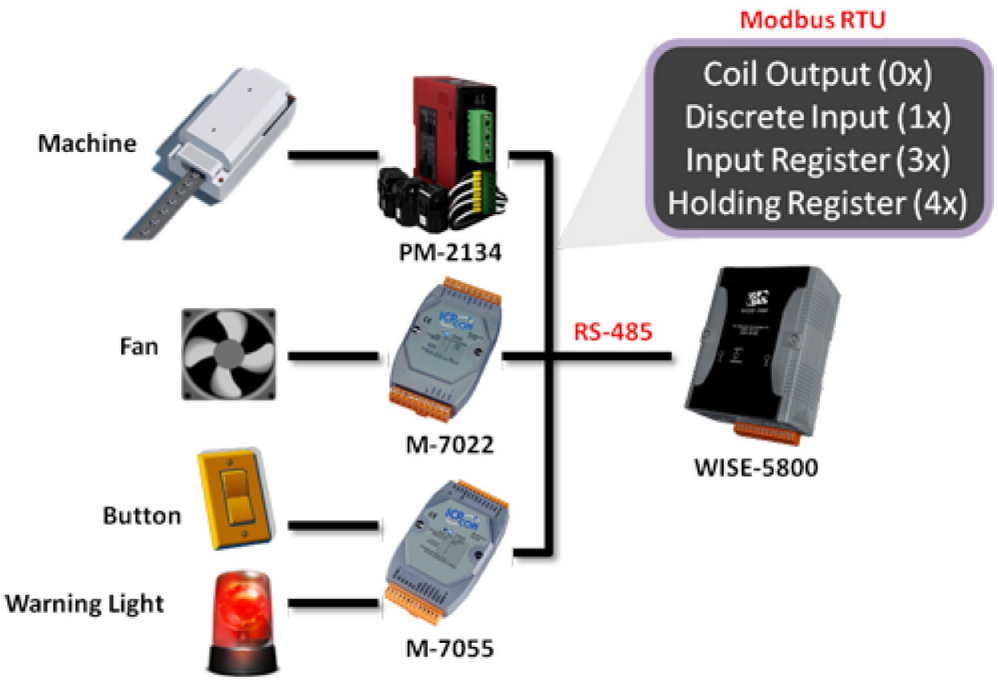
MODBUS

Antônio Augusto Fröhlich
LISHA / UFSC

SECCOM 2015

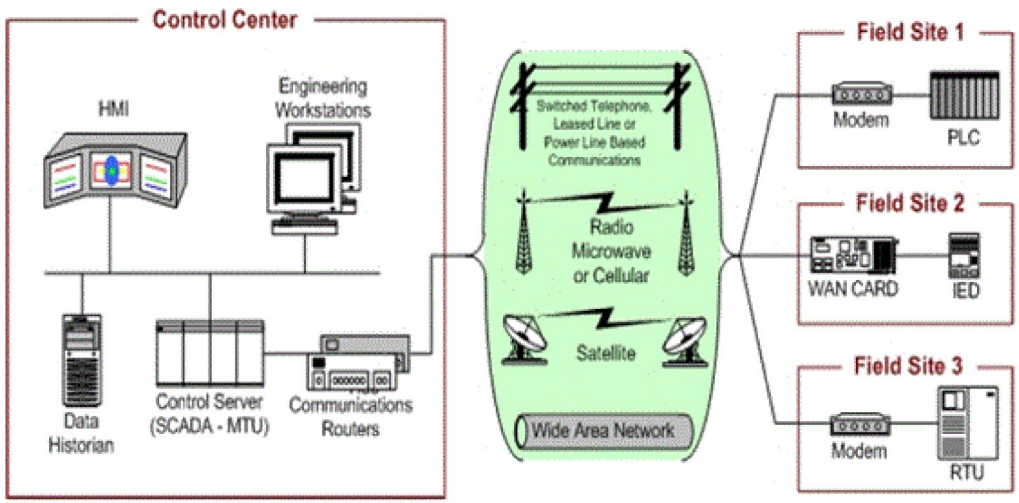
History

- Modbus is a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLC)
- Open and royalty-free
- De facto industry standard to connect industrial electronic devices to SCADA or HMI



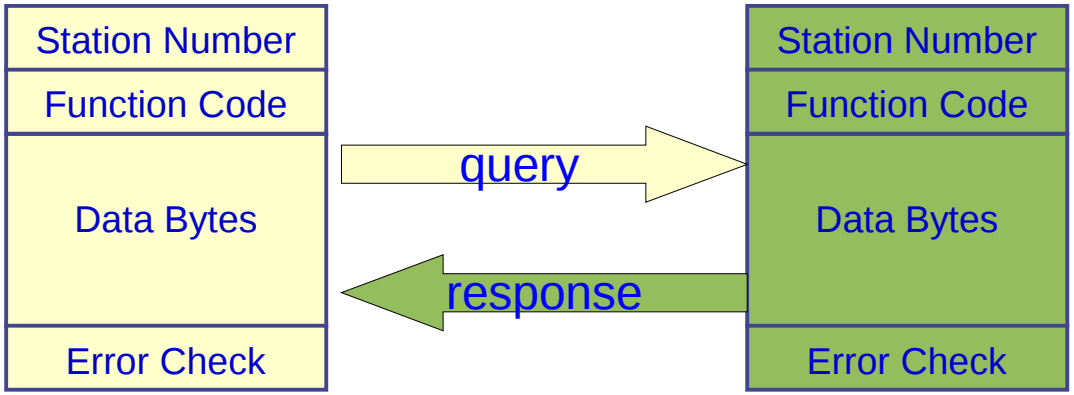
SCADA: Supervisory Control and Data Acquisition

- Remote equipment monitoring and control
- Architecture
  - Control Center (CC)
  - Remote Terminal Unit (RTU): sensors/actuators
  - Programmable Logic Controller (PLC): controllable sensors/actuators
  - Telemetry System: connects RTU/PLCs to CC



Modbus Protocol

- Request/reply protocol



- Serial data transmission modes
  - ASCII: 10 bits (1-7-O/E-1 or 1-7-2)
  - RTU (Binary): 11 bits (1-8-O/E-1 or 1-8-2)

- Communication interface
  - RS-232/485
  - Ethernet

Modbus Frame Format

- ASCII

1	2	1	n	2	2	bytes
Start	Station Number	Function Code	Data	LRC	CR+LF	

- RTU

28	8	8	n x 8	16	28	bits
Start (silence/mark)	Station Number	Function Code	Data	CRC	End (silence/mark)	

- Network

2	2	2	1	1	n	bytes
Trans.	Proto	Len	Station Number	Function Code	Data	

Big Endian

CRC = CRC16 IBM

LRC = see manual

Station Number = 1 .. 247

Modbus Data Types

- Coils: 1 bit r/w
- Discrete Inputs: 1 bit r/o
- Input Registers: 16 bits r/o (sensed data and status)
- Holding Registers: 16 bits r/w (configuration)

Modbus Functions (Requests)

Type			Name	Code
Data	**1-bit**	*Physical Discrete Inputs*	Read Discrete Inputs	2
		Internal Bits or Physical Coils	Read Coils	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bits	*Physical Input Registers*	Read Input Registers	4
		Internal Registers or Physical Output Registers	Read Holding Registers	3
			Write Single Holding Register	6
			Write Multiple Holding Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43

Modbus Exceptions (Responses)

- Success = repeat function code
- Error = function code + 128 and a 1-byte exception code

Code	Text
1	Illegal Function
2	Illegal Data Address
3	Illegal Data Value
4	Slave Device Failure
5	Acknowledge
6	Slave Device Busy
7	Negative Acknowledge
8	Memory Parity Error
10	Gateway Path Unavailable
11	Gateway Target Device Failed to Respond