ICS 29.240.30
CCS F 21

中华人民共和国国家标准

GB/T 25320.4—2024
代替 GB/Z 25320.4—2010

电力系统管理及其信息交换 数据和通信安全 第4部分:包含MMS的协议集及其附件

Power systems management and associated information exchange—Data and communications security—Part 4: Profiles including MMS and derivatives

（IEC 62351-4:2018,MOD）

2024-12-31 发布　　2025-07-01 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4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的协议集及其附件；

——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 25320.4—2010《电力系统管理及其信息交换　数据和通信安全　第4部分：包含MMS的协议集》，与GB/Z 25320.4—2010相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了适用范围(见第1章，2010年版的第1章)；

b) 更改了术语和定义，增加了缩略语(见第3章，2010年版的第3章)；

c) 更改了本文件涉及的安全问题(见第4章，见2010年版的第4章)；

d) 删除了应用协议集(A-Profile)安全(见2010年版的第5章)；

e) 删除了传输协议集(T-Profile)安全(见2010年版的第6章)；

f) 增加了具体要求(见第5章)；

g) 增加了传输安全(见第6章)；

h) 增加了应用层安全概述(见第7章)；

i) 增加了加密算法的应用(见第8章)；

j) 增加了对象标识符分配(见第9章)；

k) 增加了通用OSI上层需求(见第10章)；

l) 增加了端到端应用安全模型(见第12章)；

m) 增加了端到端应用安全(见第13章)；

n) 增加了端到端安全错误处理(见第14章)；

o) 增加了OSI操作环境下的端到端安全(见第15章)；

p) 增加了XMPP操作环境中的E2E安全(见第16章)；

q) 更改了一致性(见第17章，见2010年版的第7章)；

r) 增加了应用安全协议集的ANS.1规范(见附录A)；

s) 增加了端到端安全的ANS.1规范(见附录B)；

t) 增加了用于端到端安全的W3C XSD规范(见附录C)；

u) 增加了OSI操作环境下的ANS.1模型(见附录D)；

v) 增加了XMPP操作环境下的ANS.1模型和W3C模式文档XSD(见附录E)；

w） 增加了虚拟 API 模板规范(见附录 F)；

x） 增加了最终实体公钥证书规范(见附录 G)；

y） 增加了 OSI 操作环境下的底层要求(见附录 H)。

本文件修改采用 IEC 62351-4:2018《电力系统管理及其信息交换 数据和通信安全 第 4 部分:包含 MMS 的协议集及其附件》。

本文件与 IEC 62351-4:2018 的技术差异及其原因如下：

——规范性引用文件 IEC 62351-3、IEC TS 62351-8、IEC 62351-9、ISO 8601-1 更新至最新版本。

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:中国电力科学研究院有限公司、国家电网有限公司国家电力调度控制中心、中国南方电网有限公司、国网上海市电力公司、国网天津市电力有限公司、广东电网有限责任公司电力调度控制中心、国网电力科学研究院有限公司、南京南瑞继保工程技术有限公司、东方电子股份有限公司、国电南瑞南京控制系统有限公司、许继电气股份有限公司、国电南京自动化股份有限公司、长园深瑞继保自动化有限公司、积成电子股份有限公司、北京四方继保工程技术有限公司、国电南瑞科技股份有限公司、上海宽域工业网络设备有限公司。

本文件主要起草人:张金虎、纪欣、张晓、苏扬、王治华、吴金宇、高翔、卢建刚、赵瑞锋、孙丹、张小飞、李广华、温树峰、盛福、贾德顺、万首丰、刘文彪、徐浩、孙发恩、沈艳、许艾、李洪池、南 祎、汤方剑、王珍珍、安泰、张丹、张良、肖涛。

本文件及其所代替文件的历次版本发布情况为：

——2010 年首次发布为 GB/Z 25320.4—2010；

——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》,旨在尽可能地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 25320(Z)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 的协议集及其附件。目的在于规定了对基于 GB/T 16720(ISO 9506)制造报文规范(MMS)及其衍生标准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(GB/T 18657《远动设备及系统　第 5 部分:传输规约》)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 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。

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4部分，对基于GB/T 16720(ISO 9506)制造报文规范(MMS)及其衍生标准的应用进行安全防护的过程、协议扩充和算法。

电力系统管理及其信息交换 数据和通信安全 第4部分:包含MMS的协议集及其附件

1 范围

1.1 概述

本文件扩展了GB/Z 25320.4—2010[1][1)]的范围,规定了一种兼容模式——该模式提供了与基于GB/Z 25320.4—2010的实现之间的互操作性,并规定了称为原生模式的扩展功能。

本文件阐明了传输层和应用层的安全要求。GB/Z 25320.4—2010主要在应用层为基于制造消息规范(MMS)的应用在握手期间的认证提供了一些有限的支持,本文件还为握手阶段和数据传输阶段提供了对扩展完整性和认证的支持,在应用层提供了共享密钥管理和数据传输加密,并提供零个或多个中间实体的端到端安全(E2E)。GB/Z 25320.4—2010仅支持基于MMS的系统,即使用开放系统互操作(OSI)协议栈的系统,本文件还支持使用其他协议栈的应用协议,例如互联网协议套件(见4.1)。该支持扩展到保护使用XML编码的应用协议。应用层的这种扩展安全性称为E2E安全性。

除了E2E安全性之外,本文件还提供了携带安全相关信息的环境协议的映射方式。目前只考虑OSI和XMPP环境。

本文件作为需要以安全方式使用应用协议(例如MMS)的标准来规范性引用。

预计存在基于GB/Z 25320.4—2010传输安全协议集和应用安全协议集规范的实现,特别是控制中心间通信协议(ICCP)实现。因此,本文件包含了GB/Z 25320.4—2010的规范。支持这些规范的实现将与基于GB/Z 25320.4—2010的实现相互配合。

注:从严格意义上说,应用安全协议集并不是一个协议栈,但出于历史原因,该术语在此保留。

本文件定义了一组用于保护应用协议的强制性和可选的安全规范。

本文件的最初使用者是制定或使用协议的工作组成员。为了使本文件所述措施生效,协议规范应接受并引用这些措施。

本文件的后续使用者是实现这些协议的产品开发人员,以及希望为自己的环境指定需求的最终用户。

为了理解工作的目的和要求,本文件的部分内容也可能对管理人员和执行人员适用。

1.2 代码组件

购买IEC文件时,买方可根据IEC软件许可条件,直接或通过分销商向最终用户出售包含本文件代码组件的软件,该许可可在以下网址找到:www.iec.ch/CCv1。

IEC文件中包含的代码组件也可作为电子阅读器可读文件,网址为www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN_1.XSD.full.zip。

本文件中的代码组件包含在附录A、附录B、附录C、附录D和附录E中。

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

1) 方括号内的数字指参考文献。