ICS 29.240.30
F 21

中华人民共和国国家标准化指导性技术文件

GB/Z 25320.1—2010/IEC TS 62351-1:2007

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

**Power systems management and associated information exchange—
Data and communications security—
Part 1: Communication network and system security—
Introduction to security issues**

(IEC TS 62351-1:2007, 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 …… Ⅲ
引言 …… Ⅳ
1　范围和目的 …… 1
2　规范性引用文件 …… 2
3　术语、定义和缩略语 …… 2
4　信息安全标准的背景 …… 2
4.1　电力系统运行的信息安全所涉及的论据 …… 2
4.2　IEC TC 57 数据通信协议 …… 3
4.3　制定这些安全标准的历史 …… 3
5　GB/Z 25320 涉及的安全问题 …… 4
5.1　安全的一般信息 …… 4
5.2　安全威胁的类型 …… 4
5.3　安全的需求、威胁、脆弱性、攻击和应对措施 …… 6
5.4　安全对策的重要性 …… 11
5.5　安全风险评估 …… 11
5.6　认识安全需求以及安全措施对电力系统运行的影响 …… 12
5.7　五步安全过程 …… 13
5.8　应用安全防护于电力系统运行 …… 14
6　GB/Z 25320 概述 …… 15
6.1　GB/Z 25320 的范围 …… 15
6.2　认证作为关键安全需求 …… 15
6.3　GB/Z 25320 的目标 …… 15
6.4　GB/Z 25320 各部分和 IEC 协议间的关系 …… 15
6.5　GB/Z 25320.1　安全问题介绍 …… 16
6.6　GB/Z 25320.2　术语 …… 16
6.7　GB/Z 25320.3　包含 TCP/IP 的协议集 …… 17
6.8　GB/Z 25320.4　包含 MMS 的协议集 …… 17
6.9　GB/Z 25320.5　IEC 60870-5 及其衍生标准的安全 …… 18
6.10　GB/Z 25320.6　DL/T 860 的安全 …… 19
6.11　GB/Z 25320.7　网络和系统管理的数据对象模型 …… 20
7　结论 …… 23
附录 NA(资料性附录)　IEC 60870-5 的各部分与对应的我国标准以及一致性程度 …… 24
参考文献 …… 25

前　言

国际电工委员会57技术委员会（IEC TC 57）对电力系统管理及其信息交换制定了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 62351-1：2007《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》（英文版）。

本部分增加了资料性附录NA，以反映规范性引用文件IEC 60870-5（所有部分）中的各部分与对应的我国标准以及一致性程度。

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：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、福建省电力有限公司、华中电网有限公司、华东电网有限公司、辽宁省电力有限公司。

本部分主要起草人：许慕樑、南贵林、邓兆云、杨秋恒、韩水保、李根蔚、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1部分:通信网络和系统安全 安全问题介绍

1 范围和目的

1.1 范围

GB/Z 25320的本部分范围是电力系统控制运行的信息安全。本部分的主要目的是“为IEC TC 57制定的通信协议的安全,特别是IEC 60870-5、IEC 60870-6、IEC 61850、IEC 61970和IEC 61968的安全,承担标准的制定;承担有关端对端安全的标准和技术报告的制定”。

1.2 目的

具体目的包括:

- GB/Z 25320.1介绍了GB/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;
- GB/Z 25320.3～GB/Z 25320.6规定了IEC TC 57通信协议的安全标准。可以用这些标准提供各种层次的协议安全,这取决于为一个特定实现所选定的协议和参数。同样它们已被设计为具有向后兼容能力并能分阶段实现;
- GB/Z 25320.7涉及端对端信息安全的许多可能领域中的一个领域,即加强对支持电力系统运行的通信网络进行全面管理;
- GB/Z 25320后续的其他部分涉及更多的信息安全领域。

电力行业中安全性、安全防护和可靠性始终是系统设计和运行的重要问题,随着该行业越来越多依赖于信息基础设施,其信息安全正变得日益重要,这就是制定信息安全标准的理由。一些新威胁已经影响到解除管制的电力市场,因为对竞争对手的资产和其系统运作的了解可能是会从中得益的,于是截获此类信息是十分可能发生的。此外,无意的行为(如不小心和自然灾祸)能够像蓄意行为一样对信息造成危险。当前恐怖主义的外加威胁已经变得非常明显。

虽然存在“端对端”安全的许多定义,一个标准定义(多种陈述)是:“1. 对采用密码技术的安全通信系统或被保护的分布系统中的信息进行安全防护意味着从起始点到目的点的防护。2. 对信息系统中的信息,从起始点到目的点进行安全防护”[1)]。以这个定义为基础开始的四个标准是针对IEC TC 57通信协议集的安全增强,因为这些通信协议集被认为是对电力系统控制操作进行安全防护明显的第一步。然而这些安全增强仅能解决两个系统之间的安全需求,并不解决包含内部安全需求的真正“端对端”安全,包括安全对策、安全防护执行、入侵检测、内部系统和应用的健壮以及更广泛的安全需求。

因此,本章的本结束语是非常重要的:认识到增设防火墙或仅简单使用协议的加密,例如增加链路端加密盒(bump-in-the-wire)或甚至虚拟专网(VPN)技术,在许多情况下似乎并不是足够的。安全是真正的“端对端”的要求,以确保对敏感的电力系统设备的认证访问、对敏感的市场数据的授权访问、可靠且及时的设备功能执行和设备故障信息、关键系统的备份以及容许检测和再现决定性事件的审计

1) ATIS(Alliance for Telecommunications Industry Solutions)[美国为通信和相关信息技术快速制定和促进技术和运行标准的组织。ATIS得到了美国国家标准学会(ANSI)的认可。]:FS-1037C的扩充,US联邦政府电信项目的标准术语。