ICS 29.240.01
F 21

中华人民共和国国家标准化指导性技术文件

GB/Z 25320.5—2013/IEC/TS 62351-5:2009

电力系统管理及其信息交换 数据和通信安全 第5部分:GB/T 18657等及其衍生标准的安全

**Power systems management and associated information exchange—
Data and communications security—
Part 5:Security for GB/T 18657 and derivatives**

(IEC/TS 62351-5:2009,IDT)

2013-02-07 发布　　2013-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围和目的 …… 1
1.1　范围 …… 1
1.2　预期读者及用途 …… 1
1.3　超出本部分范围的内容 …… 1
1.4　与其他标准一起使用 …… 1
1.5　文件结构和研究 …… 2
1.6　一致性 …… 2
2　规范性引用文件 …… 2
3　术语和定义 …… 3
4　略缩语 …… 3
5　问题描述 …… 3
5.1　概述 …… 3
5.2　需要处理的特定威胁 …… 4
5.3　设计面临的问题 …… 4
5.4　一般原则 …… 6
6　认证运行理论(资料性) …… 8
6.1　概述 …… 8
6.2　叙述性描述 …… 8
6.3　消息序列例子 …… 10
6.4　状态机概述 …… 14
7　正式规范 …… 16
7.1　概述 …… 16
7.2　消息定义 …… 16
7.3　正式过程 …… 28
8　互操作性要求 …… 40
8.1　概述 …… 40
8.2　最低要求 …… 40
8.3　可选项 …… 42
9　特殊应用 …… 43
9.1　概述 …… 43
9.2　使用 TCP/IP …… 43
9.3　使用冗余信道 …… 43
9.4　使用外接链路加密机 …… 43

10 引用本部分的要求 …… 43
10.1 概述 …… 43
10.2 选定的可选项 …… 43
10.3 认为关键性的操作 …… 43
10.4 地址信息 …… 43
10.5 信息格式映射 …… 44
10.6 对过程的引用 …… 44
11 协议实现的一致性声明 …… 44
11.1 概述 …… 44
11.2 要求的算法 …… 44
11.3 HMAC 算法 …… 44
11.4 密钥加密算法 …… 44
11.5 最大错误计数 …… 44
11.6 错误消息的使用 …… 44
参考文献 …… 45

前　言

GB/Z 25320《电力系统管理及其信息交换　数据和通信安全》分为以下几个部分：

——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：电力企业自动化通信网络和系统的安全；

——第7部分：网络和系统管理的数据对象模型；

——第8部分：电力系统管理的基于角色访问控制。

本部分为GB/Z 25320的第5部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分采用翻译法等同采用IEC/TS 62351-5:2009《电力系统管理及其信息交换　数据和通信安全　第5部分：IEC 60870-5及其衍生标准的安全》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/Z 25320.1—2010　电力系统管理及其信息交换　数据和通信安全　第1部分：通信网络和系统安全 安全问题介绍(IEC/TS 62351-1:2007,IDT)

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

——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　包括TCP/IP的协议集(IEC/TS 62351-3:2007,IDT)

——DL/T 634.5101—2002　远动设备及系统　第5-101部分：传输规约　基本远动任务配套标准(IEC 60870-5-101:2002,IDT)

——DL/T 719—2000　远动设备及系统　第5部分：传输规约　第102篇：电力系统电能量累计量传输配套标准(IEC 60870-5-102:1996,IDT)

——DL/T 667—1999　远动设备及系统　第5部分：传输规约　第103篇：继电保护设备信息接口配套标准(IEC 60870-5-103:1997,IDT)

——DL/T 634.5104—2009　远动设备及系统　第5-104部分：传输规约　采用标准传输协议集的IEC 60870-5-101网络访问(IEC 60870-5-104:2006,IDT)

本部分由中国电力企业联合会提出。

本部分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。

本部分起草单位：华中电网有限公司、国网电力科学研究院、国家电力调度通信中心、中国电力科学研究院、南方电网、华东电网有限公司、福建省电力有限公司、辽宁省电力有限公司。

本部分主要起草人：韩水保、许慕樑、杨秋恒、南贵林、张涛、周鹏、李根蔚、邓兆云、曹连军、马骁、蒋诚智。

引　言

计算机、通信和网络技术当前已在电力系统中广泛使用。通信和计算机网络中存在着各种对信息安全可能的攻击，对电力系统的数据及通信安全也构成了威胁。这些潜在的可能的攻击针对着电力系统使用的各层通信协议中的安全漏洞以及电力系统信息基础设施的安全管理的不完善处。

为此，我们采用国际标准制定了GB/Z 25320《电力系统管理及其信息交换　数据和通信安全》，通过在相关的通信协议以及在信息基础设施管理中增加特定的安全措施，提高和增强电力系统的数据及通信的安全。

电力系统管理及其信息交换 数据和通信安全 第5部分:GB/T 18657等及其衍生标准的安全

1 范围和目的

1.1 范围

为了对基于或衍生于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,GB/Z 25320的本部分规定了所用的消息、过程和算法。本部分至少适用于表1所列的协议。

表1 所适用标准的范围

编号	名 称
IEC 60870-5-101	基本远动任务配套标准
IEC 60870-5-102	电力系统电能量累计量传输配套标准
IEC 60870-5-103	继电保护设备信息接口配套标准
IEC 60870-5-104	采用标准传输协议集的IEC 60870-5-101网络访问
DNP3	分布式网络协议(基于IEC 60870-1至IEC 60870-5并由DNP用户组控制)

1.2 预期读者及用途

本部分的初期读者预期是制定表1所列协议的工作组人员。为了使本部分所描述的措施生效,各协议规范本身就必须采纳和引用这些措施。本部分的编写目的就是使能这一过程。

本部分的后续读者预期是实现这些协议的产品开发人员。

本部分的某些部分对管理人员和行政人员也是有用的,可用以理解该工作目的和需求。

1.3 超出本部分范围的内容

根据IEC第57委员会第3工作组的指令,IEC 62351的本部分仅关注应用层认证和由此认证所产生的安全防护问题。安全防护涉及的其他问题,特别是通过加密的使用来防止窃听和中间人攻击,被认为超出本部分的范围。通过本部分和其他规范一起使用,可以增加加密功能。

1.4 与其他标准一起使用

制定表1中所列协议的各工作组可以发布和本部分一同使用的标准。要求这些标准应描述认证机制对每个特定协议的消息和过程的映射。

这些文件不应该不顾本部分所描述的作为强制性及规范性的任何安全措施。

在用于IEC 60870-5-104时,本部分应和IEC/TS 62351-3一起使用。