ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 25919.3—2026

Modbus 测试规范　第 3 部分：TCP 安全协议一致性测试规范

Modbus test specification—Part 3:TCP security protocol conformance testing specification

2026-08-28 发布　　2027-03-01 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

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。

本文件是GB/T 25919《Modbus测试规范》的第3部分。GB/T 25919已经发布了以下部分：

——第1部分：Modbus串行链路一致性测试规范；

——第2部分：Modbus串行链路互操作测试规范；

——第3部分：TCP安全协议一致性测试规范。

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：国能智深控制技术有限公司、机械工业仪器仪表综合技术经济研究所、北京卓识网安技术股份有限公司、国能智深(天津)控制技术有限公司、施耐德电气(中国)有限公司、国能吉林龙华热电股份有限公司吉林热电厂、国家能源集团吉林电力有限公司吉林热电厂、国能大渡河流域水电开发有限公司、国能大渡河大岗山发电有限公司、北京广利核系统工程有限公司、中广核数字科技有限公司、华北电力大学、国网北京市电力公司、国网辽宁省电力有限公司大连供电公司、国电电力发展股份有限公司、北京信息科技大学、北京电安信科技有限公司、四川赛霏信息安全技术有限公司、四川九天数智科技有限公司、宁波苏克自控工程有限公司、青岛乾程科技股份有限公司。

本文件主要起草人：田雨聪、翟婉波、曹宇博、刘韧、梁金宝、王勇、阎新华、周坤丽、张林广、范明石、何红荣、何建锋、刘松、王晓燕、朱镜灵、李化龙、曲佳豪、黄泽华、龚钢军、李卓群、张栖国、商宁、丁佳、马宗乐、王大为、王天堃、吴秋新、张琪、刘松茂、刘永和、沈括、孟庆军、李刚、吴旭科、李冀颖、王玉敏、李吉林。

引　言

GB/T 25919《Modbus 测试规范》旨在规范 Modbus 设备的测试方法与判定要求。拟由 3 部分构成。

——第 1 部分：Modbus 串行链路一致性测试规范。目的在于规范 Modbus 串行链路设备的一致性测试。

——第 2 部分：Modbus 串行链路互操作测试规范。目的在于规范 Modbus 串行链路设备的互操作测试。

——第 3 部分：TCP 安全协议一致性测试规范。目的在于规范 TCP 安全协议产品一致性测试。

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；

——GB/T 25919.3—2026　Modbus 测试规范　第 3 部分：TCP 安全协议一致性测试规范；

——GB/T 41868—2022　Modbus TCP 安全协议规范。

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，Modbus TCP 安全协议使用通用的 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 安全协议保持了与 Modbus TCP 一致的 ADU，这样使 Modbus TCP 通信能够容易的迁移到 Modbus TCP 安全协议。Modbus TCP 安全协议使用了 IANA 登记的 802 号端口用于安全通信。Modbus TCP 安全协议仅允许使用 TLS1.2 及以上版本。

Modbus TCP 安全协议还采用了 X.509v3 的数字签名证书，在客户端和服务端进行 TLS 协商握手时使用双向认证。同时，在证书中使用了 OID 扩展，设备厂家能利用这个扩展指定客户端的角色和权

限，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 安全协议标准的推出，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。

本文件依据 GB/T 41868—2022，对 Modbus 安全协议一致性测试的具体要求和符合程度进行了规定。

Modbus 测试规范　第 3 部分：TCP 安全协议一致性测试规范

1　范围

本文件规定了 Modbus TCP 安全协议特征测试和应用协议一致性测试的要求，描述了进行 MODBUS TCP 安全协议一致性测试的方法。

本文件适用于相关检测机构作为 Modbus TCP 产品安全协议一致性测试的依据，也为产品生产厂商开发相关产品及用户选择产品提供参考。

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。

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 19582.3—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 41868—2022　Modbus TCP 安全协议规范

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

IETF RFC 5246　传输层安全性（TLS）协议版本 1.2[The transport Layer Security(TLS)Protocol Version1.2]

IETF RFC 5280　Internet X.509 公钥基础结构证书和证书撤销列表（CRL）配置文件[Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile]

IETF RFC 5746　传输层安全性（TLS）重新协商指示扩展[Transport Layer Security (TLS) Renegotiation Indication Extension]

IETF RFC 6066　传输层安全性（TLS）扩展：扩展定义[Transport Layer Security (TLS) Extensions: Extension Definitions]

3　术语和定义

GB/T 19582.1—2008、GB/T 19582.3—2008 界定的以及下列术语和定义适用于本文件。

3.1

一致性　conformance

实现协议的实体或系统与协议标准的符合程度。

[来源：GB/T 25919.1—2010，3.1]

3.2

一致性测试　conformance test

检测实现协议的实体或系统与协议标准的符合程度。