The How, What, When, Where, and Why of Communication Protocols, Topologies, and Media between SCADA, PLCs, and Control Devices

Robert Barrett

United Water Idaho

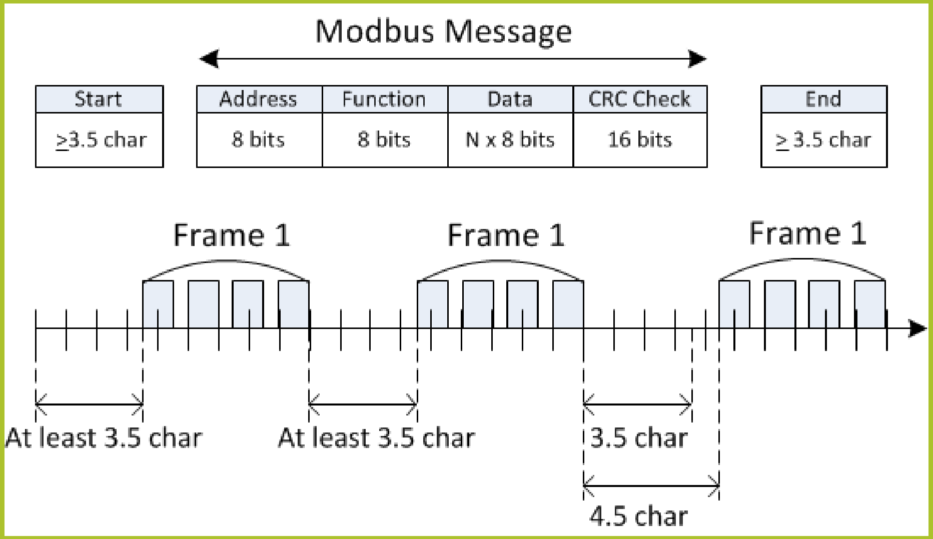
What is a Communications Protocol?

- A communication protocol is a system of rules for data exchange within or between computers, PLCs, instrumentation, control devices, etc..
- Communicating systems use well-defined formats (protocol) for exchanging messages
- Each message has an exact meaning intended to elicit a response from a range of possible responses pre-determined for that particular situation
- a protocol must define the syntax, semantics, and synchronization of communication
- A protocol can be implemented as hardware, software, or both
- Communication protocols have to be agreed upon by the parties involved. To reach agreement, a protocol may be developed into a technical standard
- Systems typically do not use a single protocol to handle a transmission. Instead they use a set of cooperating protocols, sometimes called a protocol family or protocol suite
- The protocols can be arranged based on functionality in groups

Wikipedia

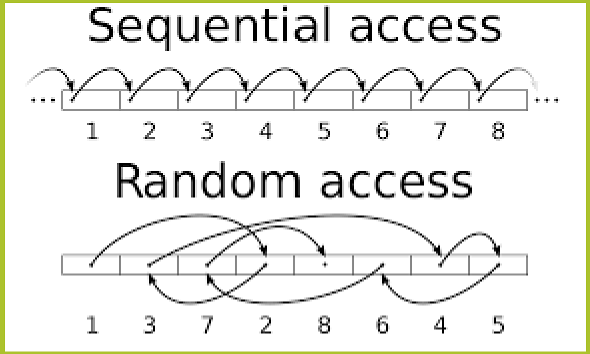
Basic Requirements of a Protocols

- Data formats for data exchange
  - Header & data
- Address formats for data exchange
  - Sender & receiver ID
- Address mapping
  - File location, IP to MAC
- Routing
  - Multiple hops
- Detection of transmission errors
  - CRC
- Acknowledgements
- Loss of information
- Direction of information flow
- Sequence control
- Flow control



Modbus Message

Start	Address	Function	Data	CRC Check	End
>3.5 char	8 bits	8 bits	N x 8 bits	16 bits	> 3.5 char

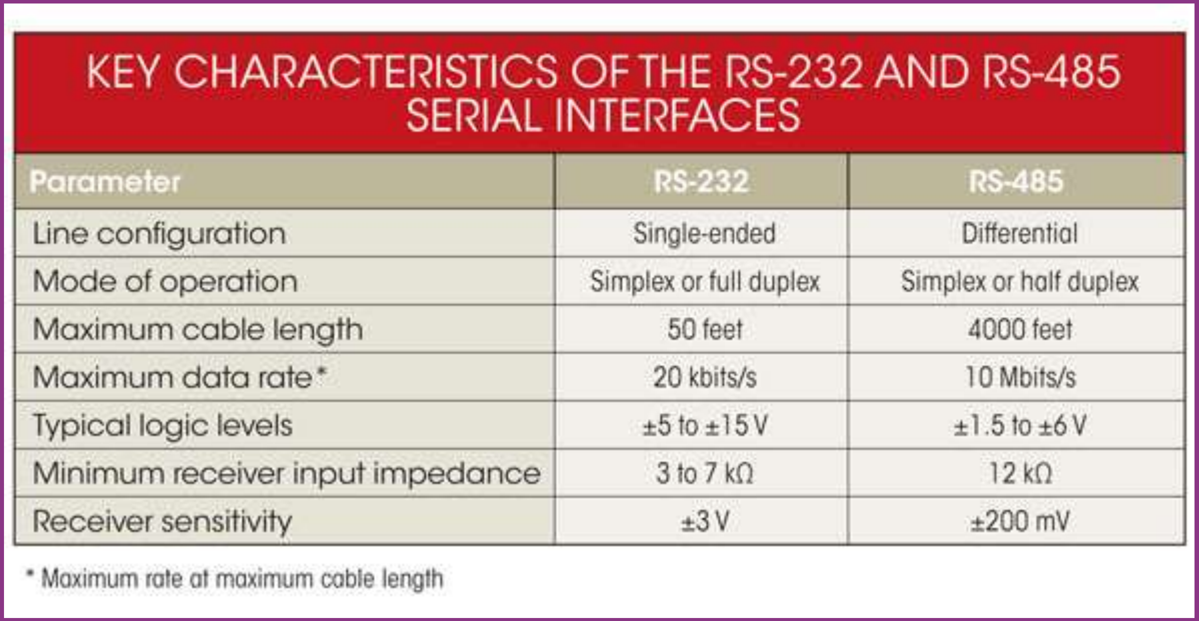


Early Protocols

- Signal Flags
- Morse Code
  - Telegraph
  - Signal lights
- Quindar Tones
  - Frequency shifting

Serial Communications

- **Serial communication is the process of sending data one bit at a time, sequentially, over a communication channel or computer bus. This is in contrast to parallel communication, where several bits are sent as a whole, on a link with several parallel channels.**
- **RS2332**
  - **2 wire**
  - **Peer to peer**
  - **2 devices**
- **RS484**
  - **2 wire**
  - **Multi-drop**
  - **32 devices**



KEY CHARACTERISTICS OF THE RS-232 AND RS-485 SERIAL INTERFACES

Parameter	RS-232	RS-485
Line configuration	Single-ended	Differential
Mode of operation	Simplex or full duplex	Simplex or half duplex
Maximum cable length	50 feet	4000 feet
Maximum data rate*	20 kbits/s	10 Mbits/s
Typical logic levels	±5 to ±15 V	±1.5 to ±6 V
Minimum receiver input impedance	3 to 7 kΩ	12 kΩ
Receiver sensitivity	±3 V	±200 mV

* Maximum rate at maximum cable length

Process Automation Protocols

- AS-i – Actuator-sensor interface, a low level 2-wire bus establishing power and communications to basic digital and analog devices
- BSAP – Bristol Standard Asynchronous Protocol, developed by Bristol Babcock Inc.
- CC-Link Industrial Networks – Supported by the CLPA
- CIP (Common Industrial Protocol) – can be treated as application layer common to DeviceNet, CompoNet, ControlNet and EtherNet/IP
- Controller Area Network utilised in many network implementations, including CANopen and DeviceNet
- ControlNet – an implementation of CIP, originally by Allen-Bradley
- DeviceNet – an implementation of CIP, originally by Allen-Bradley
- DF-1 - used by Allen-Bradley PLC-5, SLC-500, and MicroLogix class devices
- DirectNet – Koyo / Automation Direct[1] proprietary, yet documented PLC interface
- EtherCAT
- Ethernet Global Data (EGD) – GE Fanuc PLCs (see also SRTP)

Wikipedia

Process Automation Protocols

- EtherNet/IP – IP stands for "Industrial Protocol". An implementation of CIP, originally created by Rockwell Automation
- Ethernet Powerlink – an open protocol managed by the Ethernet POWERLINK Standardization Group (EPSG).
- FINS, Omron's protocol for communication over several networks, including ethernet.
- FOUNDATION fieldbus – H1 & HSE
- HART Protocol
- HostLink Protocol, Omron's protocol for communication over serial links.
- Interbus, Phoenix Contact's protocol for communication over serial links, now part of PROFINET IO
- MACRO Fieldbus - "Motion and Control Ring Optical" developed by Delta Tau Data Systems.
- MECHATROLINK – open protocol originally developed by Yaskawa, supported by the MMA.
- MelsecNet, supported by Mitsubishi Electric.
- Modbus PEMEX

Wikipedia

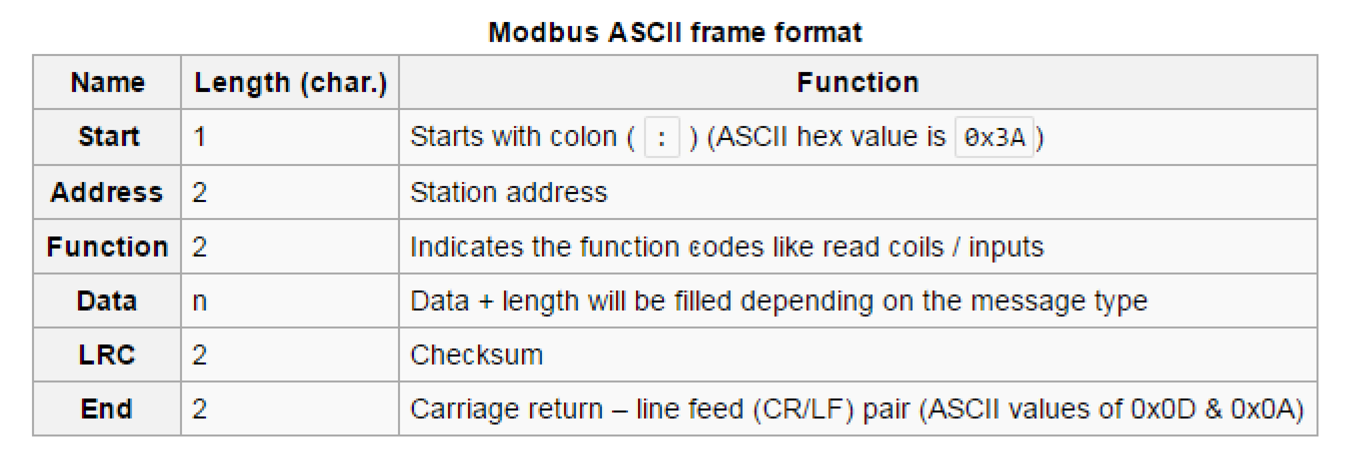
Process Automation Protocols

- Modbus Plus
- Modbus RTU or ASCII or TCP
- OSGP – The Open Smart Grid Protocol, a widely use protocol for smart grid devices built on ISO/IEC 14908.1
- Optomux – Serial (RS-422/485) network protocol originally developed by Opto 22 in 1982. The protocol was openly documented and over time used for industrial automation applications.
- PieP – An Open Fieldbus Protocol
- Profibus – by PROFIBUS International.
- PROFINET IO
- RAPIEnet – Real-time Automation Protocols for Industrial Ethernet
- Honeywell SDS – Smart Distributed System – Originally developed by Honeywell. Currently supported by Holjeron.
- SERCOS III, Ethernet-based version of SERCOS real-time interface standard
- SERCOS interface, Open Protocol for hard real-time control of motion and I/O
- GE SRTP – GE Fanuc PLCs
- Sinec H1 – Siemens

Wikipedia

Modbus Protocol

- Modbus is a serial communications protocol originally published in 1979 for use with its programmable logic controllers (PLCs).
- Simple and robust, it has since become a de facto standard communication protocol.
- The main reasons for the use of Modbus in the industrial environment are:
  - developed with industrial applications in mind
  - openly published and royalty-free
  - easy to deploy and maintain



Modbus ASCII frame format

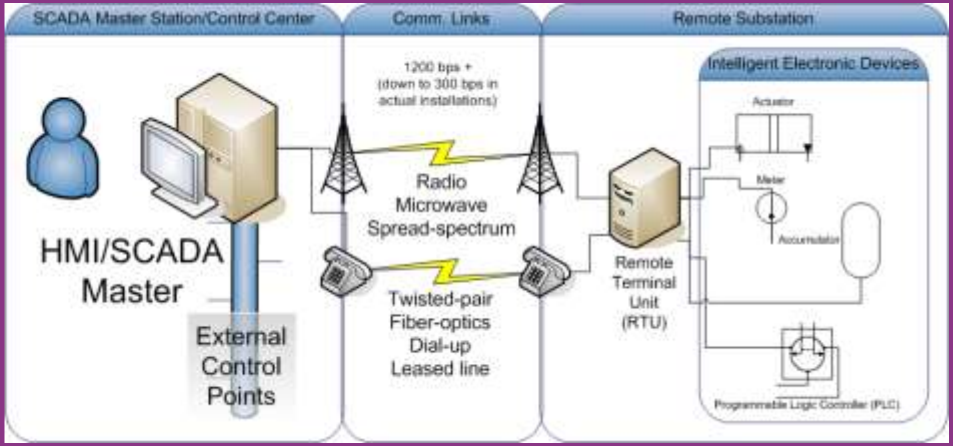
Name	Length (char.)	Function
Start	1	Starts with colon (`:`) (ASCII hex value is `0x3A`)
Address	2	Station address
Function	2	Indicates the function codes like read coils / inputs
Data	n	Data + length will be filled depending on the message type
LRC	2	Checksum
End	2	Carriage return – line feed (CR/LF) pair (ASCII values of 0x0D & 0x0A)

Modbus Limitations

- Modbus was designed in the late 1970s.
- No standard way exists for a node to find the description of a data object
- Since Modbus is a master/slave protocol, there is no way for a field device to "report by exception"
- Modbus is restricted to addressing 247 devices on one data link
- Modbus transmissions must be contiguous which limits the types of remote communications devices
- Modbus protocol itself provides no security against unauthorized commands or interception of data.
- Customized Modbus

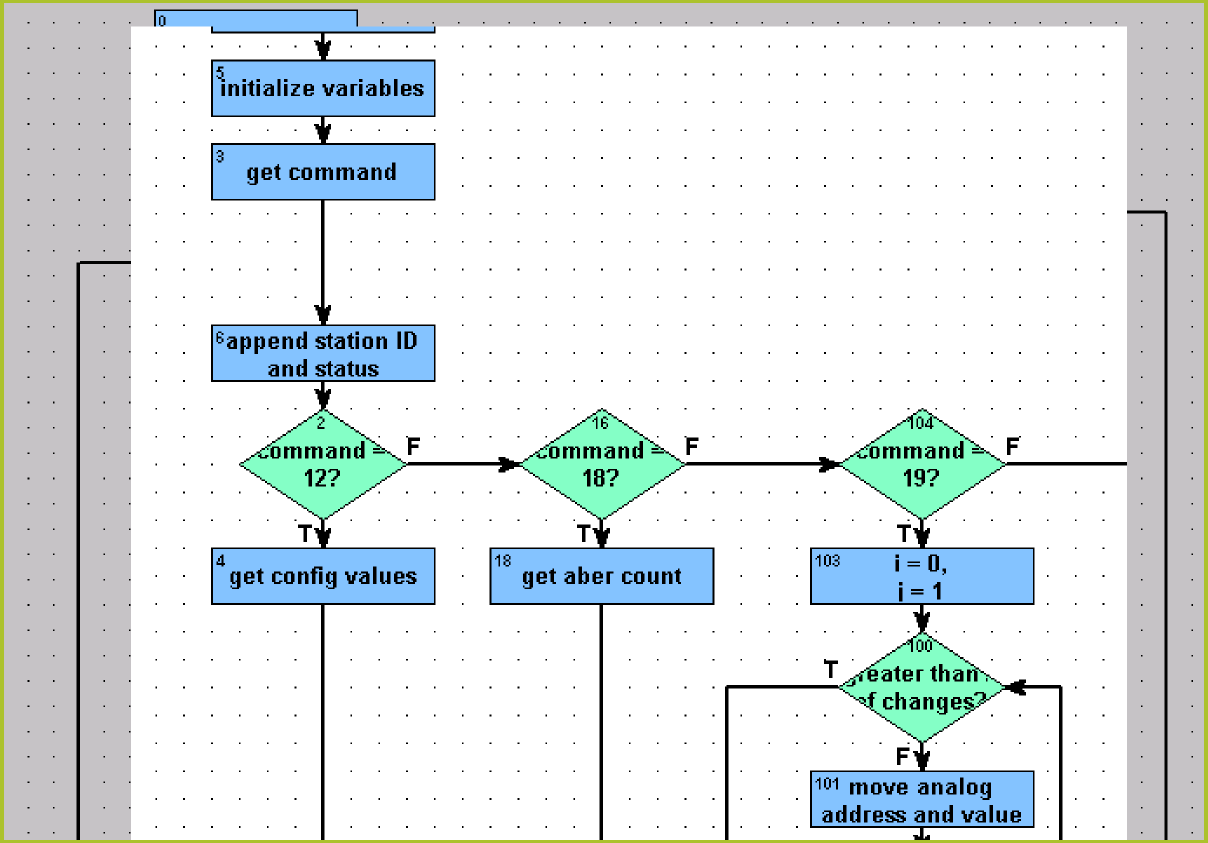
DNP3

- DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies
- Master to remote site(s)
- Static data – current valve
- Event data – a significant event(s)
- Event priority
- Event timestamp
- Open protocol & free
- "Integrity Poll"



Roll Your Own Protocol

- Special functionality
- Migration for one protocol or system to another
- Unpublished

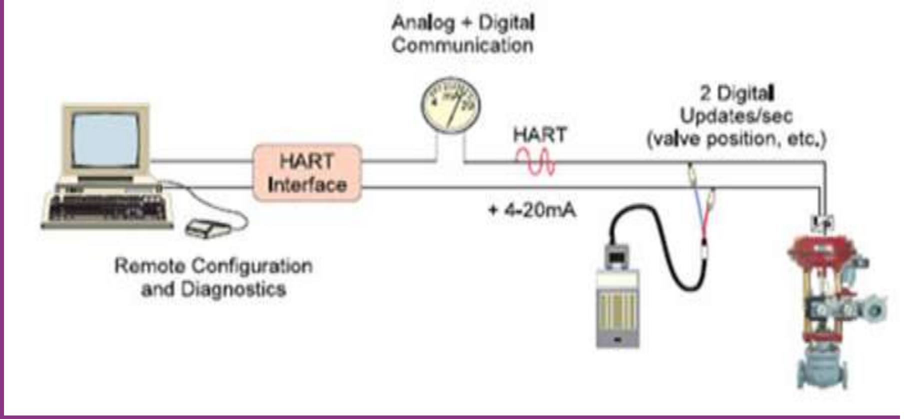


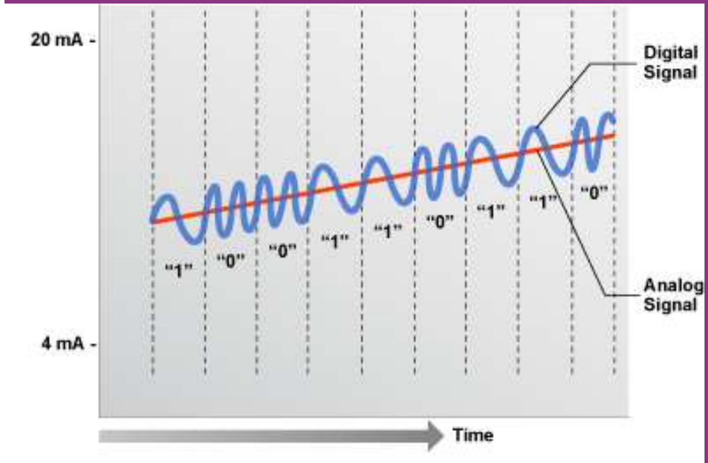
HART Protocol

- Digital Capability
  - Access to all instrument parameters & diagnostics – Device setup
  - Supports multivariable instruments
  - On-line device status
  - Advanced diagnostics
- Analog Compatibility
  - Simultaneous analog & digital communication
  - Compatible with existing 4-20 mA equipment & wiring Interoperability
  - Fully open standard
  - Common Command and data structure
  - Enhanced by Device Description Language
- Availability
  - Field proven technology with more than 1,400,000 installations
  - Large and growing selection of products
  - Used by more smart instruments than any other.
- Limitation
  - Non-Digital PID

Hart Protocol

- 2-Wire connection
- Frequency Shift Keying (FSK) standard to superimpose digital communication signals at a low level on top of the 4-20mA


Analog + Digital Communication
HART
2 Digital Updates/sec (valve position, etc.)
HART Interface
+ 4-20mA
Remote Configuration and Diagnostics

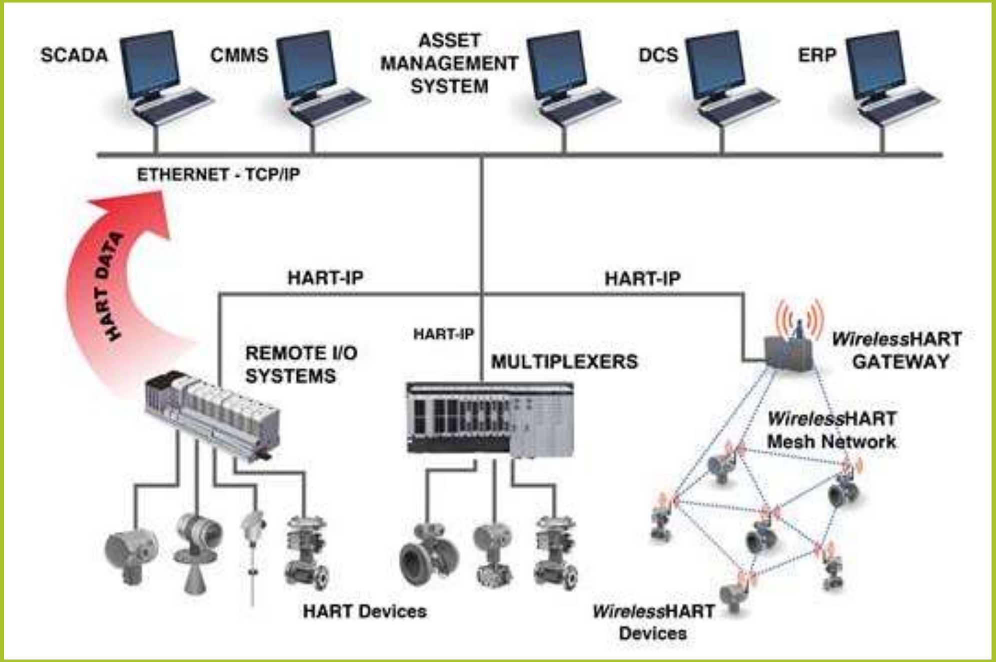


Note: Drawing not to scale

Digital over Analog

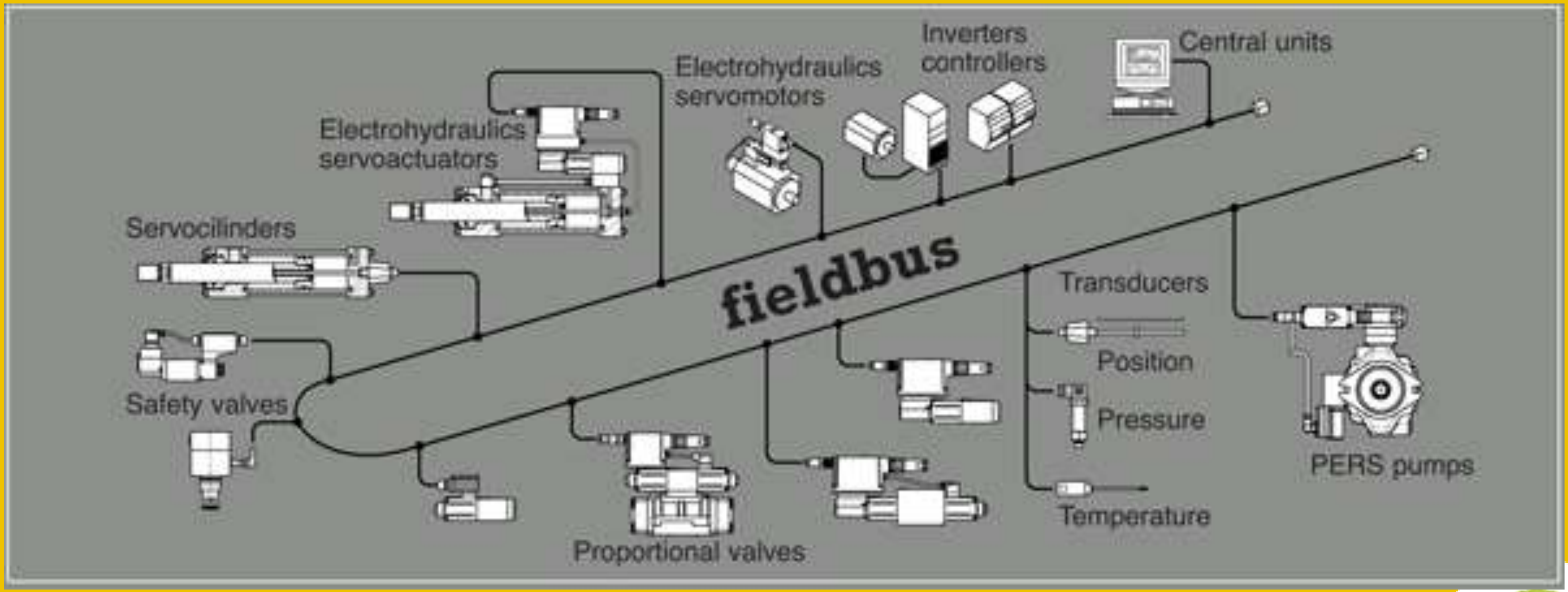
Hart-IP

- Hart functionality encapsulated inside an IP packet
- Faster speed
- Redundancy
- Power over Ethernet (PoE) for devices
- Better integration
- No translation process



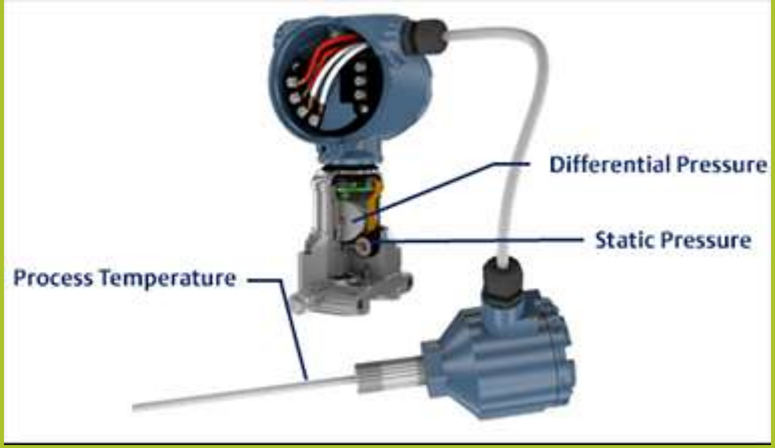
Fieldbus

- A fieldbus is an all-digital, serial two-way, multi-drop communication System.
- H1 link (31.25kbps) interconnects field equipment (Sensors, Actuators & I/O).
- HSE (High Speed Ethernet, 100mbps) provides integration of high speed controllers, subsystems and data servers and workstation.
- More data is available
- Expanded View of Process & Instrumentation



Fieldbus Advantages

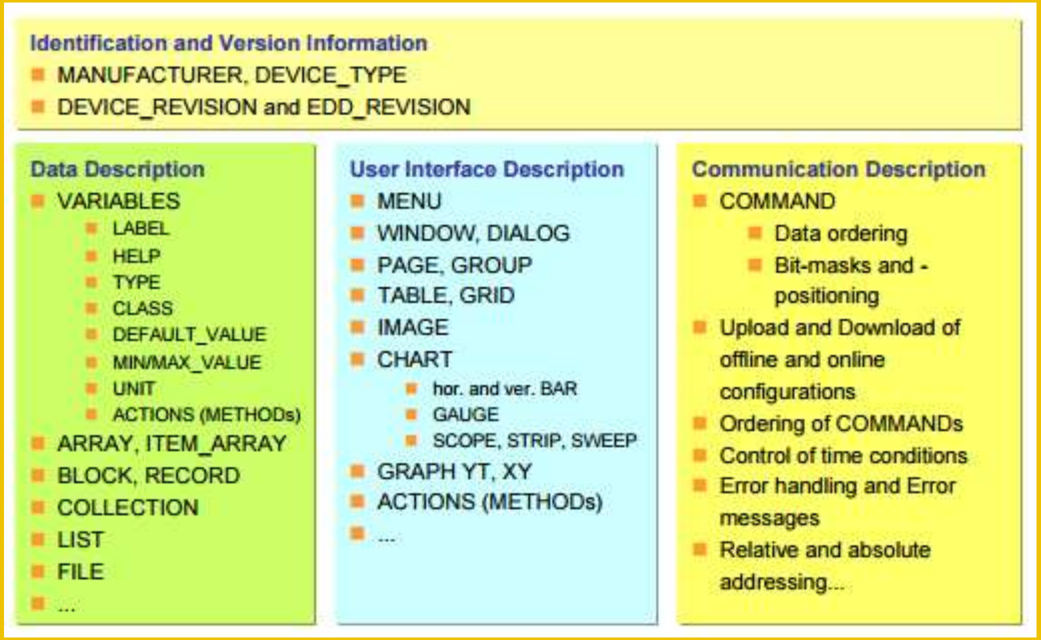
- Wide instrumentation vendor support
- Supported by most automation system suppliers
- Less wiring than 4 – 20 mA
- Multivariable instruments
- More power capability
- Advanced diagnostics



Fieldbus.org

EDDL

- EDDL (Electronic Device Description Language) was created as DD (device description) in the early 1990s at the dawn of fieldbus technology as a way to describe devices.
- The DD tells the system what function blocks are present in a device type, what parameters are available, the data types of those parameters and the default values and permitted ranges of these parameters. This data is used by the system to understand a device even before the device is present in the system.



Identification and Version Information

- MANUFACTURER, DEVICE_TYPE
- DEVICE_REVISION and EDD_REVISION

Data Description

- VARIABLES
  - LABEL
  - HELP
  - TYPE
  - CLASS
  - DEFAULT_VALUE
  - MIN/MAX_VALUE
  - UNIT
  - ACTIONS (METHODs)
- ARRAY, ITEM_ARRAY
- BLOCK, RECORD
- COLLECTION
- LIST
- FILE
- ...

User Interface Description

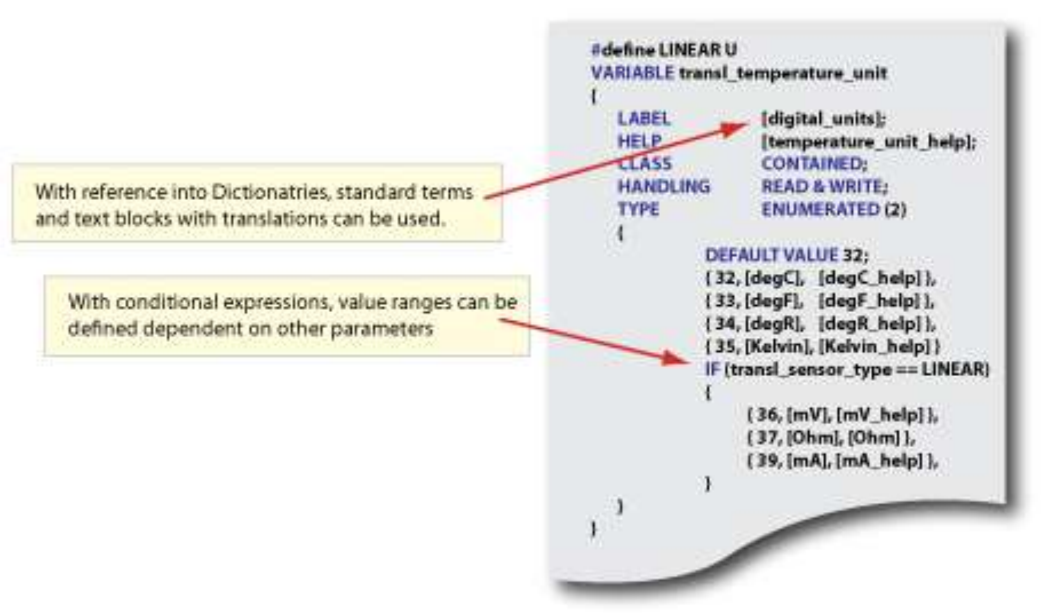
- MENU
- WINDOW, DIALOG
- PAGE, GROUP
- TABLE, GRID
- IMAGE
- CHART
  - hor. and ver. BAR
  - GAUGE
  - SCOPE, STRIP, SWEEP
- GRAPH YT, XY
- ACTIONS (METHODs)
- ...

Communication Description

- COMMAND
  - Data ordering
  - Bit-masks and -positioning
- Upload and Download of offline and online configurations
- Ordering of COMMANDs
- Control of time conditions
- Error handling and Error messages
- Relative and absolute addressing...

EDDL

- EDDL is endorsed by four major foundations – Fieldbus Foundation – HART Communication Foundation – Profibus (PNO) – The OPC Foundation
- EDDL / EDDs are Independent from: – Operating systems and versions – DCS Platforms – Communication and interface paths
- An EDD is the computer readable file written in Electronic Device Description Language (EDDL) that describes the data in a field device
- It is the file that the Host application reads in order to learn how to retrieve information from the field device



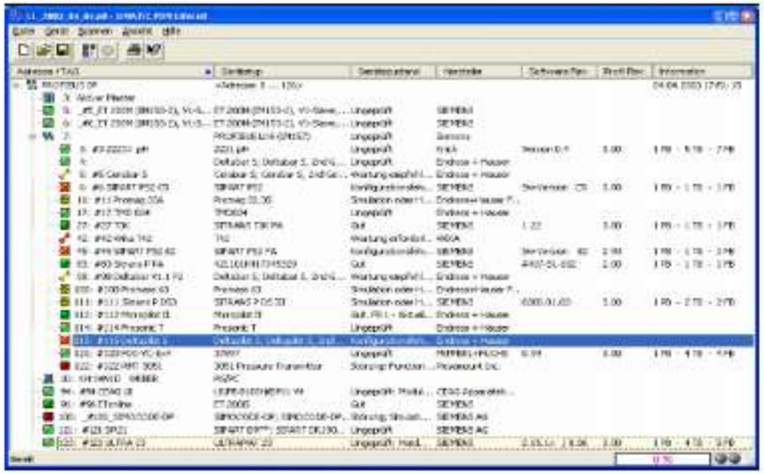
With reference into Dictionatries, standard terms and text blocks with translations can be used.

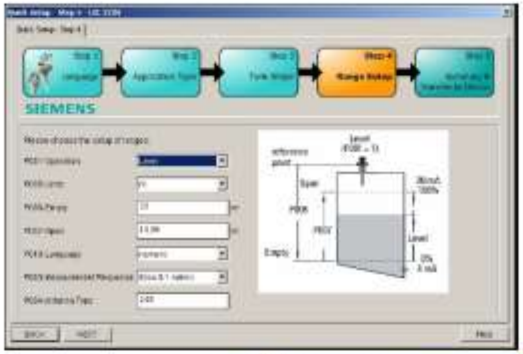
With conditional expressions, value ranges can be defined dependent on other parameters

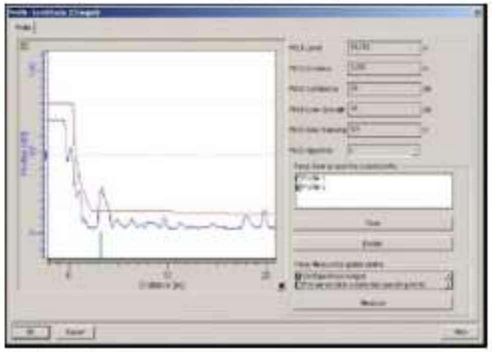
```
#define LINEAR U
VARIABLE transl_temperature_unit
{
    LABEL           [digital_units];
    HELP            [temperature_unit_help];
    CLASS           CONTAINED;
    HANDLING        READ & WRITE;
    TYPE            ENUMERATED (2)
    {
            DEFAULT VALUE 32;
            { 32, [degC],   [degC_help] },
            { 33, [degF],   [degF_help] },
            { 34, [degR],   [degR_help] },
            { 35, [Kelvin], [Kelvin_help] }
            IF (transl_sensor_type == LINEAR)
            {
                  { 36, [mV], [mV_help] },
                  { 37, [Ohm], [Ohm] },
                  { 39, [mA], [mA_help] },
            }
    }
}
```

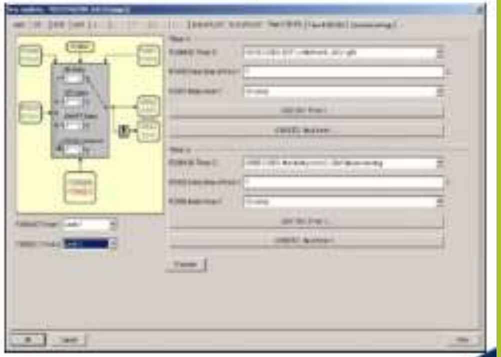
EDD

- One tool for all devices – Common transparent data base – A new device just a new EDD
- Build in state of the art graphics – Trends, Bar graphs



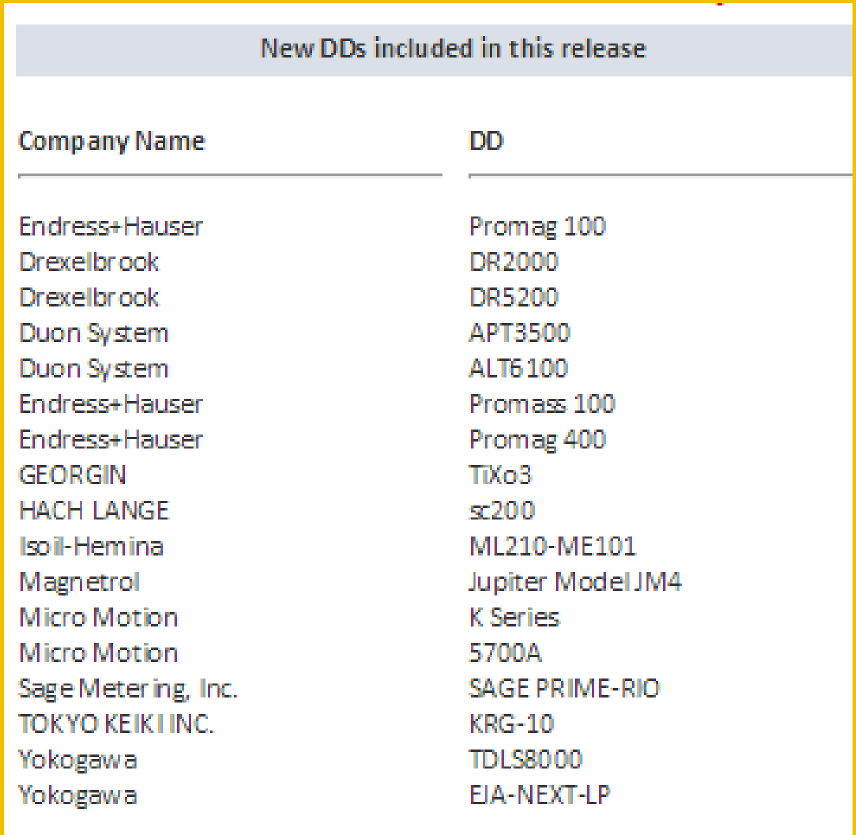






EDD Library

- Basic parameters available for new devices but may need to get latest device definition file from vendor or Hart.org
- EDD file loaded onto PC, communicator, PLC, etc.

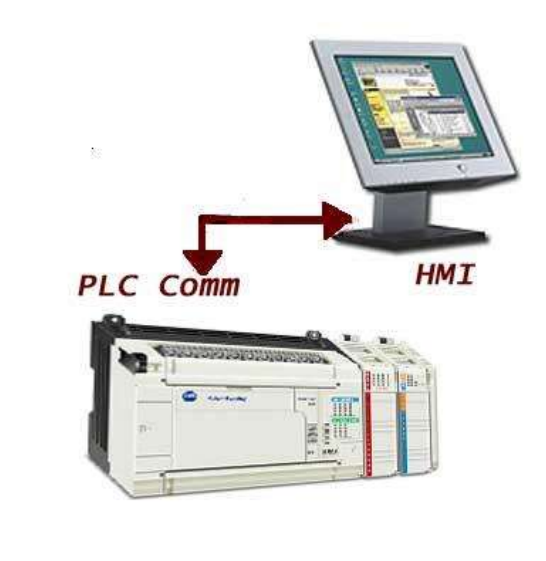


New DDs included in this release

Company Name	DD
Endress+Hauser	Promag 100
Drexelbrook	DR2000
Drexelbrook	DR5200
Duon System	APT3500
Duon System	ALT6100
Endress+Hauser	Promass 100
Endress+Hauser	Promag 400
GEORGIN	TiXo3
HACH LANGE	sc200
Isoil-Hemina	ML210-ME101
Magnetrol	Jupiter Model JM4
Micro Motion	K Series
Micro Motion	5700A
Sage Metering, Inc.	SAGE PRIME-RIO
TOKYO KEIKI INC.	KRG-10
Yokogawa	TDLS8000
Yokogawa	EJA-NEXT-LP

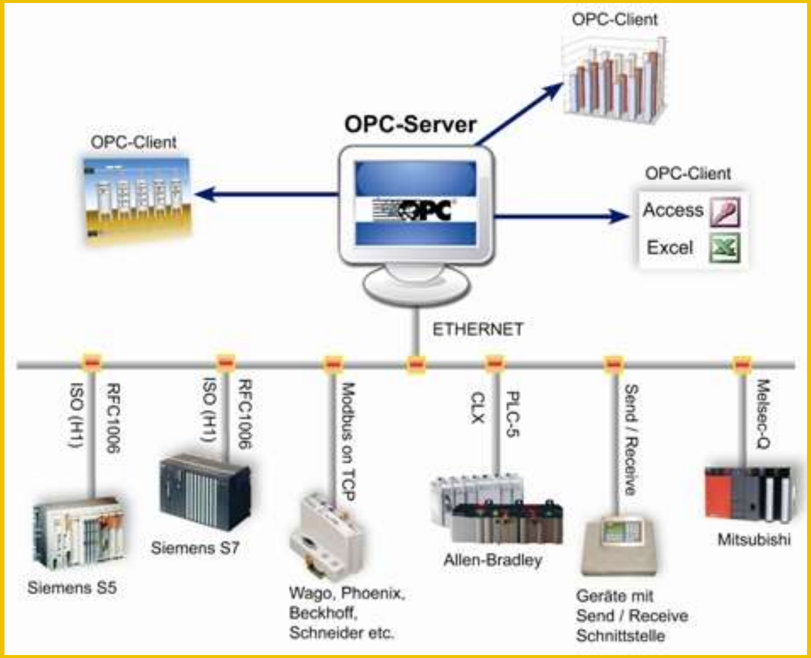
OPC

- OLE for Process Control (OPC), now known as Open Platform Communications. The standard specifies the communication of real-time plant data between control devices from different manufacturers.
- OPC Data Access is a group of standards that provides specifications for communicating real-time data from data acquisition devices such as PLCs to display and interface devices like Human-Machine Interfaces (HMI). The specifications focus on the continuous communication of data.
- Specifications for:
  - Data Access
  - Historical Data Access
  - Alarms and Events
  - XML-Data Access
  - Data eXchange
    - Server to Server
  - Complex Data
    - Binary objects and XML documents
  - Security
  - Batch



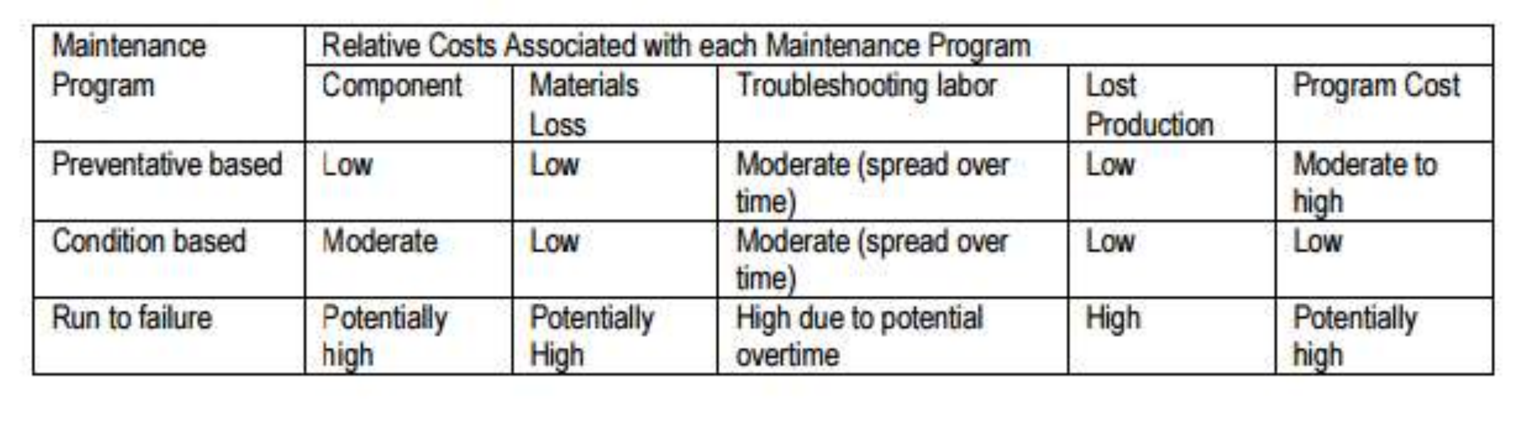
OPC

- OPC servers provide a method for many different software packages (so long as it is an OPC Client) to access data from a process control device, such as a PLC or DCS. Traditionally, any time a package needed access to data from a device, a custom interface, or driver, had to be written.
- The purpose of OPC is to define a common interface that is written once and then reused by any business, SCADA, HMI, or custom software packages.
- Ethernet or serial communications access



Setup, Maintenance, and Trouble Shooting with Automation Protocols

- Extends the useful lifecycle of assets decreasing the need for capital replacements.
- Enhances the efficiency of equipment keeping them running more efficiently and lowering power expenses.
- Enhances the performance of assets by increasing uptime.
- Enhances customer (internal or external) service because maintenance teams have less unplanned maintenance and can respond quicker to new problems.
- Contributes positively to the reputation of companies



Maintenance Program	Relative Costs Associated with each Maintenance Program				
	Component	Materials Loss	Troubleshooting labor	Lost Production	Program Cost
Preventative based	Low	Low	Moderate (spread over time)	Low	Moderate to high
Condition based	Moderate	Low	Moderate (spread over time)	Low	Low
Run to failure	Potentially high	Potentially High	High due to potential overtime	High	Potentially high

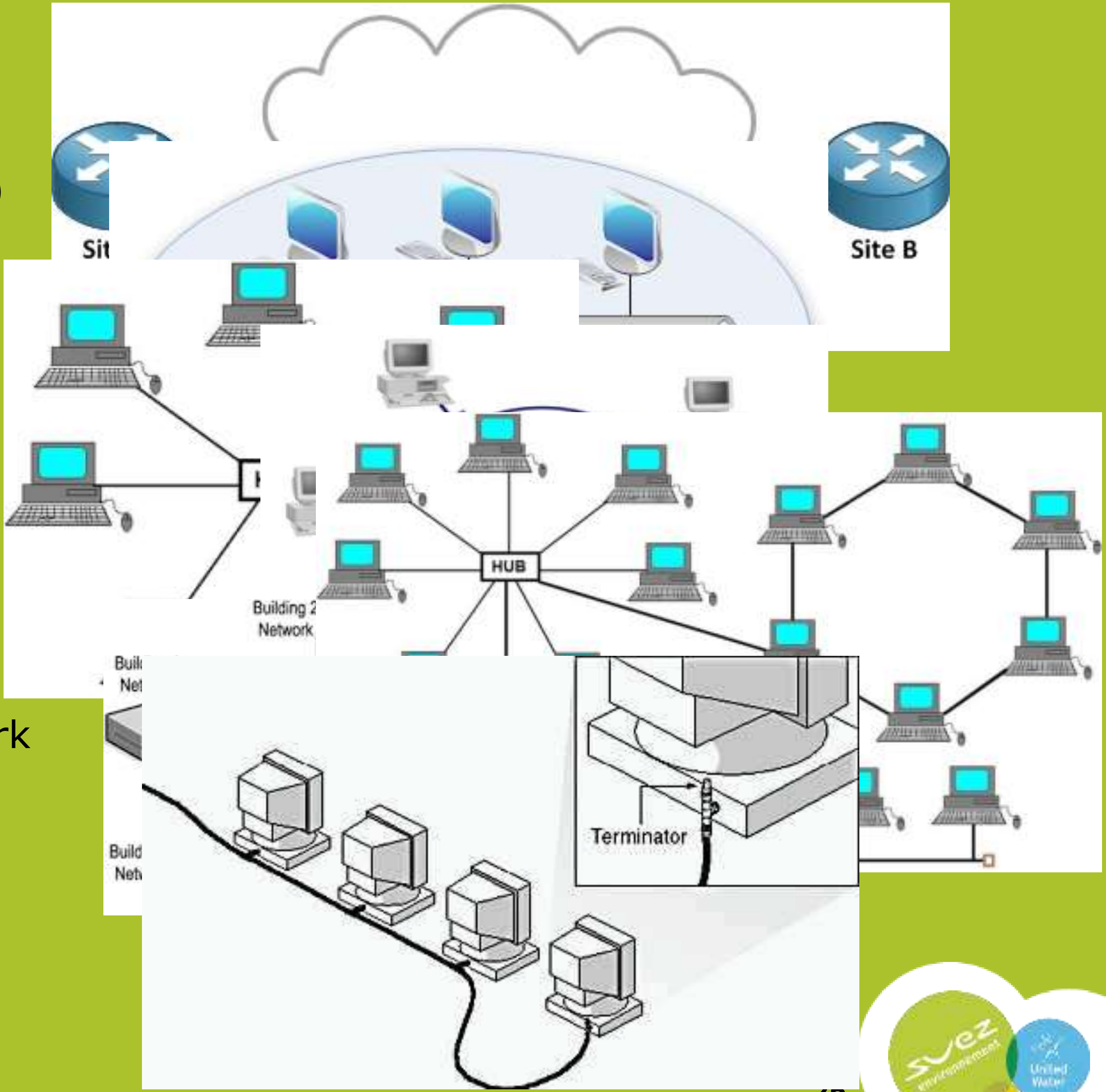
What is a Communications Topology?

- A Communications topology is the arrangement of the various elements (links, nodes, etc.) of a computer network
- May be depicted physically or logically
- Physical topology is the placement of the various components of a network
- Logical topology illustrates how data flows within a network
- The study of network topology recognizes eight basic topologies: point-to-point, bus, star, ring or circular, mesh, tree, hybrid, or daisy chain

Wikipedia

Types of Communications Topologies

- Point-to-point
  - Permanent (dedicated)
  - Switched
- Bus
  - Linear bus
  - Distributed bus
- Star
  - Extended star
  - Distributed Star
- Ring
- Mesh
  - Fully connected network
  - Partially connected
- Tree
- Hybrid
- Daisy chain



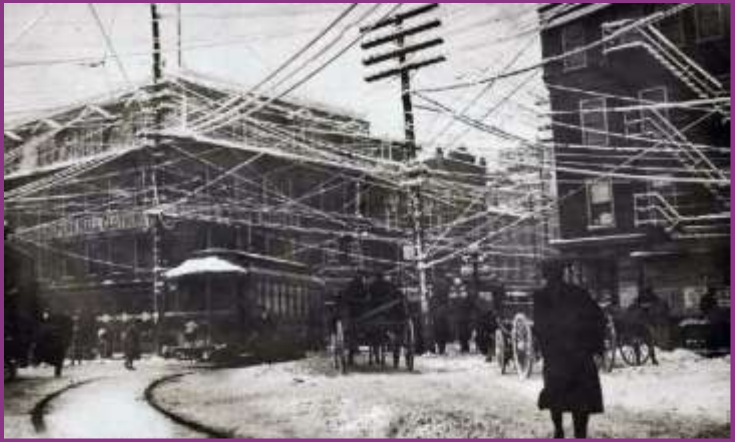
What is Communication Media?

- Communication media refers to the means of delivering and receiving data or information. In telecommunication, these means are transmission and storage tools or channels for data storage and transmission.
- Wire pairs
- Coaxial cable
- RF transmission
  - Cellular
  - Wifi
  - Analog
  - Digital
- Fiber optics

Techopedia

Telephone Communications

- Dial-up
  - Infrequent polling
  - Maintenance
- Bell 202
  - 1200 Kbp
- T1
  - Up to 1.5 Mb
- Frame-Relay
- DSL
  - 3+ Mb
- PPP
- MPLS
- Security
- Service Calls
- 3rd party provider
  - Last mile provider



Radio Communications

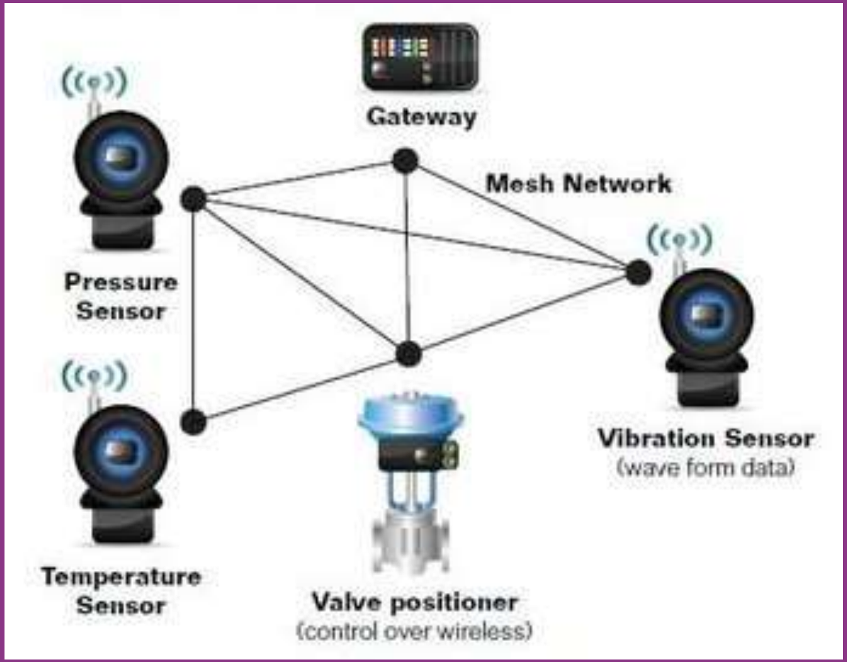
- Frequency
  - Lower the frequency the more forgiving
  - Higher the frequency the more data
- Bandwidth
  - Narrowband
- Polling
  - Master / Slave
  - Exception
- Analog/Digital
- IP radios
  - Routing
- Serial Radio
- Fixed license
- Unlicensed
- Costs

Cellular Communication M2M

- Coverage – Good overlap of sign in large metro areas but may be spotty in rural areas.
- Maintained by the cellular provider
- Discrete in nature – No antenna pole
- Data traffic within these cellular networks is set up as a private network within the cellular provider's system, ensuring the security of your communication.
- Speed
  - 2G 60-95 kbps
  - 3G 350-600 kbps
  - 4G 10-12 MB
- Reliability
  - What about during a event?
- Redundant communications
- Data limits
- Costs

Wireless Sensors

- Self- Organizing technology in which field devices create a wireless network topology.
- Communicate around obstacles
- Some require power wiring, but most use battery power
- Secure and reliable
- Monitor and control capability



Wireless Sensors

- Can store and forward data between device
- Wireless transmitters modules can be used with legacy 2 and 4 wire devices
- Can be installed virtually anywhere using battery power – hard to reach areas
- Good for locations far away from existing power or network wiring or too expensive to wire up
- Good for keeping a project on schedule and budget due to adding additional I/O
- Can reduce fixed asset inspection costs
- No need to modify existing wiring

Summary

- What is a communications protocol
- Requirements of a protocol
- Reviewed several types of protocols
  - Messaging
  - Process automation
  - Data retrieval and display
- Automation Protocols for setup, maintenance, and trouble-shooting
- What is a communications topology
  - Bus
  - Star
  - Mesh
- Communications media
- Telephone
- Radio
- Cellular
- Wireless Devices

Questions