



中华人民共和国国家标准化指导性技术文件

GB/Z 25320.4—2010/IEC TS 62351-4:2007

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

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

(IEC TS 62351-4:2007, IDT)

2010-11-10 发布

2011-05-01 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	I
引言	II
1 范围和目的	1
2 规范性引用文件	1
3 术语和定义	2
4 本部分涉及的安全问题	2
5 应用协议集(A-Profile)安全	3
6 传输协议集(T-Profile)安全	6
7 一致性	8
参考文献	10

前 言

国际电工委员会 57 技术委员会(IEC TC 57)对电力系统控制的相关数据和通信安全制定了 IEC 62351《电力系统管理及其信息交换 数据和通信安全》标准。我们采用 IEC 62351,编制了 GB/Z 25320 指导性技术文件,主要包括以下部分:

- 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:IEC 60870-5 及其衍生标准的安全;
- 第 6 部分:DL/T 860 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。

本部分等同采用 IEC TS 62351-4:2007《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》(英文版)。

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

本部分主要起草人:杨秋恒、李根蔚、许慕樑、邓兆云、南贵林、韩水保、曹连军、袁和林、林为民。

本指导性技术文件仅供参考。有关对本指导性技术文件的建议或意见,向国务院标准化行政主管部门反映。

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及在信息基础设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 4 部分:包含 MMS 的协议集

1 范围和目的

1.1 范围

为了对基于 GB/T 16720(ISO 9506)制造报文规范(Manufacturing Message Specification, MMS)的应用进行安全防护,GB/Z 25320 的本部分规定了过程、协议扩充和算法。其他 IEC TC 57 标准如需要以安全的方式使用 MMS,可以引用本部分作为其规范性引用文件。

本部分描述了在使用 GB/T 16720(ISO/IEC 9506)制造业报文规范 MMS 时应实现的一些强制的和可选的安全规范。

注:在 IEC TC 57 范围内,有两个标准 DL/T 860.81—2006(IEC 61850-8-1)及 GB/T 18700(IEC 60870-6)会受到影响。

为了保护使用 MMS 传递的信息,本部分包含一组由这些引用标准所使用的规范。其建议是基于为传送 MMS 信息所使用的特定通信协议集的协议。

DL/T 860.81—2006(IEC 61850-8-1)和 GB/T 18700(IEC 60870-6)在第 7 层的面向连接机制中使用了 MMS。这些标准中每一个均是在 OSI 协议集或 TCP 协议集上使用。

1.2 目的

本部分的初期读者预期是制定或使用 IEC TC 57 协议的工作组成员。为了使本部分描述的措施有效,对于那些使用 GB/T 16720 的协议,协议本身的规范就必须采纳和引用这些措施。本部分就是为了使得能那样做而编写的。

本部分的后续读者预期是实现这些协议的产品开发人员。

本部分的某些部分也可以被管理者和行政人员使用,以理解该工作的用途和需求。

2 规范性引用文件

下列文件中的条款通过 GB/Z 25320 的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 16720(所有部分) 工业自动化系统 制造报文规范(ISO 9506)

GB/T 18700(所有部分) 远动设备及系统(IEC 60870-6)

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

GB/Z 25320.3 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(GB/Z 25320.3—2010,IEC 62351-3:2007,IDT)

IEC TS 62351-2 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(Power systems management and associated information exchange—Data and communications security—Part 2:Glossary of terms)

ISO/IEC 9594-8:2005/ITU-T X.509 建议:2005 信息技术 开放系统互连 目录:公钥和属性