WHITE PAPER

Introduction to Modbus

Modbus is one of the most popular protocols used in the industrial world. Supporting traditional serial protocols of RS232/422/485 and Ethernet protocols allow industrial devices such a PLCs, HMIs and meters to use Modbus as their communication method. When communicating with Modbus via serial and Ethernet networks, a communication gateway is a necessity. B&B Electronics new line of Modbus serial servers, MES1A and MES1B, enable this smooth connectivity, translating Modbus/TCP to Modbus/ASCII/RTU protocols. This allows devices such as PLCs to communicate to devices such as sensors, meters and instruments.

Modbus ASCII/RTU

The Modbus protocol emerged in the mid-1970s as an early protocol for linking terminals with Modicon PLCs using a master/slave (sometimes called a master/client) relationship. A simple, open, message-based protocol, it caught on quickly and became a defacto standard in the industry. It supports asynchronous point-to-point and multidrop communications and can be used with a variety of serial interfaces (RS-232, RS-422, RS-485, modems, etc).

The original Modbus specification included two possible transmission modes: ASCII and RTU. Modbus RTU mode is the most common implementation, using binary coding and CRC error-checking. Modbus ASCII messages (though somewhat more readable because they use ASCII characters) is less efficient and uses less effective LRC error checking. ASCII mode uses ASCII characters to begin and end messages whereas RTU uses time gaps (3.5 character times) of silence for framing. The two modes are incompatible so a device configured for ASCII mode cannot communicate with one using RTU.

Modbus/TCP

Modbus/TCP is a much more recent development, created to allow Modbus ASCII/RTU protocol to be carried over TCP/IP-based networks. Modbus/TCP embeds Modbus messages inside TCP/IP frames. Although the implementation is fairly simple, characteristics associated with networking add some challenges. For example, because Modbus masters expect and require responses to their polls within a certain time frame, the non-deterministic (and other) aspects of TCP/IP networks have to be considered.

Modbus/TCP sets up connections between nodes on the network, sending requests via TCP in a half-duplex fashion. TCP allows multiple requests to be 'pipelined', or queued in a buffer waiting to be serviced. Modbus/TCP has the capability to use transaction identifiers (sequence numbers), but some early manufacturers of Modbus/TCP equipment did not use them. In some cases this can create problems for Modbus/RTU devices connected to the network through interfaces. If a request from a master is lost, or contains an improper function code, the slave does not respond. The master may re-initiate the request, or there may be other requests in the pipeline. Responses to later, or other, requests may become out of sync and the master may match the wrong response with a request. The resulting symptoms could range from appearing to receive wrong data from a slave, to slaves going off-line, to a gradually slowing down of response time.

B&B Electronics