ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41868—2022

Modbus TCP 安全协议规范

Modbus TCP security protocol specification

2022-10-12 发布　　2023-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　规范性陈述 …… 2
6　概述 …… 2
6.1　mbap 概述 …… 2
6.2　mbaps 概述 …… 3
6.3　传输层安全性概述 …… 3
7　服务定义 …… 7
8　协议规范 …… 7
8.1　TLS 协议 …… 7
8.2　TLS 握手 …… 7
8.3　密码套件选择 …… 11
8.4　mbaps 基于角色的客户端授权 …… 11
9　系统依赖性 …… 13
10　TLS 要求 …… 13
10.1　TLS 版本 …… 13
10.2　TLS v1.2 密码选择 …… 13
10.3　TLS 分片 …… 14
10.4　TLS 压缩 …… 14
10.5　TLS 会话重新协商 …… 15
附录 A（规范性）　mbaps 数据包结构 …… 16
参考文献 …… 18

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、施耐德电气(中国)有限公司上海分公司、重庆信安网络安全等级测评有限公司、国能智深控制技术有限公司、浙江中控技术股份有限公司、中国科学院沈阳自动化研究所、东方电气集团科学技术研究院有限公司、北京卓识网安技术股份有限公司、西南大学。

本文件主要起草人：冯夏维、王勇、周彦晖、王玉敏、尚羽佳、朱镜灵、陈俊瑀、章维、刘明哲、桑梓、刘韧、刘枫、梅恪。

引　言

目前已经发布的 Modbus 协议国家标准包括：

GB/T 19582.1—2008《基于 Modbus 协议的工业自动化网络规范　第 1 部分：Modbus 应用协议》；

GB/T 19582.2—2008《基于 Modbus 协议的工业自动化网络规范　第 2 部分：Modbus 协议在串行链路上的实现指南》；

GB/T 19582.3—2008《基于 Modbus 协议的工业自动化网络规范　第 3 部分：Modbus 协议在 TCP/IP 上的实现指南》；

GB/T 25919.1—2010《Modbus 测试规范　第 1 部分：Modbus 串行链路一致性测试规范》；

GB/T 25919.2—2010《Modbus 测试规范　第 2 部分：Modbus 串行链路互操作测试规范》。

Modbus 协议最初于 1979 年用于工业控制器与计算机或其他上位机通信的串行协议。1996 年，Modbus 协议进行了以太网的扩展，使用了 IANA 登记的 502 号端口，支持 Modbus TCP 基于以太网的协议。同时，Modbus TCP 保持了与 Modbus RTU 串行协议的一致与兼容，这使得 Modbus 串行设备通过 Modbus TCP 实现桥接通信变得十分容易。2002 年，Modbus 抽象出适用于串行和以太网的 Modbus 应用层，开始使用 Modbus PDU 的概念，发布了 Modbus 应用层规范，针对串行和 TCP 不同的 ADU，也发布了串行和以太网的规范。同时，Modbus 也加入了 IEC 61784 作为行规之一。

基于转化 IEC 61784 中的 Modbus 协议规范，我国发布了 GB/T 19582 Modbus 系列推荐性国家标准。

也是由于国家标准的发布，这使得依照规范标准进行互操作性测试成为可能。后来制定发布了 GB/T 25919 系列标准，这极大地改善了大量 Modbus 应用的一致性和互操作性，有利于工业自动化系统的开发和集成。

像所有的工业通信协议一样，Modbus 最初没有设计信息安全功能。随着工业通信及应用对数据保密和完整性、设备身份识别等要求的需求增加，本文件使用通用的 TLS 传输层加密技术，对 Modbus 协议进行了扩充，使加密的 Modbus 通信能够增加抵抗比如重放和中间人等常见攻击的能力。

Modbus TCP 安全保持了与 Modbus TCP 一致的 ADU，这样能够使 Modbus TCP 通信能够容易地迁移到 Modbus Security。Modbus TCP 安全使用了 IANA 登记的 802 号端口用于安全通信。Modbus security 仅允许使用 TLS1.2 及以上版本。

Modbus TCP 安全还采用了 X.509v3 的数字签名证书，在客户端和服务器进行 TLS 协商握手时使用双向认证。同时，在证书中使用了 OID 扩展，设备厂家可以利用这个扩展指定客户端的角色和权限，可以实现工业信息安全所需要的用户识别及基于角色的控制。随着 Modbus TCP 安全标准的推出，为现有大量使用 Modbus 的设备，提供了一种简洁且直接的升级路径。

Modbus TCP 安全协议规范

1 范围

本文件规定了 Modbus TCP 安全协议的服务定义、协议说明、系统依赖性以及 TLS 要求等内容。

本文件适用于开发或检测 Modbus 产品的相关机构。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

RFC 4492 用于传输层安全(TLS)的椭圆曲线密码(ECC)加密套件[Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)]

RFC 5246 传输层安全协议规范，第 1.2 版[The Transport Layer Security (TLS) Protocol，V1.2]

RFC 5280 互联网 X.509 公钥基础设施证书和证书吊销列表(CRL)配置文件[Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile]

RFC 6066 传输层安全(TLS)扩展：扩展定义(TLS extensions：Extension definitions)

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。

ADU：应用数据单元(Application Data Unit)

AuthZ：授权(Authorization)

BER：基本编码规则(Basic Encoding Rules)

CA：证书颁发机构(Certificate Authority)

CDP：CRL 分发点(CRL Distribution Point)

CRL：证书吊销列表(Certificate Revocation List)

HMAC：密钥哈希消息认证码(Keyed-hash Message Authentication Code)

IANA：互联网号码分配机构(Internet Assigned Numbers Authority)

ICS：工业控制系统(Industrial Control System)

IEC：国际电工委员会(International Electrotechnical Commission)

MAC：消息认证码(Message Authentication Code)

mbap：Modbus 应用协议(Modbus Application Protocol)

mbaps：Modbus 安全应用协议(Modbus Security Application Protocol)

OID：国际电信联盟标准化的物联网域名(Object Identifier standardized by the International Tele-