The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

1875-1

First Latin American Regional Workshop on Distributed Laboratory Instrumentation in Physics

7 January - 4 February, 2008

Industrial Networking

Anthony J. Wetherilt

Director, Administration
UNIDO-ICHET,
Sabri Ulker Sok, 38/4,Cevizlibag, Zeytinburnu
34015 Istanbul
Turkey

Industrial Networking

- *Basics of Serial Communication*
- *Common Industrial Bus systems*
- *Industrial Ethernet*

Serial Communications

- *RS 232*
- *RS 422*
- *RS 485*
- *1-Wire*
- *CAN*

EIA – RS 232

Two types:

- *Data Communications Equipment (DCE)*

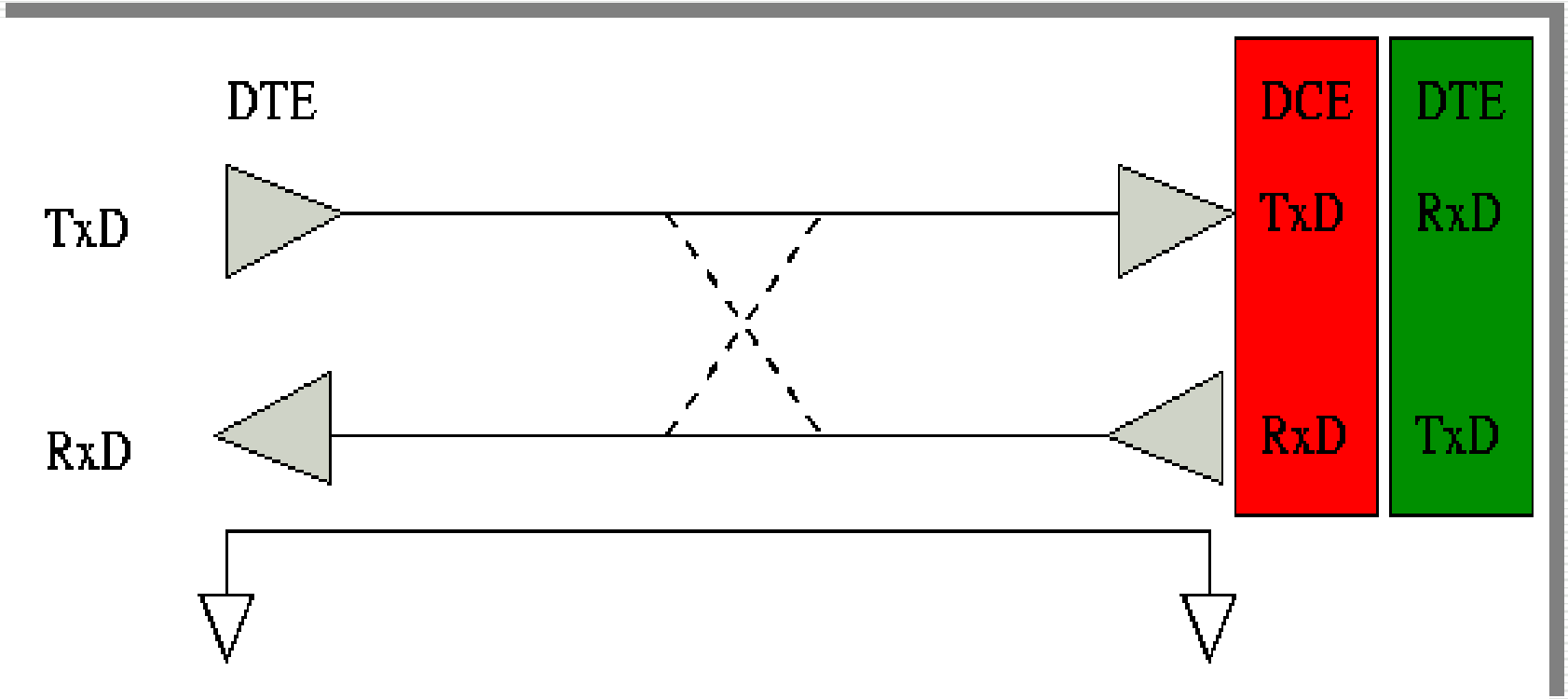
  Modems etc (female socket)
- *Data Terminal Equipment (DTE)*

  Terminals, PCs etc (male socket)

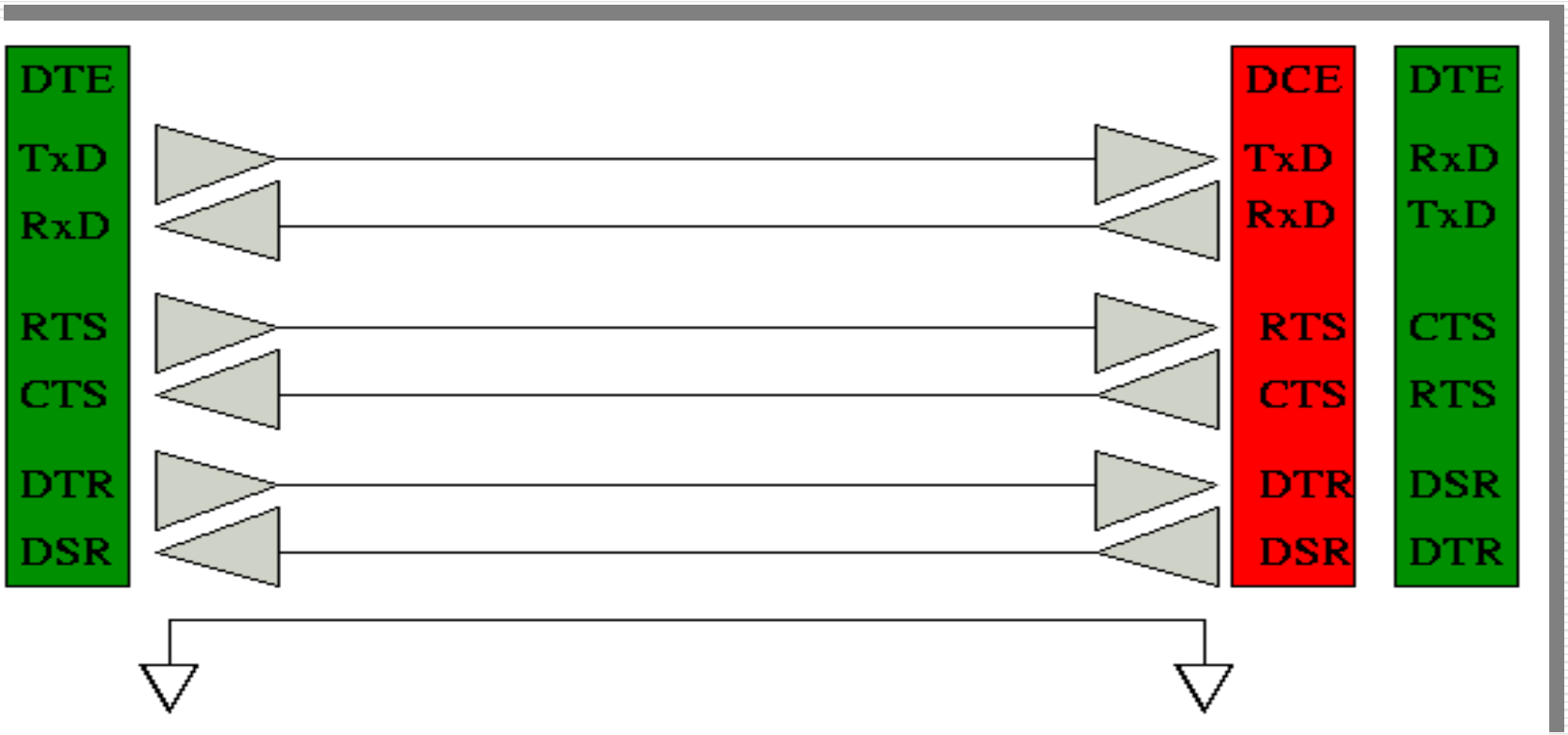
The standard defines that a DTE is connected to a DCE. But ...

EIA-RS 232

A minimal configuration:

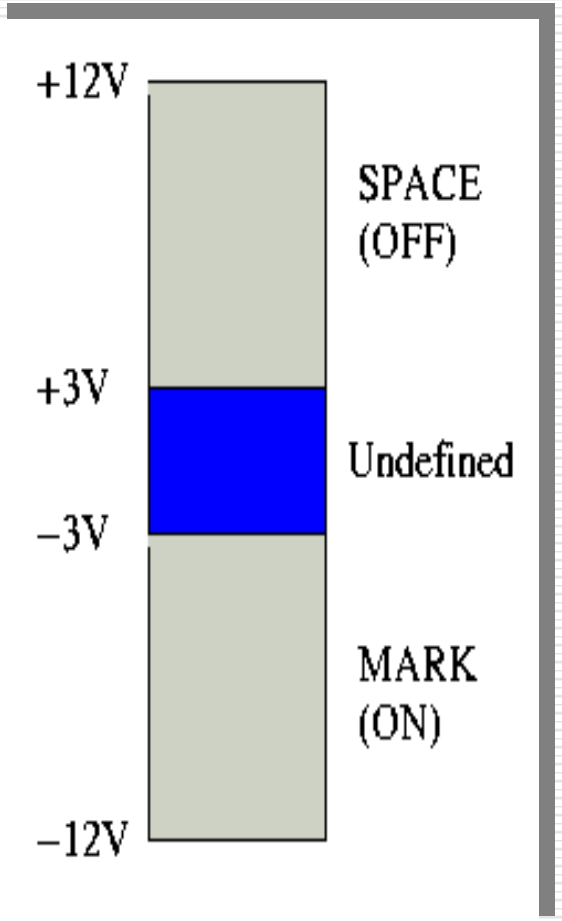


Full RS 232 configuration



EIA-RS 232

- Connectors: DB09, DB25
  (Full-2separate networks)
- Voltage levels:
  - SPACE (+3,+12V)
  - MARK (-3, -12V)
- Noise reduction (-3,+3)
- Up to 20kBaud at 15m max
- Point to point
- Problems: Length, Baud rate, multiple devices, etc.



RS 422 / 449

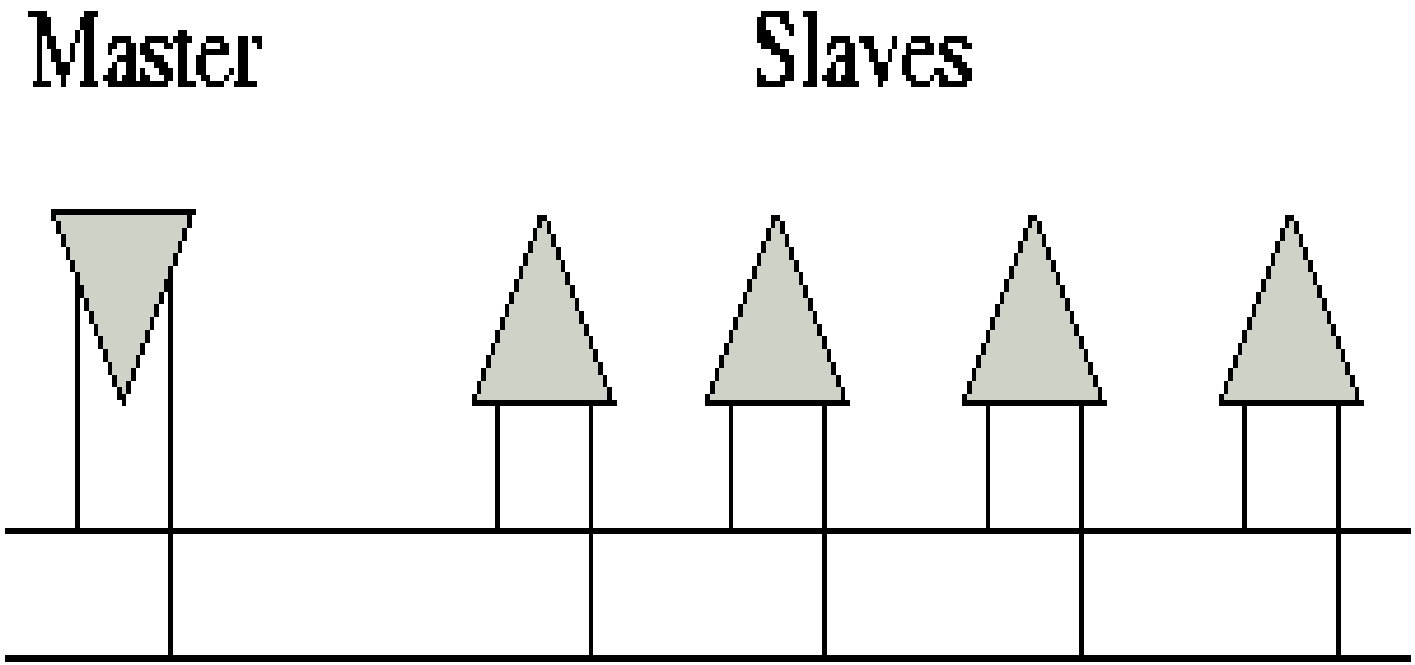
- Balanced differential drivers and receivers
- Twisted pair cables
- 100kBaud at up to 1200m
- Multi-drop systems (1 master,up to 10 slaves)

  (Output driver always active)
- 0 – 5V voltage levels,

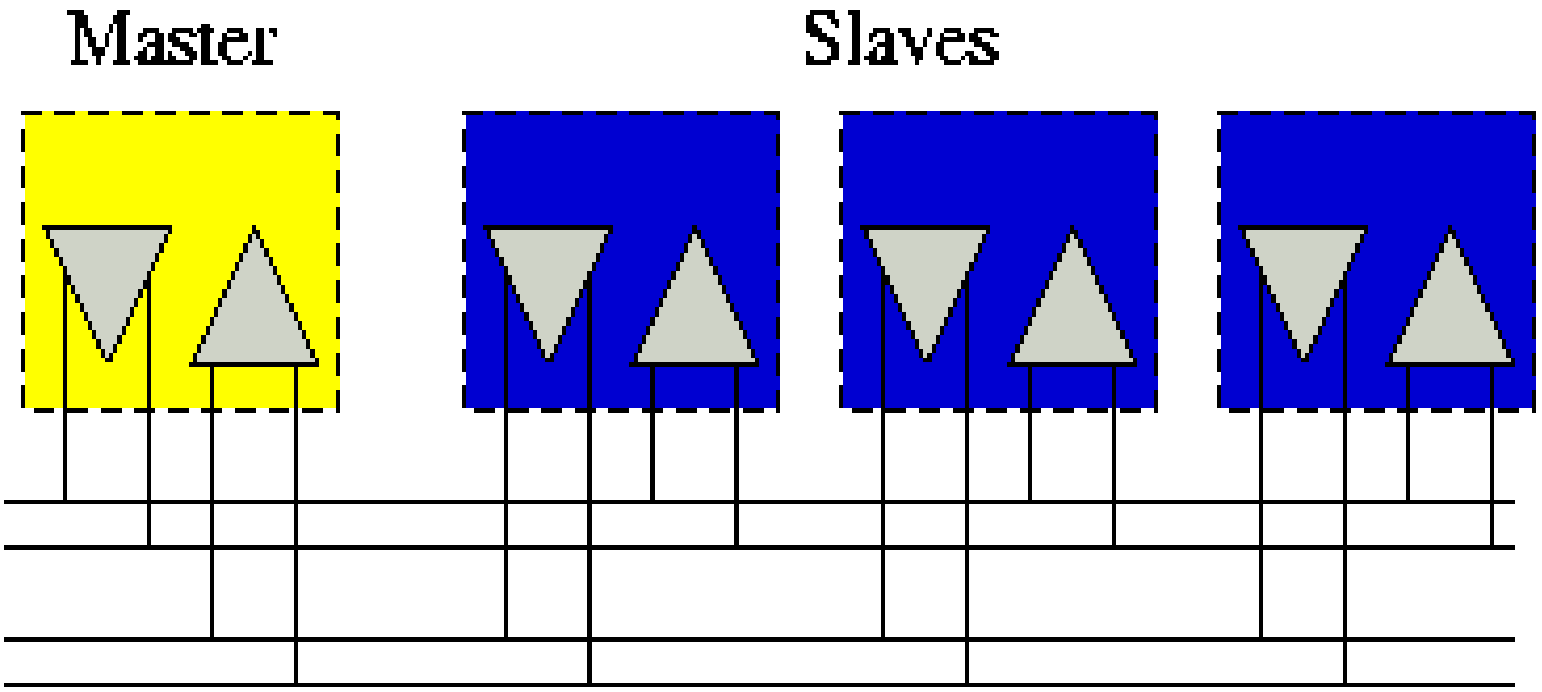
  OFF: Vdiff < -0.2

  ON: Vdiff > 0.2

Multi-drop system



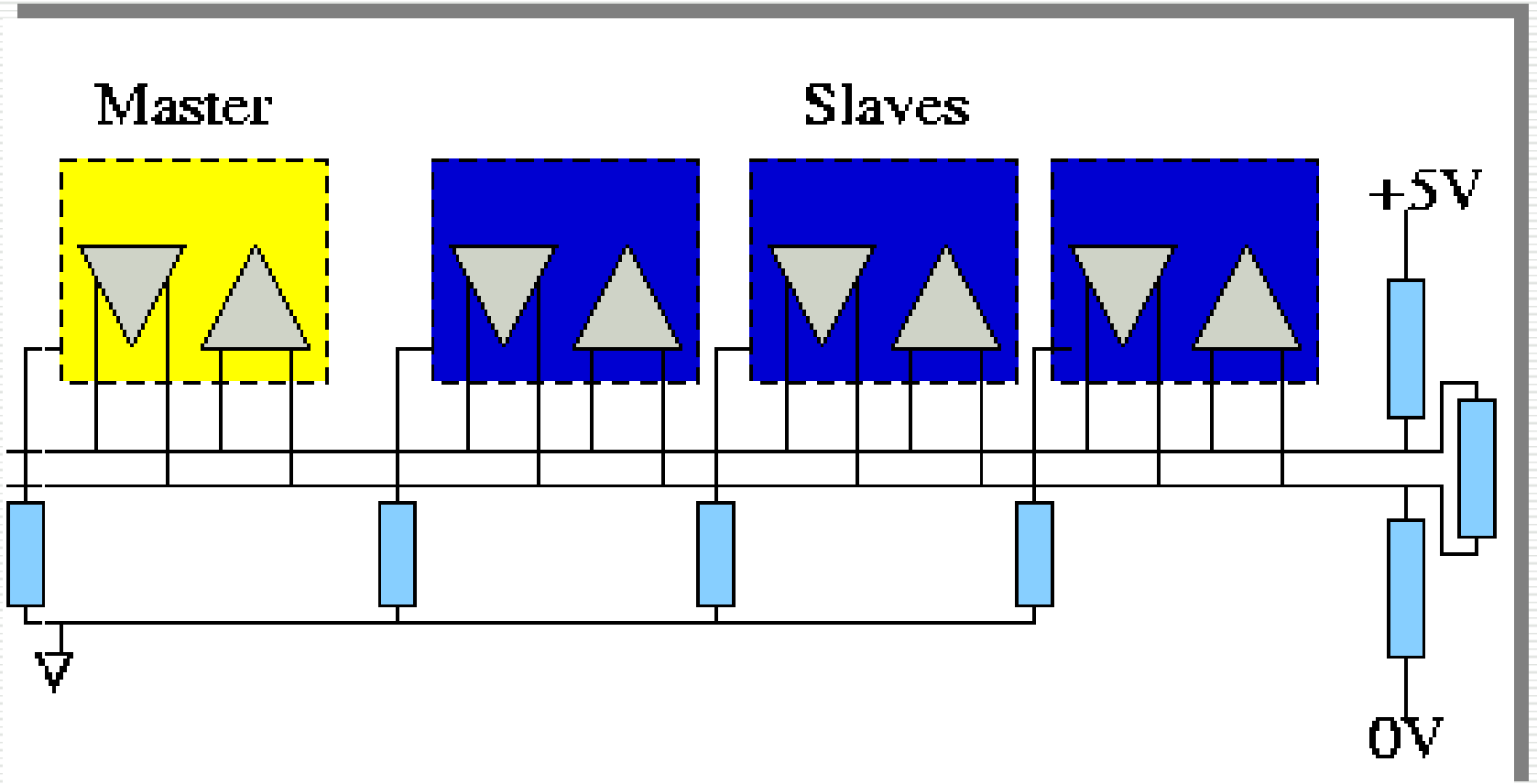
Quasi-Multipoint network



RS 485

- ***Balanced differential drivers/receivers as RS422***
- ***Increased drive capability (up to 32 devices: repeaters needed for more) at 12kOhm per device***
- ***Drivers are required to tristate (high impedance) allowing true multi-point***

Multi-point network



Practical Considerations (1)

Terminations:

- ***Pulses travelling along a transmission line will reflect back along the line.***
- ***Prevent by terminating line (at both ends) with resistor of characteristic line impedance (~120 Ohm)***
- ***Do not terminate every device (reduces drive capability)***

Practical Considerations (2)

Grounding and noise:

- ***Provide a quality common return path (ie extra line : do not rely on mains common)***
- ***Insert 100 Ohm resisters into ground line to reduce ground currents over long distances***
- ***Do not let ground currents flow in screens***
- ***Use optical isolation in severe cases of noise***

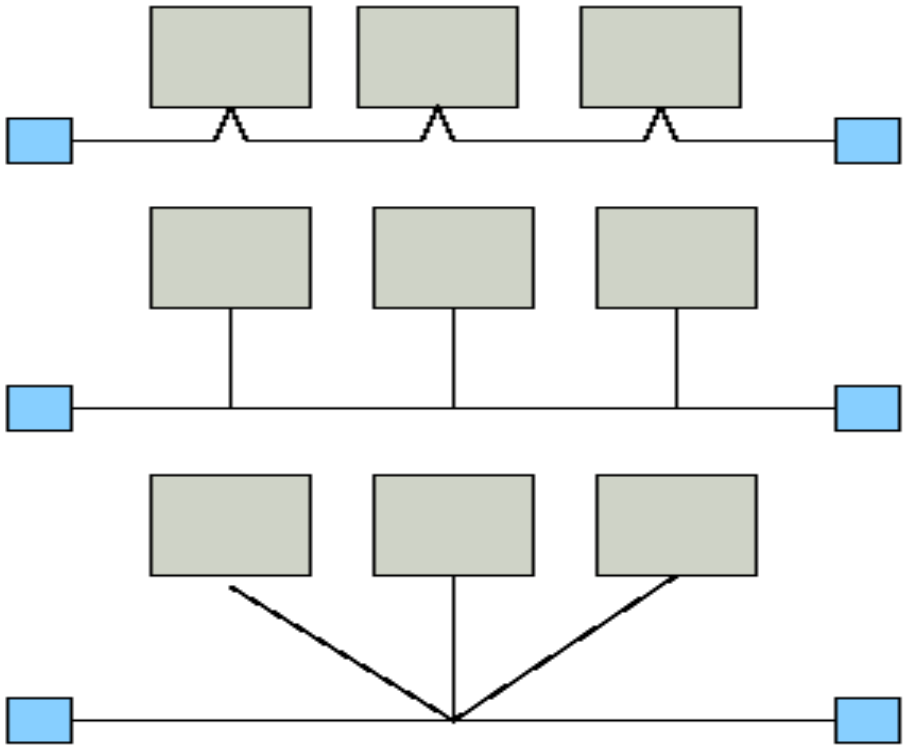
Practical Considerations (3)

Network Topology:

- ***Keep stubs as short as possible (from device to network cables). These cause reflections that introduce phase delays***

- ***Use daisy chaining to connect devices. Avoid at all costs, star networks***

Use the right network



Correct

Long stubs

Star network

(where should the resistors go?)

Controller Area Network (1)

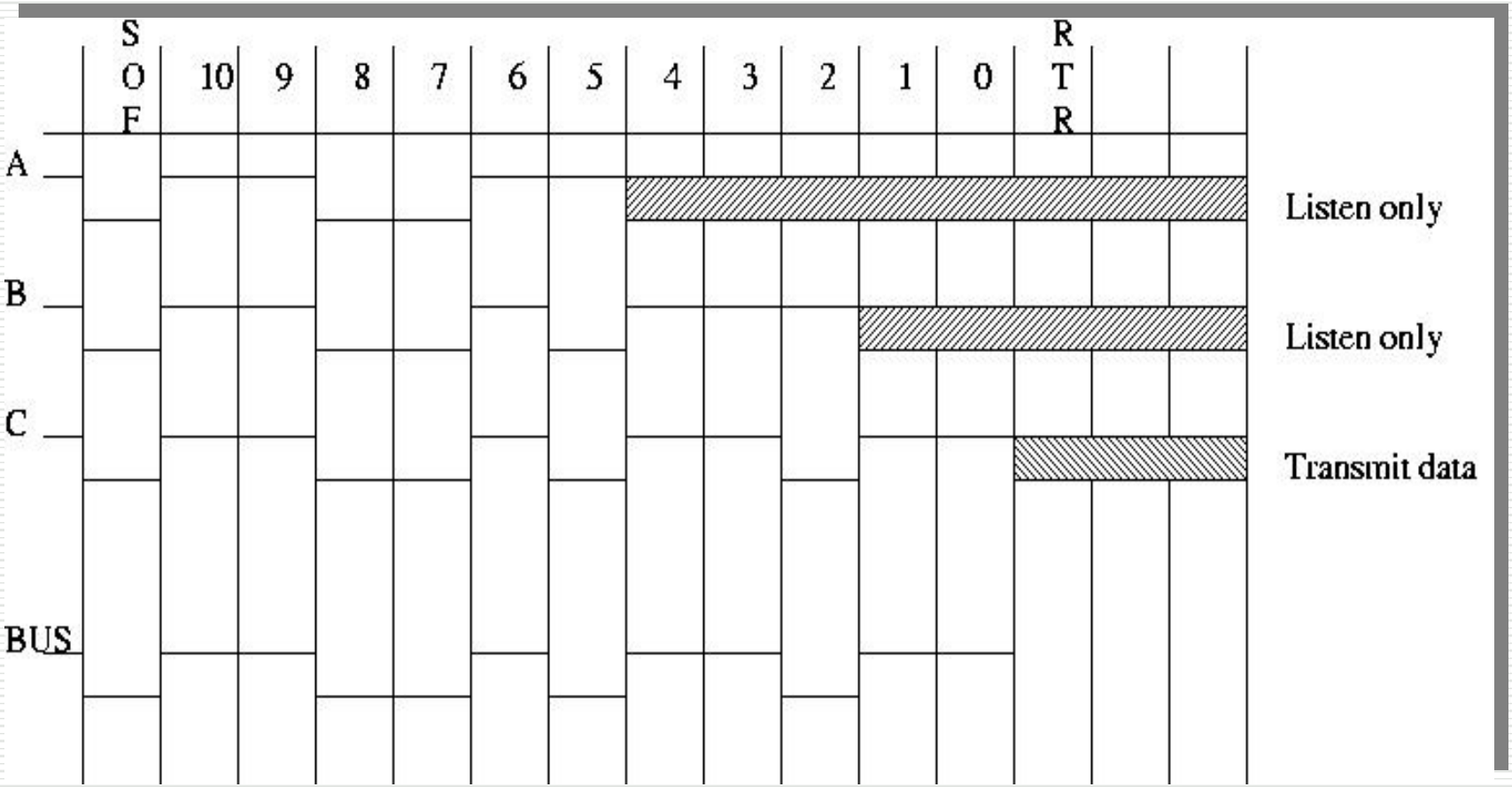
- ***Introduced in 1986 by Bosch for use in automobile industry.***
- ***Now used everywhere there are networks***
- ***Found on many micro-controllers as standard port***
- ***Can achieve data rates up to 50 kBaud at 1000m***
- ***Uses twisted pair wire***
- Up to 127 nodes

Controller Area Network (2)

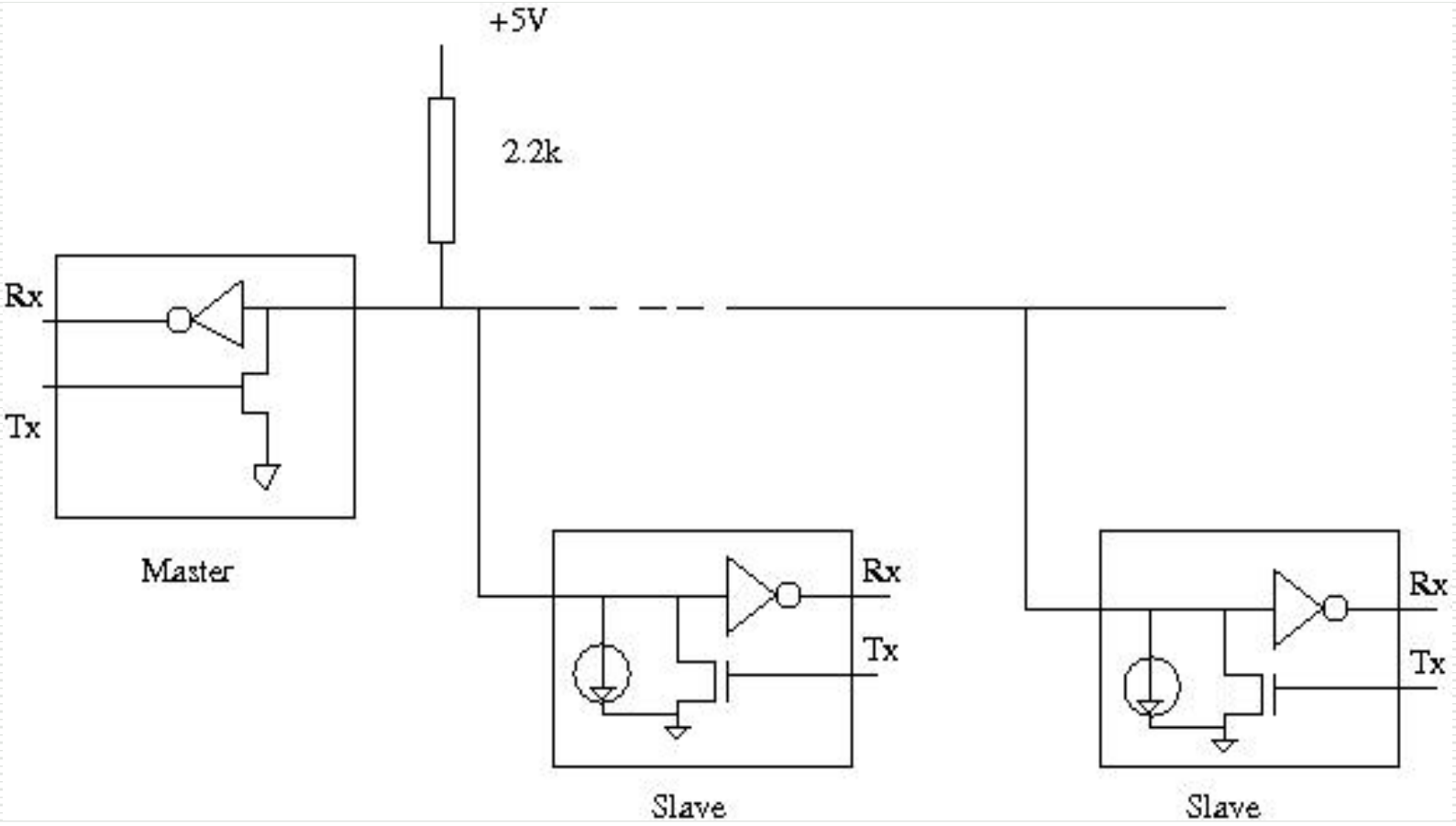
- *Differential data line pair (CAN_H and CAN_L) and common + optional shield and power*
- *Outputs are AND ed together on line*
- *State 0 is said to be Dominant and*

  state 1 is Recessive as 1 & 0 = 0

CAN Identifier message



1-Wire networking



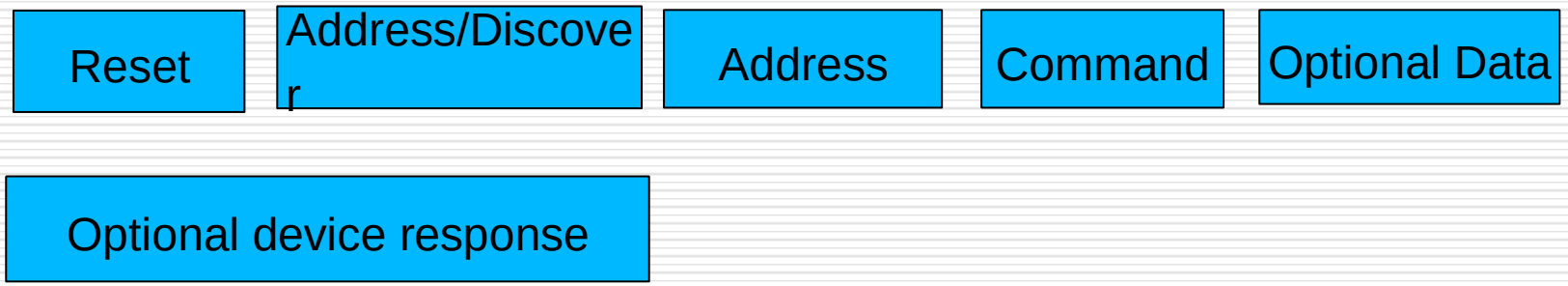
1-Wire networking (2)

- 2 speeds regular and overdrive at 16.3 and 144 kbits/s respectively
- All devices accept regular, only some overdrive
- Can put 80 -100 devices on bus over short distances (5m)
- Require twisted cable, repeaters, screening, distinct power etc for longer

1-Wire networking (3)

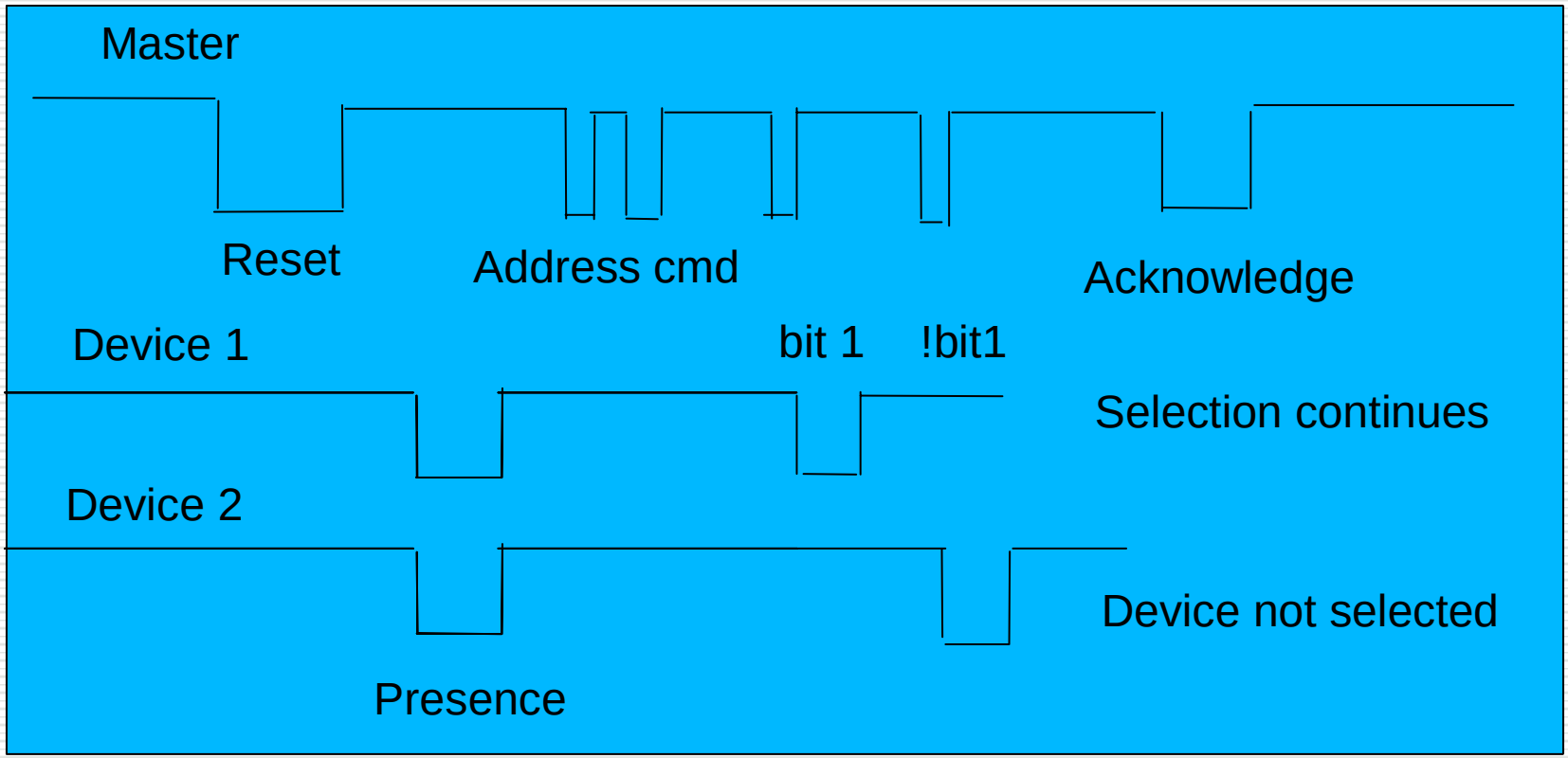
- Addresses 64 bit

- Commands



1-Wire networking

Device enumeration/selection



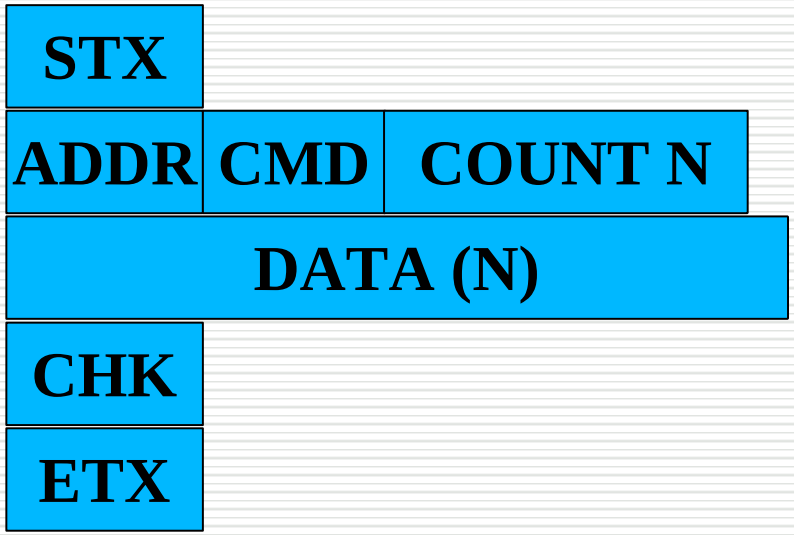
Elements of Protocols

Need a well-defined message structure

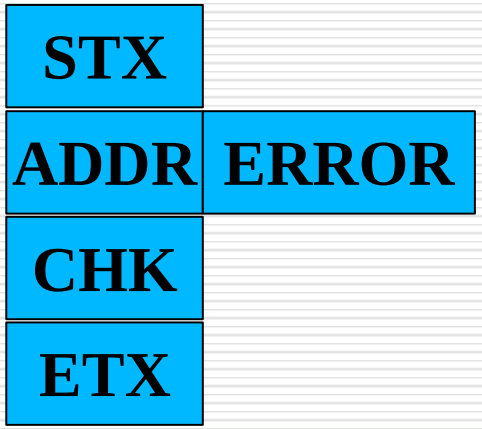
- ***Start, End, Length of data, Commands, Error checking.***
- ***Master command***
- ***Slave response***
- ***Error indication***

Elements of Protocols (2)

Master Command



Error response



Fieldbus systems

In industrial environments have:

- ***PLCs (analogue + digital)***
- ***Sensors***
- ***Digital switches and sensors***
- ***Quality control signals***
- ***Monitored using SCADA, HMI software***

Fieldbus systems (2)

- *Modbus*
- *Profibus*
- *CanOpen, DeviceNet*
- *Fieldbus*
- *+ many, many others*

Modbus

- ***Developed in the 1970/80s by Schneider for PLC networking but still default for many systems.***

- ***Open structure governed by Modbus Organisation***

- ***Uses RS 485 bus but also can use RS232 and recently has Modbus TCP/IP***

Modbus (2)

- *Has two protocols: RTU and ASCII. Each conforming implementation must support RTU*
- *Must support 9600 Baud and is expected to support 19200 Baud*
- *Must support 2 wire RS 485 (4-wire optional)*
- *Addresses between 1 and 247. 0 is broadcast address, 247 – 255 are reserved*
- *20 standard commands*
- *Allows user defined commands (up to total 127)*

Modbus (3)

RTU packet consists of:

1. Address (1byte)
2. Command (1byte)
3. Data (up to total of 255 bytes inc overhead)
4. Cyclical Redundancy Check (CRC)
5. The time separation between each byte sent is used to detect end of the packet according to:

$t < t_{1.5}$	Packet continues
$t_{1.5} < t < t_{3.5}$	Discard the packet
$t > t_{3.5}$	End of Packet

$t_{1.5} / t_{3.5}$ = 1.5/3.5 * time to transmit one byte

Modbus Commands

Structure of typical device is:

- Analogue signals from ADC (16bit registers)
- Digital bits (Coils and discretes)

Commands reflect this structure:

- Read Holding/Input registers
- Write Holding register(s)
- Read Coils/Discretes
- Write Coil(s)

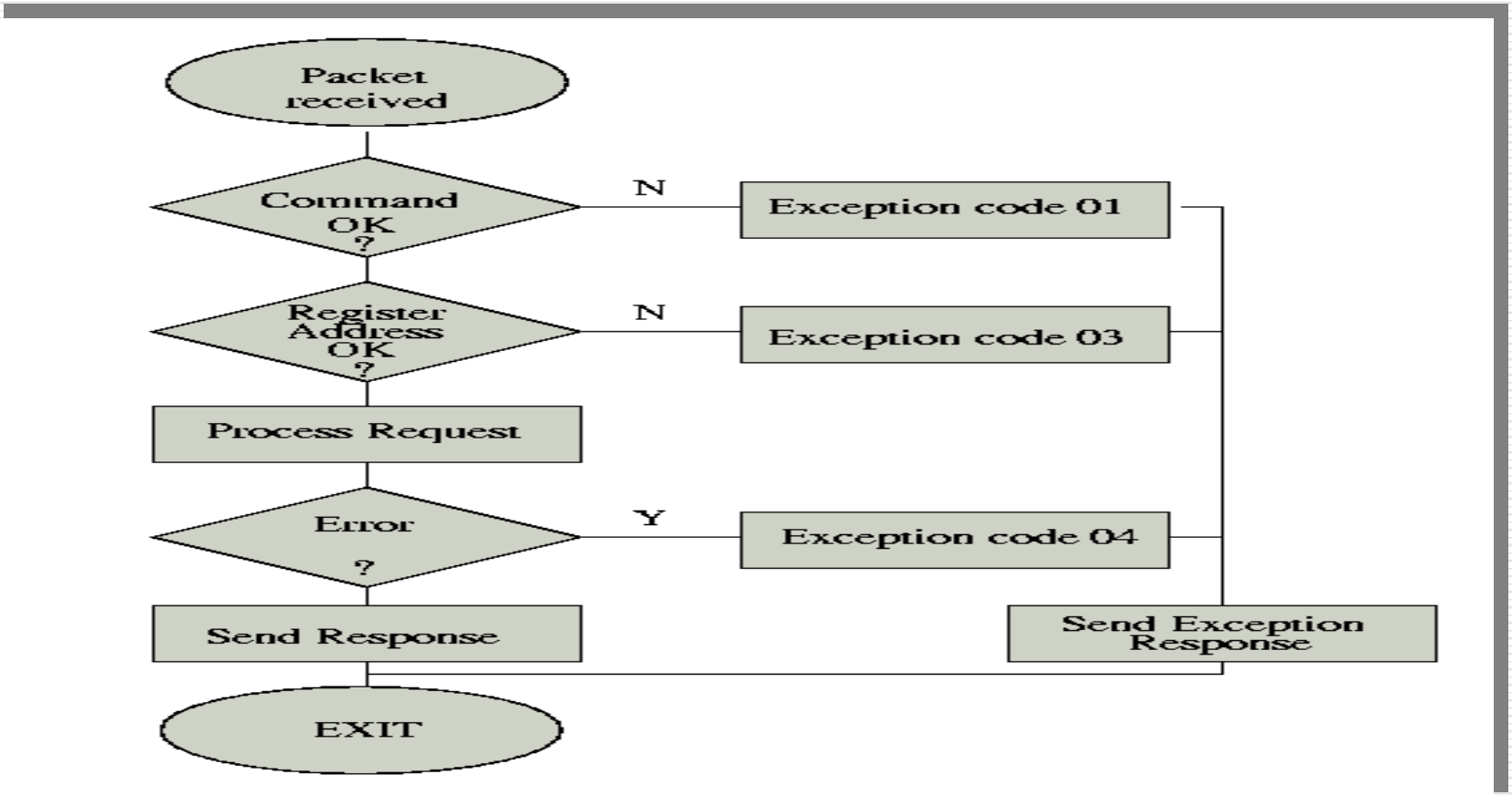
Modbus Commands (2)

- All register data are transmitted as Big Endian irrespective of processor
- Floats are not defined in standard but common format is IEEE representation (Little and Big Endian)

Modbus RTU packet for Command # 16 (Write Holding Registers)

Address	Function	Start Address	Number of registers N	Byte count	Data	CRC
1 byte	1 byte	2 bytes	2 bytes	1 byte	2N bytes	2 bytes

Modbus RTU command



Profibus

- *Started out as a proprietary protocol by Siemens*
- *Now released as a European standard and is probably the single most used system (at least in Europe)*
- *Uses modified RS 485 cabling (twisted pair, common, +5V)*
- *Up to 32 devices per segment, 127 devices in total*
- *Up to 12MBaud (over very short distances) are claimed, but 1MBaud more realistic*
- *Three varieties, Profibus DP (90%), Profibus FMS and Profibus PA*

Profibus (2)

- Profibus can have multiple bus masters but only one can be active at any one time
- Within a preset configurable time, the current master must pass a token to the next (dormant) master which is activated by receipt
- 4 types of telegram
- Each telegram must be separated by $t_{3.3}$ from previous one

Profibus (3)

Telegram

Profibus Data telegram with variable length

Start Delimiter	Length = DA+SA +DSAP+SSAP	Length	Start Delimiter	Destination Address	Source Address	Function Code
0x10			0x68			

Destination Servis Access Point	Source Servis Access Point	Data	Frame Checking Sequence	End Delimeter
		1 – 244 bytes		

Profibus (4)

GSD files:

All compliant devices must provide a GSD file which contains setup information so that any system can read the file and immediately be able to communicate with the device

CAN/CANOpen/DeviceNet Frame

CAN/CANOpen/DeviceNet Frame

SOF	IDEN	RTR	IDE	DLC	DATA	CRC	ACK	EOF

SOF/EOF:Start/End of frame; IDEN: Message identifier (11 or 29 bits)

RTR: Data or request for data; IDE: 11 or 29 bits; DLC # of data bytes

DATA: Up to 8 data bytes; ACK: Error (dominant)

Priority mechanism: Lower value identifiers (more dominant) higher priorities

Industrial Ethernet

- *More robust version of standard Ethernet (temperature range, noise immunity, connectors etc)*
- *Devices use industry standard 24VDC*
- *Backwards compatibility guaranteed for 10 years*
- *Modbus TCP/IP, Profibus (ProfiNet), FieldBus HSE etc protocols embedded in upper layers of TCP/IP stack*
- *Still not common but expected to increase*