Our energy working for you.™

Power Generation

Power topic #6046 | Technical information from Cummins Power Generation

Modbus communication protocol

White Paper

By Alberto Marvão, Lead Sales Application Engineer

Communication is one of the key factors that allows the development of advanced and complex control systems. However, the amount of communication protocols available today tend to be unaccountable. The interconnection of different control systems with the present technology is made via the use of some kind of communication, either a wire or wireless. The challenge of such diversity of control systems and communication protocols is the compatibility. What drives the main industrial communication protocols available worldwide are the Programmable Logic Controller (PLC) manufacturers. Modbus, developed by Modicon, is no exception.

Communication vs. hardwired interconnection

The term communication can sometimes be confused with hardwired interconnection between different devices that translates voltage or current levels of discrete hardware inputs/outputs. A communication protocol permits the exchange of information between two or more devices. The content of the information exchanged will depend on the devices with the communication capabilities, type of application and requirements.

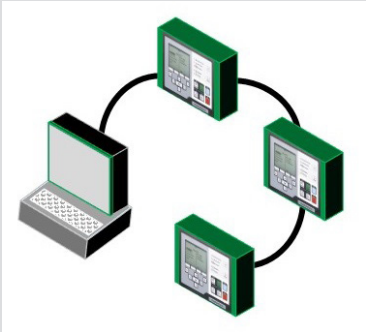

Figure 1: Representation Daisy Chain Network

OSI model

The Open Systems Interconnection (OSI) model (Figure 2) is a conceptual model that defines and creates a standard for communicating a system's internal functions by partitioning into different abstraction layers. The model was developed by the Open Systems Interconnection project at the International Organization for Standardization

(ISO) and is maintained with the reference ISO/IEC 7498-1. The model comprises seven layers.

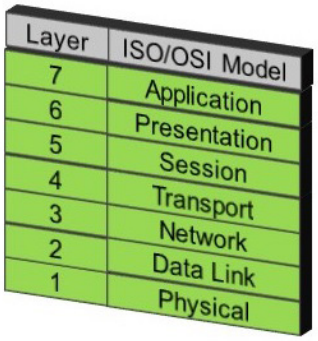

Figure 2: OSI/IEC 7498-1 Model

Modbus standard defines an application layer messaging protocol (Layer 7) that provides "client/server" communications between devices on a network. Modbus protocol over a serial line resides only on Layer 2 (Data Link) and Layer 1 (Physical) of the OSI model.

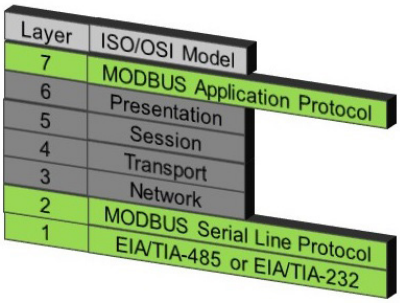

Figure 3: Modbus Protocol OSI Model

Modbus serial line protocol

The Modbus Serial Line Protocol is a master-slave protocol. As defined on the OSI model (Figure 3), this protocol takes place at Layer 2. The master-slave system comprises one master device and several slave devices. The limit of slave devices depends on the addressing capabilities of the system. The master device is the only one capable of initiating a communication and issuing explicit commands to the slave devices. The slave devices can only communicate with the master device when the master device requests some kind of information, after issuing a command. The slave devices cannot communicate among one another.

State diagrams

The master device process (Figure 4) comprises three stages: "waiting for reply," "process a reply" and "processing error." The running of the process through the different stages depends on the conditions shown on the master state diagram.

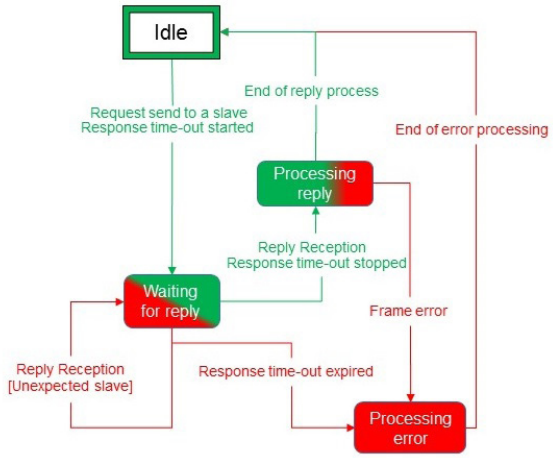

Figure 4: Modbus Master State Diagram

The slave device process (Figure 5) comprises four stages: "checking request," "processing required action," "formatting normal reply" and "processing error." The running of the process through the different stages depends on the conditions shown on the slave state diagram.

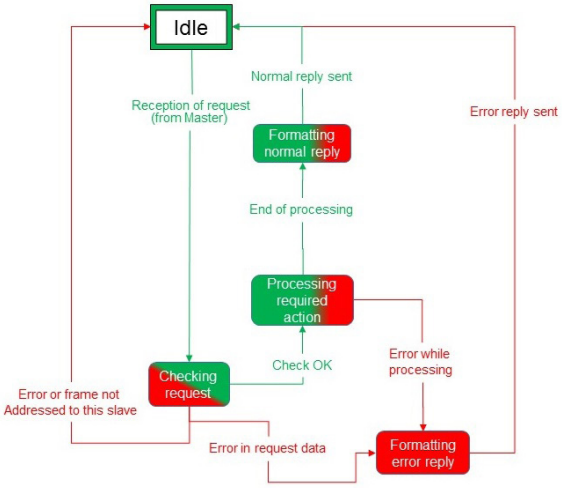

Figure 5: Modbus Slave State Diagram

Data stream

Modbus defines two different serial transmission modes: Remote Terminal Unit (RTU) and American Standard Code for Information Interchange (ASCII). The two modes define how the information is packaged (Figure 6) into the message (data stream), and all the devices on the Modbus Serial Line must use the same mode. RTU is preferred as it requires fewer bytes to send a message than ASCII. However, there are some rare devices on the market that do not support RTU. By default, Cummins-manufactured devices that support Modbus serial communication are set up to RTU mode.

Address field	Function code	Data	CRC (or LRC)
1 byte	1 byte	0 up to 252 byte(s)	2 bytes

Figure 6: Modbus Data Frame

The information interchanged between the master and the slaves is composed of several bytes: the address field, function code, data (discrete or analogue information) and CRC or LRC (bytes for error control).

The “address field” has specific values for broadcasting messages and for slave addressing, and some addresses are reserved. The different values that the field can be configured with can be seen on Figure 7. The capability of attributing unique addresses to each slave device determines the maximum number of slave devices that can be connected onto a single Modbus network.

0	Broadcast address
From 1 to 247	Slave Individual address
From 248 to 255	Reserved

Figure 7: Modbus Addressing Rules

The function code may have different values, normally ranging from 1 to 16. Function code 3 typically is used to read holding registers, and function code 6 to pre-set a single register. The function codes do not vary much from device to device, and it is up to the manufacturer of the slave device to publish what kind of function codes the slave supports and the register mapping address.

Data fields support up to 252 bytes of information. Some devices have a lower limit for the amount of data that can be supported on a single stream due to certain limitations of the transmission buffer. The master uses the data field to inform the slaves which address registers wants to retrieve information or pre-set, depending on the function code. The slave devices will use the data field to return information requested by the master device.

The CRC field uses two bytes. The CRC is the result of a binary mathematical calculation that the master and the slaves perform on each data stream received or sent. When packaging a message, the master will run the mathematical algorithm on the data that is to be sent, and at the end of the data stream, it adds the CRC bytes. When the slave receives a request, it performs the same mathematical algorithm on the data received. If the result matches with the CRC received, then the request is considered valid. If not, the request is ignored or generates an error on the network. The same operation is performed by the master when it receives the data from the slave. If the CRC bytes match, the master will consider the information valid.

Physical layer

Modbus over serial line implements an electrical interface in accordance with the EIA/TIA 485 standard (commercially known as RS485). This standard allows point-to-point and multipoint systems, in two-wire or four-wire configurations, depending on the device. Still other devices may implement EIA/TIA 232 (commercially known as RS232). Cummins Power Generation devices implement EIA/TIA 485 two-wire configurations. EIA/TIA 485 can cope with network lengths up to 1,000 meters, depending on the baud rate setup, while EIA/TIA 232 can cope with network lengths up to only 10 meters. The cables used should be a shielded type and with AWG26 or wider gauge. The topology to interconnect the different devices on the network must be a daisy chain layout (Figure 1) or by short derivation cables starting at the master device and ending in one of the slave devices. Termination resistors may be required if the starting and end devices aren’t equipped with terminating resistors. Typically the termination resistors have a value of 120 ohms, depending on the impedance of the communication cable used.

Setup options

In the design stage of the Modbus network, it is important to have a clear definition of the following (Figure 8):

- How many devices will communicate (maximum number of devices on the network that can be used limited by the addressing capabilities)
- A unique address attributed to each slave device
- Setup of the baud rate (speed of communication)
- Type of parity bit
- Number of start bits
- Number of stop bits
- Mode of communication
- Electrical interface
- Information regarding the register mapping of the slaves

Addressing	From 1 to 247
Baud Rate	From 9600 to 38400
Parity	Even, Odd , None
Start Bits	1 or 2
Stop Bits	1 or 2
Mode	RTU, ASCII
Electrical Interface	RS232 or RS485
Register	Modbus Register Map of Slaves

Figure 8: Modbus Network/ Devices Definitions

Cummins Modbus register mapping

Typically the Modbus register mapping (Figure 9) uses the register address of the parameters to be monitored or set up, depending on the type if not read-only of

About the author

Alberto Marvão is a graduate of the Coimbra Portugal Institute of Engineering with a bachelor's degree in electrical engineering - industrial electronics. He is a graduate of the Oporto Portugal Institute of Engineering with a license in electrical engineering - electronics and computers. Alberto has been with Cummins Power Generation since 2013 and is a Lead Sales Application Engineer in Kent, UK. He previously worked with Cummins Power Generation's Portuguese distributor for 12 years, and worked with the African distributor and Area Business Organization for two years, having roles as an Application, Service and Commission Engineer as well as a trainer.

the slave devices, defining which function code must be used. Let's take PC2.x for example. To monitor the battery voltage of the generator set, the register map references register 40061. To retrieve the information stored on this register, function code 4 or 3 must be used while the address of the register is only 0061. Master devices that use function code 3 or 4 and subsequently try to address register "40061" and not "0061" will have a feedback of illegal address.

			Sign: U				
40061	Battery Voltage	Read Only	Multiplier: 0.1	Unit: Vdc	Battery voltage value. Modbus and PCCnet has different multiplier value. For Modbus use only, multiplier/units = 0.1 volts		PC 2.x, PC 3.x
			Offset: 0	Lower Limit:			
			Size (bits): 16	Upper Limit:			
			Sign: U				

Figure 9: PCC Modbus Register Mapping Sample

References

- Modbus-IDA.ORG http://www.modbus.org
- Modbus over Serial Line, Specification and Implementation Guide V1.02
- Cummins QuickServe Online - https://qsol2.cummins.com/info/index.html
- Cummins Power Generation - Modbus Register Mapping A029X159 (Issue 10)

Power Generation

Our energy working for you.™
power.cummins.com

GLPT-6046-EN (12/14)