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 25320.3—2010/IEC TS 62351-3:2007

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

**Power systems management and associated information exchange—
Data and communications security—
Part 3:Communication network and system security—
Profiles including TCP/IP**

(IEC TS 62351-3:2007,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

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 62351-3:2007《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　包含TCP/IP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:辽宁省电力有限公司调度通信中心、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电网自动化研究所、福建省电力有限公司电力调度通信中心、华中电网有限公司电力调度通信中心、华东电网有限公司。

本部分主要起草人:曹连军、南贵林、许慕樑、韩水保、杨秋恒、邓兆云、李根蔚、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3部分:通信网络和系统安全 包括TCP/IP的协议集

1 范围和目的

1.1 范围

GB/Z 25320的本部分规定如何为SCADA和用TCP/IP作为消息传输层的远动协议,提供机密性、篡改检测和消息层面认证。

虽然对TCP/IP的安全防护存在许多可能的解决方案,但本部分的特定范围是在端通信实体内TCP/IP连接的任一端处,提供通信实体之间的安全。对插入其间的外接安全装置(如"链路端加密盒")的使用和规范不在本部分范围内。

1.2 目的

GB/Z 25320的本部分规定如何通过限于传输层安全协议(Transport Layer Security,TLS)(在RFC 2246中定义)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。如其他IEC TC 57标准需要为它们的基于TCP/IP协议提供防护,则本部分预期作为这些IEC TC 57标准的规范性部分而被引用。然而,决定是否引用本文件是各个协议安全防护的自主选择。

本部分反映了目前IEC TC 57协议的安全需求。如果其他标准将来提出新的需求,本部分也许需要修订。

本部分的初期读者预期是在IEC TC 57中制定或使用这些协议的工作组成员。为使本部分描述的措施有效,对于使用TCP/IP的协议本身,其规范就应采纳和引用这些措施。本部分就是为了使得能这样处理而编写的。

本部分的后续读者预期是实现这些协议的产品的开发人员。本部分的某些部分也可以被管理人员和执行人员使用,以理解该工作的目的和需求。

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/Z 25320.1 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(GB/Z 25320.1—2010,IEC TS 62351-1:2007,IDT)

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

RFC 2246 传输层安全协议(TLS)(RFC 2246:1999,The TLS Protocol Version 1.0[1])

1) T. Dierks,C. Allen。通常该标准称为SSL/TLS(安全套接层/传输层安全协议)。