



中华人民共和国国家标准化指导性技术文件

GB/Z 25320.7—2015/IEC/TS 62351-7:2010

电力系统管理及其信息交换 数据和通信安全 第7部分:网络和 系统管理(NSM)的数据对象模型

Power systems management and associated information exchange—
Data and communications security—
Part 7: Network and system management (NSM) data object models

(IEC/TS 62351-7:2010, IDT)

2015-05-15 发布

2015-12-01 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 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语和定义 | 1 |
| 4 略缩语 | 1 |
| 5 网络和系统管理(NSM)需求的背景(资料性的) | 1 |
| 5.1 IEC NSM 标准的目的 | 1 |
| 5.2 目前缺乏相互紧密结合的信息基础设施 | 5 |
| 5.3 入侵检测系统(IDS) | 6 |
| 5.4 网络和系统管理(NSM)概念 | 9 |
| 6 电力系统运行安全性和可靠性的 NSM 需求(资料性的) | 10 |
| 6.1 NSM 需求:网络和协议的监视和控制 | 10 |
| 6.2 NSM 要求:端系统的监视和管理 | 12 |
| 6.3 NSM 需求:入侵检测功能 | 13 |
| 7 NSM 抽象数据类型 | 15 |
| 7.1 缩略语 | 15 |
| 7.2 NSM 数据对象的构成 | 17 |
| 7.3 高层 NSM 数据类型结构 | 18 |
| 8 NSM 抽象数据对象 | 22 |
| 8.1 通信状况 NSM 数据对象 | 22 |
| 8.2 端系统状况 NSM 数据对象 | 25 |
| 8.3 入侵检测的 NSM 数据对象 | 26 |
| 参考文献 | 30 |

前 言

GB/Z 25320《电力系统管理及其信息交换 数据和通信安全》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：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 8 部分：基于角色的访问控制。

本部分是 GB/Z 25320 的第 7 部分。

本部分根据 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用 IEC/TS 62351-7: 2010《电力系统管理及其信息交换 数据和通信安全 第 7 部分：网络和系统管理(NSM)的数据对象模型》。

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。

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、国网电力科学研究院、国家电力调度通信中心、华东电网有限公司、北京科东电力控制系统有限责任公司、华中电网有限公司、福建省电力有限公司、辽宁省电力有限公司、南方电网、中国华能集团公司、西北电网有限公司。

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

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7部分:网络和 系统管理(NSM)的数据对象模型

1 范围

电力系统运行正越来越依赖于信息基础设施,包括通信网络、智能电子设备(IED, Intelligent Electronic Device),以及自定义的通信协议。因此,为了在电力系统运行中提供必要的高安全性和高可靠性,对信息基础设施的管理已经变得至关重要。采用 IETF 用于网络管理的“简单网络管理协议”(SNMP, Simple Network Management Protocol)标准中所提出的概念,本部分定义了电力系统运行所特有的网络和系统管理(NSM, Network and System Management)的数据对象模型。这些 NSM 数据对象将被用于监视网络和工作状况,发现可能发生的安全入侵,以及对信息基础设施的性能和可靠性进行管理。

NSM 数据对象使用了为 IEC 61850 制定的命名规则,扩展后去解决 NSM 问题。这些数据对象及其包含的数据类型,被定义为数据对象的抽象模型。数据对象的位和字节的实际格式将取决于这些抽象的 NSM 数据对象对特定协议的映射,例如 IEC 61850、IEC 60870-5、IEC 60870-6、IEC 61968/61970 (CIM 公共信息模型)、web 服务、SNMP 或任何其他适当的协议。那些映射在若干独立的文件中标准化。那些映射的标准化将独立成文。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

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)

3 术语和定义

GB/Z 25320.2—2013 中界定的术语和定义适用于本文件。

4 缩略语

GB/Z 25320.2—2013 中界定的缩略语适用于本文件。

5 网络和系统管理(NSM)需求的背景(资料性的)

5.1 IEC NSM 标准的目的

5.1.1 端对端安全的范围

端对端的安全不仅包括蓄意攻击,也包括无意行为。这个说法对理解本部分范围是至关重要的。