ICS 29.240.01
F 21

中华人民共和国国家标准

GB/T 36572—2018

电力监控系统网络安全防护导则

Guidelines of cyber security protection for electric power system supervision and control

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
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　缩略语 …… 3
5　电力监控系统特性及安全防护原则 …… 3
5.1　电力监控系统特性 …… 3
5.2　电力监控系统面临的网络安全威胁 …… 4
5.3　电力监控系统网络安全防护原则 …… 4
5.4　电力监控系统网络安全防护体系 …… 5
6　安全防护技术 …… 6
6.1　基础设施安全 …… 6
6.2　体系结构安全 …… 6
6.3　监控系统本体安全 …… 8
6.4　可信安全免疫 …… 9
7　应急备用措施 …… 10
7.1　冗余备用 …… 10
7.2　应急响应 …… 10
7.3　多道防线 …… 10
8　全面安全管理 …… 11
8.1　融入电力安全生产管理体系 …… 11
8.2　全体人员安全管理 …… 12
8.3　全部设备及系统的安全管理 …… 12
8.4　全生命周期安全管理 …… 12
附录A（规范性附录）　发电厂监控系统安全防护 …… 13
附录B（规范性附录）　变电站监控系统安全防护 …… 14
附录C（规范性附录）　电网调度控制系统安全防护 …… 15

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国电力企业联合会提出。

本标准由全国电力监管标准化技术委员会(SAC/TC 296)、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)、全国电网运行与控制标准化技术委员会(SAC/TC 446)、全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)、全国工业机械电气系统标准化技术委员会(SAC/TC 231)联合归口。

本标准起草单位:国家能源局、国家电网有限公司、南瑞集团有限公司、全球能源互联网研究院有限公司、中国电力科学研究院有限公司、中国南方电网公司、中国华能集团公司、国家信息技术安全研究中心、中国信息安全测评中心、公安部、机械工业仪器仪表综合技术经济研究所、中国科学院沈阳自动化研究所、中国科学院沈阳计算技术研究所、国网江西省电力公司电力科学研究院、许继集团有限公司、北京四方继保自动化股份有限公司、东方电子股份有限公司、北京和利时系统工程有限公司、浙江大学、北京启明星辰信息安全技术有限公司、北京国电智深控制技术有限公司。

本标准主要起草人:辛耀中、苑舜、胡红升、许洪强、许海铭、易俗、余勇、朱世顺、郭建成、南贵林、陶洪铸、孙炜、高昆仑、崔书昆、梁寿愚、郭森、李京春、李冰、李斌、张翀斌、郭启全、祝国邦、范春玲、李明、马跃、杨维永、邓兆云、杨浩、王志皓、马骁、李凌、梁智强、陈雪鸿、王玉敏、尚文利、尹震宇、吕忠、汪强、任雁铭、慈国兴、冯冬芹、孟雅辉、朱镜灵、刘森、张亮、王斐。

引　言

随着计算机和网络通信技术在电力监控系统中的广泛应用，电力监控系统网络安全问题日益凸显。为了加强电力监控系统的安全管理，防范黑客及恶意代码等对电力监控系统的攻击侵害，保障电力系统的安全稳定运行，根据国家发展改革委员会2014年第14号令《电力监控系统安全防护规定》和国家信息系统等级保护等相关规定制定本标准。

电力监控系统网络安全防护导则

1 范围

本标准规定了电力监控系统网络安全防护的基本原则、体系架构、防护技术、应急备用措施和安全管理要求。

本标准适用于发电、输配电、用电、电网调度等电力生产各环节的电力监控系统安全防护，覆盖其规划设计、研究开发、施工建设、安装调试、系统改造、运行管理、退役报废等各阶段。

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/T 9361 计算机场地安全要求

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能组件

GB/T 20272—2006 信息安全技术 操作系统安全技术要求

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 21028—2007 信息安全技术 服务器安全技术要求

GB/T 21050—2007 信息安全技术 网络交换机安全技术要求(评估保证级3)

GB/T 22186—2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25058—2010 信息安全技术 信息系统安全等级保护实施指南

GB/T 25068.3—2010 信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护

GB/Z 25320(所有部分) 电力系统管理及其信息交换 数据和通信安全

GB/T 30976.1—2014 工业控制系统信息安全 第1部分：评估规范

IEC 62443(所有部分) 工业自动化和控制系统安全(Security for Industrial Automation and Control Systems)

3 术语和定义

下列术语和定义适用于本文件。

3.1

电力监控系统 electric power system supervision and control

用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及智能设备，以及作为基础支撑的通信及数据网络等，包括电力数据采集与监控系统(SCADA)、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和安全自动装

置、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统、电力调度数据网络等。

3.2

网络安全防护体系　cyber security protection architecture

为保障核心业务系统的网络信息安全而建立一整套综合安全防护措施所形成的体系，安全防护体系由安全防护技术、应急备用措施、全面安全管理所形成的三维立体结构组成。

3.3

生产控制大区　production control zone

由具有数据采集与控制功能、纵向联接使用专用网络或专用通道的电力监控系统构成的安全区域。

3.4

控制区　control sub zone

由具有实时监控功能、纵向联接使用电力调度数据网的实时子网或者专用通道的各业务系统构成的安全区域。

3.5

非控制区　non-control sub zone

在生产控制范围内由在线运行但不直接参与控制、是电力生产过程的必要环节、纵向联接使用电力调度数据网的非实时子网的各业务系统构成的安全区域。

3.6

管理信息大区　management information zone

生产控制大区之外的，主要由企业管理、办公自动化系统及信息网络构成的安全区域。

3.7

横向隔离　lateral isolation

在不同安全区间禁止通用网络通信服务，仅允许单向数据传输，采用访问控制、签名验证、内容过滤、有效性检查等技术，实现接近或达到物理隔离强度的安全措施。

3.8

纵向认证　vertical authentication

采用认证、加密、访问控制等技术实现数据的远方安全传输以及纵向边界的安全防护的措施。

3.9

本体安全　self security

电力监控系统软件及设备自身的安全、可控，包括业务系统软件的安全、操作系统和基础软件的安全、计算机和网络设备及电力测控设备的安全、核心处理器芯片的安全。

3.10

可信安全免疫　trust security immunology

基于可信计算技术实现电力监控系统的安全免疫，保障操作系统和电力监控软件安全可信，防范已知和未知的病毒、木马及恶意代码的侵害。

3.11

对称密码　symmetric cipher

在加密和解密算法中都是用相同秘密密钥的密码技术。

3.12

非对称密码　asymmetric cipher

基于非对称密码技术的体制，公开变换用于加密，私有变换用于解密，反之亦然。

3.13

身份认证　authentication

专用于确定传输、消息或发信方的有效性的安全措施，或者对接受特定的信息类别的个人授权进行验证的手段。

4　缩略语

下列缩略语适用于本文件。

BIOS：基本输入输出系统(Basic Input Output System)

DTU：配电终端装置(Distribution Terminal Unit)

FTP：文件传输协议(File Transfer Protocol)

FTU：馈线终端装置(FeederTerminalUnit)

HTTP：超文本传输协议(Hyper-Text Transfer Protocol)

IED：智能电子设备(Intelligent Electronic Device)

LAN：局域网络(Local Area Network)

MPLS：多协议标记交换(Multi-Protocol Label Switching)

PLC：可编程序控制器(Programmable Logical Controller)

PVC：永久虚拟电路(Permanent Virtual Circuit)

RAS：远程访问服务器(Remote Access Server)

SCADA：监视控制与数据采集系统(Supervisory Control And Data Acquisition)

SDH：同步数字传输体系(Synchronous Digital Hierarchy)

SNMP：简单网络管理协议(Simple Network Management Protocol)

USB：通用串行总线(Universal Serial Bus)

VLAN：虚拟局域网(Virtual Local Area Network)

VPN：虚拟专用网(Virtual Private Networks)

WAN：广域网络(Wide Area Network)

5　电力监控系统特性及安全防护原则

5.1　电力监控系统特性

电力监控系统具有如下特性：

a) **可靠性**。电力监控系统的可靠稳定运行是确保电力生产安全的基础，安全防护措施应融入生产控制业务中，减少中间环节，提高电力监控系统的可靠性。

b) **实时性**。电力监控系统从过程数据的实时采集、传输到控制指令的下达执行，周期短，安全措施应适应电力监控系统的实时性，保证系统正常运行。

c) **安全性**。电力监控系统大量采用计算机及通信技术，应在保障电力生产过程安全的同时，确保系统及网络安全，能够抵御网络安全威胁。

d) **分布性**。电力监控系统具有实时闭环控制的特性，采集、传输、控制等业务模块采用地理或空间位置上的分散布置方式，生产过程的实时性越高分布性越强，网络安全防护应适应其分布性。

e) **系统性**。电力监控系统在时间上具有时变性和连续性，在空间上具有分布参数和分布处理的特性，在技术上涉及技术领域和设备系统较多，在管理上涉及业务部门和层级较多，对系统性要求很高，网络安全防护具有很强的系统性。

5.2 电力监控系统面临的网络安全威胁

电力监控系统面临的主要网络安全威胁如表1所示。

表1 电力监控系统面临的主要网络安全威胁

序号	安全威胁	描　述
1	黑客入侵	有组织的黑客团体对电力监控系统进行恶意攻击、窃取数据，破坏电力监控系统及电力系统的正常运行
2	旁路控制	非授权者对发电厂、变电站发送非法控制命令，导致电力系统事故，甚至系统瓦解
3	完整性破坏	非授权修改电力监控系统配置、程序、控制命令；非授权修改电力市场交易中的敏感数据
4	越权操作	超越已授权限进行非法操作
5	无意或故意行为	无意或有意地泄漏口令等敏感信息，或不谨慎地配置访问控制规则等
6	拦截篡改	拦截或篡改调度数据广域网传输中的控制命令、参数设置、交易报价等敏感数据
7	非法用户	非授权用户使用计算机或网络资源
8	信息泄漏	口令、证书等敏感信息泄密
9	网络欺骗	Web服务欺骗攻击；IP欺骗攻击
10	身份伪装	入侵者伪装合法身份，进入电力监控系统
11	拒绝服务攻击	向电力调度数据网络或通信网关发送大量雪崩数据，造成网络或监控系统瘫痪
12	窃听	黑客在调度数据网或专线信道上搭线窃听明文传输的敏感信息，为后续攻击做准备

5.3 电力监控系统网络安全防护原则

结合电力监控系统特性和面临网络安全威胁，网络安全防护应遵循以下基本原则：

a) **建立体系不断发展**。逐步建立电力监控系统网络安全防护体系，主要包括基础设施安全、体系结构安全、系统本体安全、可信安全免疫、安全应急措施、全面安全管理等，形成多维栅格状架构，并随着技术进步而不断动态发展完善。

b) **分区分级保护重点**。根据电力监控系统的业务特性和业务模块的重要程度，遵循国家信息安全等级保护的要求，准确划分安全等级，合理划分安全区域，重点保护生产控制系统核心业务的安全。

c) **网络专用多道防线**。电力监控系统应采用专用的局域网络(LAN)和广域网络(WAN)，与外部因特网和企业管理信息网络之间进行物理层面的安全隔离；在与本级其他业务系统相连的横向边界，以及上下级电力监控系统相连的纵向边界，应部署高强度的网络安全防护设施，并对数据通信的七层协议采用相应安全措施，形成立体多道安全防线。

d) **全面融入安全生产**。应将安全防护技术融入电力监控系统的采集、传输、控制等各个环节各业务模块，融入电力监控系统的设计研发和运行维护；应将网络安全管理融入电力安全生产管理体系，对全体人员、全部设备、全生命周期进行全方位的安全管理。

e) **管控风险保障安全**。电力监控系统安全直接影响电网安全，关乎国家安全和社会稳定，应全面加强网络安全风险管控，保障电力监控系统安全，确保电力系统安全稳定经济运行。

5.4 电力监控系统网络安全防护体系

电力监控系统网络安全防护体系存在多种描述方式，本标准从安全防护技术、应急备用措施、全面安全管理的三维描述安全防护体系的立体结构，三个维度相互支撑、相互融合、动态关联，并不断发展进化，形成动态的三维立体结构，如图 1 所示。

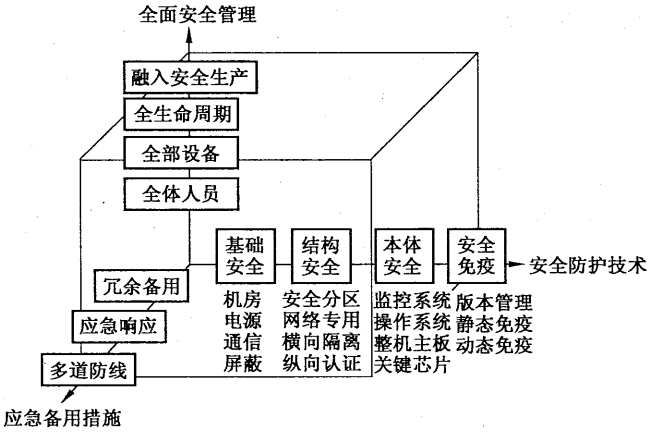

图 1 电力监控系统网络安全防护体系三维立体结构示意图

其中，安全防护技术维度主要包括基础设施安全、体系结构安全、系统本体安全、可信安全免疫等；应急备用措施维度主要包括冗余备用、应急响应、多道防线等；全面安全管理维度主要包括全体人员安全管理、全部设备安全管理、全生命周期安全管理、融入安全生产管理体系。如图 2 所示。

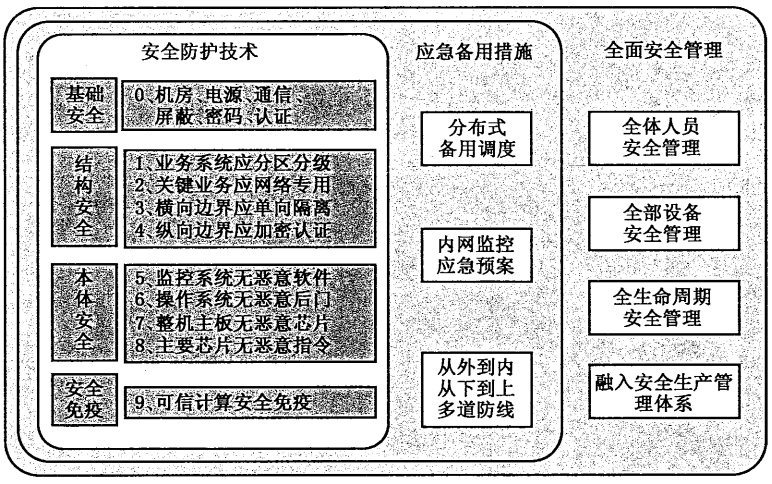

图 2 电力监控系统网络安全防护体系示意图

网络安全防护体系应融入电力监控系统的规划设计、研究开发、施工建设、安装调试、系统改造、运行管理、退役报废等各个阶段，且应随着计算机技术、网络通信技术、安全防护技术、电力控制技术的发展而不断发展完善。

6 安全防护技术

6.1 基础设施安全

电力监控系统机房和生产场地应选择在具有防震、防风和防雨等能力的建筑内，应采取有效防水、防潮、防火、防静电、防雷击、防盗窃、防破坏措施；机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁(见 GB/T 9361)。

应在机房供电线路上配置稳压器和过电压防护设备，设置冗余或并行的电力电缆线路为计算机系统供电，应建立备用供电系统，提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；生产控制大区机房与管理信息大区机房应独立设置，应安排专人值守并配置电子门禁系统及具备存储功能的视频、环境监控系统以加强物理访问控制；应对生产控制大区关键区域或关键设备实施电磁屏蔽。(见 GB/T 22239—2008 中的四级系统物理安全和三级系统物理安全等部分。)

生产控制大区所有的密码基础设施，包括对称密码、非对称密码、摘要算法、调度数字证书和安全标签等，应符合国家有关规定，并通过国家有关机构的检测认证。

6.2 体系结构安全

6.2.1 总体要求

结构安全是电力监控系统网络安全防护体系的基础框架，也是所有其他安全防护措施的重要基础。电力监控系统结构安全应采用“安全分区、网络专用、横向隔离、纵向认证”的基本防护策略，如图 3 所示。

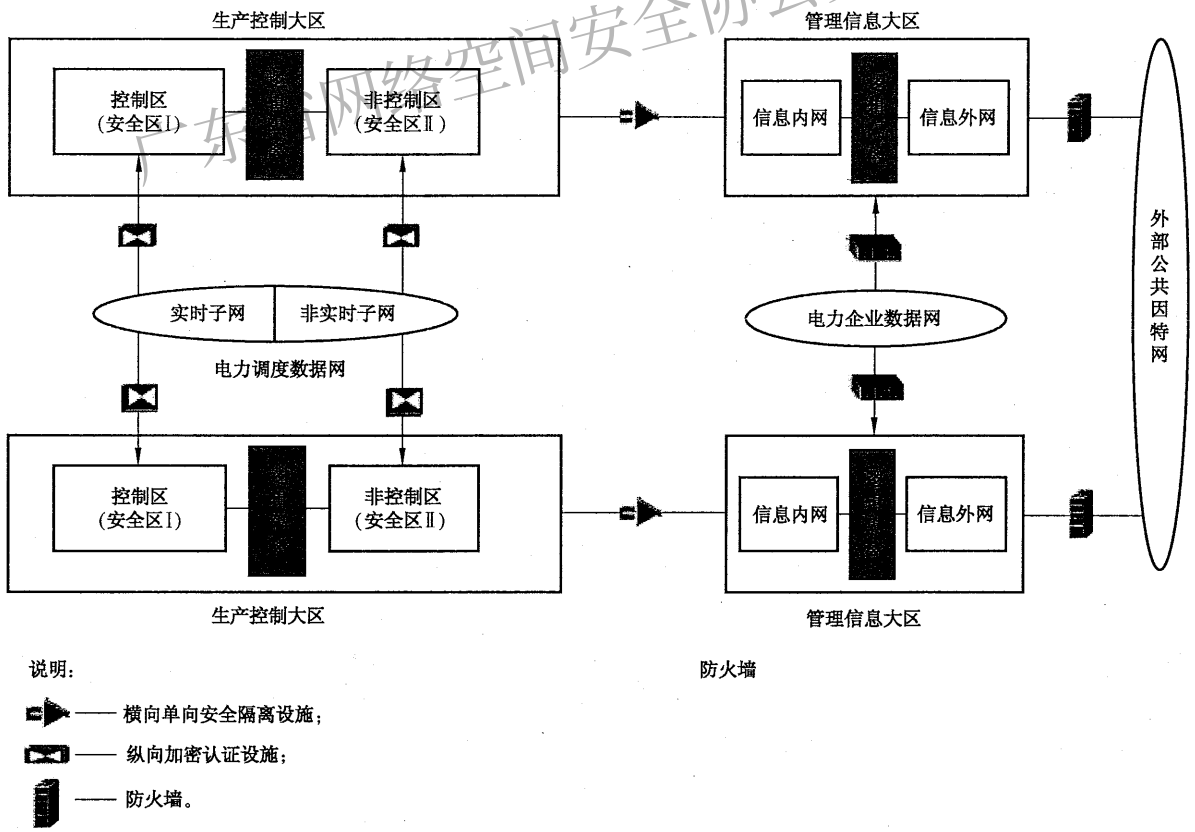

图 3 电力监控系统结构安全总体框架示意图

6.2.2 分区分级

电力监控系统应划分为生产控制大区和管理信息大区。生产控制大区可以分为控制区(安全区Ⅰ)和非控制区(安全区Ⅱ);管理信息大区内部在不影响生产控制大区安全的前提下,可以根据各企业不同安全要求划分安全区;生产控制大区的纵向互联应与相同安全区互联,避免跨安全区纵向交叉联接。对于小型变电站和发电厂可根据具体情况简化安全区的设置,应按就高不就低的原则对简化后的安全区进行防护,同时避免形成不同安全区的纵向交叉联接。

生产控制大区的业务系统在与其终端的纵向联接中使用无线通信网、电力企业其他数据网(非电力调度数据网)或者外部公用数据网的虚拟专用网络方式(VPN)等进行通信的,应设立安全接入区,如图4所示。

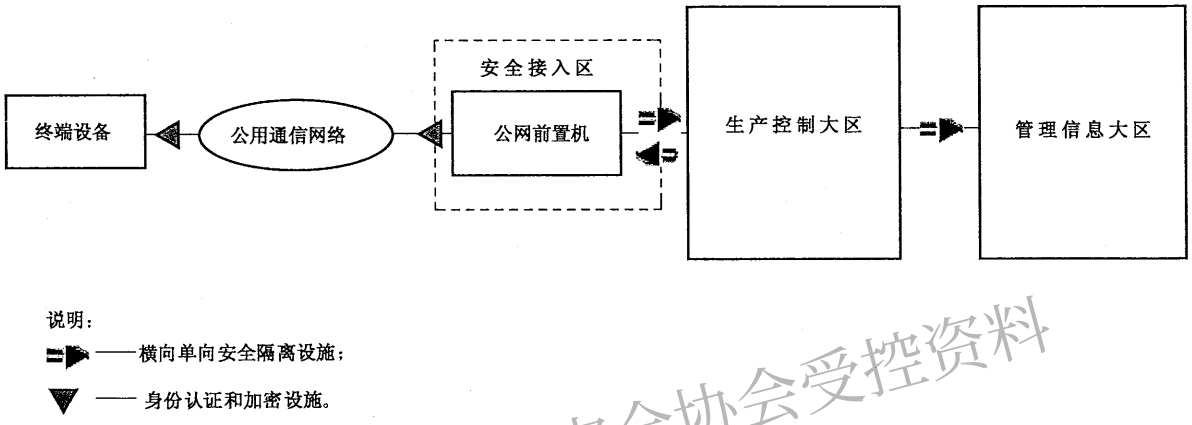

图4 安全接入区防护结构示意图

各区域安全边界应采取必要的安全防护措施,禁止任何穿越生产控制大区和管理信息大区之间边界的通用网络服务(如FTP、HTTP、TELNET、MAIL、RLOGIN、SNMP等)。

应遵循国家信息安全等级保护要求,准确划分电力监控系统安全等级(见GB 17859—1999的第4章、GB/T 22240—2008中的5.5、GB/T 25058—2010中的5.3),生产控制大区的控制区(安全区Ⅰ)的安全等级最高,非控制区(安全区Ⅱ)次之,管理信息大区再次之。

6.2.3 网络专用

电力监控系统的生产控制大区应在专用通道上使用独立的网络设备组网,采用基于SDH不同通道、不同光波长、不同纤芯等方式,在物理层面上实现与其他通信网及外部公用网络的安全隔离。

生产控制大区通信网络可进一步划分为逻辑隔离的实时子网和非实时子网,采用MPLS-VPN技术、安全隧道技术、PVC技术、静态路由等构造子网。

生产控制大区数据通信的七层协议均应采用相应安全措施,在物理层应与其他网络实行物理隔离,在链路层应合理划分VLAN,在网络层应设立安全路由和虚拟专网,在传输层应设置加密隧道,在会话层应采用安全认证,在表示层应有数据加密,在应用层应采用数字证书和安全标签进行身份认证[见GB/Z 25320(所有部分)]。

6.2.4 横向隔离

在生产控制大区与管理信息大区之间应设置通过国家有关机构安全检测认证的电力专用横向单向安全隔离装置,隔离强度应接近或达到物理隔离,只允许单向数据传输,禁止HTTP、TELNET等双向的通用网络安全服务通信;生产控制大区内部的安全区之间应采用具有访问控制功能的设备、防火墙或

者相当功能的设施，实现逻辑隔离。

生产控制大区到管理信息大区的数据传输采用正向安全隔离设施，仅允许单向数据传输；管理信息大区到生产控制大区的数据传输采用反向安全隔离设施，仅允许单向数据传输，并采取基于非对称密钥技术的签名验证、内容过滤、有效性检查等安全措施。

安全接入区与生产控制大区中其他部分的联接处应设置通过国家有关机构安全检测认证的电力专用横向单向安全隔离装置。

6.2.5 纵向认证

在生产控制大区与广域网的纵向联接处应设置通过国家有关机构安全检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施。

6.2.6 数字证书和安全标签

依照电力调度管理体制建立基于公钥技术的分布式电力调度数字证书及安全标签，生产控制大区中的重要业务系统应采用加密认证机制。

6.2.7 防火墙和入侵检测

生产控制大区内不同系统间应采用逻辑隔离措施，实现逻辑隔离、报文过滤、访问控制等功能（见GB/T 25068.3—2010的第6章和第7章）。

生产控制大区可部署入侵检测措施，合理设置检测规则，及时捕获网络异常行为，分析潜在威胁，进行安全审计，宜保持特征码及时更新，特征码更新前应进行充分的测试，禁止直接通过因特网在线更新。

6.2.8 防病毒和防木马

生产控制大区应部署恶意代码防范措施，宜保持特征码以离线方式及时更新，特征码更新前应进行充分的测试，更新过程应严格遵循相关安全管理规定，禁止直接通过因特网在线更新。

6.2.9 拨号认证设施

拨号认证设施主要用于必要的远程维护，该设施平时应断电关机，需要时临时开机，仅允许单用户登录并严格监管审计，用完应及时关机。拨号认证设施，如远程访问服务器（RAS），应使用安全加固的操作系统，采用数字证书进行登录认证和访问认证，并通过国家有关机构安全检测认证。

6.3 监控系统本体安全

6.3.1 基本要求

在电力监控系统网络安全防护体系架构中，构成体系的各个模块应实现自身的安全，依次分为电力监控系统软件的安全、操作系统和基础软件的安全、计算机和网络设备及电力专用监控设备的安全、核心处理器芯片的安全，均应采用安全、可控、可靠的软硬件产品，并通过国家有关机构的安全检测认证。本体安全的相关要求主要适用于新建或新开发的电力监控系统，在运系统具备升级改造条件时可参照执行，不具备升级改造条件的应强化安全管理和安全应急措施。

发电厂监控系统安全防护要求见附录A，变电站监控系统安全防护要求见附录B，电网调度控制系统安全防护见附录C。

6.3.2 电力监控系统软件安全

电力监控系统中的控制软件，在部署前应通过国家有关机构的安全检测认证和代码安全审计，防范

恶意软件或恶意代码的植入。

电力监控系统软件应在设计时融入安全防护理念和措施，业务系统软件应采用模块化总体设计，合理划分各业务模块，并部署于相应安全区，重点保障实时闭环控制核心模块安全。

调度控制系统可通过内部专用设施进行维护，采用身份认证和安全审计实施全程监控，保障维护行为可追溯。变电站和发电厂监控系统可通过远程拨号认证设施进行远程维护。严格禁止直接通过因特网进行生产控制大区的远程维护。

6.3.3 操作系统和基础软件的安全

重要电力监控系统中的操作系统、数据库、中间件等基础软件应通过国家有关机构的安全检测认证，防范基础软件存在恶意后门。

生产控制大区业务系统应采用满足安全可靠要求的操作系统、数据库、中间件等基础软件（见GB/T 20272—2006中的4.3和4.4），使用时应合理配置、启用安全策略；操作系统和基础软件应仅安装运行需要的组件和应用程序，并及时升级安全补丁，补丁更新前应进行充分的测试，禁止直接通过因特网在线更新。

6.3.4 计算机和网络及监控设备的安全

电力监控系统中的计算机和网络设备，以及电力自动化设备、继电保护设备、安全稳定控制设备、智能电子设备（IED）、测控设备等，应通过国家有关机构的安全检测认证，防范设备主板存在恶意芯片。

生产控制大区应采用符合国家相关要求的计算机和网络设备（见GB/T 21028—2007的第4章和第5章、GB/T 21050—2007中的7.1和7.2、GB/T 18336.2—2015的第7章），使用时应合理配置、启用安全策略；应封闭网络设备和计算机设备的空闲网络端口和其他无用端口，拆除或封闭不必要的移动存储设备接口（包括光驱、USB接口等），仅保留调度数字证书所需要的USB端口。

6.3.5 核心处理器芯片的安全

重要电力监控系统中的核心处理器芯片应通过国家有关机构的安全检测认证，防范芯片存在恶意指令或模块。

重要电力监控系统应采用符合国家相关要求的处理器芯片（见GB/T 22186—2016中的7.1），采用安全可靠的密码算法、真随机数发生器、存储器加密、总线传输加密等措施进行安全防护。

6.4 可信安全免疫

6.4.1 基本要求

在构成电力监控系统网络安全防护体系的各个模块内部，应逐步采用基于可信计算的安全免疫防护技术，形成对病毒木马等恶意代码的自动免疫。重要电力监控系统应在有条件时逐步推广应用以密码硬件为核心的可信计算技术，用于实现计算环境和网络环境安全免疫，免疫未知恶意代码，防范有组织的、高级别的恶意攻击。安全免疫的相关要求主要适用于新建或新开发的重要电力监控系统，在运系统具备升级改造条件时可参照执行，不具备升级改造条件的应强化安全管理和安全应急措施。

6.4.2 强制版本管理

重要电力监控系统关键控制软件应采用基于可信计算的强制版本管理措施，操作系统和监控软件的全部可执行代码，在开发或升级后应由生产厂商采用数字证书对其签名并送检，通过检测的控制软件程序应由检测机构用其数字证书对其签名，生产控制大区应禁止未包含生产厂商和检测机构签名版本的可执行代码启动运行。

6.4.3 静态安全免疫

重要电力监控系统应采用基于可信计算的静态安全启动机制。服务器加电至操作系统启动前对BIOS、操作系统引导程序以及系统内核执行静态度量，业务应用、动态库、系统内核模块在启动时应对其执行静态度量，确保被度量对象未被篡改且不存在未知代码，未经度量的对象应无法启动或执行。

6.4.4 动态安全免疫

重要电力监控系统应采用基于可信计算的动态安全防护机制，对系统进程、数据、代码段进行动态度量，不同进程之间不应存在未经许可的相互调用，禁止向内存代码段与数据段直接注入代码的执行。

重要电力监控系统应对业务网络进行动态度量，业务连接请求与接收端的主机设备应可以向对端证明当前本机身份和状态的可信性，不应在无法证明任意一端身份和状态可信的情况下建立业务连接。

7 应急备用措施

7.1 冗余备用

地市及以上电网调度控制中心应实现实时数据采集、自动化系统、调度控制职能、调度场所、调控人员等层面的冗余备用，形成分布式备用调度体系。

发电厂和变电站应实现数据备份及关键设备的冗余备用；对于特别重要的设备，除自动化控制方式外，应设有现地手工操作控制机构。

各级电网调度控制中心、发电厂和变电站应建立电力监控系统恢复机制，支撑系统故障的快速处理和恢复，保障电力监控系统业务的连续性。

7.2 应急响应

各电力企业应建立电力监控系统的应急机制，制定相关制度和应急处理预案，并定期开展协同演练；当生产控制大区出现安全事件，尤其是遭到黑客、恶意代码攻击和其他人为破坏时，应按应急处理预案，立即采取安全应急措施，报告上级业务主管部门和安全主管部门，必要时可断开生产控制大区与管理信息区之间的横向边界连接，在紧急情况下可协调断开生产控制大区与下级或上级控制系统之间的纵向边界连接，以防止事态扩大，同时注意保护现场，以便进行调查取证和分析；上级业务主管部门和安全主管部门也应将安全事件及时通报相关电力企业，形成联合防护机制。

7.3 多道防线

电力监控系统应在外部公共因特网、管理信息大区、生产控制大区的控制区及非控制区等横向边界部署相应安全措施，形成电力监控系统横向从外到内四道安全防线，实现核心控制区安全防护强度的累积效应，如图5所示。

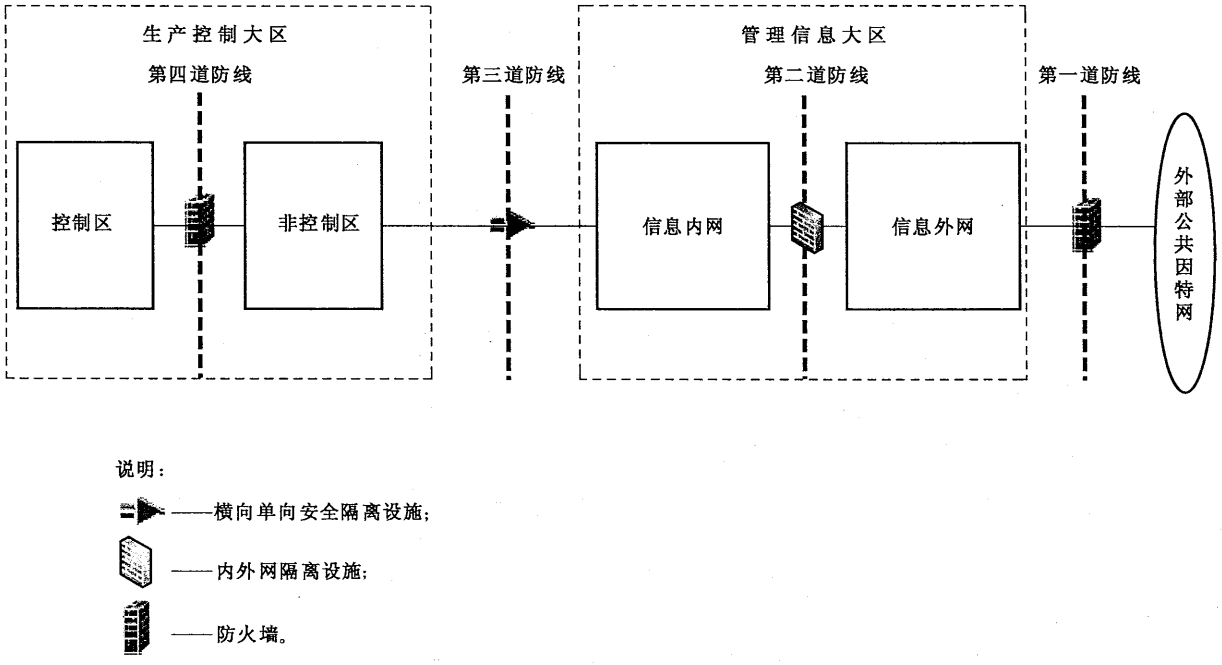

图 5　电力监控系统横向四道防线示意图

电力监控系统应在国调、网调、省调、地调、县调间，以及各级调度机构与其直调的发电厂、变电站之间的纵向边界，部署相应安全措施，形成电力监控系统纵向从下到上四道安全防线，实现高安全等级控制区安全防护强度的累积效应，如图 6 所示。

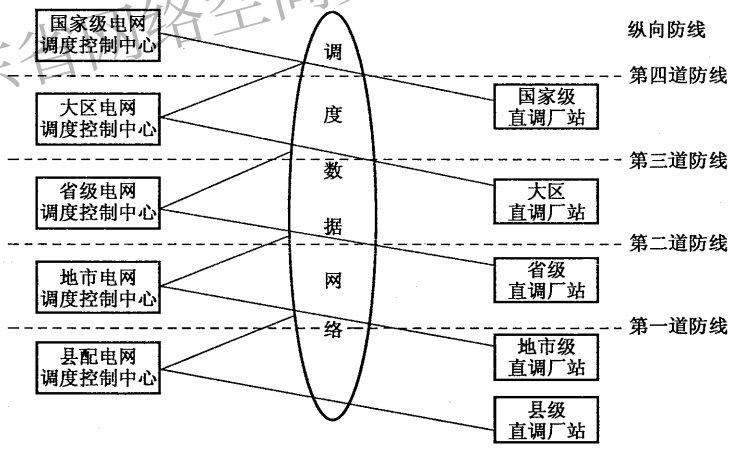

图 6　电力监控系统纵向四道防线示意图

各级电网调度控制中心应部署内网安全监视措施，实时监测相关横向和纵向防线上的安全告警，一旦发生网络安全事件，能够快速响应、及时处置，实现各防线联合防御。

8　全面安全管理

8.1　融入电力安全生产管理体系

各电力企业应把电力监控系统的网络安全管理融入安全生产管理体系中，按照“谁主管、谁负责；谁运营、谁负责；谁使用、谁负责”的原则，健全电力监控系统安全防护的组织保证体系和安全责任体系，落

实国家行业主管部门的安全监管责任、各电力企业的安全主体责任、各级电网调度控制机构的安全技术监督责任。各电力企业应设立电力监控系统安全管理工作的职能部门，由企业负责人作为主要责任人，宜设立首席安全官。开发制造单位应承诺其产品无恶意安全隐患并终身负责，检测评估单位、规划设计单位等均应对其工作终身负责。

8.2 全体人员安全管理

各电力企业应加强电力监控系统安全防护人员的配备，设立安全主管、安全管理等岗位，配备安全管理员、系统管理员和安全审计员，明确各岗位职责，并指定专人负责数字证书系统等关键系统及设备的管理。

应加强对电力监控系统安全防护的管理、运行、维护、使用等全体人员的安全管理和培训教育，特别要加强对厂家维护及评估检测等第三方人员的安全管理，提高全体内部人员和相关外部人员的安全意识(见 GB/T 22239—2008 中的 7.2.3)。

8.3 全部设备及系统的安全管理

应对电力监控系统中全部业务系统软件模块和硬件设备，特别是安全防护设备，建立设备台账，实行全方位安全管理。

在安全防护设备和重要电力监控系统及设备在选型及配置时，应禁止选用被国家相关部门检测通报存在漏洞和风险的特定系统及设备；相关系统、设备接入电力监控系统网络时应制定接入技术方案、采取相应安全防护措施，并经电力监控系统安全管理部门的审核、批准；应定期进行安全风险评估(见 GB/T 20984—2007 的第 5 章和第 6 章、GB/T 30976.1—2014 的第 5 章)，针对发现的问题及时进行加固。

8.4 全生命周期安全管理

电力监控系统系统及设备在规划设计、研究开发、施工建设、安装调试、系统改造、运行管理、退役报废等全生命周期阶段应采取相应安全管理措施。

应采用安全、可控、可靠的软硬件产品，供应商应保证所提供的设备及系统符合本标准以及国家与行业信息系统安全等级保护的要求，并在设备及系统生命期内对此负责；重要电力监控系统及专用安全防护产品的开发、使用及供应商，应按国家有关要求做好保密工作，防止安全防护关键技术和设备的扩散。

电力监控系统及设备的运维单位应依据相关标准和规定进行安全防护专项验收；加强日常运维和安全防护管理，定期开展运行分析和自评估，保障系统及设备的可靠运行；系统和设备退役报废时应按相关要求，销毁含敏感信息的介质和重要安全设备。

附 录 A
（规范性附录）
发电厂监控系统安全防护

发电厂现场过程级电力监控系统应在遵循总体防护原则的基础上，重点强化生产控制大区边界防护、物理安全防护、运行维护人员安全、系统及设备供应链安全管理等内部安全措施，保障电力监控系统现场运行安全。

发电厂过程级电力监控系统应合理划分局域网络，如火电厂不同机组间网络应采取一定隔离措施，防止不同机组电力监控系统网络直接相连；核电厂常规岛电力监控系统网络应与核岛相关网络间采取一定隔离措施；光伏、风电等新能源电厂应严格按照“安全分区、网络专用、横向隔离、纵向认证”的原则，落实电力监控系统安全防护要求，电厂生产控制大区与管理信息大区应严格遵循物理隔离要求，禁止生产控制大区通过任何方式与因特网相连[见 IEC 62443(所有部分)]。

禁止设备生产厂商或其他外部企业(单位)远程连接发电厂生产控制大区中的监控系统及设备。发电厂现场涉及远方控制功能的装置及设备应采用加密及身份认证等安全防护措施。发电厂生产控制大区中除安全接入区外，应禁止选用具有无线通信功能的设备。

发电厂生产控制大区中脱硫脱硝等业务系统与地方环保等部门进行数据传输时，其边界防护应采用类似生产控制大区与管理信息大区之间的安全防护措施。

新建发电厂在设备选型及配置时，禁止选用被国家相关部门检测通报存在漏洞和风险的特定系统及设备(如控制器、PLC、工业以太网交换机、工控主机等关键设备)；已经投入运行的电厂监控系统及设备如存在已知的漏洞和风险，应按照要求及时进行加固，并强化网络隔离、安全管控等措施，保障运行安全。

新开发的发电厂监控系统应将安全防护设施融入监控系统设计、研发中，利用数字证书、安全标签保护电力生产控制过程。

典型发电厂电力监控系统如图 A.1 所示。

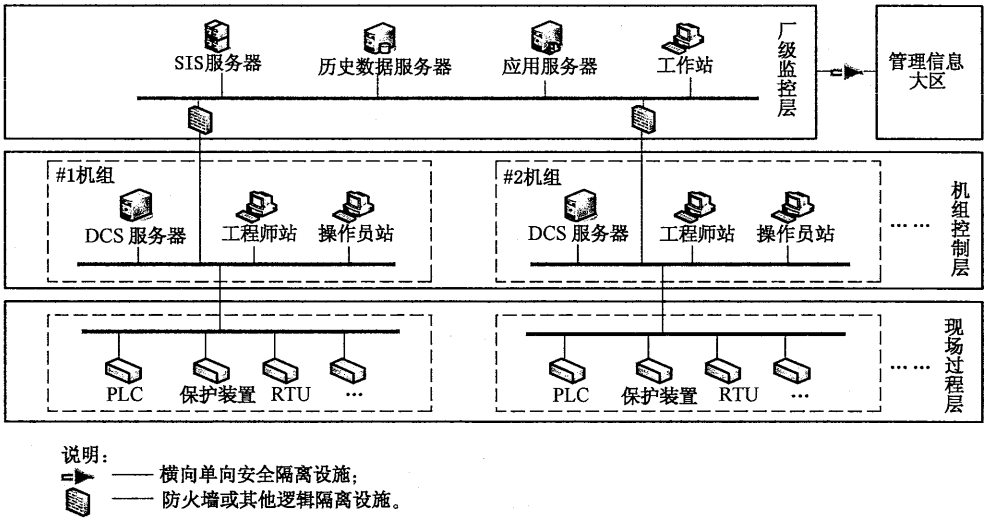

图 A.1 典型发电厂监控系统示意图

发电厂现场运行系统及设备关键部位，除自动化控制机制外，还应设置人工手动操作设施，作为自动化控制系统失效时的应急备用措施。

附 录 B
（规范性附录）
变电站监控系统安全防护

变电站现场过程级电力监控系统应在遵循总体防护原则的基础上，重点强化生产控制大区边界防护、物理安全防护、运行维护人员安全等内部安全措施，保障不同电压等级变电站、换流站、开关站，以及发电厂升压站或开关站的电力监控系统现场运行安全。

变电站过程级电力监控系统应划分站控层、间隔层和过程层等层次网络，不同层次网络间应采用访问控制等安全措施，防止内部网络与外部网络直接相连；变电站等现场涉及远方控制功能的装置及设备应采用加密及身份认证等安全防护措施[见 IEC 62443(所有部分)]。

新建变电站在设备选型及配置时，禁止选用被国家相关部门检测通报存在漏洞和风险的特定系统及设备(如工业以太网交换机、工控主机等关键设备)；已经投入运行的变电站监控系统及设备如存在已知的漏洞和风险，应按照要求及时进行加固，并强化网络隔离、安全管控等措施，保障运行安全。

新开发的变电站监控系统应将安全防护设施融入监控系统设计、研发中，利用数字证书、安全标签保护电力生产控制过程。

典型变电站电力监控系统如图 B.1 所示。

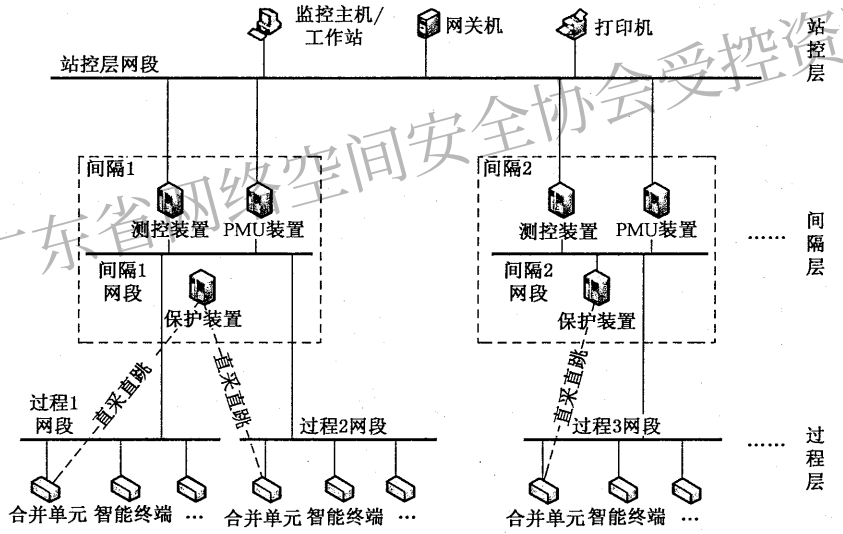

图 B.1 典型变电站监控系统示意图

变电站现场运行系统及设备关键部位，除自动化控制机制外，还应设置人工手动操作设施，作为自动化控制系统失效时的应急备用措施。

附 录 C
（规范性附录）
电网调度控制系统安全防护

各级电网调度控制中心应按照“安全分区、网络专用、横向隔离、纵向认证”的防护原则建立栅格状安全防护架构，横向与管理信息大区采用专用物理隔离设施进行隔离，纵向与上下级调度及直调厂站生产控制大区采用纵向加密认证设施进行防护，应防止出现纵向交叉互联。

生产控制大区的业务系统在与其终端（如 DTU、FTU 等）的纵向联接中使用无线通信网、电力企业其它数据网（非电力调度数据网）或者外部公用数据网的虚拟专用网络方式（VPN）等进行通信的，应设立安全接入区。

禁止配电网调度自动化系统与智能用电系统直接相连，禁止配电自动化通信网络与调度数据网络直接相连。

中 华 人 民 共 和 国
国 家 标 准
电力监控系统网络安全防护导则
GB/T 36572—2018
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 35 千字
2018年9月第一版 2018年9月第一次印刷
*
书号:155066·1-61321 定价 21.00 元

GB/T 36572-2018

打印日期:2018年10月17日 F007