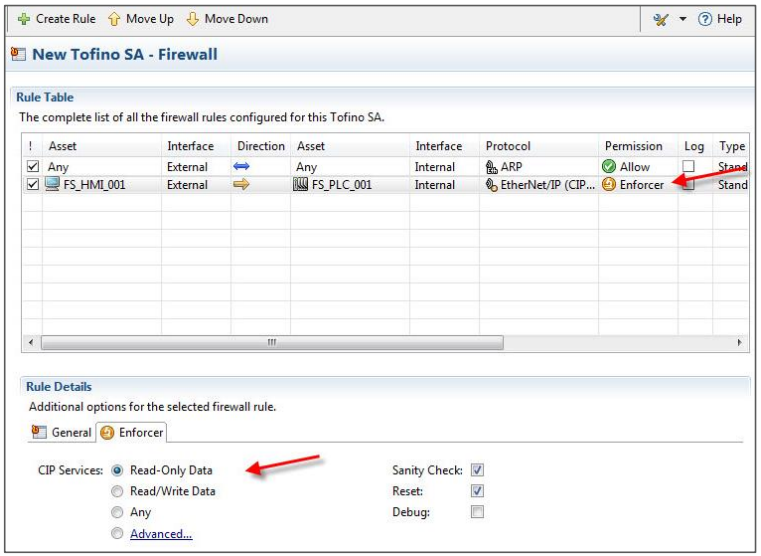
Commonly used ICS protocols: Profibus

Ethernet Industrial Protocol: EtherNet/IP

Security Aspect

- Concerns
  - Is a real-time ethernet protocol => has all the vulnerabilities of Ethernet
  - When using UDP => transaction-less, so no reliability, data integrity,…
  - CIP does not define mechanisms for security
  - Use of Required objects for device identification
  - Use of Common application objects for device information exchange
  - Use of UDP and Multicast facilitates manipulation

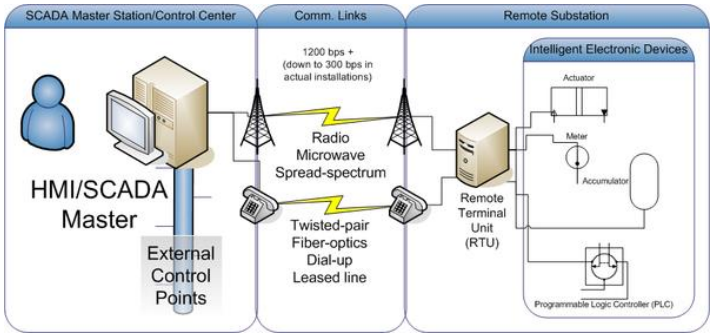
- Recommendations
  - Provide Ethernet- and IP-based security at perimeter of any EIP network
  - Packet inspection / application layer firewalls
  - Passive network monitoring



Commonly used ICS protocols: DNP

Distributed network protocol (DNP)

- Began as a serial protocol between master stations and slave devices
- DNP3 was initially introduced in 1990 by Westronic (Now GE-Harris Canada)
  - Based on early drafts of IEC 60870-5 standard
  - Primary motivation was to provide reliable communications within the electric utility industry
- Extended to be used over IP in 1998
- Now widely used in electric utility, oil, gas, water and wastewater industries
- Commonly implemented between master control station and RTUs in a remote station or Interconnecting RTUs and IEDs



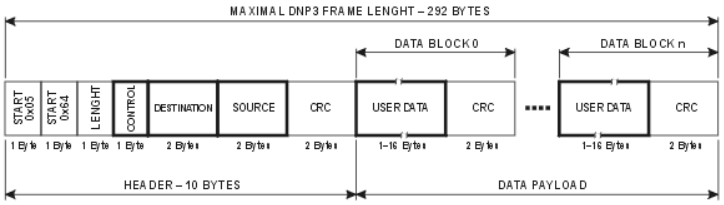
Commonly used ICS protocols: DNP

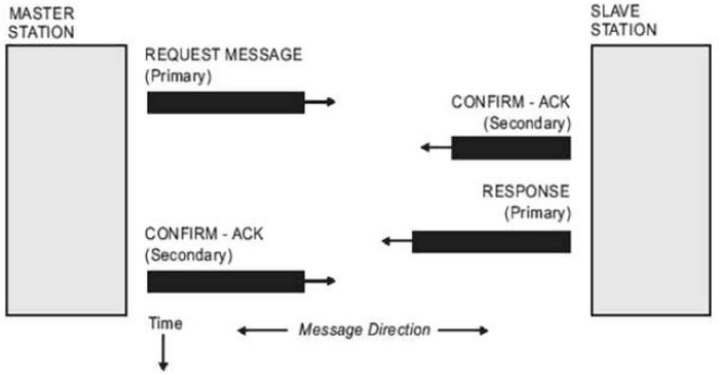
Distributed network protocol (DNP)

How it works

- Master Station(s) **(control stations)** with slave devices **(outstations)**
- **Biderectional communication:** Master-slave; Slave-Master
- Each Station has an unique device address between 0 and 65519
- High degree of **realibility**
  - mutiple CRCs => high degree of reliability (CRC octets for every 16 data octets)
  - link layer confirmation => succesful receipt of the frame is ensured

  ⇒ Added overhead, less efficient protocol
- **Flexible** payload
- Two kinds of data
  - Class 0: data that represents a static value
  - Class 1: event data, a change such as an alarm condition
- Master station is only required to retreive new information resulting from a point change or change event on the outstation





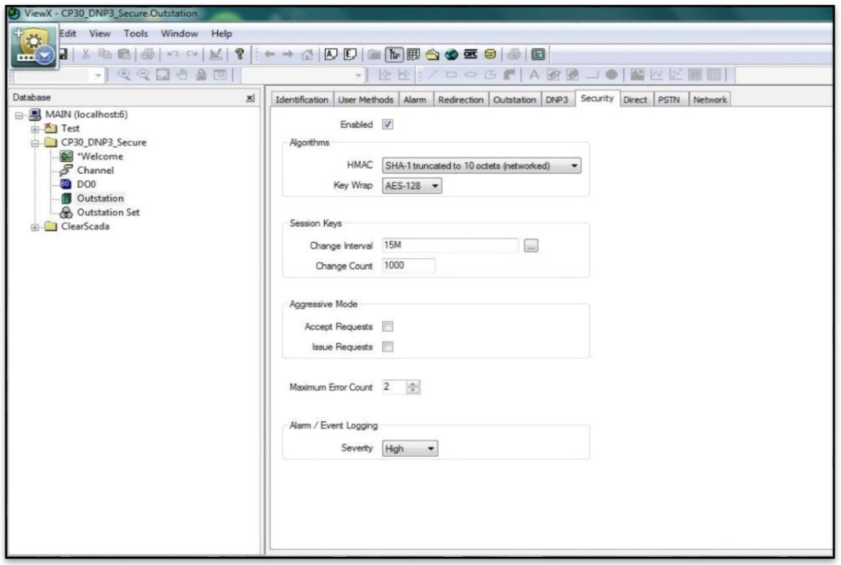
Commonly used ICS protocols: DNP

Distributed network protocol (DNP)

Security Aspect

- Concerns
  - No encryption (<>there is a secure version of DNP3)
  - Several known vulnerabilities (reported by ICS-CERT)
  - Susesible to MitM attacks

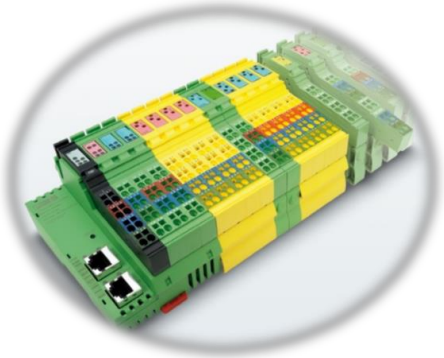
- Recommendations
  - Implement the Secure Version of DNP3
  - DPN3 stations and outstations should always be isolated into a unique zone consisting only of authorized devices
  - Monitoring of sessions
  - ICS-aware intrusion protection systems



Commonly used ICS protocols: PROFINET

PROcess Field NET: PROFINET

- Development by the PROFIBUS User Organization (PNO) and Siemens in 2003
- NOT PROFIBUS over Ethernet!
- Open Industrial Ethernet Standard, compatible with standard Ethernet
- Real time ethernet implimentation
- Commonly implemented in the field and between controllers and HMI/engineering



Variants

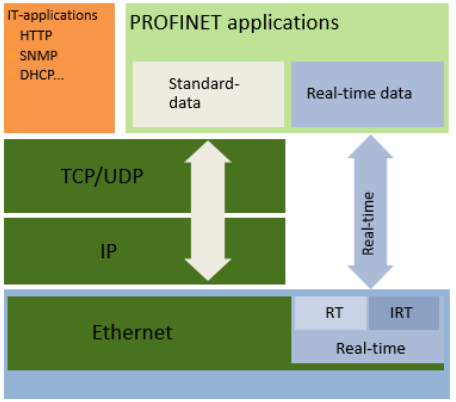
- PROFINET CBA:
  - Communication between controllers
  - TCP/IP and real-time
- PROFINET IO
  - Communication with distributed I/O
  - Non-Real-Time (NRT), Real-Time (RT) and Isochronous real-time (IRT)

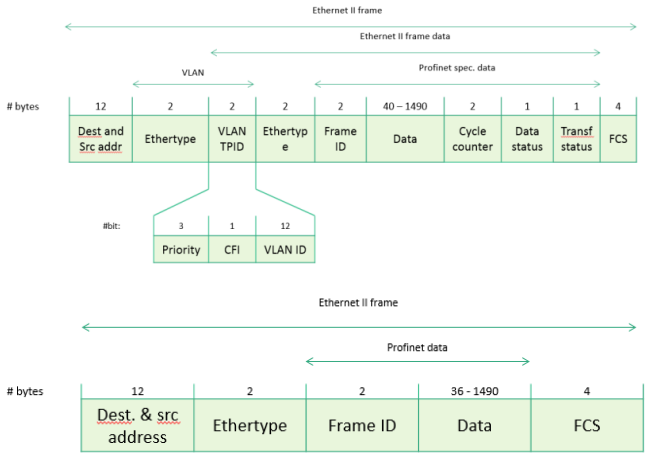
Commonly used ICS protocols: PROFINET

PROcess Field NET: PROFINET

How it works

- Provider/consumer
- Data encapsulated in ethernet Frame
- Uses Device names to identify the profinet devices
- **Cyclic data**
  - Unacknowledged real-time data
  - I/O data
- **Acyclic data**
  - Diagnostic information
  - Error Log entries (alarms and error messages)
  - Identification information
  - Information functions
  - Readback of I/O data





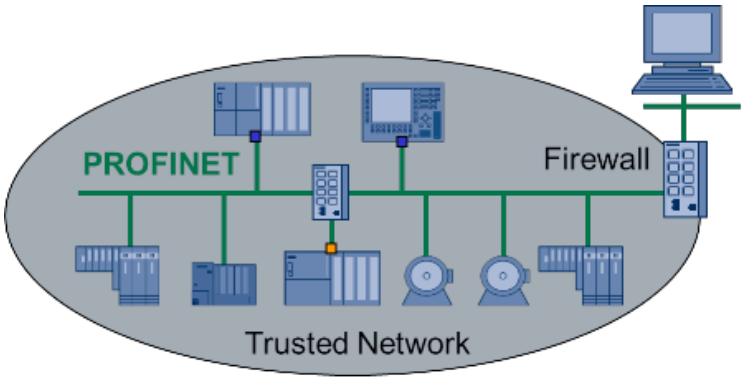
Commonly used ICS protocols: PROFINET

PROcess Field NET: PROFINET

Security Aspect

- Concerns
  - Is a real-time ethernet protocol => has all the vulnerabilities of Ethernet
  - No authentication
  - No encryption

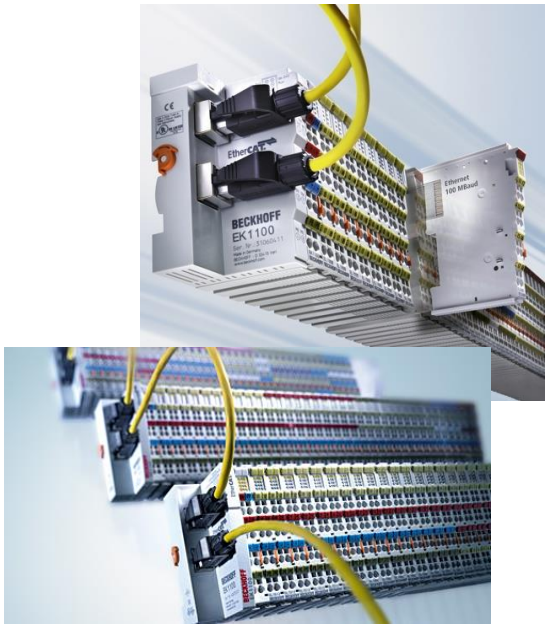
- Recommendations
  - Carefull implementation of zones and conduits
  - Provide Ethernet- and IP-based security at perimeters
  - Packet inspection / application layer firewalls
  - Passive network monitoring



Commonly used ICS protocols: PROFINET

EtherCAT

- Introduced in April 2003 by Beckhoff Automation. EtherCAT technology group was founded in November 2003
- Uses ethernet Frame
- Is optimized for short cyclic process data, the use of protocol stacks (TCP/IP or UDP/IP) are eliminated
- EtherCAT master sends a telegram that passes through each node.
- EtherCAT master is the only node within a segment allowed to actively send an EtherCAT frame

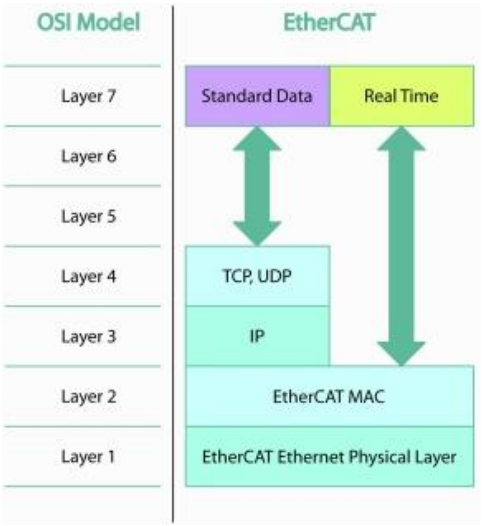


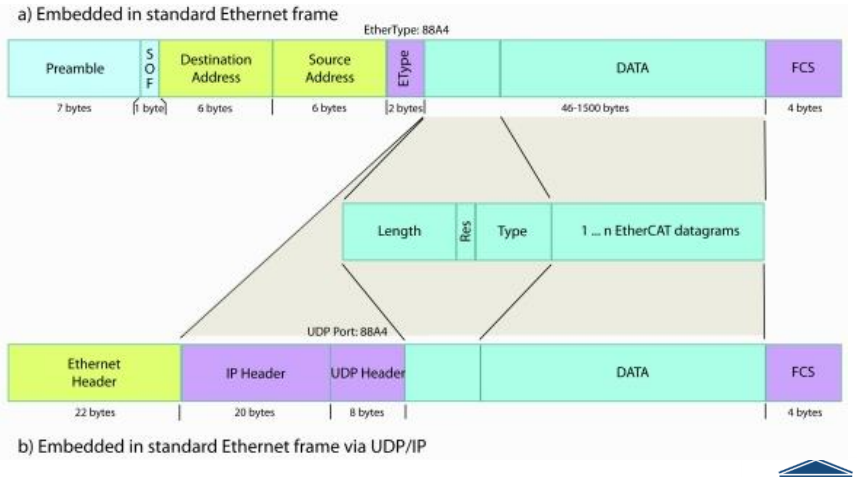
Commonly used ICS protocols: PROFINET

EtherCAT

How it works

- overcomes the packet overhead problem, since a single ethernet frame is shared by multiple devices for both receiving and transmitting data
- The EtherCAT frame contains one or more datagrams (type indicated by datag. header)
  - Read, write, read-write
  - Access to a specific slave device through direct addressing, or access to multiple slave devices through logical addressing (implicit addressing)





Commonly used ICS protocols: PROFINET

EtherCAT

Security Aspect

- Concerns
  - Is a real-time ethernet protocol => has all the vulnerabilities of Ethernet
  - No authentication
  - No encryption

- Recommendations
  - Carefull implementation of zones and conduits
  - Provide Ethernet- and IP-based security at perimeters
  - Packet inspection / application layer firewalls
  - Passive network monitoring

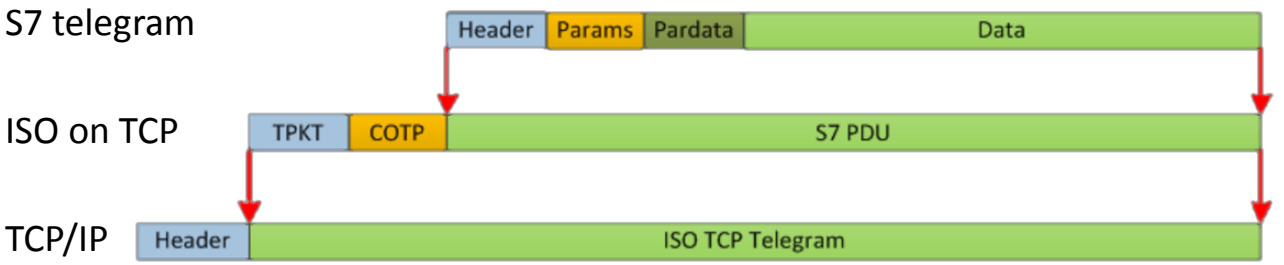
Commonly used ICS protocols: S7comm

S7comm

SIEMENS

- S7 Protocol, is the backbone of the Siemens communications, its Ethernet implementation relies on ISO TCP (RFC1006)
- S7 Protocol is Function oriented or Command oriented, i.e. each transmission contains a command or a reply to it.
- Each command consists of
  - A header.
  - A set of parameters.
  - A parameters data.
  - A data block.
- The first two elements are always present, the other are optional.

	OSI layer	Protocol
7	Application Layer	S7 communication
6	Presentation Layer	S7 communication
5	Session Layer	S7 communication
4	Transport Layer	ISO-on-TCP (RFC 1006)
3	Network Layer	IP
2	Data Link Layer	Ethernet
1	Physical Layer	Ethernet



Commonly used ICS protocols: S7comm

S7comm

SIEMENS

S7 Protocol partial compatibility list (See also § LOGO and S7200)

	CPU						CP	DRIVE
	300	400	WinAC	Snap7S	1200	1500	343/443/IE	SINAMICS
DB Read/Write	O	O	O	O	O	O(3)	-	O
EB Read/Write	O	O	O	O	O	O	-	O
AB Read/Write	O	O	O	O	O	O	-	O
MK Read/Write	O	O	O	O	O	O	-	-
TM Read/Write	O	O	O	O	-	-	-	-
CT Read/Write	O	O	O	O	-	-	-	-
Read SZL	O	O	O	O	O	O	O	O
Multi Read/Write	O	O	O	O	O	O	-	O
Directory	O	O	O	O	-	-	O	(2)
Date and Time	O	O	O	O	-	-	-	O
Control Run/Stop	O	O	O	O	-	-	(1)	O
Security	O	O	O	O	-	-	-	-
Block Upload/Down/Delete	O	O	O	-	-	-	O	O

Snap7S = Snap7Server

(1) After the "Stop" command, the connection is lost, Stop/Run CPU sequence is needed.
(2) Tough DB are present and accessible, directory shows only SDBs.
(3) See S71200/1500 notes.

- **Commonly used ICS protocols**
  - "Industrial Ethernet" Versus "Traditional Ethernet"
  - Overview of ethernet based ICS protocols
  - Security considerations for commonly used protocols
  - **Hands-on: Wireshark captures**

Commonly used ICS protocols: WireShark

Sample captures for the following Protocols

protocol:	*Wireshark filter:*	*Ports:*
• BACnet	***bacnet***	UDP/47808
• DNP3	***dnp3***	TCP/20000, UDP/ 20000
• Ethercat	***ecat***	UDP/34980
• Ethernet Powerlink V2	***epl***	
• Hart-IP	***hart_ip***	TCP/5094, UDP/5094
• LonTalk	***lon***	UDP/1628, UDP/1629
• Modbus TCP	***mbtcp***	TCP/502
• Profinet	***pn_rt***	TCP/34962-34964, UDP/ 34962-34964
• S7comm	***s7comm***	TCP/102
• S-Bus	***sbus***	UDP/5050
• OPC UA	***opcua***	TCP/4870 (*variable*)
• Smartgrid		
• C12.22 smartmeters	***C1222***	TCP/1153**,** UDP/1153
• C37.118 Synchrophasors	***synphasor***	TCP/4712**,** UDP/4713

Commonly used ICS protocols: WireShark

Hands-on