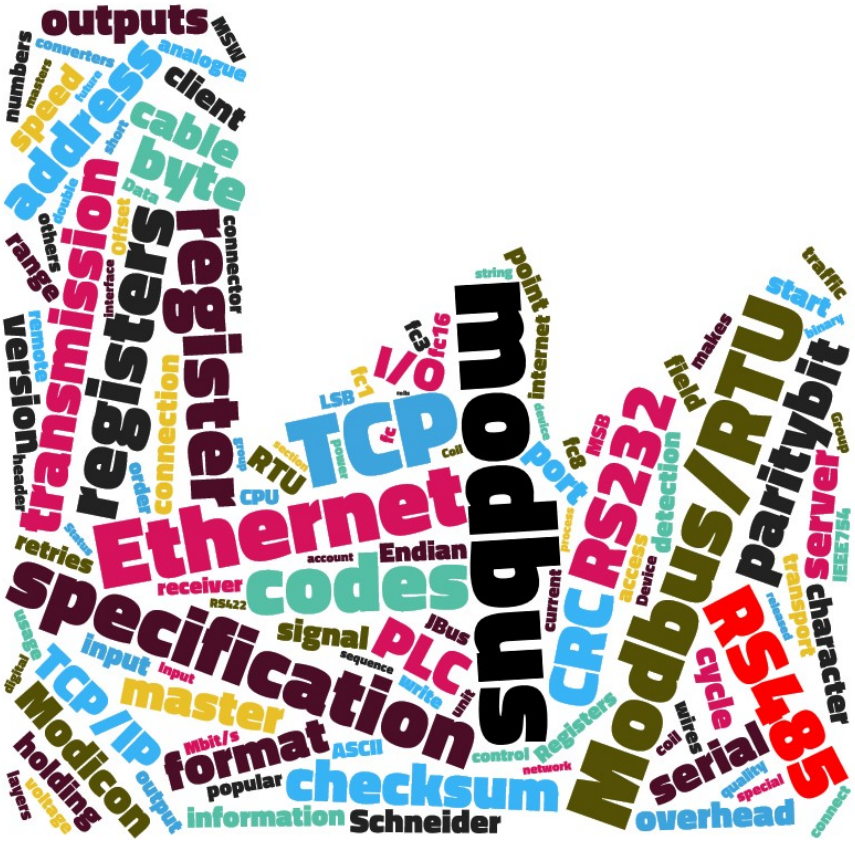
MODBUS

THE MANUAL



March 2019

About the author

Author Rob Hulsebos has been involved with industrial networks since their beginning in 1993. He studied Computer Science with a specialization in data communication. Working as a software-engineer for a PLC vendor, he made implementations for Profibus, AS-Interface, Bitbus, Ethernet, TCP/IP, various proprietary protocols, and several Modbus versions.

As of 1998 he has been active as a teacher for Mikrocentrum (Eindhoven, The Netherlands), providing courses on the basics of industrial networks, Profibus and industrial Ethernet, for more than 3500 students. He also publishes about ongoing developments in industrial networking for the Dutch trade press, and has written several books about this subject.

In 2010, Rob found the missing link during the reverse engineering of the Stuxnet virus, after which the operation of the virus could be explained. Since then, Rob is active in the field of industrial cybersecurity, where his experience in software-development and the implementations of protocol stacks helps to improve industrial products.

But as of 2019 Rob is still using Modbus! In recent years he made two new implementations of Modbus for an industrial controls vendor. Customers encountering Modbus for the first time still face the same issues as twenty years ago: lack of documentation. For unknown reasons no-one ever wrote a book about Modbus, despite its popularity. This book is the first attempt to fill that void, where all the theory of Modbus and Rob's personal experience are put together. Undoubtedly there are many improvements possible to this edition; the author welcomes your comments and ideas about improvements!

Contact the author at:

Het Kempke 8, 5672 PL Nuenen, The Netherlands

-or-

r dot hulsebos at onsnet dot nu

Thank you

The author would like to thank all those who helped improving the draft version of this book, either by pointing to typo's or grammatical errors, providing additional documentation, or supplying examples of the use of Modbus in daily life.

ISBN: 9789463867641

CHAPTER 1. PAST AND FUTURE

1. The history

The original development of Modbus was done by Modicon in 1979 for use with its own PLC's. Later Modicon was acquired by AEG which itself was acquired by Schneider, which is still considered the 'owner' of Modbus, even though the intellectual rights were transferred to the Modbus Organization (www.modbus.org).

The first member of the Modbus family, Modbus/ASCII, could be made on slow (according to modern standards: 1..10 MHz) processors because the protocol is very simple. It also had very relaxed timing requirements which made it usable on telephone modem links.

Later Modbus/RTU came into being, offering more performance, but at the expense of requiring a faster CPU needed for the protocol handling.

Around 2000, with the start of industrial Ethernet, Schneider launched Modbus/TCP which became very popular due to the absence of serious competitors, which were in development until ca. 2005. Even then, protocols like Ethernet/IP and ProfiNet still had to develop their market share, so Modbus/TCP was the most popular industrial Ethernet protocol until ca. 2012. In 2018 it was still the #4 of all industrial Ethernet protocols.

Around 2002, Schneider found Modbus/TCP to be technically obsolete. It decided to develop a modern industrial Ethernet protocol in cooperation with the German company Jetter. Later they christened the new protocol "IDA" and formed a trade association also called IDA, attracting other vendors (such as Phoenix Contact), with the idea of creating an "open" protocol specification, to compete with ProfiNet. A first version of the IDA-protocol was released in 2002. When the IDA association members could find no common ground on how to develop IDA further, both Schneider and Phoenix left IDA. This left both companies without any modern industrial Ethernet technology. Phoenix subsequently joined ProfiNet (Siemens), and Schneider joined Ethernet/IP (Rockwell, Allen/Bradley). It was then decided to integrate Modbus/TCP into the Ethernet/IP specification, allowing it to run concurrently with Ethernet/IP.

IDA continued for a few years, but showed no results. It merged with the Modbus User's Organization, to become the Modbus/IDA group. After a few years, the IDA developments were silently stopped and files and documents removed from the website.

On the 12th of April 2002 Schneider transferred its "right, title and interest' in the protocol copyright on Modbus to the Modbus/IDA group, a non-profit organization formed in 2002 to advance the use of Modbus in the world.

Despite the advances in other industrial Ethernet protocols, Modbus/TCP stood its ground. Due to Schneider moving on to Ethernet/IP, it was expected that Modbus/TCP would not be developed any further. But due to weaknesses in the protocol, Modbus/TCP devices became the #1 target for hackers searching the Internet for industrial equipment to hack. Many studies were made about a "Secure Modbus", but nothing much happened. Then in 2015 Schneider released the M580 controller with a version of Modbus called "Secure Modbus/TCP". It uses the "IPSec" (IP Secure) protocol, giving authentication of devices and detection of rogue network messages, without sacrificing speed. In August 2018, there was the surprising announcement of the release of the specification for "Modbus/TCP Security" [MBUSSECURE].

2. Where do we find Modbus?

Modbus is found in lots of equipment, ranging from very simple embedded devices to PLC's and (industrial) controllers and SCADA products. Due to the simplicity of Modbus and the low costs for electronic parts it is a good fit for embedded devices. In many SCADA systems the Modbus implementation is often available for free, making it the first choice for smaller industrial systems. Traditionally this is almost always the Modbus/ASCII or /RTU version, as it can be run over simple serial ports. For embedded devices Modbus/TCP is also more and more seen, because Ethernet-implementations have become very cheap.

Modbus is also available in the (industrial Ethernet protocol) called Ethernet/IP, as Schneider has chosen this protocol as its standard "Industrial Ethernet" protocol. As a consequence, to help existing customers to migrate from Modbus to Ethernet/IP, the Ethernet/IP system was extended to also officially support Modbus (also eased by Schneider becoming a member in the board of directors of the Ethernet/IP user group).

Modbus/TCP is also often found in devices supporting TCP/IP. When TCP/IP is available, an implementation of Modbus/TCP can be easily added. Since many industrial Ethernet protocols (i.e. ProfiNet) support TCP/IP for all non-real-time tasks, one can use Modbus/TCP next to the real-time protocol.

Finally, we see Modbus/TCP appear in cybersecurity devices called "intrusion detection systems", "firewalls" or "secure router". This is because many Modbus devices are not properly protected against incorrect network messages, messages from other devices, messages with unusual commands, etc. The protection devices scan all Modbus traffic, and reject all Modbus messages not fitting certain criteria. It is not that other industrial protocols are invulnerable, only that Modbus/TCP is very popular and it easy to implement.

3. The specification

The Modbus User's Group (www.modbus.org) is the entry point for all specifications about Modbus. On this website, the specification documents are freely available. The current (2018) version number is 1.1b3, which was last changed in 2012. In comparison with the previous version, not much was changed, except now it has become a "client/server" protocol instead of a "master/slave" protocol.

Technically this does not make any difference, and the Modbus protocol itself also hasn't changed. Furthermore the specification was written to be more conformant to "standardese" jargon and abbreviations, which makes it more difficult to read.

The reason for changing the terminology is unknown; it may have to do with historical reasons, or with marketing reasons, as client/server sounds more sophisticated. Anyway, the change will bring confusion[1] to a market which for more than 30 years has learned to live with the master/slave terminology.

Before the Modbus User's Group existed, Schneider was the owner of the specification. The original specification document is called "PI_MBUS-300", and can still be found on internet in many places. For reference purposes, it is also available from www.modbus.org. Although outdated, the document is surprisingly easy to read, so may be a good starting point for learning about the Modbus/ASCII and RTU protocols.

After the introduction of Modbus/TCP, the Modbus User's Group has rewritten the specification, so the description of the function codes is now separate from the physical layer specification. Also, the specification has been updated with more examples and flowcharts, to remove ambiguity on how to process incoming network messages.

Be aware that many Modbus implementations do not follow the specifications to the letter[2], especially the error handling.

4. The market position

The industrial network market consists of several hundreds of protocols, many small contenders, and a few with large market shares. We see this in every application area: machinery, discrete automation, process installations, building automation, automotive, embedded systems, etc. Historically, Modbus has a PLC-background, so it is not a surprise that it is still used in that market. But Modbus is also strong in process automation applications and in building automation. Surprisingly it is also popular in small embedded systems, due to its simplicity and low cost.

Around the year 2000, the migration to Ethernet-based industrial network protocols started, creating "industrial Ethernet". Modbus/TCP was on the market very early, and this helped to boost its market share. Implementations for Modbus/TCP were up-and-running, while many other

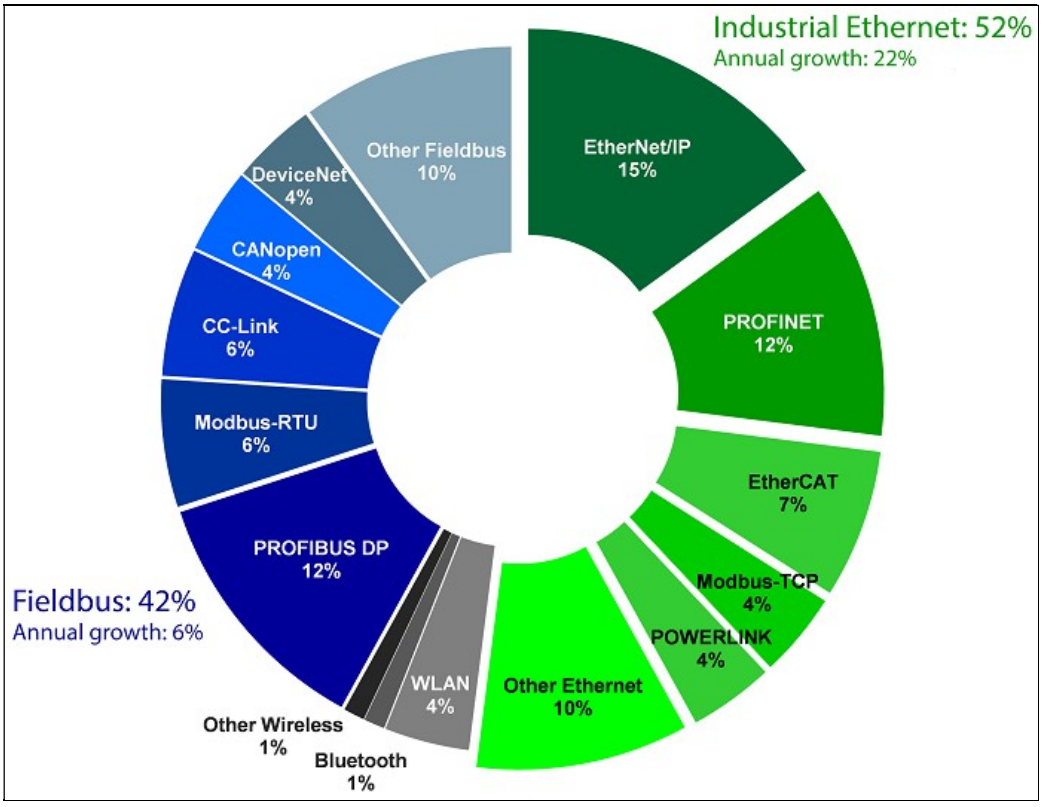
[1] *Personally, I find the effort could have better been spent in changing the ancient Modicon PLC terminology, like "coils". Who knows what a coil does nowadays in an industrial controller?*

[2] *Examples of this are a) the requirement for support of even parity on serial networks, which now often support 8N1, and b) the requirement for using 2 stop bits when no parity is used. In practice this gives problems on a lot of HMI masters which do not support 2 stop bits.*

protocols existed only on paper. For many years, Modbus/TCP was the most-popular industrial Ethernet protocol.

This changed slowly after 2005, but today (2016) Modbus is still the #3 most popular industrial Ethernet protocol, after ProfiNet and Ethernet/IP. It is difficult to find good market statistics, as this depends on whom is asked (vendors, customers), in which continent (Americas, Europe or Asia), and which market is researched. Also, many questionnaires fail to recognize the distinction between (for example) Modbus, Modbus/TCP, TCP/IP and Ethernet: if you are a Modbus/TCP user on Ethernet, which technology should you tick in a questionnaire? And what if you use Modbus/TCP in Ethernet/IP?

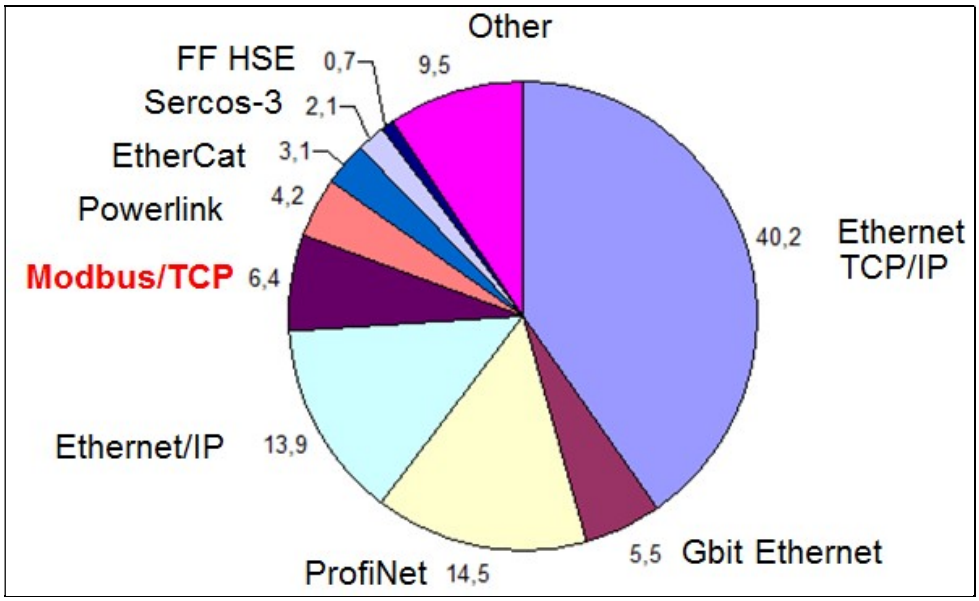
The Swedish company HMS publishes a yearly (since 2015) overview of the market shares of industrial network protocols, based on sales of their own products. In 2015 the serial Modbus was the 2nd most popular fieldbus protocol (7% market share) and Modbus/TCP the 4th Ethernet protocol (4%). In 2017, the market shares hadn't changed much (see figure below).



Industrial network market shares 2018 according to HMS

The products of HMS do not cover the complete industrial network market, i.e. there are no protocols listed typically used in process automation or building automation. Mainly, protocols that are used in machinery automation and embedded systems are listed. These are application areas where Modbus is not very popular; nevertheless Modbus/TCP is still listed as the #4 protocol of industrial Ethernet, and #2 of the first generation industrial networks. Probably the figures would change considerably if protocols from other parts of industry would be counted in.

Market researcher IMS published a study about the industrial Ethernet market shares in 2011 and 2015. Below are their projections for 2015, which have not changed much from the figures for 2011. Note that these diagrams show that Modbus/TCP's market-share is in decline against the other industrial Ethernet protocols *used for high-speed control*, which Modbus/TCP is not meant for.



5. Where can I use Modbus?

Modbus is a very general protocol, allowing for use in many sorts of application. I have seen it in machinery automation, process control systems, building automation, test systems, ships, press brakes, safety controllers, etc. After all, "a bit is a bit" and the network protocol doesn't much care what the bit is used for.

There is one exception to this: Modbus cannot (may not!) be used for safety applications, for example a PLC reading/setting safety I/O signals, such as for emergency stops and light curtains. Why not? The protocol is not "safe" enough; it cannot guarantee that the data sent and received is of the quality necessitated by the legal requirements for safety systems. It also cannot guarantee that the safety system's components will respond in time.

Now, Modbus is not unique – it turns out that most modern industrial network protocols cannot be used in safety applications (for the same reasons). In order to allow this, an additional layer of software[3] is needed to add the extra functionality. These have been written for various industrial network protocols, giving us ProfiSafe (=on top of Profibus/DP), CIP Safety (on top of CIP), Ethercat Safety, and many more. Unfortunately there is *no* Modbus/Safety!

[3] *This publication is not the right place to describe what this extra layer must do, but a book has been written about safety networks: Reinert, "Sichere Bussysteme für die Automation" Hüthig Verlag 2001, ISBN 3-7785-2797-5 (yes, it is in German).*

6. The future of Modbus

Even though Modbus is approaching its 40th birthday, it is still "alive and kicking". Despite its simplicity (as compared to modern industrial network protocols), or perhaps because of its simplicity, it is still very popular. It is still being implemented in new devices, due to its low cost requirements for electronics and software.

Despite this popularity, the Modbus User's Group is not active in designing new extensions to Modbus. Modbus/TCP was the last major innovation (and a very successful one at that!).

Surprisingly, Schneider Electronics launched the "M580 EPAC" (Ethernet Programmable Automation Controller) with Modbus/TCP allowing the use of the "IPSec" (IP Secure). IPSec adds a level of safety to a network: confidentiality (by encrypting data), integrity (no modification to data), authentication (knowing that you are communicating with the right party), and anonymity (not knowing with whom you are communicating). The M580 does not support all of IPSec; the data part of a TCP/IP network message is not encrypted. TCP/IP's administrative fields in a network message are encrypted. This still prevents modification of network messages, and the insertion of false messages in a TCP/IP data stream. So a hacker can still listen in on the data being transmitted, but he cannot influence the communication in Modbus/TCP. The advantage of not encrypting all data is that the speed of Modbus/TCP is not decreased.

According to a publication of security-company DigitalBond it became known that Schneider was working on an implementation of "Secure Modbus/TCP" (or Modbus/TLS). A presentation on Youtube (https://www.youtube.com/watch?v=kgvFWYv7Wwk) given during the S4x17 security conference (January 2017) gives more details about ongoing developments. Finally, in August 2018 the specification became publicly available, see [MBUSSECURE].

7. Usage in industrial Ethernet protocols

Modbus/TCP can also be used within ProfiNet and Beckhoff's Ethercat and any other industrial Ethernet protocol with support for TCP/IP. All these protocols have a method of guaranteeing their real-time behaviour, and they allow non-real time traffic using TCP/IP if spare bandwidth is available.

8. Literature

All documents can be retrieved directly from the website www.modbus.org. Older versions can be found everywhere on internet.

[MBUS300]	PI_MBUS_300.PDF June 1996	Version J of the "Modicon Modbus Protocol Reference Guide" was *the* Modbus specification for several decades. It is still being referenced by many vendors. The document is no longer formally valid; it has been split up in two separate documents (see below), describing the physical layer and application layer.
[MBUSSERIAL]	Modbus_over_serial_line_V1.02.pdf December 2006	A formalized description of the serial line interface, valid for Modbus/ASCII and Modbus/RTU.
[MBUSAPPL]	Modbus_Application_Protocol_V1_1b3.pdf	The description of all the commands (function codes), valid for Modbus/ASCII, Modbus/RTU and Modbus/TCP.
[MBUSSECURE]	Modbus/TCP Security MB-TCP-Security-v21_2018-07-24	The specification of the Modbus/TCP Security protocol.

CHAPTER 2. VERSIONS

1. The family

Modbus is not a single protocol, but a whole family, developed during three decades. Some of them are still used, others have already disappeared. Here's an overview (not chronological):

Modbus/ASCII	The first version, where the messages are sent as text (hence the "ASCII"). Occasionally it is still used.
Modbus/RTU	The successor of Modbus/ASCII, about twice as fast due to half the overhead. This is still a very popular version for use on RS232 or RS485 networks.
Modbus/TCP	The "industrial Ethernet" version of Modbus/RTU, running on top of TCP and therefor usable on almost anything that has a TCP/IP interface. For several years Modbus/TCP was the most popular industrial Ethernet protocol, and is today (2016) still #3!
Modbus/UDP	A variant of Modbus/TCP, using UDP (User Datagram Protocol) instead of TCP. This is much faster than TCP, allows for sending broadcast messages, but is less reliable than TCP. Some vendors claim to support Modbus/UDP, but there is no official specification for this protocol, so it is very likely that devices from different vendors cannot operate with each other as they will have completely different implementations.
Modbus/SFB	(Sequential Frequency Band) is a very special version of Modbus, as it is an implementation of Modbus on top of another protocol: Intel's "Bitbus". Twenty years ago this was a very fast technology (375 Kbit/s). SFB is hardly seen in practice, and Intel has stopped with supporting Bitbus in its processors.
Modbus/1	An alternative name for Modbus/ASCII or /RTU. It came into being when Modbus/2 was developed, and the need arose to distinguish the 'older' versions. But the name never caught on.
Modbus/2 (also called Modbus-II)	Originally thought as the successor of Modbus/1, this version was hardly ever used due to its difficult cabling methodology (RG6 coaxial cable). It has now disappeared from the market.