



# 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 .....	III
引言 .....	V
1 范围与目的 .....	1
1.1 范围 .....	1
1.2 命名空间名称和版本 .....	1
1.3 代码组件发布 .....	1
2 规范性引用文件 .....	2
3 术语、定义和缩略语 .....	3
3.1 术语和定义 .....	3
3.2 缩略语 .....	3
4 本文件应对的安全问题 .....	4
4.1 影响安全选项选择的运行问题 .....	4
4.2 应对的安全威胁 .....	4
4.3 应对的攻击方法 .....	4
5 IEC 61850 部分与 IEC 62351 各部分的相关性 .....	4
5.1 概述 .....	4
5.2 IEC 61850-8-1 客户端/服务器通信协议集 .....	5
5.3 使用 VLAN ID 规范的 IEC 61850 安全性 .....	6
5.4 IEC 61850-8-2 客户端/服务器通信的协议集 .....	6
5.5 用于客户端/服务器服务的发布者 ID .....	6
6 多播关联协议 .....	6
6.1 概述 .....	6
6.2 防重放攻击(Replay Protection) .....	7
7 SNTP 安全 .....	13
8 IEC 61850-8-1 GOOSE 和 IEC 61850-9-2 采样值的 2 层安全性简介 .....	13
8.1 Ethertype 概述(资料性) .....	13
8.2 扩展 PDU .....	13
9 变电站配置语言扩展 .....	18
9.1 服务能力 .....	18
9.2 启用安全性的发布 .....	19
9.3 模拟(Simulation)的使用 .....	19
10 LGOS 和 LSVS 的扩展 .....	19
11 一致性 .....	20

11.1 一致性概述 .....	20
11.2 声明符合 IEC 61850-8-1 ISO 9506(应用协议集)安全性实现的一致性 .....	20
11.3 声明 VLAN 协议集安全实现的一致性 .....	22
11.4 声明 SNTP 协议集安全实现的一致性 .....	24
参考文献 .....	25
图 1 MMS 安全协议集(MMS Security Profiles) .....	5
图 2 GOOSE 防重放攻击状态机 .....	7
图 3 SV 防重放攻击状态机 .....	11
图 4 扩展 PDU 的一般格式 .....	13
图 5 Reserved1 定义 .....	14
图 6 MAC 计算域 .....	15
图 7 AES-GCM 在 2 层 GOOSE/SV 报文中的应用 .....	16
表 1 标准应用范围 .....	1
表 2 IEC 61850-9-2 的摘录(资料性) .....	10
表 3 LGOS 类的扩展 .....	19
表 4 LSVS 类的扩展 .....	20
表 5 一致性表 .....	20
表 6 IEC 61850-8-1 ISO 9506(应用协议集)的 PICS .....	21
表 7 使用 ACSE 认证的 TLS IEC 61850-8-1 客户端/服务器的 PICS .....	21
表 8 VLAN 协议集的 PICS .....	22
表 9 IEC 61850-8-1 2 层 GOOSE 安全 .....	22
表 10 IEC 61850-9-2 2 层 SV 安全 .....	23
表 11 IEC 61850-8-1 可路由 GOOSE .....	23
表 12 IEC 61850-9-2 可路由 SMV .....	24
表 13 SNTP 协议集的 PICS .....	24

## 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 的运动环境。
- 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,规定了对基于或派生于 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。

**GB/T 25320.6—2023/IEC 62351-6:2020**

——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。