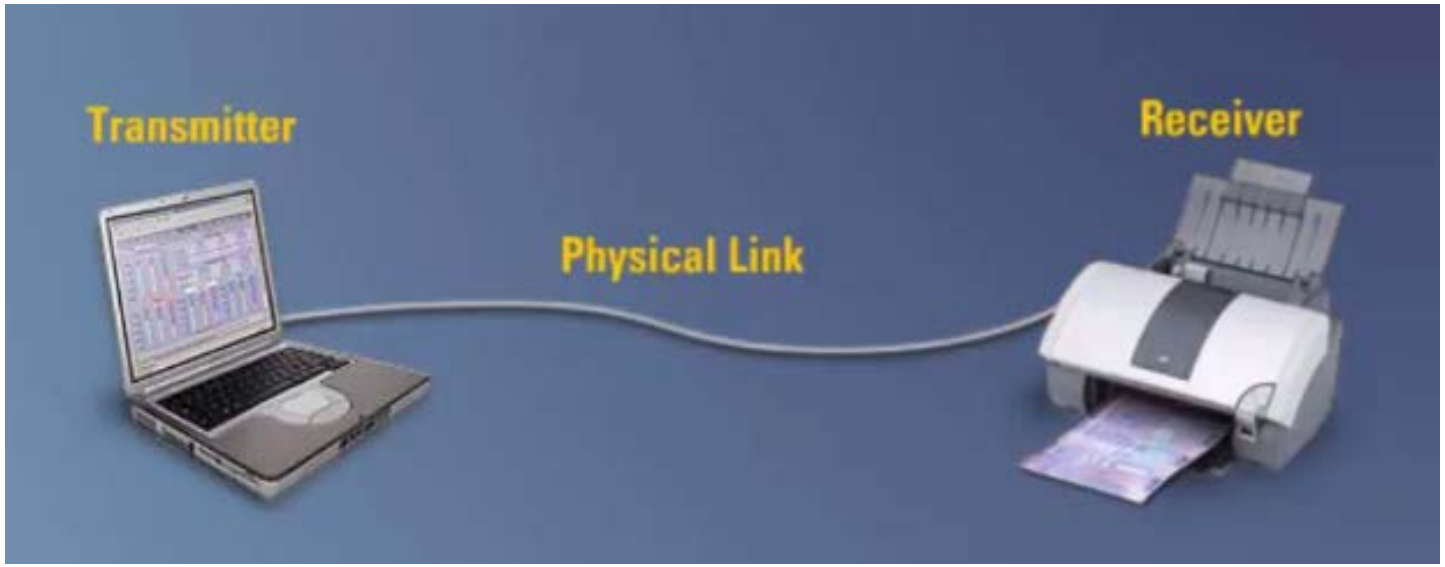
AGENDA

- Introduction – Basics of Data Communication
- Serial Communication
- Ethernet Communication
- Modbus Protocol
- DNP Protocol

Data Communication



Communication Link

- Symplex
- Half-Duplex
- Full-Duplex

Broadband

- Many different channels
- Ex: Home cable

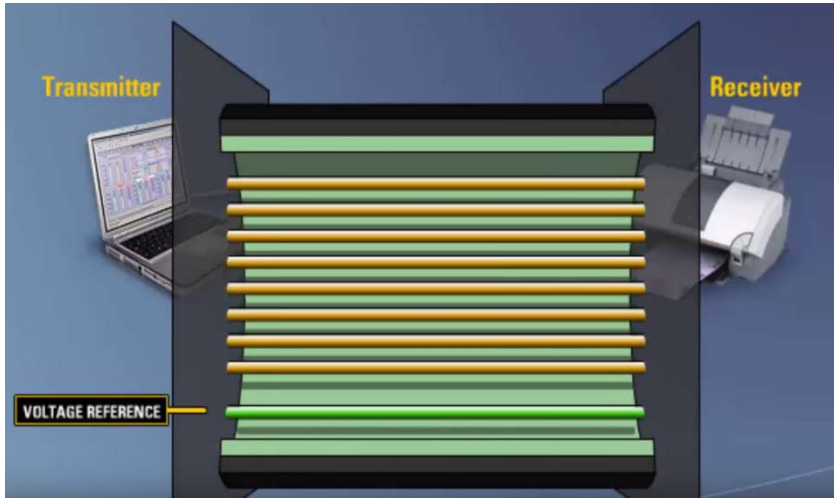
Baseband

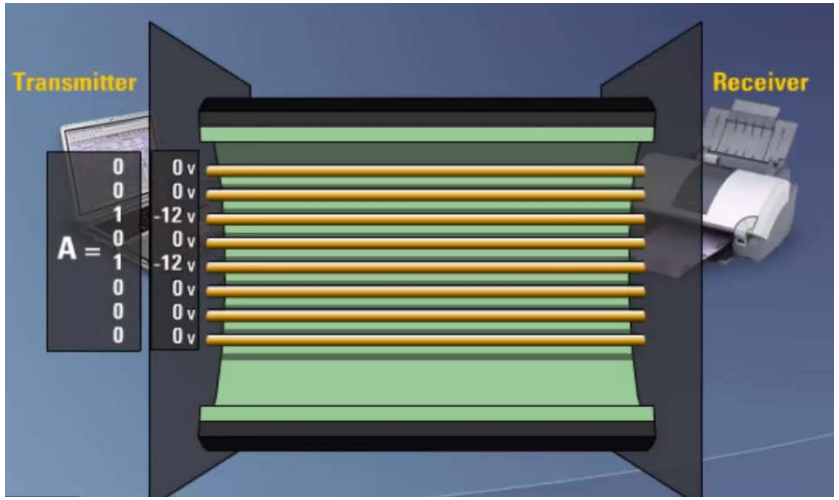
- Single channel
- Entire bandwidth of link transmits one bit

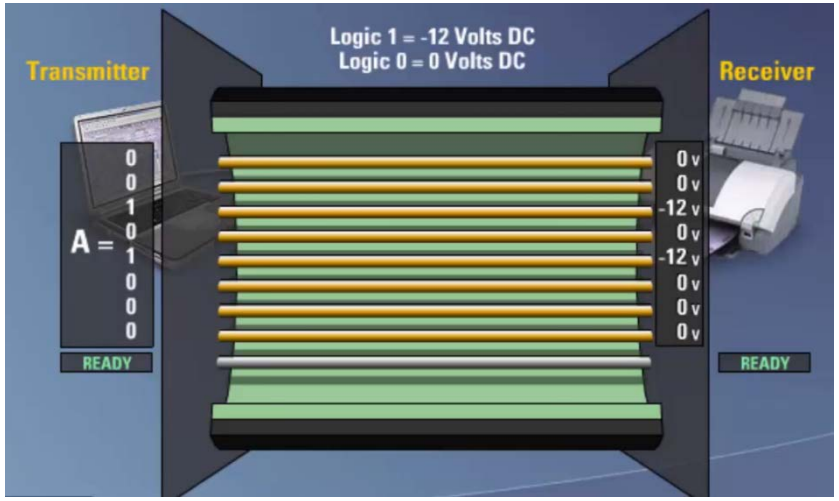
Character Encoding

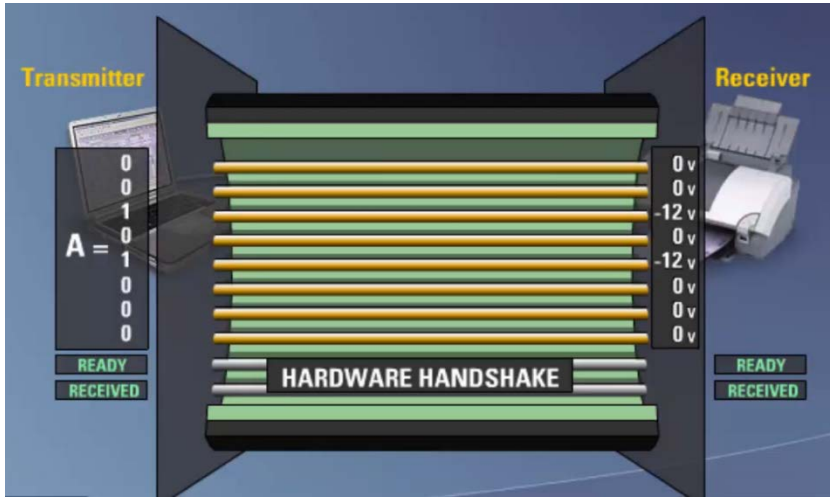
- ASCII
  - Ex A = 00101000
- Hexadecimal
  - Base of 16
  - Digits 0-9 and letters A-F

PARALLEL COMMUNICATION



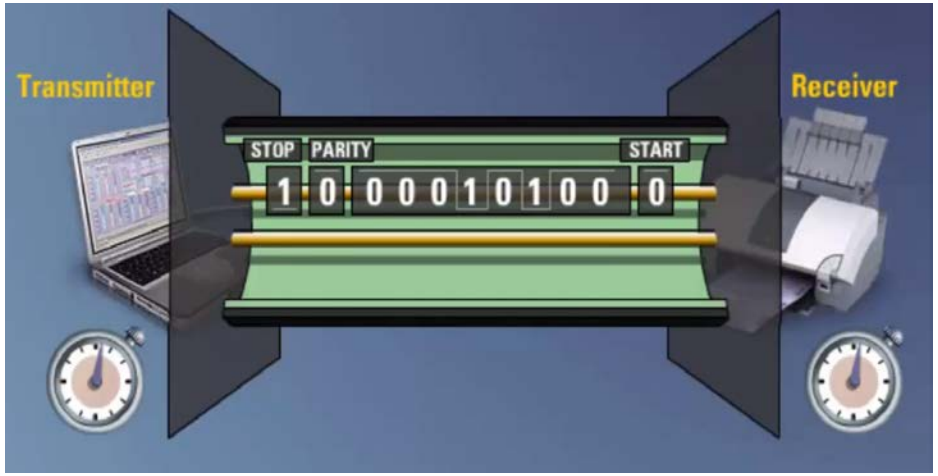






SERIAL COMMUNICATION

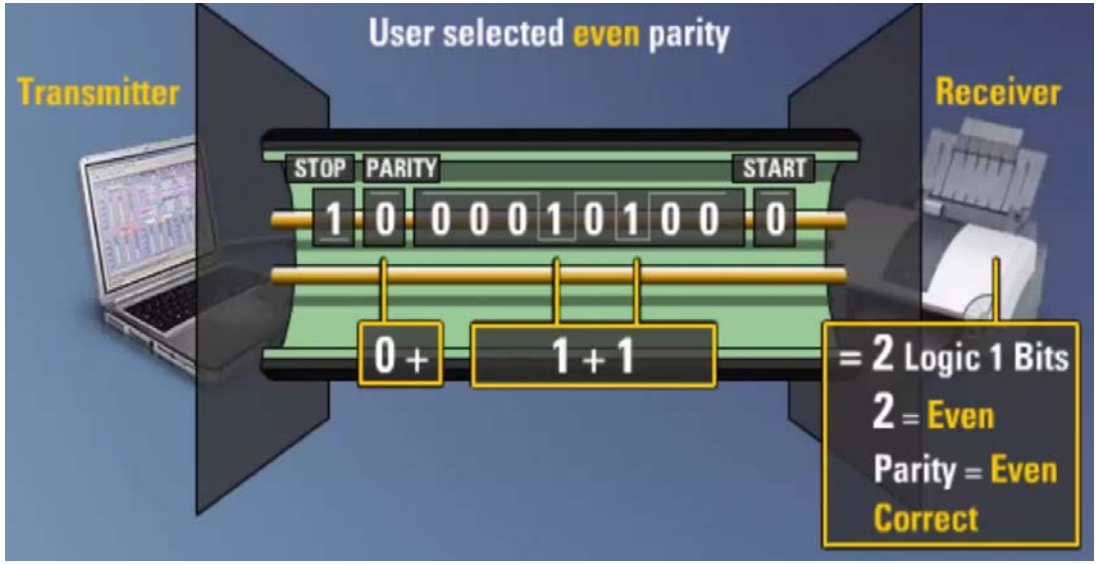
- Only 2 wires are required between transmitter and receiver
- 8 electrical on/off voltage signals are sent in a sequence w.r.t a time base
- Data transfer is done bit by bit arranged in a particular format

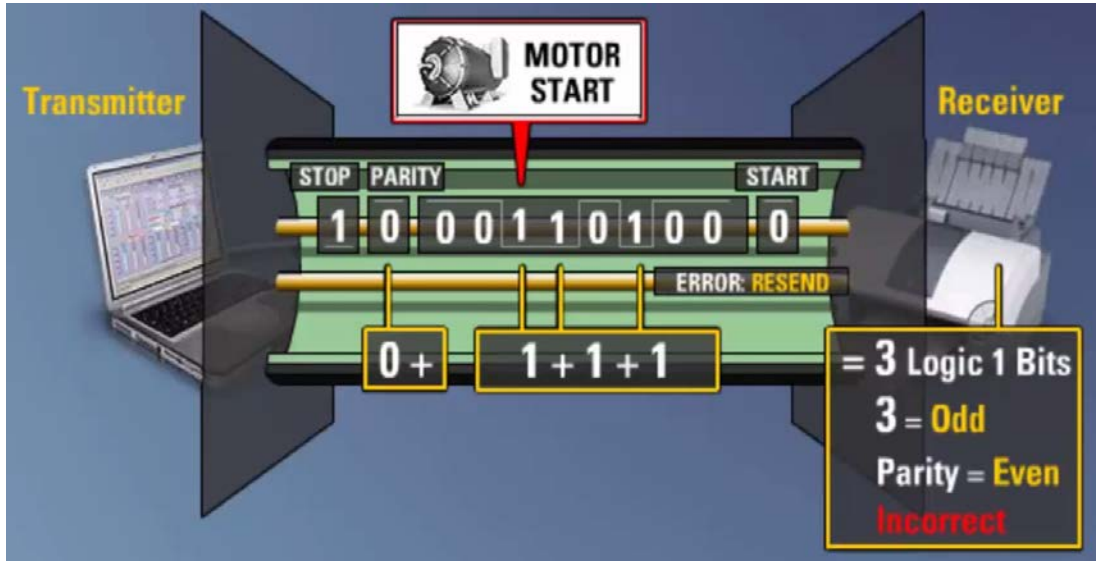


- Baud Rate
  - A measure of how fast serial data is moving between devices per second
- Data Packet
  - Characters transmitted one after the other in short bursts.
  - Contains address, data and error check

Parity Error

- Errors inevitably occur in the transfer of data due to noise and timing errors
- Parity error checking is a very simple form of error detection
- Limited to detection of a single bit error
- User can use even or odd parity





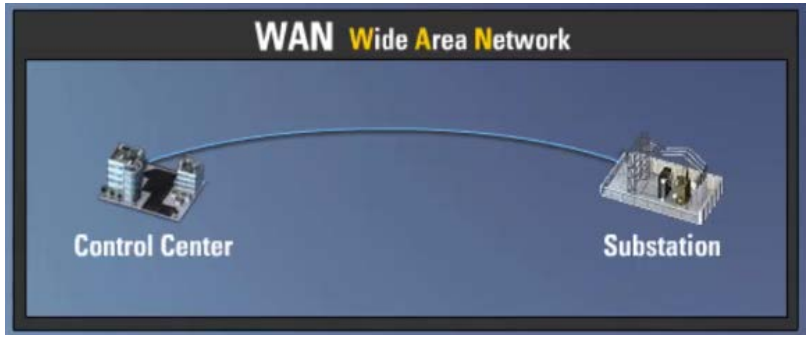
NETWORKS

- The transfer of bits in a communication systems using on/off voltages requires a tightly controlled electrical environment
- For data communication across short distances between components – Parallel communication links
- For data communication with external devices located some distance away has electrical noise - Serial communication such as LAN

NETWORKS


LAN


MAN Metropolitan Area Network
LAN
LAN
LAN


WAN Wide Area Network
Control Center
Substation

Network Topologies

- SCADA communication topologies classification:
  - Physical Topology: Physical connection of wires between the devices in a network.
  - Logical Topology: Refers to how the information is through the network among the devices.
  - In many instances, the logical topology is same as the physical topology.
- Physical topologies:
  - Point to point and multi-point (multi-drop)
  - Bus topology
  - Ring topology
  - Star topology
  - Mesh topology

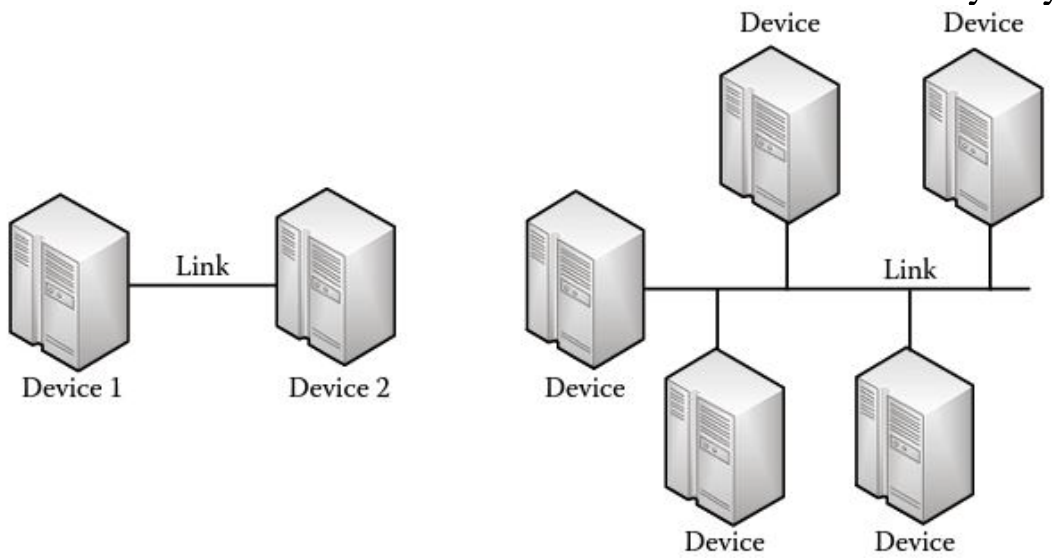
Network Topologies

Point to point

- Dedicated communication link is used to connect two devices
- Whole capacity of the link is used by the two devices.

Multi-point (multi-drop)

- Single communication link is shared by more than two devices.
- Time sharing: Specific time slots are allotted for each device.
- Spatial sharing: The devices use the channel simultaneously by sharing the channel capacity.

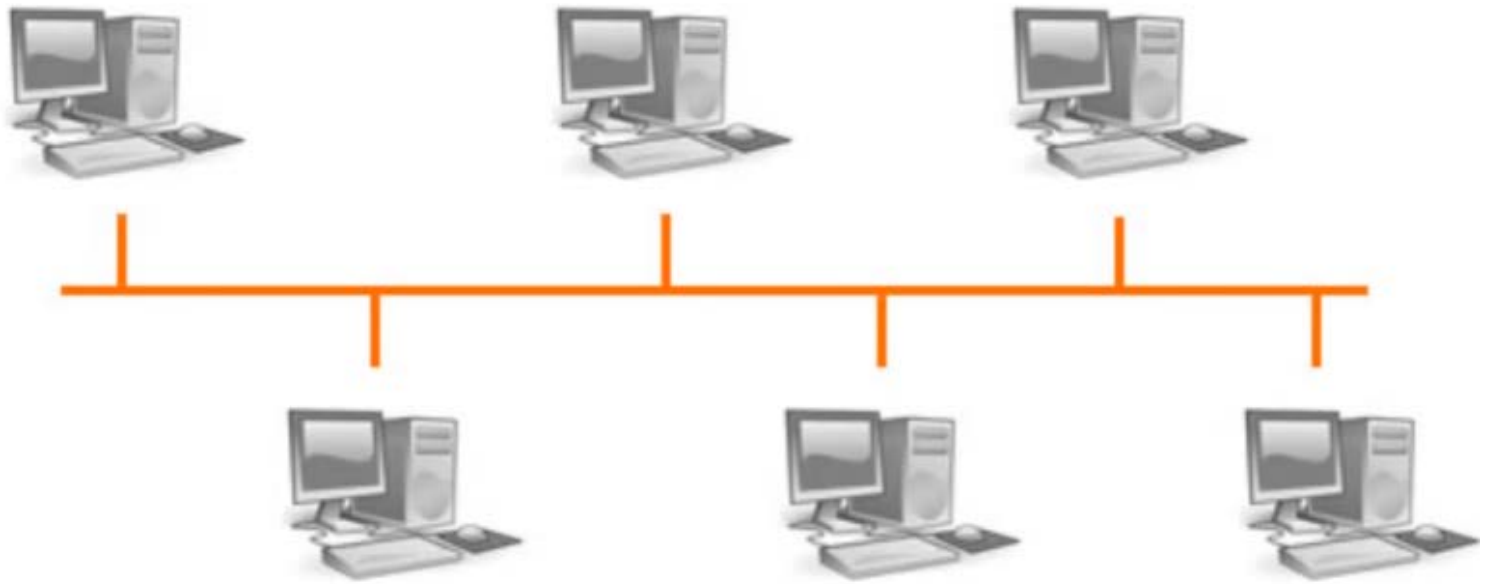


Point to point Multi-point

NETWORK TOPOLOGIES

Bus topology

- Commonly used for master station communication
- Each node is connected to a single or redundant bus that carries the message
- Advantages: Cost effective, reliable and easy to expand
- Disadvantages: Bus failure and delay in message transmission during heavy traffic.



NETWORK TOPOLOGIES

- Ring topology
- All the nodes including the master form a ring

Open and Closed

Closed

- Specific to one manufacturer
- Work with specific hardware connections and protocols
- Developed before standardization

Open

- Confirm to specification and guidelines, which are open to all
- Updated on frequent basis
- Take advantage of latest hardware and software technologies
- Optimal configuration: All devices directly connected to the LAN eliminating the need for a relaying device (data concentrator and delays)
- Support is more common with increase in power of modern microprocessor based devices

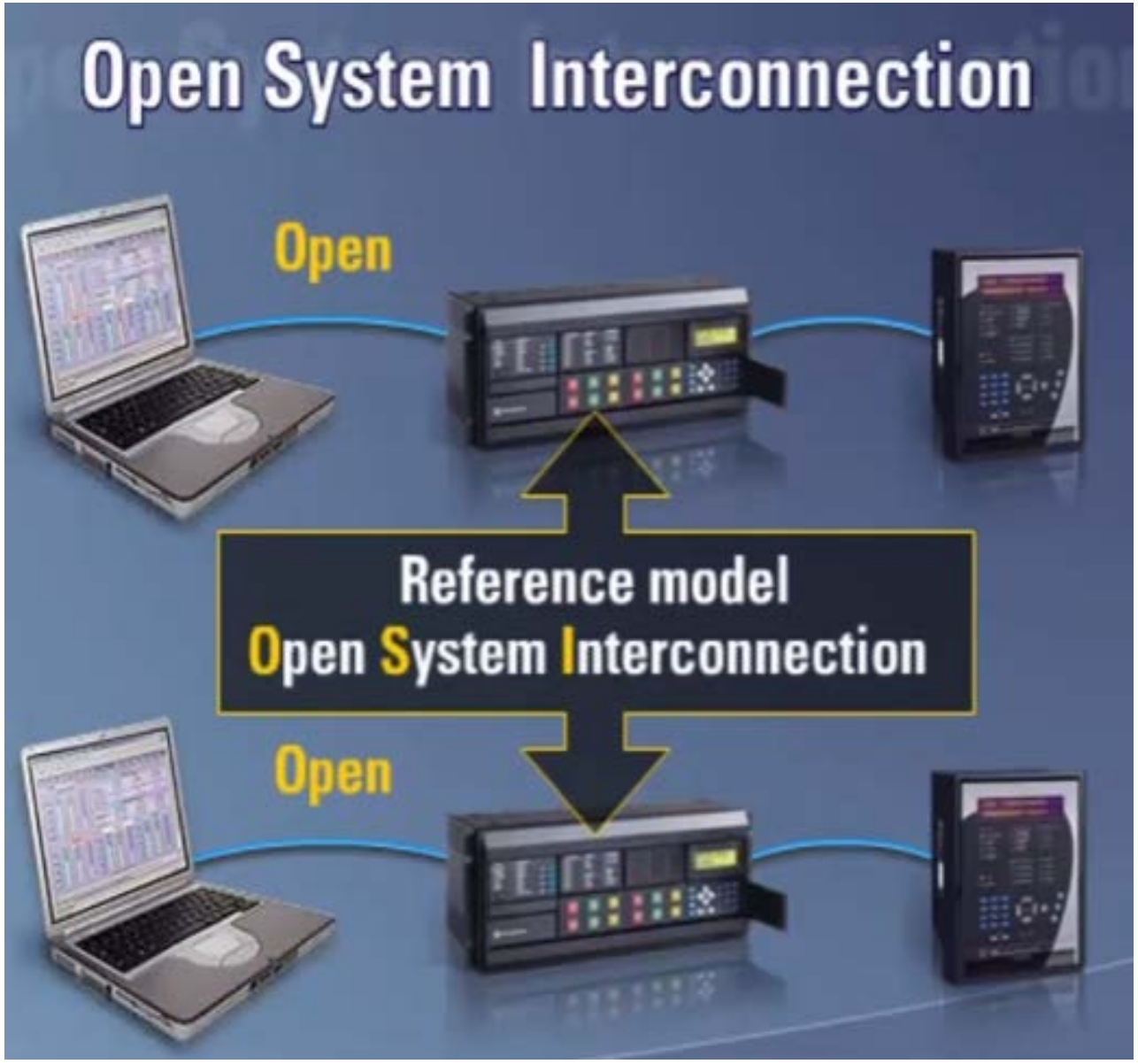
STANDARDS

- Need for a common set of rules

COMPATIBILITY

- The pure physical connection standard
- The existence of complementary software standards used in conjunction with the physical standards
- Confirmability of physical connection and software to open system interconnected model

Open System Interconnection



OPEN SYSTEM INTERCONNECTION

PHYSICAL

- Physical connection between the device and network
- Network Topology
- Electrical aspects of signaling voltages and currents
  - Which voltages are considered as logic zero and logic one
  - How much current the transmitter must be capable of supplying
- Signal modulation technique
  - On/Off technique, FM or AM etc.
- Mechanical aspects

Commonly used physical standards:

- RS-232, RS-423, RS-485, 10/100 Base T, 10/100 Base F

OPEN SYSTEM INTERCONNECTION

DATA LINK

- Provides service that allow communication between devices
- Framing or separation of messages
- Error detection
- Correction mechanism
- Addressing mechanism
- Direct exchange of frames among devices on a single communications channel

OPEN SYSTEM INTERCONNECTION

NETWORK

- Responsible for device-to-device data delivery and optimal routing across multiple data links

TRANSPORT

- Guaranteed-delivery messaging service ensuring data is error free and correctly sequenced
- Allowing process-to process communications between devices across a network or multiple networks

SESSION

- Mechanism for the establishment of a communication session between applications running within the devise

OPEN SYSTEM INTERCONNECTION

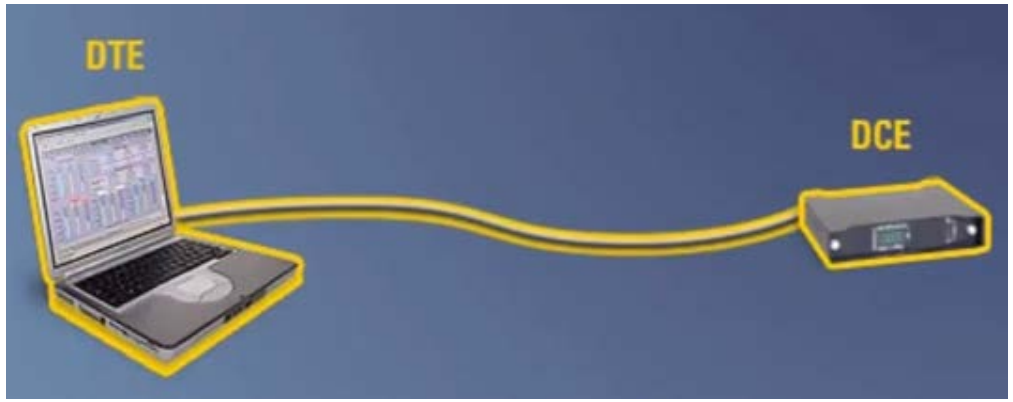
PRESENTATION

- Ensures the correct translation of data

APPLICATION

- Provides the facilities or interface to allow the applications protocols or drivers such as Modbus or DNP to use the network

RS 232/423



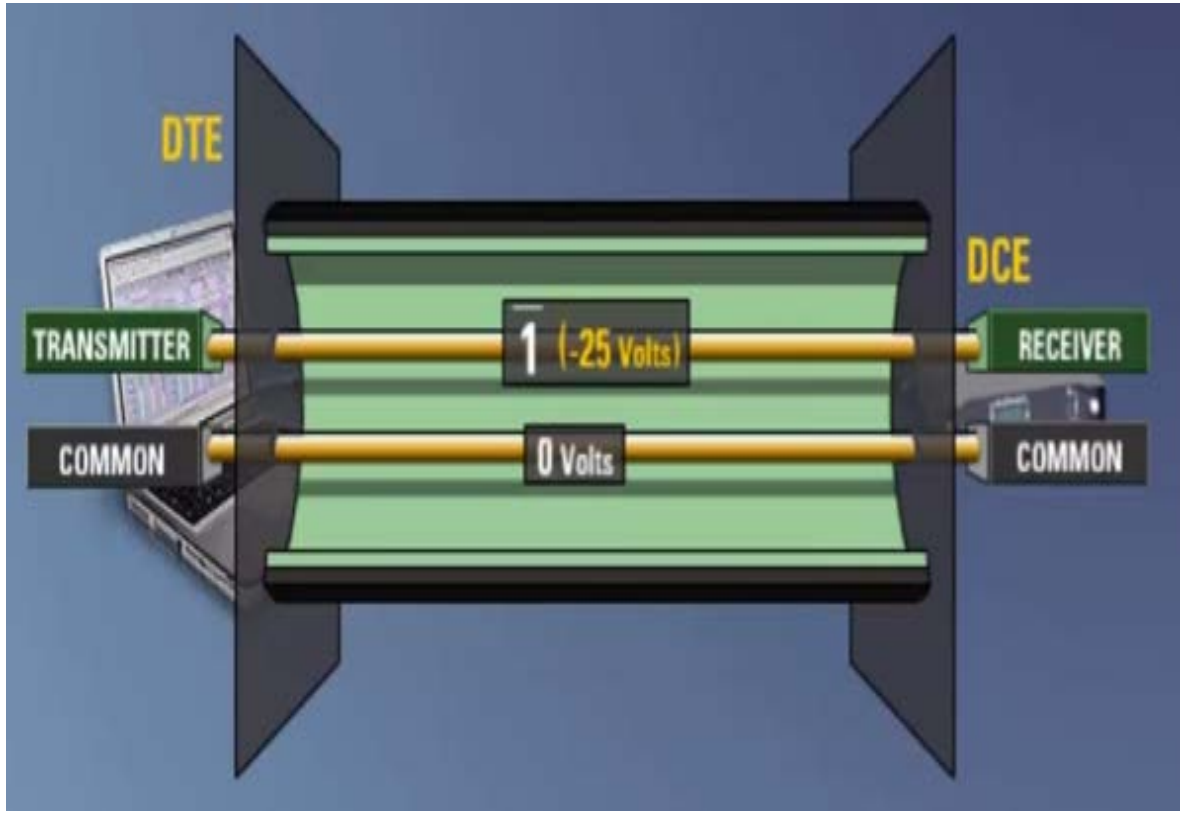
Example Female RS-232 Connection

- 1969: EIA developed and introduced RS 232
- Defined electrical and mechanical details of the interface for serial transfer of characters between Data Terminal Equipment such as printers and computers to Data Communication Equipment.
- A lot of flexibility open to the designer of the hardware regarding the rules of data exchange

RS 232/423

For the Receiver

- Logic one = - 3V to -25V
- Logic zero = +3V to +25V
- Undefined signal = > -3V and <+3V

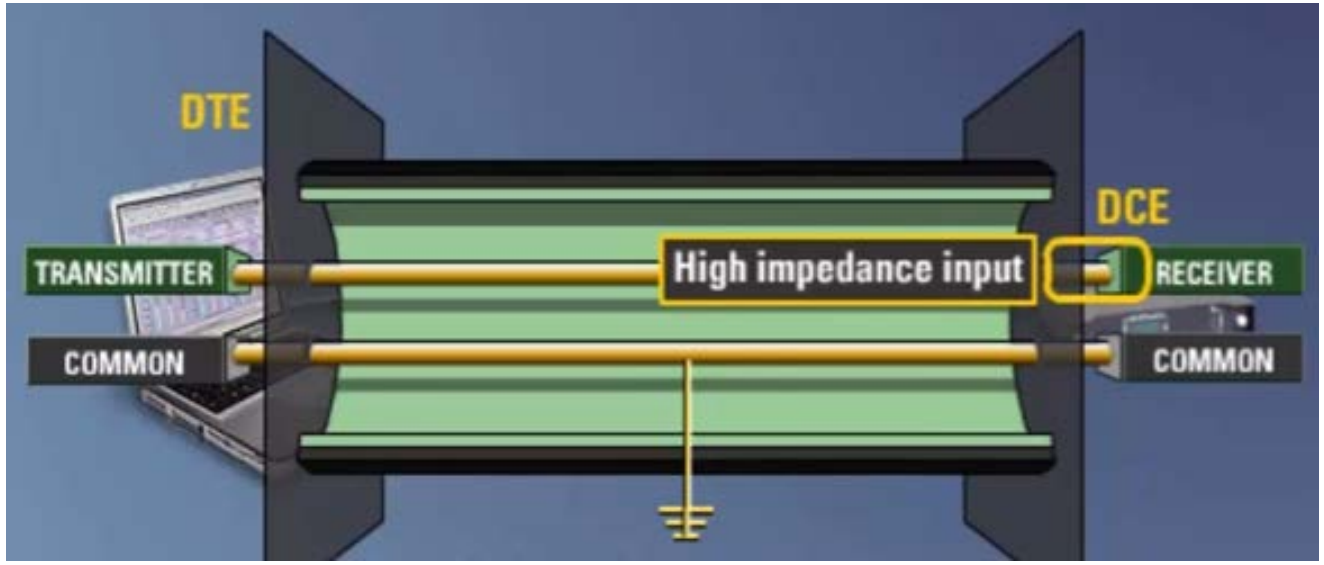


Slew Rate

- It will take sometime for the transmitter output to swing from +25V to -25V. This delay is called the slew rate
- Slew rate is one of the factors that limits the maximum transmission rate

RS 232/423

- RS 232 is susceptible to noise at higher baud rates
- Signal common is capacitively or directly coupled to ground
- Receive wire is connected to receiver high impedance input
- Longer the conductor ⇨ Higher probability of noise
- Electromagnetic lines of radiation for sources such as a motor can induce voltage on the receiver wire
- This could superimpose a voltage that could change logic 1 voltage level to logic 0 voltage level
- Therefore this type of communication link is only considered reliable over relatively short distances (approximately 15m or less) and at lower baud rates (19.2 kilobits per second or less)



RS 232/423

RS 423

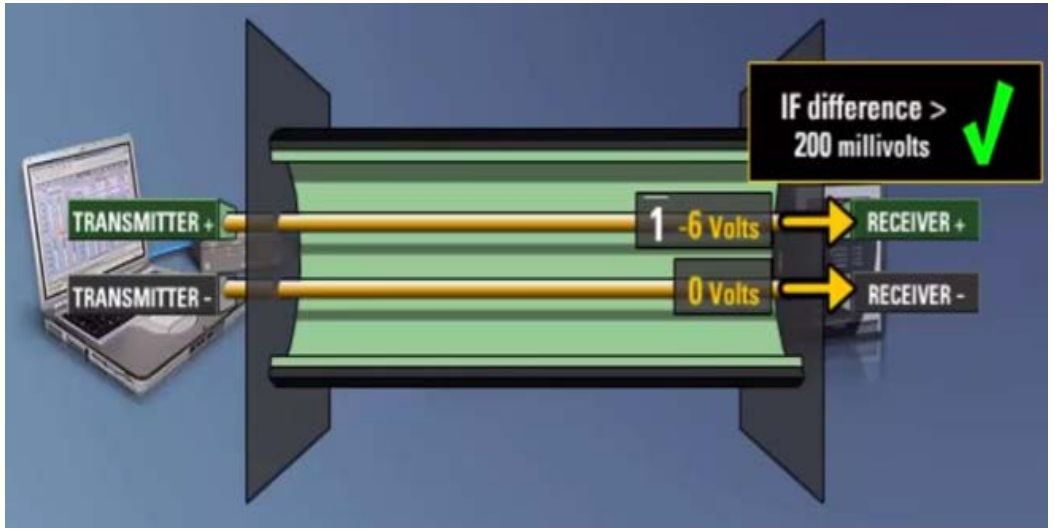
- Logic 1 is between -3.6 to -6V DC
- Logic 0 is between +3.6 to +6V DC
- Reduction in voltage magnitude range allows transmission of data at higher rates
- Transmitters current rating increased to permit upto 10 receivers
- Permits reliable communication upto 1200 meters with data rates upto 100 kilobits per second

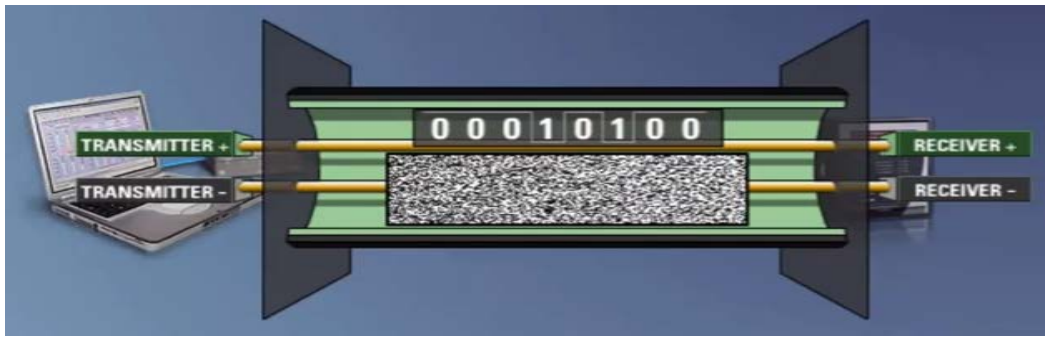
RS 485

- 32 devices can be connected in parallel or daisy chained using a 2 conductor cable that is terminated at either end in the characteristics impedance of the cable
- Cables have to be terminated correctly to ensure data is received error free
- Data manufacturers specify how cables are terminated
- Each cable is referred to as a segment having a maximum length of 4000 ft or 1200 meters
- The conductors are not connected to ground i.e. electrically floating

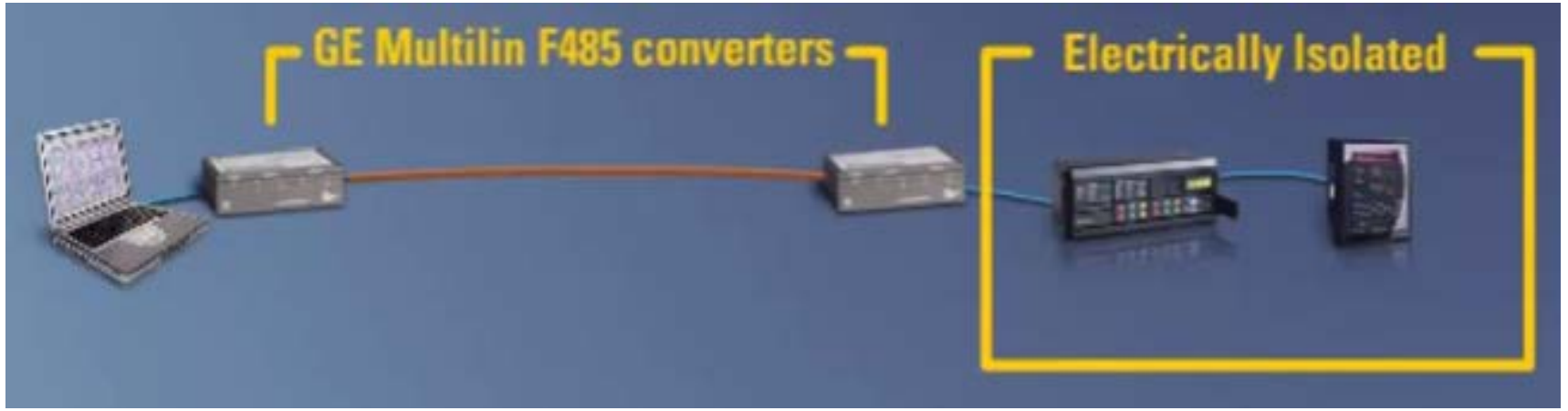
Connection of Relays using RS-485

- All the devices have to be electrically isolated to reduce potential equipment damage
- Transmitter (also referred to as driver) has 3 states – Logic 1, Logic 0 and High Impedance (driver not connected to the segment)
- Logic 1: -1.5 to -6 V
- Logic 0: +1.5 to +6 V
- Protocol will ensure that only one driver is active at any time
- Receivers measures the potential difference between the 2 conductors (embedded in the same cable)
- Difference should be > 200 mV for the receiver to detect logic 1 or logic 0
- If a voltage is induced in one conductor due to EMI affect the same voltage will be induced in 2nd conductor as well
- This allows RS485 LANs to communicate successfully at higher baud rates and higher distances than RS232/RS423 LANs.





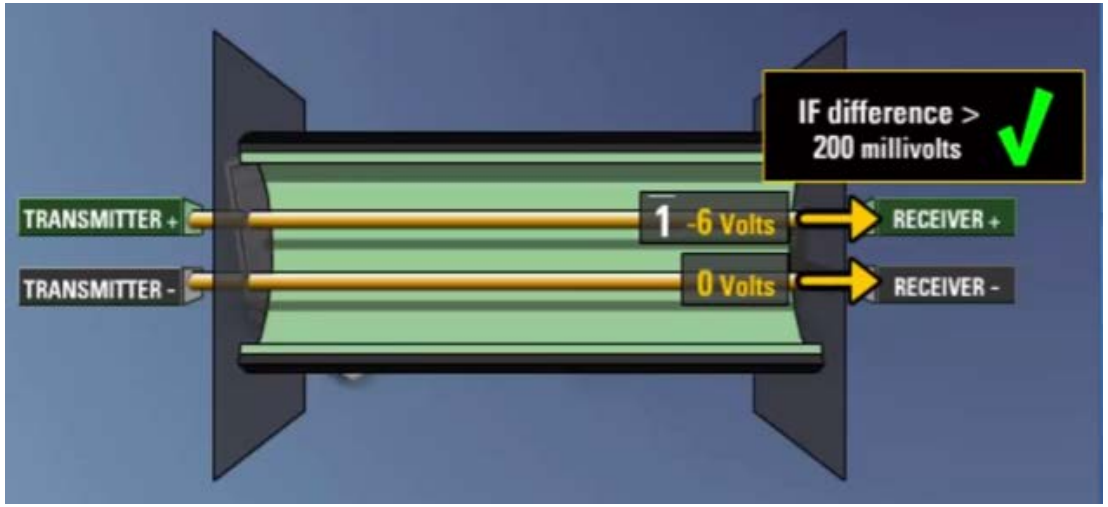
ELECTRICAL ISOLATION



- Sections of RS485 LAN should be isolated from each other for reliable operation
- Reduces potential damage to equipment and ensures data is received error free
- Isolation is highly recommended when
- Sections of the LAN are situated on different ground planes (different buildings)
- Long distance between groupings or clusters of RS485 devices
- More than 32 devices must be located on a single RS485 LAN

RS422

- Introduced in early 1970's and it is older than RS485
- Similar to RS485 it is a differential system using 2 conductors
- Goal was to provide a simplex connection from a master up to 10 slaves
- 1 driver transmitter and up to 10 receivers are permitted in the RS422 LAN
- Driver output:
- Logic 1: -2 to -6V
- Logic 0: +2 to +6V



ETHERNET COMMUNICATION FUNDAMENTALS

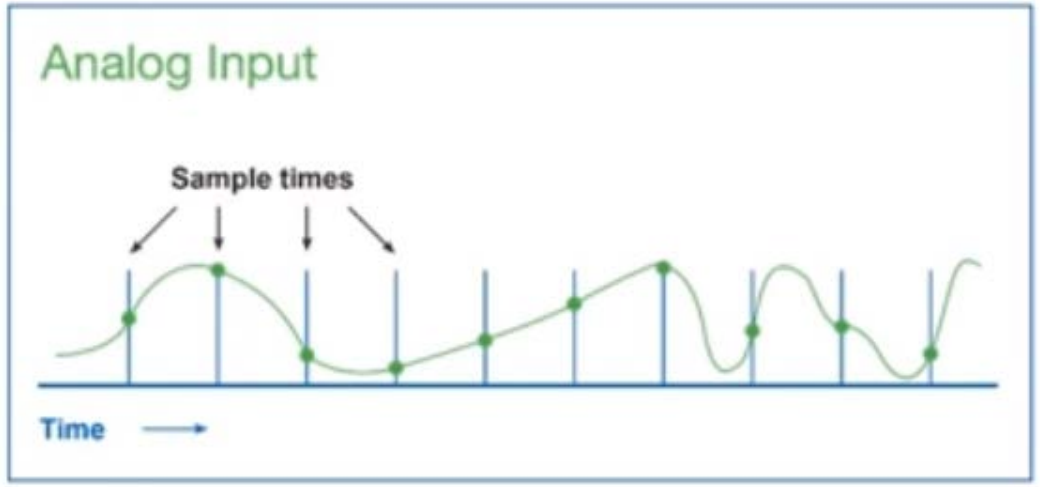
ETHERNET

- Standard high speed technology at the physical through network layers.
- Industry and utility power applications are migrating from RS 232 & RS 485 based LAN technology to Ethernet.
- Older standards: Half duplex operation
- Modern standards: Support full duplex Ethernet
- Popular physical layer standards:
  - 10/100 BASE T and 10/100 BASE F.
  - Both support full duplex operation.
  - 10/100 ⇒ Baud rates of 10 megabits/sec and 100 megabits/sec.
  - BASE ⇒ Baseband: Entire bandwidth of the LAN is used to transmit one signal.
  - T ⇒ Twisted pair: Devises use wire pairs for differential signals which are twisted together.

MODBUS

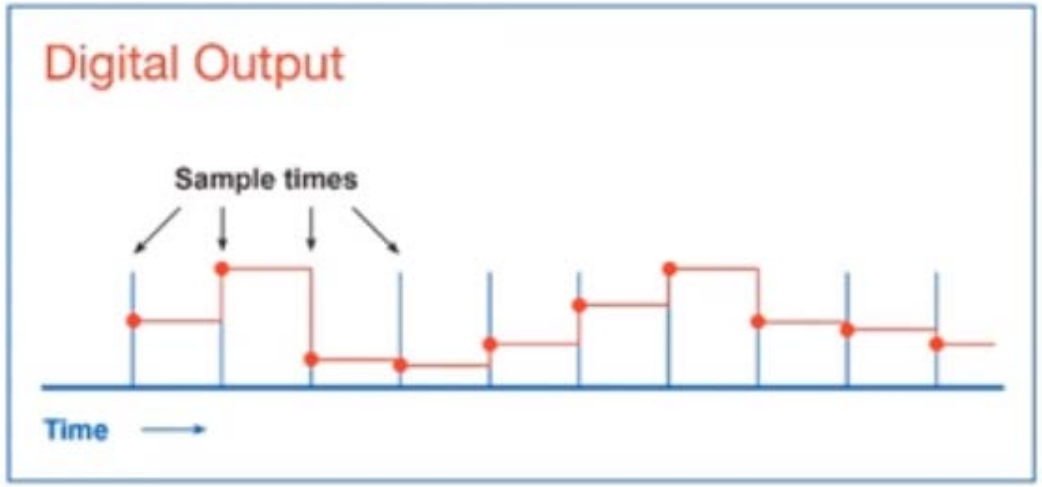
- What is Modbus?
- Digital communication of 2 or more devices
- An application layer protocol
- Open source code
- Published by Schneider electric

MODBUS



Analog Signals

- Analog signals have an infinite number of possible values over time
- Example
- 12.9 mA
- 4.563 mA

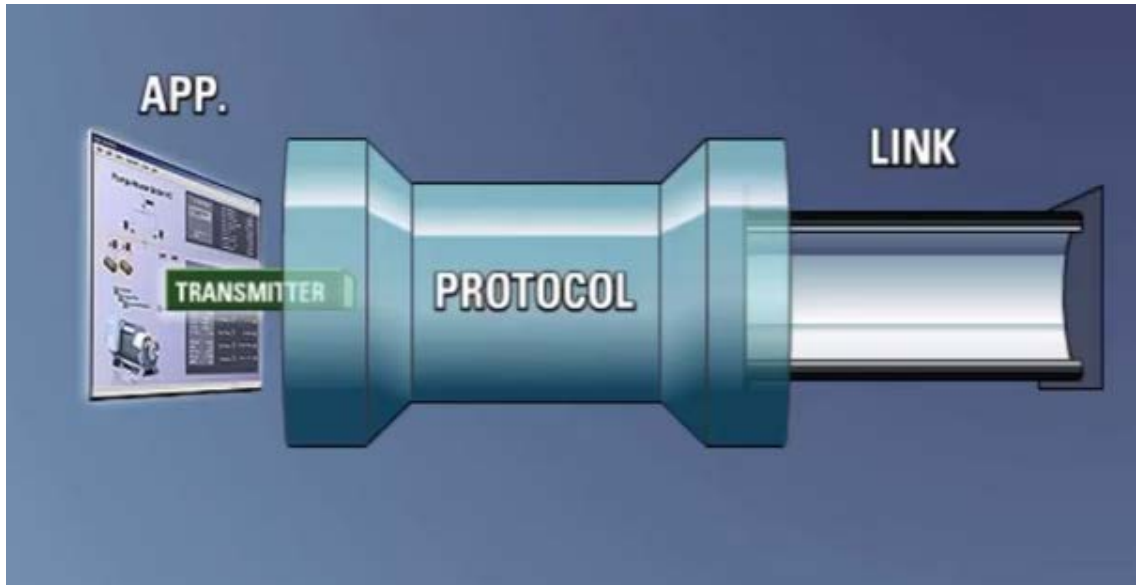


Digital Signals

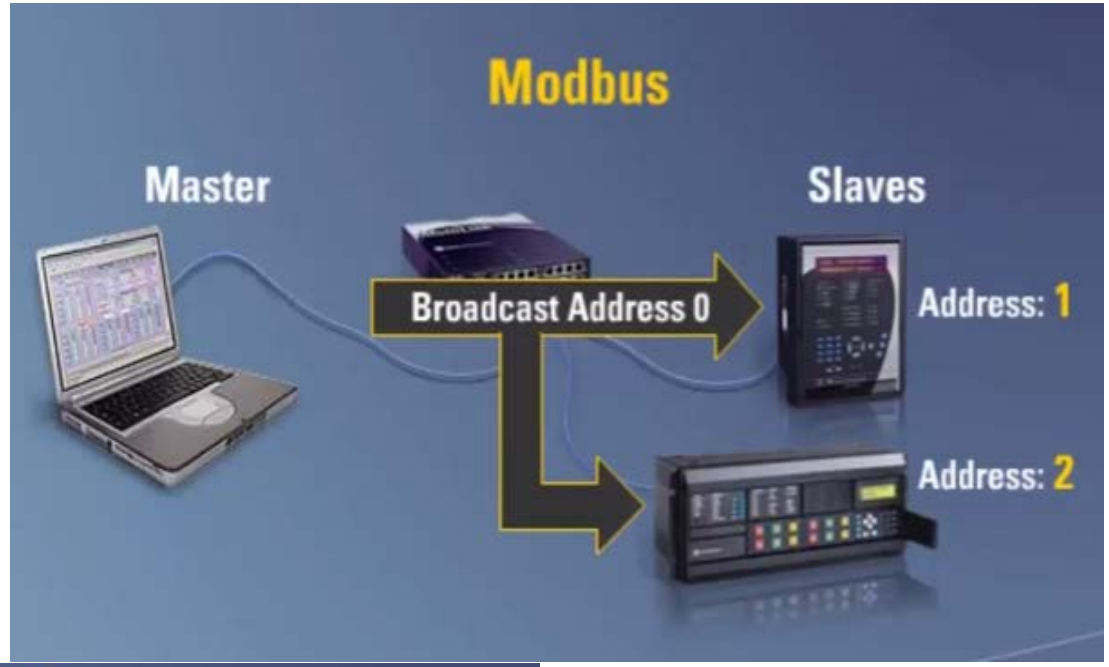
- Discrete number of values from 2 to billions determined by number of bits
- Vary with sample times

PROTOCOL

- Protocol can be considered as a bridge between application and communication link
- Functions as a common set of rules governing the exchange of data between devices on a network
- Determines the point at which devices agree to exchange data (data initialization)
- Determines the supported services (reading/writing, flow control, frame format, synchronization etc.)



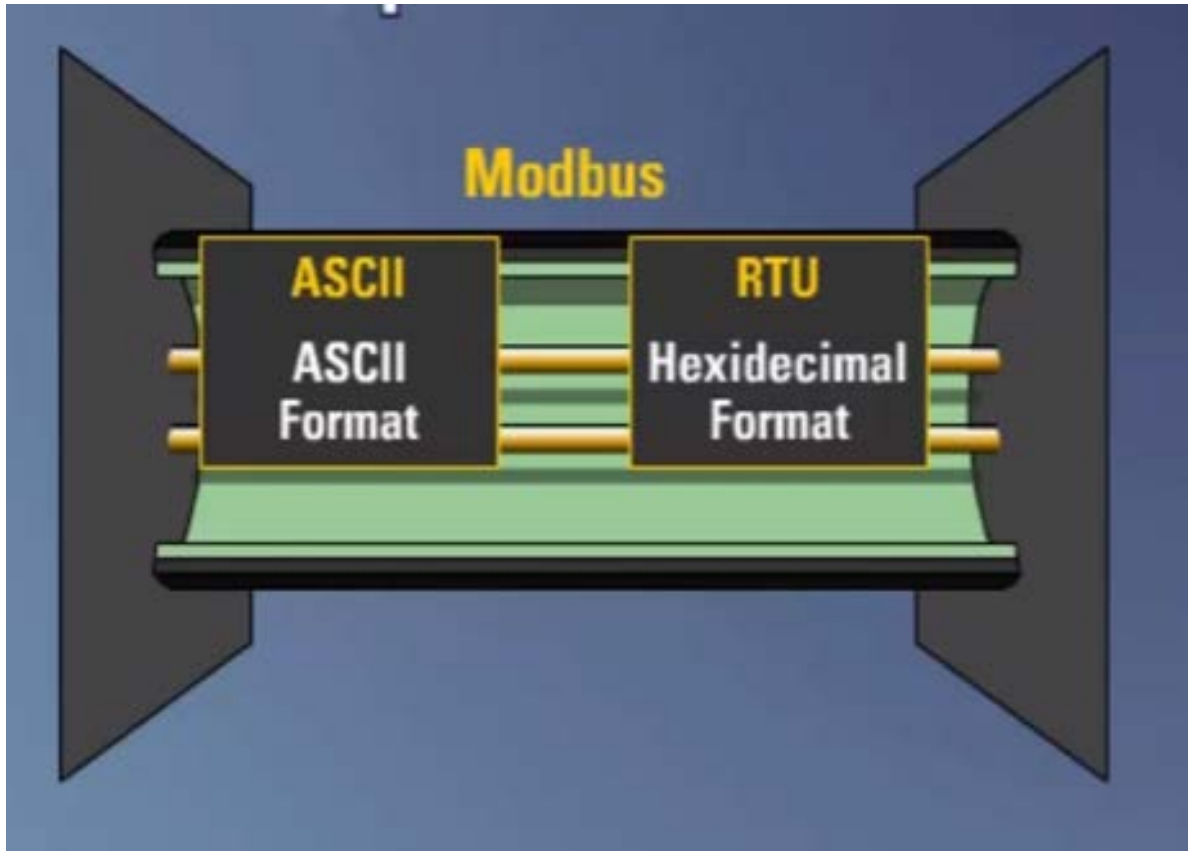

Modbus
Master
Slaves
Message to Slave 1
Address: 1
Address: 2


Modbus
Master
Slaves
Broadcast Address 0
Address: 1
Address: 2


Modbus
Master
Slaves
Master writes to Slave 1
Address: 1
Address: 2
Master reads from Slave 2

MODBUS IMPLEMENTATION

- Works well when the maximum required data update is less than half of what the protocol and network are capable of delivering
- Physical Layer: RS232, RS484, 10/100 Base T, 10/100 Base F Ethernet
- Data flow is half duplex in all configurations
- Master transmits a command and the slave responds

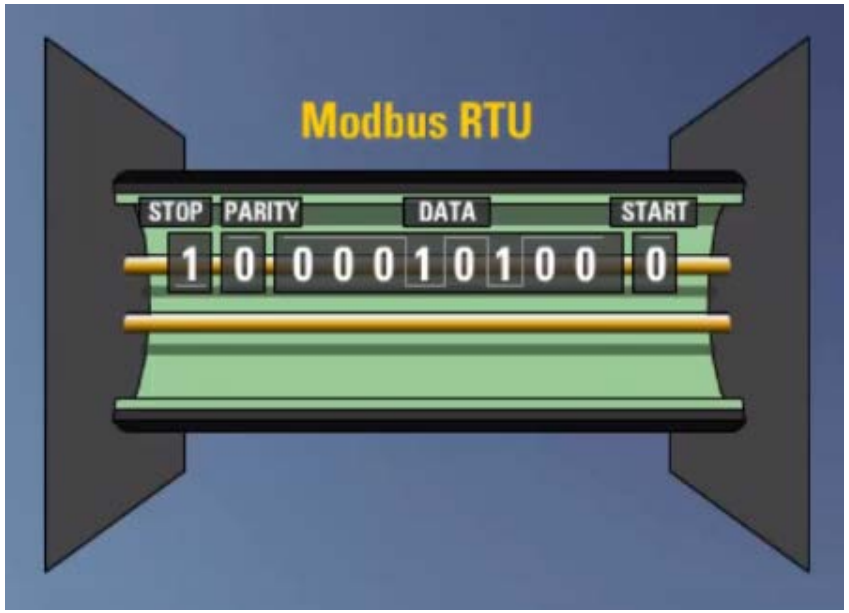


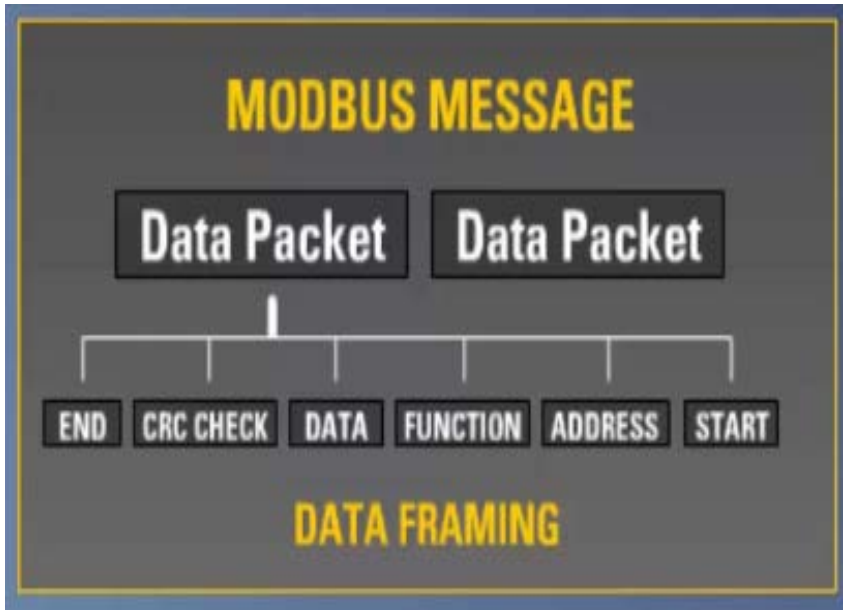
MODBUS IMPLEMENTATION

- Modbus communication takes place in packets – Groups of asynchronously transmitted bytes of data arranged in a specific order
- The packets are referred to as data frames
- Data link layer: Responsible for ensuring that the data is framed correctly
- Master transmits a packet to a slave and the slave responds with a packet

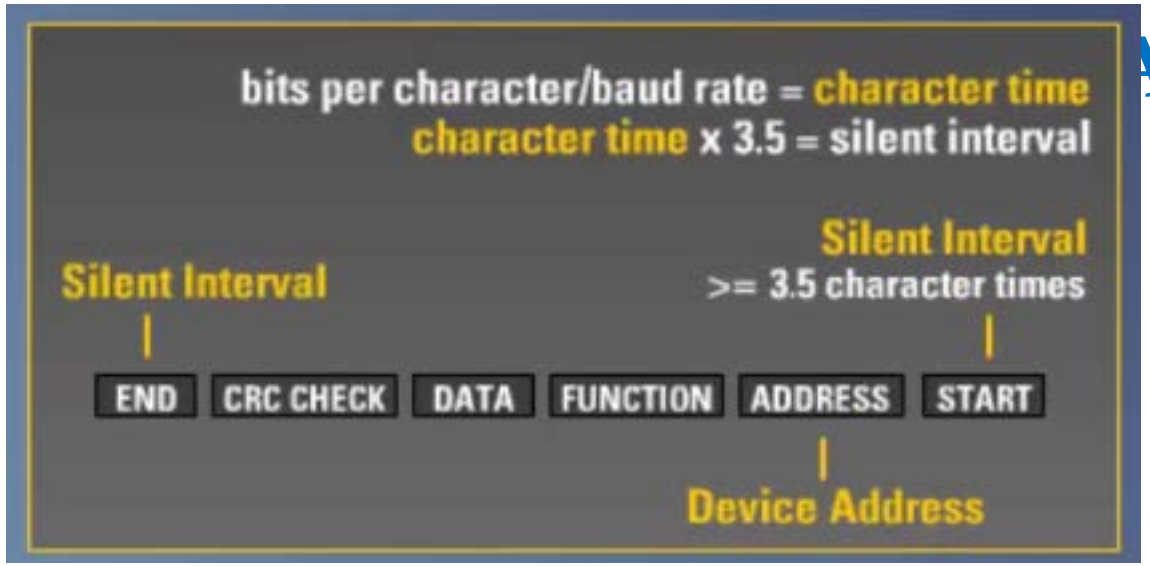
Data Transfer

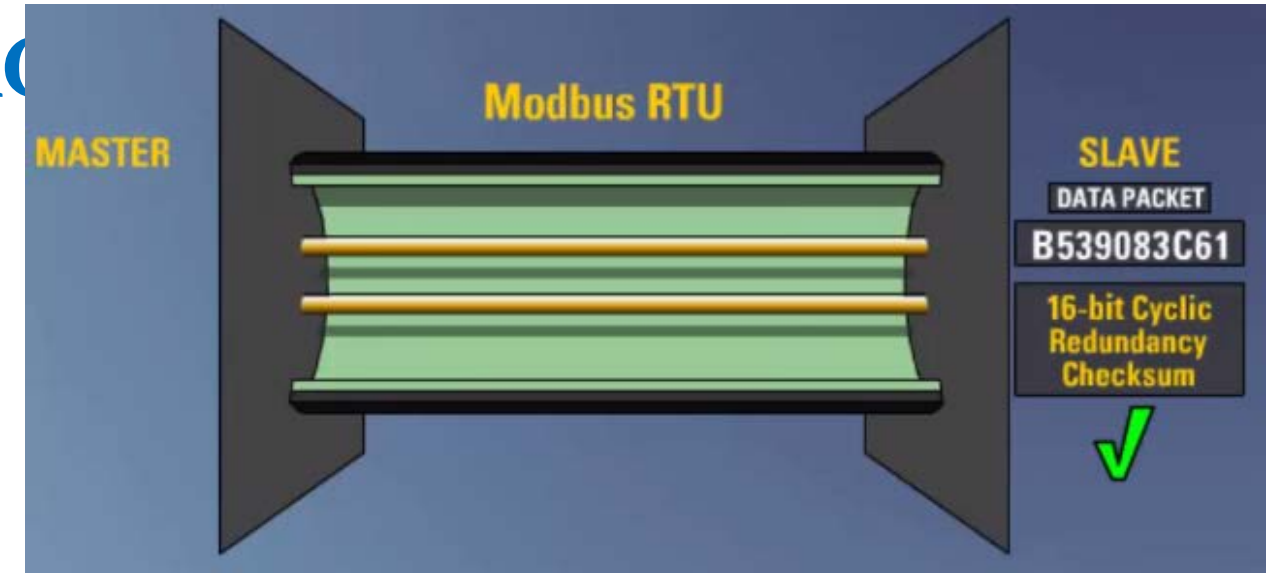
- Each character is transmitted in an asynchronous format
- Consists of one start bit, 8 data bits, 1 stop bit and 1 parity bit
- 10-11 bit character data may not be supported at baud rates greater tan 300 by many modems
- Messages transmitted over Modbus are comprised of one or more data packets
- Each data packet is made up of multiple characters
- Characters are separated into multiple groupings. Each group performs a specific function during communication
- The arrangement in functions of groups of these characters is known as Data Framing

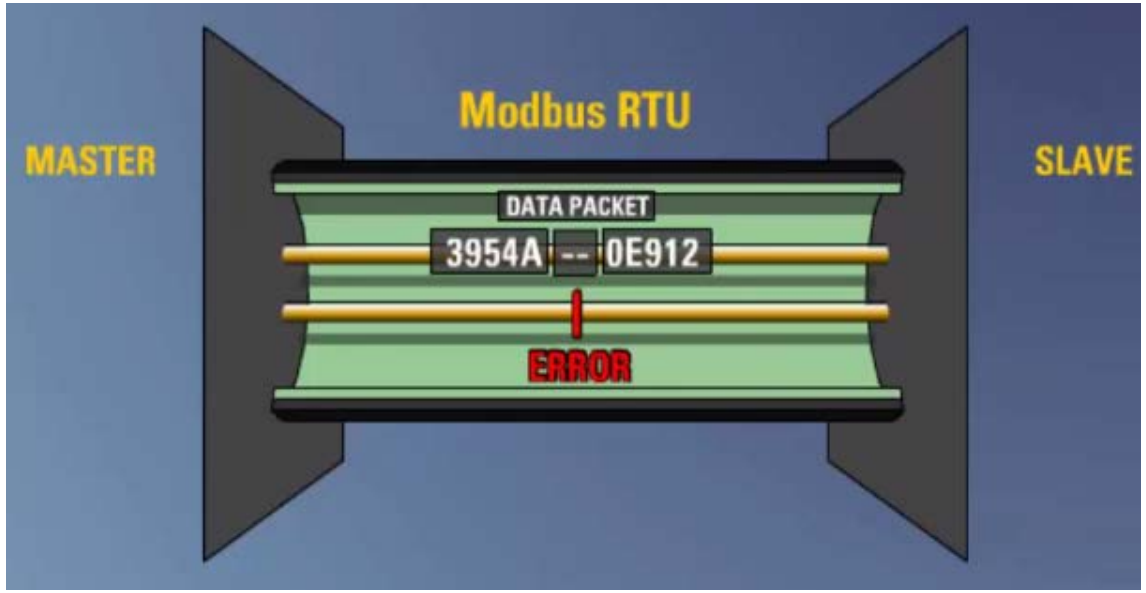


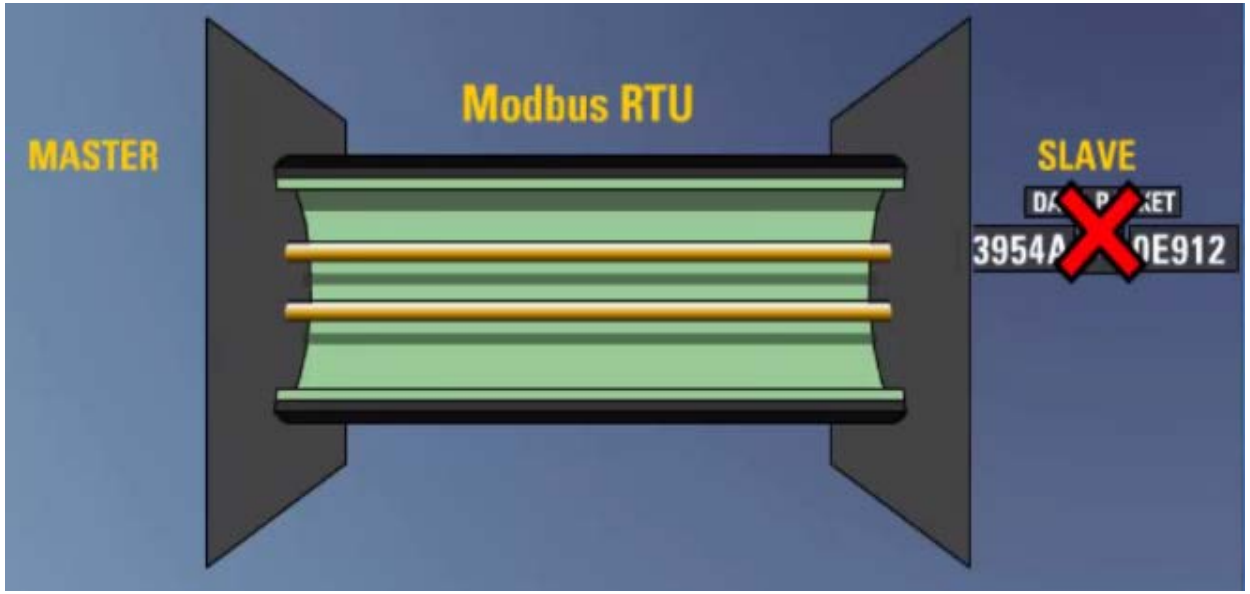


Framing of Modbus RTU Command Data



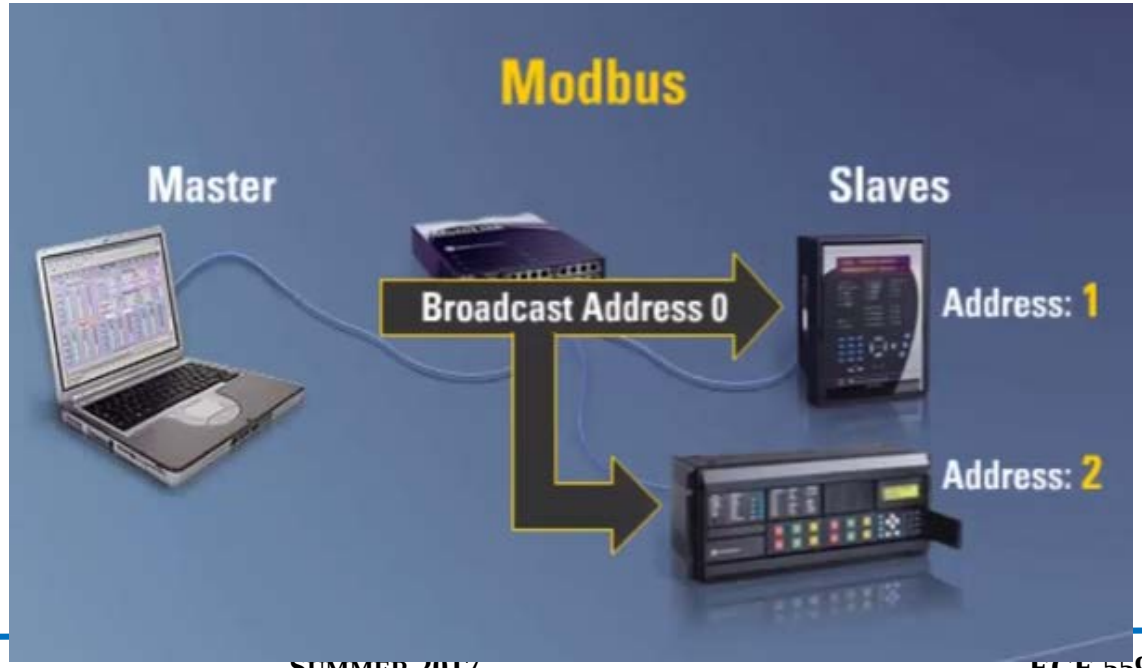


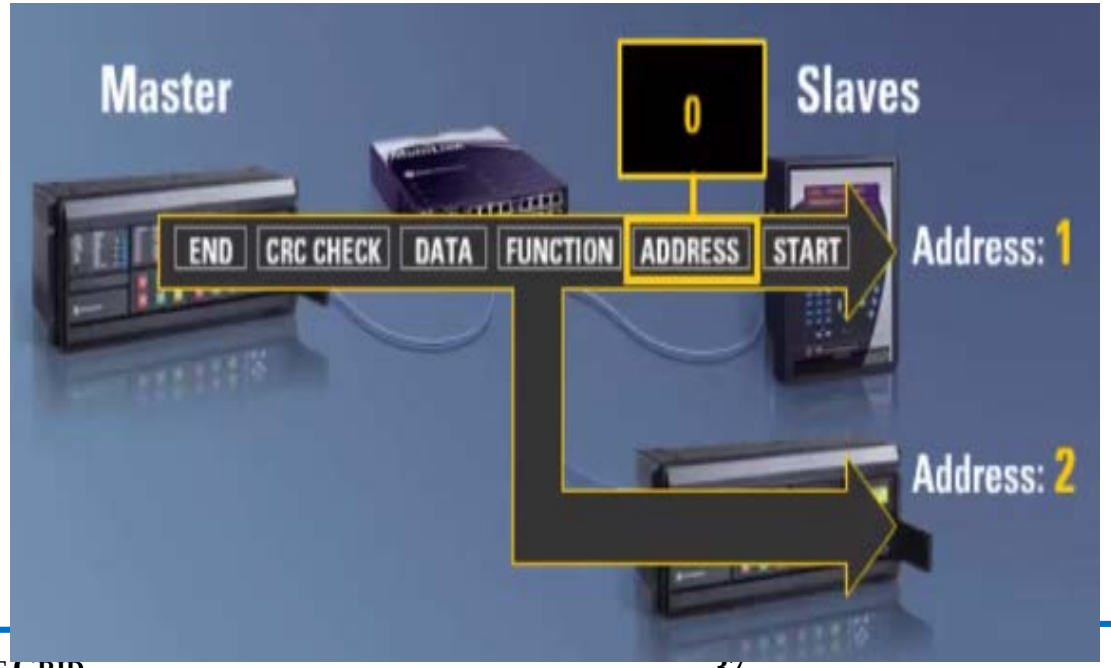




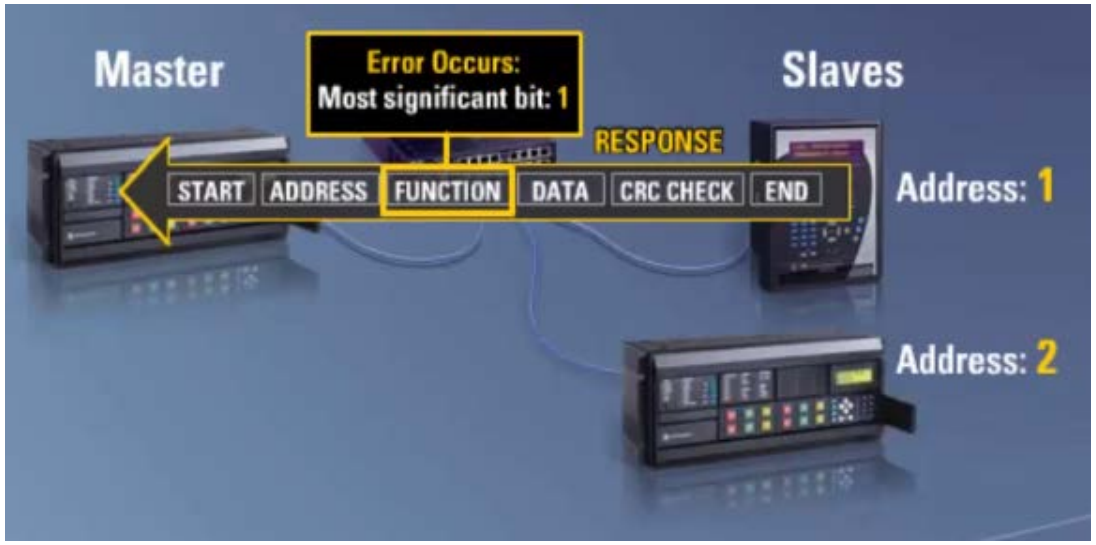

Modbus
Master
Slaves
Message to Slave 1
Address: 1
Address: 2

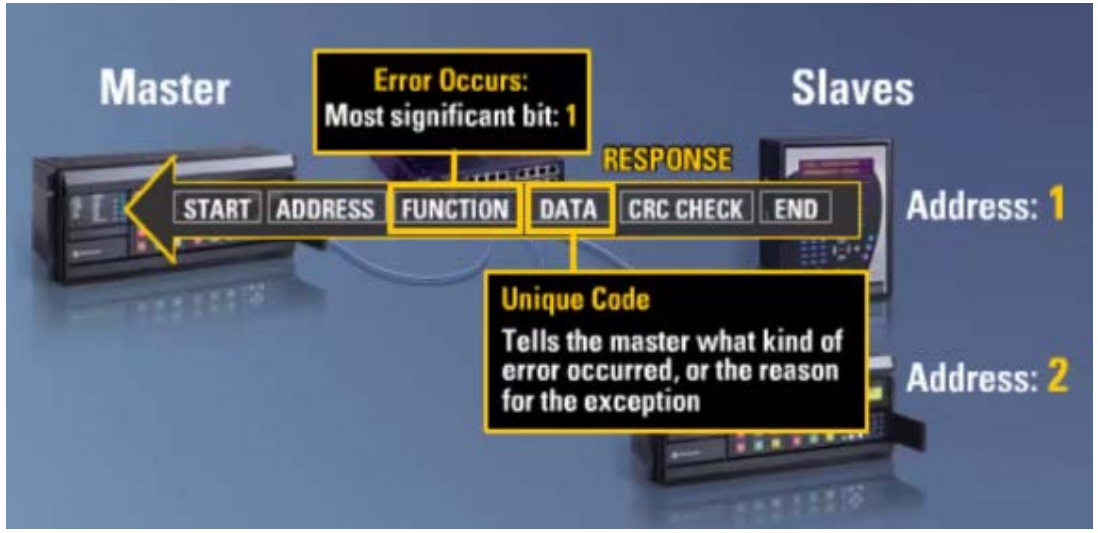

Master
8 bits
1-247
Slaves
END
CRC CHECK
DATA
FUNCTION
ADDRESS
START
Address: 1
Address: 2

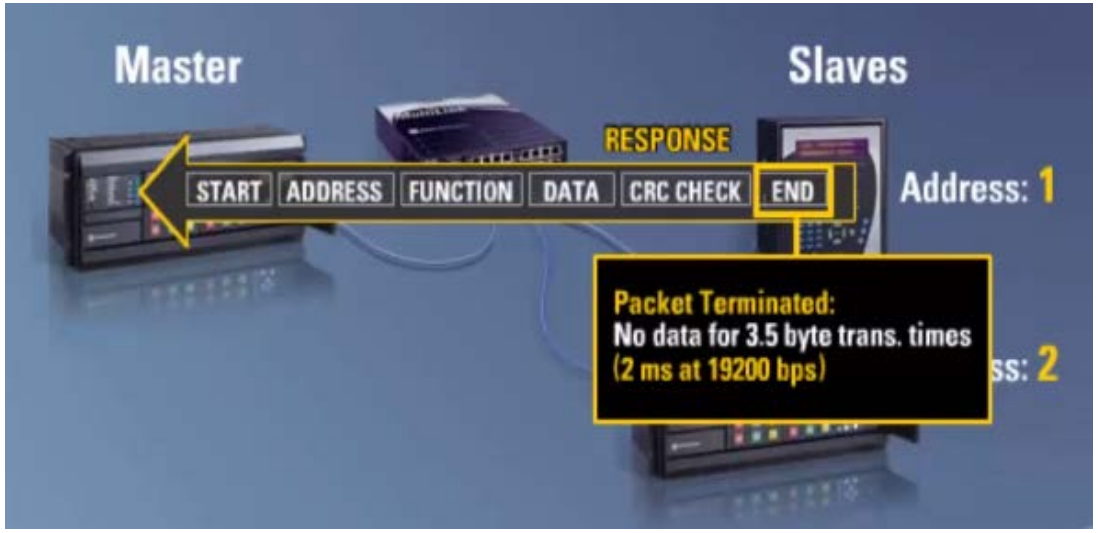

Modbus
Master
Slaves
Broadcast Address 0
Address: 1
Address: 2


Master
0
Slaves
END
CRC CHECK
DATA
FUNCTION
ADDRESS
START
Address: 1
Address: 2


Master
Error Free:
Returns same code
Slaves
RESPONSE
START
ADDRESS
FUNCTION
DATA
CRC CHECK
END
Address: 1
Address: 2


Master
Error Occurs:
Most significant bit: 1
Slaves
RESPONSE
START
ADDRESS
FUNCTION
DATA
CRC CHECK
END
Address: 1
Address: 2


Master
Error Occurs:
Most significant bit: 1
Slaves
RESPONSE
START
ADDRESS
FUNCTION
DATA
CRC CHECK
END
Address: 1
Unique Code
Tells the master what kind of error occurred, or the reason for the exception
Address: 2


Master
Slaves
RESPONSE
START
ADDRESS
FUNCTION
DATA
CRC CHECK
END
Address: 1
Packet Terminated:
No data for 3.5 byte trans. times
(2 ms at 19200 bps)
ss: 2

FUNCTION CODE		MODBUS DEFINITION	GE MULTILIN DEFINITION
HEX	DEC		
03	3	Read Holding Registers	Read Actual Values or Settings
04	4	Read Holding Registers	Read Actual Values or Settings
05	5	Force Single Coil	Execute Operation
06	6	Preset Single Register	Store Single Setting
10	16	Preset Multiple Registers	Store Multiple Settings