SIEMENS

James Powell, P. Eng.

Profibus and Modbus: a comparison

We live in a multi-protocol world – and this will likely not change anytime soon. Different protocols work better in different applications. I have not come to bury Modbus or Profibus, nor to praise them, but rather to add some perspective and knowledge.

In this article, we will provide an overview of both protocols and discuss their key strengths and applications. Comparing the two, we'll see that both protocols have their own particular strengths. We'll also discuss which one works best in which applications – although there is some overlap in what each can do. What's more, they can complement each other in joint applications.

Introduction to Modbus

Modbus is the "granddaddy" of industrial communication protocols. It was originally designed in the mid-1970s by Modicon as a way to link intelligent devices with PLCs using a simple master/slave concept.

"Simple" is a key descriptor for Modbus – and also its biggest strength. It is easy to implement and easy to use. When it was first introduced, it was a proprietary protocol that only Modicon could use. However, it was later published royalty-free so that anyone could use it. Finally, Modicon made it an open protocol. When it was published, a number of companies started using it, creating different interpretations and modifications of the original specification. As a result, there are now quite a few variations in the field.

The specification document is fewer than 100 pages in length, which is a good indication of the protocol's low level of complexity. In comparison, Profibus' specification document is thousands of pages long.

The term "Modbus" typically refers to one of three related protocols: Modbus ASCII, Modbus RTU, or Modbus TCP/IP:[1]

- Modbus ASCII was the first Modbus and is a serial protocol, typically running on

either the RS-232 or RS-485 physical layer. All slaves are polled on demand by the master, and there is only one master. The message frame can be up to 252 bytes in length, and up to 247 addresses are possible. The message frame and function codes, shown in Figures 1 and 1.1, are very simple.

- Modbus RTU is really just a small variation on the Modbus ASCII protocol. The only difference is in the encoding of the data. ASCII encodes the message in ASCII characters, while RTU uses bytes, thus increasing the protocol's throughput. In general, RTU is more popular, particularly in new installations.
- Modbus TCP/IP was added much later. One simple way of thinking about Modbus TCP/IP is to picture it as simply encapsulating a Modbus RTU packet within a TCP/IP packet. There is a bit more to it than that, but this is essentially what Modbus did. As a result, Modbus TCP/IP is also very simple to implement. The tradeoff is that, because it uses TCP/IP protocol for all messages, it is slow compared to other Ethernet industrial protocols – but still fast enough for monitoring applications.

How Modbus works

As already noted, Modbus is a simple master-slave protocol. The master has full control of communication on the bus, whereas a slave will only respond when spoken to. The master will record outputs and read in inputs from each of its slaves, during every cycle, as shown in Figure 2.

The protocol is pretty basic. There is no additional requirement for the slave or master to have a watchdog timer to ensure that communications occur within a certain time. The slave devices do not "join" the network. They simply respond whenever a master talks to them. If the master never talks to them, then they are idle.

There is also no requirement for diagnostics related to the slave's health. If the master requests data that does not make sense to the slave, then the slave can send an exception response. However, if the process variable is bad or if the device has problems functioning, there is nothing in the protocol that requires the slave to report this.

The physical layer

Modbus ASCII and RTU both typically use either the RS-232 or RS-485 physical layer, but can also use other physical layers such as phone lines or wireless.

Recommended Standards (RS) 232 and 485 were established physical layers when Modbus was first developed. RS-232 is for point-to-point, while RS-485 is for multi-drop applications. In both cases, Modbus did not add any new requirements to these physical layers.

This worked, but it has caused a few problems in the case of RS-485. The problem is that the physical layer has a number of variations: 2-wire, 4-wire, use of common and variations in drivers and grounding methods. Anyone who has worked with Modbus on RS-485 from multiple vendors will already know how to manage all the variations when connecting two types in a point-to-point configuration. The difficulty comes when the site is multi-vendor and several variations have to be combined on one cable.

There are a number of standards for both phone lines and for wireless. Modbus has excelled in these applications because of the small number of timing constraints in the protocol. Phone lines as well as wireless modems introduce delays in messages. Sometimes these delays are non-linear throughout the message, which can cause real problems for many protocols. However, Modbus either does not have a problem with this, or it can be adapted so that it will work in these applications.

Typical applications

1. Controller/monitor to a smart device (Figure 3) – In this application, there is one smart device from which data needs to be pulled. This point-to-point application is a common Modbus ASCII/RTU task. The variations in both

Address field	Function code	Data	Error check

Figure 1: Modbus message frame

Function code	Action	Table name
01 (01 hex)	Read	Discrete output coils
05 (05 hex)	Write single	Discrete output coil
15 (0F hex)	Write multiple	Discrete output coils
02 (02 hex)	Read	Discrete output contacts
04 (04 hex)	Read	Analog input contacts
03 (03 hex)	Read	Analog output holding registers
06 (06 hex)	Write single	Analog output holding register
16 (10 hex)	Write multiple	Analog output holding registers

Figure 1.1: Modbus function codes

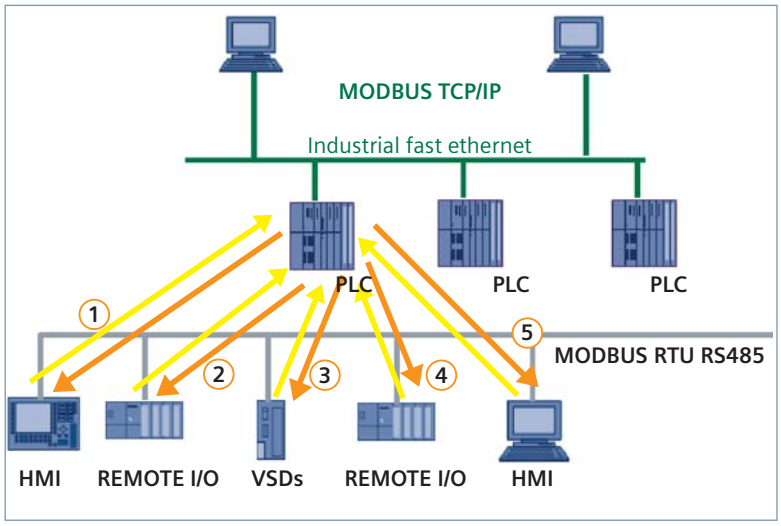

Figure 2: Modbus scan

Figure 3: Controller/monitor to one device, in this case, Milltronics BW500 weighing integrators from Siemens.

Figure 4: Controller/monitor to many devices of same type,

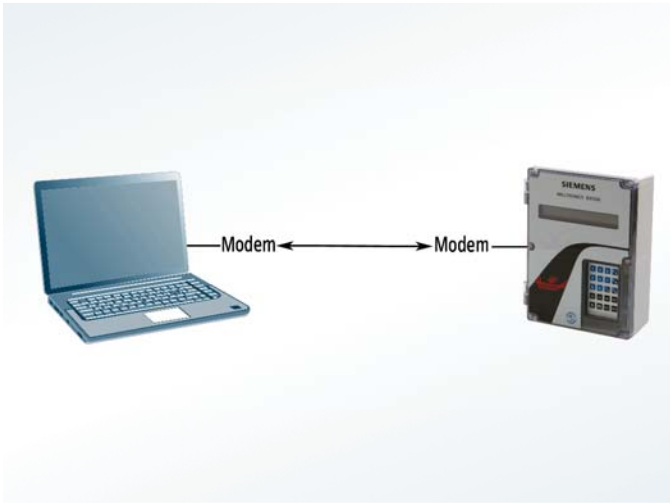

Figure 5: Remote monitoring of information from one device via modem

the protocol and the physical layer are easy to manage, and this application is simple to get working.

2. Controller/monitor to many smart devices from the same vendor (Figure 4) – Like the first application, this is very easy to implement. The variations in the protocol are generally not a problem.

3. Remote monitoring of information from a smart device (Figure 5) – Since the Modbus protocol is modem-friendly and has no watchdog timers, implementing remote data collection is very easy.

Introduction to Profibus

If Modbus is the "granddaddy" of protocols, then Profibus is the young athlete – lean and fast. Profibus was designed in the 1990s to meet all industrial communication needs for both factory and process automation (Figure 6). As with Modbus, there are a number of terms associated with this protocol: Profibus DP, Profibus PA, Profisafe, Profidrive, and Profinet.

One way of visualizing how these terms fit together is to think of Profibus as a book with many chapters. The book would be called Profibus DP (Decentralized Peripheral). The book's chapters would be called Profibus PA (Process Automation), Profisafe for safety application, and Profidrive for high-speed drive applications. In addition, there would be a second book by the same authors called Profinet, with many chapters, including Profisafe and Profidrive.

How does Profibus work?

Profibus is also a master-slave type protocol like Modbus (see Figure 2) but with an additional token ring protocol to allow for multiple masters. Also, unlike Modbus, all devices go through a startup sequence during which they "join" the network. Each slave maintains a failsafe timer. If the master does not talk to it within a certain time limit, the slave goes into a safe state; the master must then go through the startup sequence again before further data exchange can occur. This, in combination with a watchdog timer in the master, ensures that all communication occurs every bus cycle with a certain time value.

The general bus scan would happen as shown in Figure 7. Master A receives the token, which gives it control of the bus. It will then exchange data with each of its slaves, and when complete, pass on the token to the next master (if there is one).

The requirement for detailed diagnostics from each slave is also built into the protocol. During normal data exchange, a slave can alert the master that it has diagnostics, which the master will then read during the next bus scan.

Profinet is built on the same principle as Profibus. But unlike Modbus – which basically took the Modbus RTU packet and encapsulated it into a TCP/IP packet – Profinet was designed to take advantage of Ethernet and permit easy addition of higher-end Profibus functions like Profisafe.

Physical layer

The main physical layer for Profibus DP is based on RS-485, which Modbus uses. However, in the case of Profibus, the Profibus specification does not simply refer to the existing RS-485 specification. Instead, it extends the RS-485 specification. The physical layer was tightened up to require only two wires, with speeds as fast as 12 megabits per second. The Profibus specification also standardized on the connectors. All of this is beneficial when working with multiple vendors – wiring is easy and consistent.

For instrumentation, Profibus PA also has another physical layer called IEC 61158-2, Manchester Encoded, bus-powered, intrinsically safe (MBP-IS). This physical layer provides power and communications on the same two wires. The intrinsically safe concept has a big advantage when it comes to installation costs. Working with hazardous environments, there are two approaches: The power going to the instrument in the hazardous area can be contained, or the power going out into the hazardous area can be limited. The containment method is the traditional one and the one that is required for

Modbus. It uses a metal conduit and seals to "contain" the energy. Both the conduit and seals are expensive to buy and install. The second approach is used by Profibus PA. It limits the power going to the field and is considered intrinsically safe. With it, no conduits or seals are needed (except maybe at the starting cabinet), resulting in significant cost savings.

Profibus noise immunity

Both of Profibus' main physical layers (modified RS-485 and MBP-IS) are highly detailed and have excellent noise immunity, proven over and over again at countless sites. Once Profibus is designed and installed properly, it is next to bulletproof.

Standardized outputs and function block design

For instrumentation, there is a part of the Profibus standard called the profile standard, which is a standardization of an instrument from the point of view of the bus. It defines not only standard inputs and outputs, but also functions and functionalities that are within the instrument. This helps in both the setup and integration of field instruments and allows for easy multi-vendor applications.

For example, the output from all Profibus PA transmitters is five bytes long. The first four bytes are the IEEE floating point value of the process variable. The fifth byte is the status byte that indicates whether or not the process variable can be trusted. The major status codes are all standardized in the specification. A value of x80, for example, indicates that everything is okay. This applies to all transmitters from all manufacturers [Figure 8]. This significantly lowers the amount of engineering required for device integration. Whereas with Modbus, every device's data and diagnostics are completely individualized and must be adapted, this is not the case with Profibus.

Use with modems

Profibus DP and Profinet both have tight timing constraints. However, a number of vendors have been able to make a variety of modems (phone lines, wireless, cell) work well with both of them.

Typical applications

Profibus was designed to automate an entire plant, regardless of its size or whether the plant is factory automation (composed of discrete input/output) or process automation (made up of analog input/output). It also does not matter if all the sections are local or remote: Profibus can handle it all well.

To review: Profibus vs. Modbus

Let's review the comparison of Profibus and Modbus, based on the factors discussed here.

Modbus is a very simple, easy to use, modem-friendly protocol. However, there is a fair amount of variation in the protocol itself and in its physical layer definition, which creates problems in multi-vendor applications. Profibus is a very robust protocol that was designed to automate entire plants. It works extremely well in multi-vendor applications, with modems, and has detailed diagnostics.

When connecting a controller to one smart device in a point-to-point configuration, or if there is only one remote site, Modbus is an easy solution. For situations where there are more points, where different vendors are involved, or where there is a hazardous environment, Profibus is a better solution.

Combined application

One application that is gaining in popularity offers the best of both worlds. This application uses Modbus as the data transport between a master controller/data concentrator and has a remote station that uses Profibus.

One example of this application is shown in Figure 9: A small PLC (S7-1200) polls data from some radar units (Sitrans LR250) using Profibus, and passes the information up to the control system using Modbus.

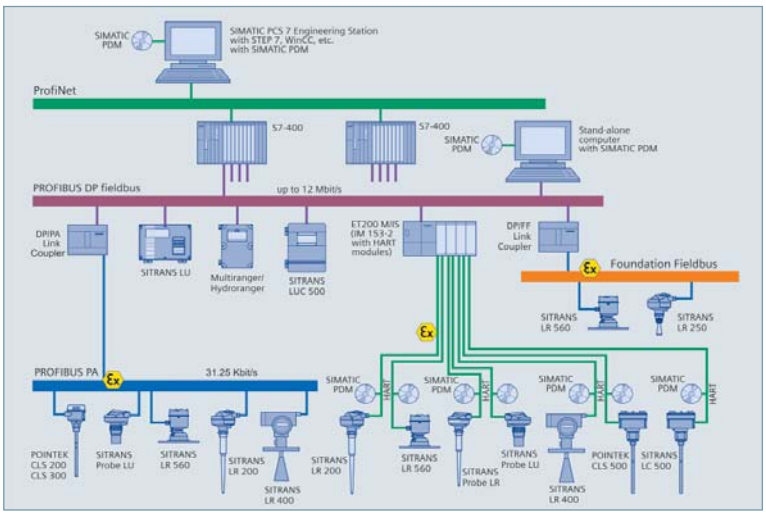

Figure 6: Profibus network

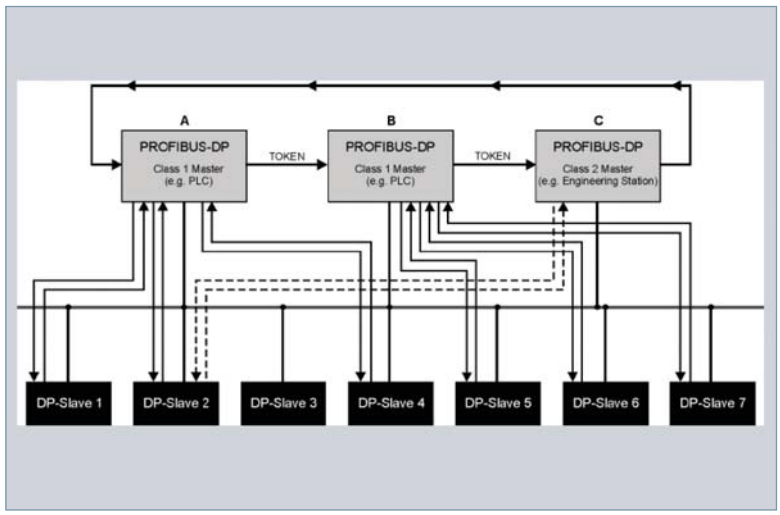

Figure 7: Profibus scan

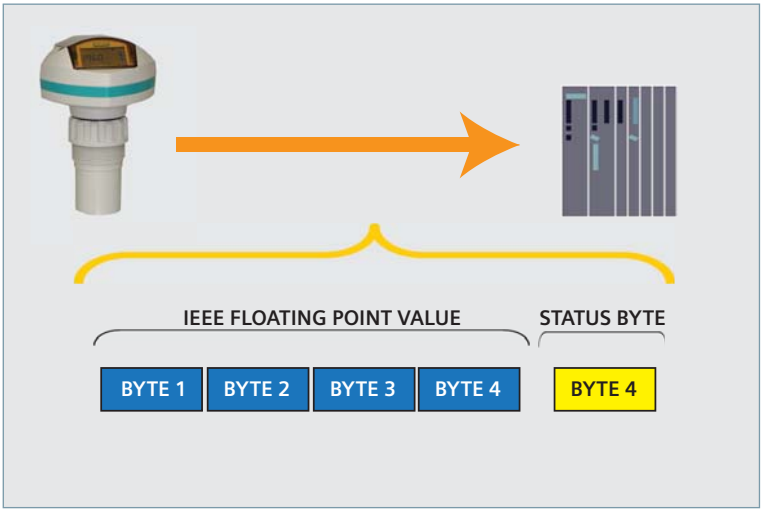

Figure 8: Profibus PA standardized output

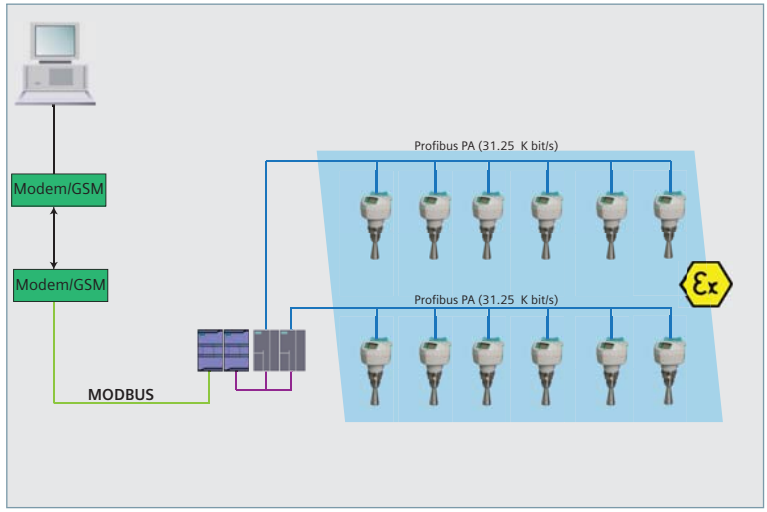

Figure 9: Profibus in a hazardous area

The benefits of this type of setup are significant. On the Modbus side:

- Easy modem support
- Simple implementation

On the Profibus side:

- Standardized output and diagnostics from the instruments
- Robust physical layer
- Intrinsically safe installation, thereby reducing installation costs
- Ability to communicate to field instruments via the bus

Profibus/Profinet's robust communications and ease of use in hazardous and/or multi-vendor applications make it an ideal protocol for all industrial applications. Modbus is easy to use in small applications and provides a good link between a SCADA system and data concentrator, as seen in Figure 9.

Both protocols will live long and prosper – Profibus/Profinet for most applications, and Modbus/Modbus TCP/IP for point-to-point applications.

	Modbus	Profibus
Detail in protocol	Simple (<100 pages)	Very detailed (thousands of pages)
Use for control	No watchdog timer	Detailed watchdog timer in master and slave
Interoperability	Problematic	Great interoperability
Profile standard	No	Yes
Redundancy	No	Yes
IS	No	Yes
Bus powered	No	Yes
Ease of use	Operators need only standard knowledge	Requires more knowledge; still easy to use
Noise immunity	Depends on drivers used	Excellent

[1] There is another 'Modbus' called 'Modbus Plus' that was developed by Modicon. This protocol was never made public and is no longer being used in new applications.

Siemens AG
Industry Sector
Sensors and Communications
76181 KARLSRUHE
GERMANY