ICS 29.240.01
CCS F 21

中华人民共和国国家标准化指导性技术文件

GB/Z 25320.1003—2023

电力系统管理及其信息交换 数据和通信安全 第 100-3 部分：IEC 62351-3 的一致性测试用例和包括 TCP/IP 协议集的安全通信扩展

Power systems management and associated information exchange—Data and communication security—Part 100-3：Conformance test cases for IEC 62351-3，the secure communication extension for profiles including TCP/IP

（IEC TS 62351-100-3：2020，MOD）

2023-12-28 发布　　2024-07-01 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(Z) 25320《电力系统管理及其信息交换　数据和通信安全》的第100-3部分。GB/T(Z) 25320已经发布了以下部分：

——第1部分：通信网络和系统安全 安全问题介绍；

——第2部分：术语；

——第3部分：通信网络和系统安全　包含TCP/IP的协议集；

——第4部分：包含MMS的协议集；

——第5部分：GB/T 18657等及其衍生标准的安全；

——第6部分：IEC 61850的安全；

——第7部分：网络和系统管理(NSM)的数据对象模型；

——第11部分：XML文件的安全；

——第100-1部分：IEC TS 62351-5和IEC TS 60870-5-7的一致性测试用例；

——第100-3部分：IEC 62351-3的一致性测试用例和包括TCP/IP协议集的安全通信扩展。

本文件修改采用IEC TS 62351-100-3：2020《电力系统管理及其信息交换　数据和通信安全　第100-3部分：IEC 62351-3的一致性测试用例和包括TCP/IP协议集的安全通信扩展》。文件类型由IEC技术规范调整为我国的国家标准化指导性技术文件。

本文件与IEC TS 62351-100-3：2020的技术差异及原因如下：

——删除了“参考标准要求”的内容。新版标准中删除了“参考标准要求”，本文件删除相应的内容。

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。

本文件由中国电力企业联合会提出。

本文件由全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本文件起草单位：国网电力科学研究院有限公司、中国电力科学研究院有限公司、南京南瑞继保电气有限公司、东南大学、国电南京自动化股份有限公司、国网江苏省电力公司电力科学研究院、国电南瑞科技股份有限公司、国网江苏省电力有限公司、南方电网科学研究院有限责任公司、国网智能电网研究院有限公司、国家电网有限公司信息通信分公司。

本文件主要起草人：孙丹、姬广龙、孔红磊、王珍珍、温树峰、张丹、袁莉、杨宇、王宇、窦仁晖、王自成、吴在军、陈新之、窦晓波、张小飞、刘文彪、彭志强、李超、郑王里、刘清弘、吴净天、傅中兴、洪超、姚启桂、马睿、方帅。

引　言

GB/T(Z) 25320《电力系统管理及其信息交换　数据和通信安全》,旨在尽可能的减少通信和计算机网络中存在的恶意攻击对电力系统的数据及通信安全产生的危害,完善电力系统使用的各层通信协议中的安全漏洞以及提高电力系统信息基础设施的安全管理。拟由以下部分构成。

——第1部分:通信网络和系统安全　安全问题介绍。目的在于介绍GB/T(Z) 25320的其他部分,主要向读者介绍应用于电力系统运行的信息安全的各方面知识。

——第2部分:术语。目的在于介绍在GB/T(Z) 25320中所使用的关键术语。

——第3部分:通信网络和系统安全　包含TCP/IP的协议集。目的在于规定如何通过限于传输层安全协议的消息、过程和算法的规范,对基于TCP/IP的协议进行安全防护,使这些协议能适用于IEC TC 57的远动环境。

——第4部分:包含MMS的协议集。目的在于描述在使用GB/T 16720(ISO/IEC 9506)制造报文规范MMS时应实现的一些强制和可选的安全规范。

——第5部分:GB/T 18657等及其衍生标准的安全。目的在于定义了应用程序配置文件(a-profile)安全通信机制,规定了对基于或衍生于IEC 60870-5的所有协议的运行进行安全防护的消息、过程和算法。

——第6部分:IEC 61850的安全。目的在于规定了对基于或派生于IEC 61850的所有协议的运行进行安全防护的报文、过程与算法。

——第7部分:网络和系统管理(NSM)的数据对象模型。目的在于定义了电力系统运行所特有的网络和系统管理的数据对象模型。

——第8部分:电力系统管理基于角色的访问控制。目的在于为电力系统管理提供基于角色的访问控制。

——第9部分:电力系统设备的网络安全密钥管理。目的在于通过指定或限制要使用的密钥管理选项来定义实现密钥管理互操作性的要求和技术。

——第10部分:安全架构指南。目的在于描述基于基本安全控制的电力系统安全架构指南。

——第11部分:XML文件的安全。目的在于规范智能变电站通信过程中的配置文件(XML文件)的安全性。

——第12部分:分布式能源资源(DER)信息物理系统　电力系统用安全建议。目的在于提高分布式能源(DER)系统的安全性和可靠性。

——第13部分:覆盖标准和规范的安全主题指南。目的在于提供关于电力行业使用的标准和规范(IEC或其他)中可能或应该涵盖哪些安全问题。

——第90-1部分:电力系统基于角色的访问控制处理指南。目的在于开发用于定义和设计自定义角色以及角色映射的标准化方法。

——第90-2部分:加密通信的深度包检查。目的在于说明应用于IEC 62351保护的通信信道的DPI最新技术。

——第90-3部分:网络和系统管理导则。目的是提供处理IT和OT数据的导则。

——第100-1部分:IEC TS 62351-5和IEC TS 60870-5-7的一致性测试用例。目的在于提供了IEC 62351-5:2023和IEC TS 60870-5-7:2013的一致性和/或互操作性测试的测试用例。

——第100-3部分:IEC 62351-3的一致性测试用例和包括TCP/IP协议集的安全通信扩展。目的在于提供了IEC 62351-3:2023一致性测试用例及验证影响安全扩展程序和协议行为的所有

参数的配置。

——第100-6部分：IEC 61850-8-1和IEC 61850-9-2的网络安全一致性测试。目的在于提供了变电站自动化系统和远动系统的数据和通信安全互操作性一致性测试的测试用例。

GB/T(Z) 25320《电力系统管理及其信息交换　数据和通信安全》定义了电力系统相关通信协议(IEC 60870-5、IEC 60870-6、IEC 61850、IEC 61970和IEC 61968系列)的数据和通信安全，也定义了通信过程中可能遭受到的安全威胁和安全攻击以及安全应对措施。

电力系统管理及其信息交换 数据和通信安全 第100-3部分：IEC 62351-3的一致性测试用例和包括TCP/IP协议集的安全通信扩展

1 范围

本文件给出了远动设备、变电站自动化系统(SAS)和SCADA的前置机的数据和通信安全的测试案例。

本文件提供一种协议实现的标准测试方法达到互操作性，以验证设备满足IEC 62351-3要求。符合标准的一致性不能保证不同设备之间的互操作性，但期望使用本文件测试将不能互操作的风险降到最低。互操作性的基本条件是两个设备都能通过一致性测试。

本文件规定了IEC 62351-3的一致性和/或互操作性测试的通用可行的过程和定义。本文件定义的一致性测试用例专注于验证IEC 62351-3中规定的基础认证/加密协议(TLS)的一致性集成，以保护基于TCP/IP的通信。

本文件不涉及测试IEC 62351-3要求的基于TCP/IP(TLS)的基础身份验证/加密协议。基于TCP/IP的身份验证/加密协议的一致性测试不在本文件的讨论范围之内。

本文件涉及数据和通信安全一致性测试，不涉及其他要求，例如安全性或EMC。这些要求由其他标准(如果适用)涉及，这部分内容的合规性证明遵循其他标准。

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/Z 25320.2—2013 电力系统管理及其信息交换 数据和通信安全 第2部分：术语(IEC TS 62351-2：2008，IDT)

IEC 62351-3：2023 电力系统管理及其信息交换 数据和通信安全 第3部分：通信网络和系统安全 包含TCPIP的协议集(Power systems management and associated information exchange—Data and communications security—Part 3：Communication network and system security—Profiles including TCP/IP)

注：GB/Z 25320.3—2010 电力系统管理及其信息交换 数据和通信安全 第3部分：通信网络和系统安全 包含TCPIP的协议集(IEC TS 62351-3：2007，IDT)

3 术语、定义和缩略语

3.1 术语和定义

GB/Z 25320.2—2013界定的以及下列术语和定义适用于本文件。