ICS 29.240.01
CSS F 21

中华人民共和国国家标准

GB/T 25320.6—2023/IEC 62351-6:2020
代替 GB/Z 25320.6—2011

电力系统管理及其信息交换 数据和通信安全 第6部分:IEC 61850的安全

Power systems management and associated information exchange—Data and communications security—Part 6: Security for IEC 61850

（IEC 62351-6:2020,IDT）

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6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　包括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。

本文件代替GB/Z 25320.6—2011《电力系统管理及其信息交换　数据和通信安全　第6部分:IEC 61850的安全》,与GB/Z 25320.6—2011相比,除结构调整和编辑性改动,主要技术变化如下:

a) 更改了范围(见第1章,2011年版的第1章);

b) 更改了IEC 61850部分与IEC 62351部分的相关性的概述(见5.1,2011年版的5.1.1);

c) 增加了术语、定义和缩略语(见第3章);

d) 将GOOSE和SV的响应时间小于4 ms更改为小于3 ms(见4.1,2011年版的4.1);

e) 增加了IEC 61850-8-2客户端/服务器通信协议集(见5.4);

f) 增加了发布者ID用于客户端/服务器服务(见5.5);

g) 增加了多播关联协议(见第6章);

h) 增加了MAC(见8.2.2.2);

i) 增加了版本,本版本为1(见8.2.3.2);

j) 增加了当前密钥时间(见8.2.3.3);

k) 增加了下一个密钥时间(见8.2.3.4);

l) 增加了初始化向量(见8.2.3.5);

m) 增加了密钥ID(见8.2.3.6);

n) 增加了变电站配置语言扩展(见第9章);

o) 删除了变电站配置语言(SCL)(见2011年版的7.2.3);

p) 增加了LGOS和LSVS的扩展(见第10章);

q) 增加了支持IEC 61850-8-2和支持可路由的GOOSE和SV的安全一致性(见11.1表5);

r) 增加了使用ACSE认证的TLS(见11.1表7);

s) 增加了IEC 61850-8-1 L2 GOOSE安全一致性(见11.1表9);

t) 增加了IEC 61850-8-1 L2 SV安全一致性(见11.1表10);

u) 增加了IEC 61850-8-1 L2 GOOSE可路由安全一致性(见11.1表11);

v) 增加了IEC 61850-8-1 L2 SV可路由安全一致性(见11.1表12)。

本文件等同采用 IEC 62351-6:2020《电力系统管理及其信息交换　数据和通信安全　第 6 部分:IEC61850 的安全》。

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、国电南京自动化股份有限公司、东南大学、国家电网有限公司、国电南瑞能源有限公司、南京南瑞继保电气有限公司、南京工业职业技术大学、上海思源弘瑞自动化有限公司、南京工程学院、国家电网有限公司华东分部、国网江苏省电力有限公司、北京科东电力控制系统有限责任公司、国网智能电网研究院有限公司、中国电力科学研究院有限公司、国网上海市电力公司。

本文件主要起草人:孙丹、温树峰、王珍珍、刘文彪、吴在军、张小飞、孔红磊、孙建锋、张丹、姬广龙、郭王勇、赵天恩、李广华、王自成、石卫军、盛立健、汝雁飞、王振曦、张春晓、赵上林、陈洪才、王保东、赵汝英、张亮、王黎明、梁野、邵志鹏、朱朝阳、金明辉、高骏。

本文件及其所代替文件的历次版本发布情况为:

——2011 年首次发布为 GB/Z 25320.6—2011;

——本次为第一次修订。

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。目的在于规定了对基于GB/T 16720(ISO 9506)制造报文规范(MMS)的应用进行安全防护的过程、协议扩充和算法。

——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: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(DER)系统的快速恢复和安全建议。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:标准和规范中涉及的安全主题指南。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:电力系统中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测。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:网络和系统管理指南。目的是提供处理IT和OT数据的导则。

——第100-1部分:IEC 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。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6部分:IEC 61850的安全

1 范围与目的

1.1 范围

本文件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。

表1 标准应用范围

编号	名称
IEC 61850-8-1	电力自动化通信网络和系统 第8-1部分:特定通信服务映射(SCSM)-映射到MMS(ISO 9506-1和ISO 9506-2)及ISO/IEC 8802-3
IEC 61850-8-2	电力自动化通信网络和系统 第8-2部分:特定通信服务映射(SCSM)-映射到可扩展消息存在协议(XMPP)
IEC 61850-9-2	电力自动化通信网络和系统 第9-2部分:特定通信服务映射(SCSM)-基于ISO/IEC 8802-3的采样值
IEC 61850-6	电力自动化通信网络和系统 第6部分:与智能电子设备有关的变电站内通信配置描述语言

本文件的初期读者预期是开发或使用表1中所列举协议的工作组成员。为了使本文件中描述的措施有效,对于这些协议本身,其文件应采纳和引用这些措施。

本文件就是为此而编写的。

本文件的后续读者预期是实现这些协议的产品的开发人员。

本文件的部分内容也可被管理人员和执行人员使用,以理解该工作的目的和需求。

1.2 命名空间名称和版本

本条款对任何IEC 61850命名空间(IEC 61850-7-1部分所定义)都是强制的。

新版本命名空间参数定义如下:

——命名空间版本:2020;

——命名空间版次:A;

——命名空间名称:“IEC 62351-6:2020A”;

——命名空间发布号:1。

下表提供了该命名空间所有已发布版本的概况。

版本	发布日期	网络索引	命名空间
1.0	2020-10	IEC 62351-6:2020	IEC 62351-6:2020

1.3 代码组件发布

当前没有为代码组件下载区域发布代码组件。