ICS 27.100
CCS F 30

DL

中华人民共和国电力行业标准

DL/T 2202—2020

发电厂监控系统信息安全防护技术规范

Technical specification for information security of power plant monitoring and control system

2020-10-23发布　　2021-02-01实施

国家能源局　发布

目　　次

前言…… II
1　范围…… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　监控系统信息安全基本要求…… 3
5　监控系统信息安全技术要求…… 5
6　监控系统信息安全评估…… 19
附录 A（资料性）　发电厂监控系统的脆弱性及主要威胁 …… 21
参考文献…… 23

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中国电力企业联合会提出。

本文件由电力行业热工自动化与信息标准化技术委员会（DL/TC 28）归口。

本文件起草单位：国网河南省电力公司电力科学研究院、淮浙煤电有限责任公司凤台发电分公司、国网浙江省电力有限公司电力科学研究院、华能集团有限公司、大唐集团有限公司、浙江大唐乌沙山发电有限责任公司、大唐延安发电厂、中电华创电力技术研究有限公司、浙江浙能技术研究院有限公司、润电能源科学技术有限公司、北京天地和兴科技有限公司、杭州安恒信息技术有限公司、北京信达探索者科技有限公司、沈阳凯风技术股份有限公司、上海工业控制安全创新科技有限公司、浙江国华浙能发电有限公司、大唐中南电力试验研究院、杭州聚盛广科技有限公司。

本文件主要起草人：郭志民、吕卓、刘道远、李辉、莫坚松、郝振、苏烨、俞荣栋、陈小强、冯博、李国胜、陶振国、余程、吴永存、张之刚、郝涛、叶鹏、金光宇、谢东、陈君、刘虹、陈岑、郭祥富、杨文、李敏、杜永春、倪华、孙长生。

本文件为首次发布。

本文件在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

发电厂监控系统信息安全防护技术规范

1 范围

本文件规定了发电厂监控系统信息安全防护的基本要求、技术要求和安全评估要求。

本文件适用于发电厂监控系统信息安全防护工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全保护等级定级指南

GB/T 25058 信息安全技术 网络安全等级保护实施指南

GB/T 25069 信息安全技术 术语

GB/T 26863 火电站监控系统术语

GB/T 30976.1 工业控制系统信息安全 第1部分：评估规范

国能安全〔2014〕318号 电力行业信息安全等级保护管理办法

电监信息〔2007〕44号 电力行业信息系统等级保护定级工作指导意见

3 术语和定义

GB/T 25069、GB/T 26863、GB/T 30976.1 界定的以及下列术语和定义适用于本文件。

3.1

发电厂监控系统 power plant monitoring and control system

用于监视和控制发电厂生产过程、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，包括发电厂的主控制系统（3.7）、辅助控制系统（3.8）、控制区电气二次系统（3.9）、现场总线设备与智能化仪表等控制区（3.2）实时系统，以及厂级监控信息系统等非控制区监控系统（3.10）。

3.2

控制区 control sub zone

由具有实时监控功能、纵向连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。

3.3

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、纵向连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。

3.4

生产控制大区 production control zone

由控制区（3.2）和非控制区（3.3）构成的安全区域。

3.5

管理信息大区　management information zone

发电厂生产控制大区以外的管理业务系统的集合。

3.6

安全管理中心　security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台或区域。

3.7

主控制系统　main control systems

对发电厂发电过程实施集中或分布式控制的主要监控系统、独立控制装置与智能仪表等，主要包括火电厂单元机组的分散控制系统与可编程控制器系统、水电厂集中监控系统、梯级水电站调度监控系统、风电场监控系统、光伏电站运行监控系统等。

3.8

辅助控制系统　auxiliary control systems

对发电厂全厂公用的外围辅助设备系统进行控制的监控系统、独立控制装置与智能仪表等，主要包括燃煤电厂外围公用的水、煤、灰控制系统，燃气轮机电厂全厂辅助控制系统、火警探测系统，以及其他电厂全厂辅助设备的相关控制系统等。

3.9

控制区电气二次系统　electric secondary systems in control sub zone

对发电厂电气设备与发电机实施保护、测控与调度的自动化系统与设备，主要包括升压站监控系统、自动发电控制系统（automatic generation control，AGC）和自动电压控制系统（automatic voltage control，AVC）、发电机励磁系统、五防监控系统、继电保护及安全自动化装置、相量测量装置等。

3.10

非控制区监控系统　monitoring and control system in non-control sub zone

对发电厂运行参数与监控信息进行在线监测分析但不直接参与控制的系统，主要包括火电厂厂级监控信息系统、梯级水库调度自动化系统、水情自动测报系统、水电厂水库调度自动化系统、光功率预测系统、风功率预测系统、电能量采集装置、电力市场报价终端、故障录波装置及信息管理终端等。

3.11

威胁　threat

能够通过未授权访问、毁坏、揭露、数据修改和/或拒绝服务对系统造成潜在危害的任何环境或事件。

3.12

脆弱性　vulnerability

在信息系统、系统安全程序、管理控制、物理设计、内部控制或系统实现中的，可能被攻击者利用来获得未授权的信息或破坏关键处理的弱点。

3.13

身份鉴别　identity authentication

验证实体所声称的身份。

3.14

访问控制　access control

防止对资源的未授权使用，包括防止以未授权方式使用某一资源。

3.15

安全审计　security audit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的

动作。

3.16

安全域　security domain

在信息系统中，单一安全策略下运行的实体的汇集。

4　监控系统信息安全基本要求

4.1　等级保护

4.1.1　发电厂监控系统实行国家网络安全等级保护制度，信息安全防护应满足信息安全等级保护的相关要求。

4.1.2　发电厂信息安全等级保护坚持自主定级、自主保护的原则，根据不同安全区域的安全防护要求，确定其安全等级和防护水平，从安全物理环境、安全通信网络、安全区域边界和安全计算环境等方面进行安全防护。

4.1.3　发电厂应按照 GB/T 22239—2019、GB/T 25058 及《电力行业信息安全等级保护管理办法》的规定具体实施等级保护工作。

4.1.4　发电厂监控系统的定级，应按照 GB/T 22240 和《电力行业信息系统等级保护定级工作指导意见》的规定进行。

4.2　关键信息基础设施安全保护

被认定为关键信息基础设施的发电厂监控系统，其信息安全防护工作应满足国家对关键信息基础设施的安全保护要求。

4.3　信息安全防护基本原则

4.3.1　通用要求

4.3.1.1　发电厂监控网络与系统，应遵循“安全分区、网络专用、横向隔离、纵向认证、综合防护”的总体原则。安全防护的主要对象，应包括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网络。

4.3.1.2　发电厂监控系统根据不同的功能特性，应划分为不同的安全区域，重点强化边界的安全防护；同时应加强安全区域内部的物理安全、网络安全、主机安全、应用安全和数据安全，加强安全管理制度、机构、人员、系统建设、系统运维的管理。

4.3.1.3　发电厂监控系统的分区结构与边界防护，应满足图 1 的基本形式。发电厂监控系统与企业的管理信息系统之间，只允许进行单向通信，应采用物理隔离方式保证其边界安全，且所有的网络安全措施不应影响监控系统的基本功能和运行性能。

4.3.2　安全分区

4.3.2.1　发电厂网络与信息系统应按业务功能划分为生产控制大区和管理信息大区。

4.3.2.2　发电厂监控系统属于生产控制大区，应满足下述要求：

a）　生产控制大区应根据系统的重要性和对电力系统的影响，进一步划分为控制区（安全区Ⅰ）及非控制区（安全区Ⅱ）。

b）　在生产控制大区内，个别业务系统或其功能模块（或子系统）需要使用公用通信网、无线通信网，以及处于非可控状态下的网络设备和终端进行通信时，应设立安全接入区。

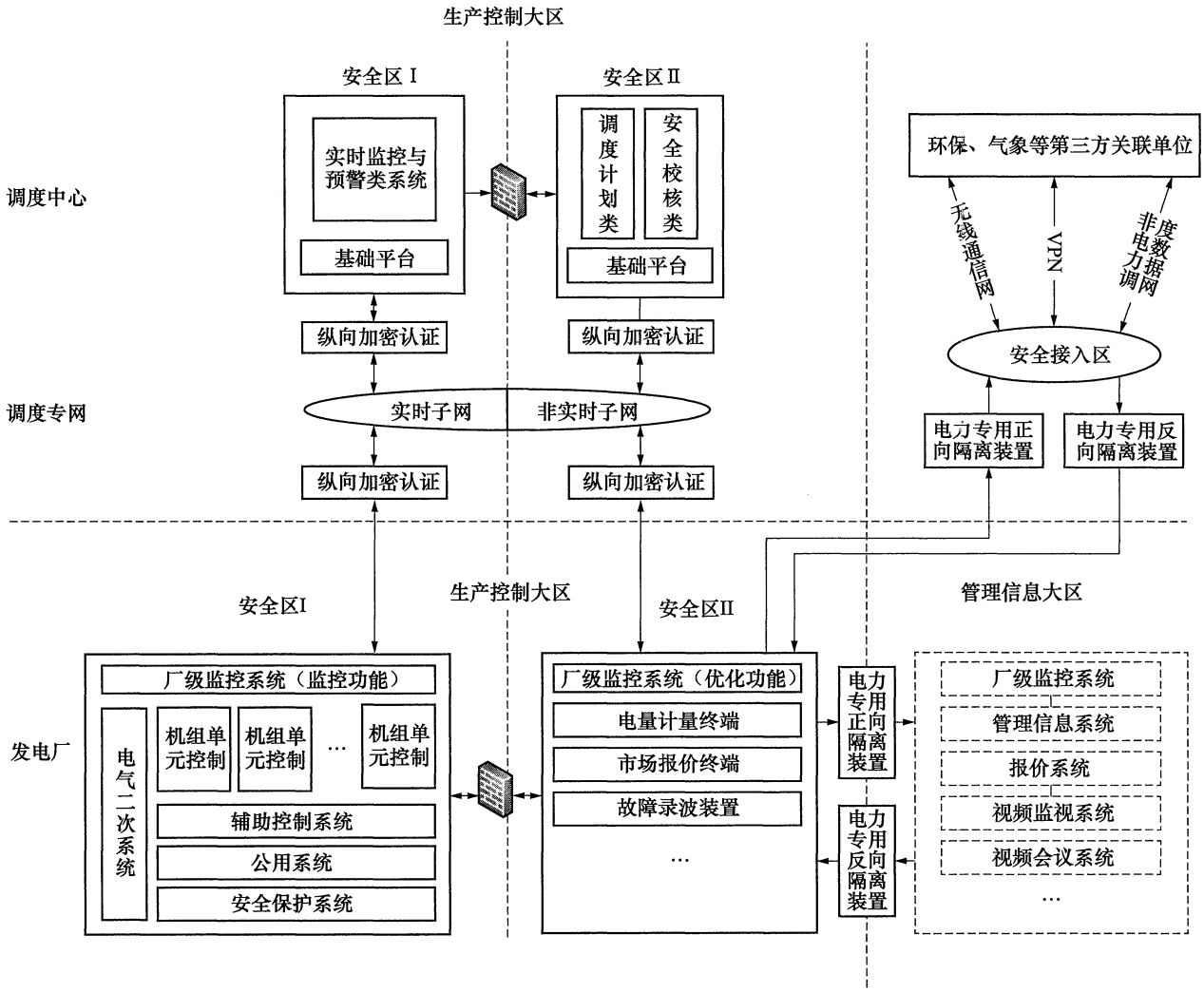


图 1　发电厂监控系统分区结构与边界防护示意图

4.3.3　网络专用

4.3.3.1　电力调度数据网应是为生产控制大区服务的专用数据网络。

4.3.3.2　发电厂端的电力调度数据网，应在专用通道上使用独立的网络设备组网，在物理层面上实现与电厂其他数据网及外部公共信息网络的安全隔离。

4.3.3.3　发电厂端的电力调度数据网，应划分为逻辑隔离的实时子网和非实时子网，分别连接控制区和非控制区。

4.3.4　横向隔离

4.3.4.1　生产控制大区与管理信息大区之间，应设置经国家指定部门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。

4.3.4.2　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网络设备、防火墙或者相当功能的设施，实现逻辑隔离。

4.3.4.3　安全接入区与生产控制大区中的其他部分的连接处，应设置经国家指定部门检测认证的电力专用横向安全隔离装置（包括正向隔离装置和反向隔离装置）。

4.3.5 纵向认证

发电厂生产控制大区中的业务系统与调度端的系统，通过电力调度数据网进行远程通信时，应设置经过国家指定部门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。

4.3.6 综合防护

发电厂应在实现 4.3.1～4.3.5 要求的基础上，结合国家信息安全等级保护工作的相关要求，对发电厂监控系统从上位机、网络设备、恶意代码防范、应用安全控制、审计、备份及容灾等多个层面进行信息安全的综合防护。

5 监控系统信息安全技术要求

5.1 安全物理环境

5.1.1 物理位置的选择

5.1.1.1 物理位置的选择包括下列要求：

a） 控制设备间的场地应选择在具有防震、防风和防雨等能力的建筑内。

b） 控制设备间的场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

c） 控制设备间外安装的设备应符合发电行业相关标准对所选用设备使用的物理和环境的要求。

d） 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固，箱体或装置具有透风、散热、防盗、防雨和防火等能力。

e） 室外控制设备的放置应远离强电磁干扰、强热源等环境。

5.1.1.2 物理位置选择的不同等级保护系统有下列要求：等级保护一、二、三级系统应满足 5.1.1.1 中 a）～e）的要求。

5.1.2 电源系统安全

5.1.2.1 电源系统安全包括下列要求：

a） 应在控制设备间的供电线路上配置稳压器和过电压保护设备。

b） 应为控制设备间提供短期的备用电力供应，至少应满足设备在断电情况下的正常运行要求。

c） 应设置冗余或并行的电力电缆线路为计算机系统供电。

5.1.2.2 电源系统安全的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.1.2.1 中 a）的要求。

b） 等级保护二级系统应满足 5.1.2.1 中 a）、b）的要求。

c） 等级保护三级系统应满足 5.1.2.1 中 a）～c）的要求。

5.1.3 温、湿度控制

5.1.3.1 温、湿度控制包括下列要求：

a） 应设置必要的温、湿度调节设施，使控制设备间温、湿度的变化在设备运行所允许的范围之内。

b） 控制设备间应设置温、湿度自动调节设施，使控制设备间温、湿度的变化在设备运行所允许的范围之内。

c） 控制设备间外安装的设备应符合发电行业相关标准对所应用的物理和环境的要求。

5.1.3.2 温、湿度控制的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.1.3.1 中 a）、c）的要求。

b） 等级保护二、三级系统应满足 5.1.3.1 中 b）、c）的要求。

5.1.4 防火

5.1.4.1 防火包括下列要求：

a） 控制设备间应设置相应的灭火设备。

b） 控制设备间应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

c） 控制设备间及相关的工作房间和辅助房间应采用具有耐火等级的建筑材料。

d） 应对控制设备间划分区域进行管理，区域和区域之间应设置隔离防火措施。

5.1.4.2 防火的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.1.4.1 中 a）的要求。

b） 等级保护二级系统应满足 5.1.4.1 中 b）、c）的要求。

c） 等级保护三级系统应满足 5.1.4.1 中 b）、c）、d）的要求。

5.1.5 防水和防潮

5.1.5.1 防水和防潮包括下列要求：

a） 水管安装，不应从控制设备间的屋顶和活动地板下穿过。

b） 控制设备间应采取措施防止雨水通过控制设备间的窗户、屋顶和墙壁渗入。

c） 控制设备间应采取措施防止控制设备间内的水蒸气结露和地下积水的转移与渗透。

d） 控制设备间应安装对水敏感的检测仪表或元件，对控制设备间进行防水检测和报警。

e） 控制设备间外安装的设备应符合发电行业相关标准对其所选用设备使用的物理和环境的要求。

5.1.5.2 防水和防潮的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.1.5.1 中 a）、b）、c）、e）的要求。

b） 等级保护三级系统应满足 5.1.5.1 中 a）～e）的要求。

5.1.6 防雷

5.1.6.1 防雷包括下列要求：

a） 应将各类机柜、设施和设备等通过接地系统安全接地，接地电阻应满足相关标准的要求；

b） 应采取措施防止感应雷，如设置防雷保安器或过电压保护装置等。

5.1.6.2 防雷的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.1.6.1 中 a）的要求。

b） 等级保护三级系统应满足 5.1.6.1 中 a）、b）的要求。

5.1.7 电磁防护

5.1.7.1 电磁防护包括下列要求：

a） 电源线和通信线缆应隔离铺设，避免互相干扰；

b） 应对关键设备实施电磁屏蔽。

5.1.7.2 电磁防护的不同等级保护系统有下列要求：

a） 等级保护一级系统无要求。

b） 等级保护二级系统应满足 5.1.7.1 中 a）的要求。

c） 等级保护三级系统应满足 5.1.7.1 中 a）、b）的要求。

5.1.8 防静电

5.1.8.1 防静电包括下列要求：

a） 控制设备间外安装的设备应符合发电行业相关标准对其所选用设备使用的物理和环境的要求。
b） 控制设备间应安装防静电地板或采取必要的接地等防静电措施。
c） 应采取措施防止静电的产生，如采用静电消除器、佩戴防静电手环等。

5.1.8.2 防静电的不同等级保护系统有下列要求：
a） 等级保护一级系统应满足 5.1.8.1 中 a）的要求。
b） 等级保护二级系统应满足 5.1.8.1 中 a）、b）的要求。
c） 等级保护三级系统应满足 5.1.8.1 中 a）～c）的要求。

5.1.9 防盗和防外力破坏

5.1.9.1 防盗和防外力破坏包括下列要求：
a） 应将设备或主要部件进行固定，并设置明显的不易除去的标识。
b） 应对通信线缆实施防护，将其敷设在安全处（如可铺设在地下或管道中），并设置清晰的线路标识和警示标识，警示标识位置合理。
c） 应设置控制设备间防盗报警系统或设置有专人值守的视频监控系统。

5.1.9.2 防盗和防外力破坏的不同等级保护系统有下列要求：
a） 等级保护一级系统应满足 5.1.9.1 中 a）的要求。
b） 等级保护二级系统应满足 5.1.9.1 中 a）、b）的要求。
c） 等级保护三级系统应满足 5.1.9.1 中 a）～c）的要求。

5.1.10 物理访问控制

5.1.10.1 物理访问控制包括下列要求：
a） 被控制区域的边界，应有明确的防止非授权人员接触的提示标识。
b） 应有防止非授权人员进入的物理防护措施（如栅栏）。
c） 控制设备间出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
d） 控制设备间出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

5.1.10.2 物理访问控制的不同等级保护系统有下列要求：
a） 等级保护一级系统应满足 5.1.10.1 中 a）、c）的要求。
b） 等级保护二级系统应满足 5.1.10.1 中 a）～c）的要求。
c） 等级保护三级系统应满足 5.1.10.1 中 a）、b）、d）的要求。

5.2 安全通信网络

5.2.1 网络架构安全

5.2.1.1 网络架构安全包括下列要求：
a） 监控系统网络与发电厂其他信息系统网络应划分为两个区，区间应采用单向的技术隔离手段。
b） 监控系统网络内部，应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。
c） 应划分为不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
d） 应避免将重要网络区域部署在网络边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
e） 监控系统中涉及实时控制和数据传输的系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网的隔离。
f） 应保证网络设备的业务处理能力满足业务高峰期需要。
g） 应保证网络各个部分的带宽满足业务高峰期需要。

h） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

5.2.1.2 网络架构安全的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.2.1.1 中 a）～c）的要求。

b） 等级保护二级系统应满足 5.2.1.1 中 a）～e）的要求。

c） 等级保护三级系统应满足 5.2.1.1 中 a）～h）的要求。

5.2.2 通信传输安全

5.2.2.1 通信传输安全包括下列要求：

a） 应采用校验技术保证通信过程中数据的完整性，监控系统应拒绝任何非法会话标识符的使用。

b） 在监控系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

c） 应在用户退出或其他会话结束（包括浏览器会话）后使会话标识符失效。

5.2.2.2 通信传输安全的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.2.2.1 中 a）的要求。

b） 等级保护二级系统应满足 5.2.2.1 中 a）、b）的要求。

c） 等级保护三级系统应满足 5.2.2.1 中 a）～c）的要求。

5.2.3 使用拨号通信

5.2.3.1 使用拨号通信包括下列要求：

a） 监控系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施。

b） 拨号服务器和客户端均应使用经过安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施。

5.2.3.2 使用拨号通信的不同等级保护系统有下列要求：

a） 等级保护一级系统无要求。

b） 等级保护二级系统应满足 5.2.3.1 中 a）的要求。

c） 等级保护三级系统应满足 5.2.3.1 中 a）、b）的要求。

5.2.4 无线通信安全

5.2.4.1 无线通信安全包括下列要求：

a） 应对无线连接的授权、监视及使用进行限制。

b） 应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一的识别标识，并具备对其进行识别的能力。

c） 应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权，并确保其对无线通信的使用与其授权相符。

d） 应能识别在监控系统物理环境中使用的未经授权的无线设备，对未经授权的试图接入或干扰监控系统的行为进行报警。

e） 应对无线通信采取传输加密的安全措施，保证传输报文的机密性。

5.2.4.2 无线通信安全的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.2.4.1 中 a）、b）的要求。

b） 等级保护二级系统应满足 5.2.4.1 中 a）～c）的要求。

c） 等级保护三级系统应满足 5.2.4.1 中 a）～e）的要求。

5.2.5 可信验证

5.2.5.1 可信验证包括下列要求：

a） 应能基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

b） 应能基于可信根对通信设备的重要配置参数、通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

c） 可信验证结果应形成审计记录送至安全管理中心。

5.2.5.2 可信验证的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.2.5.1 中 a）的要求。

b） 等级保护二级系统应满足 5.2.5.1 中 a）、b）的要求。

c） 等级保护三级系统应满足 5.2.5.1 中 a）～c）的要求。

5.3 安全区域边界

5.3.1 边界安全防护

5.3.1.1 边界安全防护包括下列要求：

a） 在生产控制大区与管理信息大区之间，应设置经国家指定部门检测认证的电力专用横向单向安全隔离装置，不应有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。

b） 在与电力调度数据网等广域网的纵向连接处，应设置经国家指定部门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。

c） 使用无线通信网、非电力调度数据网或者外部公用数据网的虚拟专用网（VPN）等进行通信的，应当设立“安全接入区”。

d） 生产控制大区与“安全接入区”的连接处，应设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。

e） 生产控制大区内部控制网络和非控制网络之间，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。

f） 应对控制网络和非控制网络的边界，以及控制网络内安全域和安全域之间的边界进行监视，并控制区、域之间的边界通信。

g） 应在控制网络和非控制网络的边界，以及控制网络内安全域和安全域之间的边界默认拒绝所有非必要的网络数据流，但可允许例外的网络数据流。

h） 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界上阻止任何非必要的通信。

i） 应在控制网络和非控制网络的边界防护机制失效时，能阻止所有边界通信（也称故障关闭），但故障关闭功能的设计不应干扰相关安全功能的运行。

j） 应在控制网络内安全域和安全域之间的边界防护机制失效时及时进行报警，并保障关键设备的通信。

k） 应能识别控制网络和非控制网络边界上的入侵行为，并进行有效阻断。

l） 生产控制大区中除安全接入区外，不应选用具有无线通信功能的设备。

m） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

n） 应能够对非授权设备私自连接到内部网络的行为进行检查或限制。

o） 应能够对内部用户非授权连接到外部网络的行为进行检查或限制。

p） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

5.3.1.2 边界安全防护的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.3.1.1 中 a）～e）、l）、m）的要求。

b） 等级保护二级系统应满足 5.3.1.1 中 a）～g）、k）～m）的要求。

c） 等级保护三级系统应满足 5.3.1.1 中 a）～p）的要求。

5.3.2 访问控制

5.3.2.1 访问控制包括下列要求：

a） 对一个可配置的时间或事件序列，应支持高权限主管手动超驰当前用户的授权。

b） 应能通过手动启动，或在一个可配置的非活动周期后系统自动启动会话锁定功能，以防止对系统的进一步访问。会话锁定应一直保持有效，直到拥有会话权限的用户或其他授权的用户使用适当的身份标识和鉴别规程重新建立访问。

c） 应在一个可配置的非活动时间周期后自动地或由发起会话的用户手动终止远程会话。

d） 应在网络边界或安全域边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外，受控接口拒绝所有通信。

e） 应删除多余的或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

f） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

g） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

h） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

i） 应在发电厂监控系统与企业其他系统之间部署访问控制设备，配置访问控制策略，不应有任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

j） 应在发电厂监控系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

5.3.2.2 访问控制的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.3.2.1 中 b）～f）、i）的要求。

b） 等级保护二级系统应满足 5.3.2.1 中 b）～g）、i）、j）的要求。

c） 等级保护三级系统应满足 5.3.2.1 中 a）～j）的要求。

5.3.3 入侵防范

5.3.3.1 入侵防范包括下列要求：

a） 应在关键网络节点处监视网络攻击行为。

b） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

c） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

d） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

e） 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

5.3.3.2 入侵防范的不同等级保护系统有下列要求：

a） 等级保护一级系统无要求。

b） 等级保护二级系统应满足 5.3.3.1 中 a）的要求。

c） 等级保护三级系统应满足 5.3.3.1 中 a）～e）的要求。

5.3.4 恶意代码防范

5.3.4.1 恶意代码防范包括下列要求：

a） 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

b） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

5.3.4.2 恶意代码防范的不同等级保护系统有下列要求：

a） 等级保护一级系统无要求。

b） 等级保护二级系统应满足 5.3.4.1 中 a）的要求。

c） 等级保护三级系统应满足 5.3.4.1 中 a）、b）的要求。

5.3.5 安全审计

5.3.5.1 安全审计包括下列要求：

a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

d） 应对审计进程进行保护，防止未经授权的中断。

e） 应在可配置的频率下，对各系统的时钟进行同步，以便于对审计记录的集中分析。

f） 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

5.3.5.2 安全审计的不司等级保护系统有下列要求：

a） 等级保护一级系统无要求。

b） 等级保护二级系统应满足 5.3.5.1 中 a）～c）的要求。

c） 等级保护三级系统应满足 5.3.5.1 中 a）～f）的要求。

5.3.6 可信验证

5.3.6.1 可信验证包括下列要求：

a） 应能基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

b） 应能基于可信根对通信设备的重要配置参数、通信应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警。

c） 可信验证结果应形成审计记录送至安全管理中心。

5.3.6.2 可信验证的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.3.6.1 中 a）的要求。

b） 等级保护二级系统应满足 5.3.6.1 中 a）、b）的要求。

c） 等级保护三级系统应满足 5.3.6.1 中 a）～c）的要求。

5.4 安全计算环境

5.4.1 设备安全

5.4.1.1 系统软件及版本更新

5.4.1.1.1 系统软件及版本更新包括下列要求：

a） 监控系统上位机应采用经国家指定机构认证的安全操作系统或进行安全加固。

b） 跟踪监控系统上位机和设备系统软件的版本更新、漏洞和补丁发布情况，严格进行软件升级和补丁安装等工作管理，防止病毒、木马等恶意代码的侵入。

c） 系统软件的升级、补丁安装前，应对其进行安全性评估和验证，并对更新进行记录；评估和验证工作应在与生产环境一致的验证环境或平台上进行，主要评估其有效性、安全性和对系统安

全稳定运行的影响，必要时应聘请有资质的第三方机构开展评估和验证工作。

5.4.1.1.2 系统软件及版本更新的不同等级保护系统有下列要求：等级保护一、二、三级系统应满足5.4.1.1.1 中 a）～c）的要求。

5.4.1.2 身份鉴别

5.4.1.2.1 身份鉴别包括下列要求：

a） 应对所有登录的用户和信息设备进行唯一的身份标识和鉴别，身份鉴别信息应具有满足相关法律、法规和标准的复杂度要求和更换周期。

b） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关功能。

c） 应能初始化鉴别器内容，系统一经安装完成，立即改变所有鉴别器的默认值，改变或者刷新所有的鉴别器；当存储或者传输时，要保护鉴别器免受未经授权的泄露和修改。

d） 在身份鉴别可能对系统实时性产生影响并影响系统正常操作的，应采用其他替代的安全手段或通过管理手段来进行弥补。

e） 应能够隐藏鉴别过程中反馈的鉴别信息。

f） 监控系统原则上不允许进行远程管理，对确有远程管理需要的系统，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

g） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且至少其中有一种鉴别技术使用密码技术来实现。

5.4.1.2.2 身份鉴别的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.1.2.1 中 a）～e）的要求。

b） 等级保护二级系统应满足 5.4.1.2.1 中 a）～f）的要求。

c） 等级保护三级系统应满足 5.4.1.2.1 中 a）～g）的要求。

5.4.1.3 访问控制

5.4.1.3.1 访问控制包括下列要求：

a） 应对登录的用户分配账户和权限。

b） 应重命名或删除默认账户，应修改所有账户的默认口令。

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

d） 对包括管理用户在内的用户进行权限分配时应采用最小权限原则，对管理用户应实现权限分离。

e） 应在一个可配置的非活动时间周期后自动地或由发起会话的用户手动终止远程会话。

f） 应由授权用户配置访问控制策略，由访问控制策略规定访问主体对客体的访问规则。

g） 访问控制策略的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。

h） 应对重要主体和客体设置安全标记，并控制主体对有安全标记的信息资源的访问。

5.4.1.3.2 访问控制的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.1.3.1 中 a）、b）、c）的要求。

b） 等级保护二级系统应满足 5.4.1.3.1 中 a）～e）的要求。

c） 等级保护三级系统应满足 5.4.1.3.1 中 a）～h）的要求。

5.4.1.4 可信验证

5.4.1.4.1 可信验证包括下列要求：

a） 应能基于可信根对监控系统上位机和设备的系统引导程序、系统程序进行可信验证，在检测到其可信性受到破坏后进行报警。

b） 应能基于可信根对监控系统上位机和设备的重要配置参数和通信应用程序进行可信验证，在检测到其可信性受到破坏后进行报警。

c） 可信验证结果应形成审计记录送至安全管理中心。

5.4.1.4.2 可信验证的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.1.4.1 中 a）的要求。

b） 等级保护二、三级系统应满足 5.4.1.4.1 中 a）～c）的要求。

5.4.1.5 入侵防范

5.4.1.5.1 入侵防范包括下列要求：

a） 所有监控系统上位机均应采用最小化原则进行系统安装，除了必要的安全组件或软件外，只安装与自身业务相关的操作系统组件及应用软件。例如，工程师站、操作员站只安装组态软件、监控软件、编程软件、报表软件及与此相关的操作系统组件；OPC 服务器、实时数据库服务器只安装数据库软件、服务器软件及与此业务相关的操作系统组件。

b） 应关闭不需要的系统服务、默认共享和高危端口。

c） 应通过设定终端接入方式或网络地址范围等措施，限制通过网络进行管理的管理终端。

d） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

e） 应能发现可能存在的漏洞，并在经过充分测试评估后及时修补漏洞。

f） 应自动执行可配置的使用限制，包括防止使用便携式或移动设备、要求访问特定内容的授权、限制便携式或移动设备的代码读写和数据传输操作。

g） 应能通过手动启动，或在一个可配置的非活动周期后系统自动启动会话锁定操作，以防止对系统的进一步访问；会话锁定应一直保持有效，直到拥有会话权限的用户或被授权的其他用户使用适当的身份标识和鉴别规程重新建立访问；可能对实时性产生影响，进而影响系统正常操作的，应采用其他替代安全手段或通过管理手段来进行弥补。

h） 应能有效地识别和处理错误状况，并在此过程中不泄露任何与安全相关的信息，除非该信息是及时排除故障所必需的信息。

i） 应能够检测到对重要节点的入侵行为，并在发生严重入侵事件时提供报警。

5.4.1.5.2 入侵防范的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.1.5.1 中 a）、b）的要求。

b） 等级保护二级系统应满足 5.4.1.5.1 中 a）～h）的要求。

c） 等级保护三级系统应满足 5.4.1.5.1 中 a）～i）的要求。

5.4.1.6 恶意代码防范

5.4.1.6.1 恶意代码防范包括下列要求：

a） 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

b） 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并进行有效阻断。

5.4.1.6.2 恶意代码防范的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.4.1.6.1 中 a）的要求。

b） 等级保护三级系统应满足 5.4.1.6.1 中 a）、b）的要求。

5.4.1.7 安全审计

5.4.1.7.1 安全审计包括下列要求：

a） 应启用安全审计功能，审计应覆盖每个用户，对重要的用户行为和重要安全事件进行审计。
b） 审计记录应包括事件的日期和时间、用户、事件的类型、事件是否成功及其他与审计相关的信息。
c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
d） 应对审计进程进行保护，防止未经授权的中断。
e） 应在可配置的频率下，对各系统的时钟进行同步，以便于对审计记录的集中分析。

5.4.1.7.2 安全审计的不同等级保护系统有下列要求：

a） 等级保护一级系统无要求。
b） 等级保护二级系统应满足 5.4.1.7.1 中 a）～c）的要求。
c） 等级保护三级系统应满足 5.4.1.7.1 中 a）～e）的要求。

5.4.1.8 资源控制

5.4.1.8.1 资源控制包括下列要求：

a） 在不影响当前安全状态的情况下，系统应能在正常供电电源和应急电源之间进行切换。
b） 应参照供应商提供的指南，根据所推荐的网络和安全配置进行系统设置。
c） 应对重要节点，如工程师站、操作员站和服务器等系统的运行资源进行监视，监视内容包括 CPU、硬盘和内存等资源的使用情况，在资源使用情况达到预先设置的阈值时，应触发报警。
d） 应能对重要节点的服务水平进行检测，并在其降低到预先设定的最小值时进行报警。
e） 应能实时监控设备的运行和通信状态，并在发现异常时能及时进行报警。
f） 应提供重要节点设备的硬件冗余，保证系统的可用性。
g） 应对任何给定设备的每个接口限制并发会话数量。
h） 应把当前的安全配置设置生成一个设备可读的报告列表。

5.4.1.8.2 资源控制的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.4.1.8.1 中 a）、b）的要求。
b） 等级保护三级系统应满足 5.4.1.8.1 中 a）～h）的要求。

5.4.1.9 监控设备

5.4.1.9.1 监控设备包括下列要求：

a） 监控设备应实现本文件所要求相应级别的身份鉴别、访问控制和安全审计等要求，如受条件限制监控设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制。
b） 应在不影响系统安全稳定运行的情况下，对监控设备进行补丁更新、固件更新等工作；更新前应对补丁和固件等进行充分的安全性评估和验证，并对更新进行记录；评估和验证工作应在与生产环境一致的验证环境或平台上进行，主要评估其有效性、安全性和对系统安全稳定运行的影响，必要时应聘请有资质的第三方机构开展评估和验证工作。
c） 应关闭或拆除监控设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理。
d） 应使用专用设备和专用软件对监控设备进行更新。
e） 应保证监控设备在上线前经过安全性检测，避免监控设备固件中存在恶意代码程序。

5.4.1.9.2 监控设备的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.4.1.9.1 中 a）、b）的要求。
b） 等级保护三级系统应满足 5.4.1.9.1 中 a）～e）的要求。

5.4.2 应用软件和数据安全

5.4.2.1 软件的升级和更新

5.4.2.1.1 软件的升级和更新包括下列要求：

a） 应跟踪监控系统应用软件的版本更新、漏洞和补丁发布情况，并严格进行软件升级和补丁安装的工作管理，防止病毒、木马等恶意代码的侵入。

b） 在重要监控系统的软件升级、补丁安装前，应对其进行安全性评估和验证，并对更新进行记录；评估和验证工作应在与生产环境一致的验证环境或平台上进行，主要评估其有效性、安全性和对系统安全稳定运行的影响，必要时应聘请有资质的第三方机构开展评估和验证工作。

5.4.2.1.2 软件的升级和更新的不同等级保护系统有下列要求：等级保护一、二、三级系统应满足5.4.2.1.1 中 a）、b）的要求。

5.4.2.2 身份鉴别

5.4.2.2.1 身份鉴别包括下列要求：

a） 应对登录的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应满足相关法律、法规和标准要求的复杂度和更换周期。

b） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关功能；当无效访问次数超出限制后，应进行报警。

c） 应强制用户首次登录时修改初始口令，口令设置应具备对最小长度、多字符类型组合等通用原则的校验功能，未达到强度要求的口令设置不能生效。

d） 对口令设置可能对系统的实时性产生影响，进而影响系统正常操作的，应采用其他身份鉴别手段替代或通过管理手段进行弥补。

e） 应能够隐藏鉴别过程中反馈的鉴别信息。

f） 监控系统原则上不准许进行远程管理，对确有远程管理需要的系统，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

g） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中至少有一种鉴别技术使用密码技术来实现。

5.4.2.2.2 身份鉴别的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.2.2.1 中 a）～e）的要求。

b） 等级保护二级系统应满足 5.4.2.2.1 中 a）～f）的要求。

c） 等级保护三级系统应满足 5.4.2.2.1 中 a）～g）的要求。

5.4.2.3 访问控制

5.4.2.3.1 访问控制包括下列要求：

a） 应提供访问控制功能，对登录的用户分配账号和权限。

b） 应具备默认账号重命名或账号默认口令修改的管控机制，不应在工程师站、操作员站、服务器等各种监控系统和设备中使用默认账户。

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在。

d） 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

e） 账号权限的授予应遵循最小化原则，授权应仅以完成其自身任务为限，并在不同角色的账户之间形成相互制约的关系。

f） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。

g） 应通过手动或在一个可配置的非活动周期后自动启动会话锁定操作，以防止对系统的进一步访问；会话锁定应一直保持有效，直到拥有会话权限的用户或被授权的其他用户使用适当的身份标识和鉴别规程重新建立访问；可能对实时性产生影响，进而影响系统正常操作的，应采用其他替代安全手段或通过管理手段来进行弥补。

h） 应对敏感信息资源设置安全标记，并控制主体对有安全标记的信息资源的访问。

5.4.2.3.2 访问控制的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.2.3.1 中 a）、b）、c）、d）的要求。

b） 等级保护二级系统应满足 5.4.2.3.1 中 a）～g）的要求。

c） 等级保护三级系统应满足 5.4.2.3.1 中 a）～h）的要求。

5.4.2.4 可信验证

5.4.2.4.1 可信验证包括下列要求：

a） 应能基于可信根对监控系统上位机和设备的系统引导程序、系统程序进行可信验证，在检测到其可信性受到破坏后进行报警。

b） 应能基于可信根对监控系统上位机和设备的重要配置参数和通信应用程序进行可信验证，在检测到其可信性受到破坏后进行报警。

c） 可信验证结果应形成审计记录送至安全管理中心。

5.4.2.4.2 可信验证的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.2.4.1 中 a）的要求。

b） 等级保护二、三级系统应满足 5.4.2.4.1 中 a）～c）的要求。

5.4.2.5 安全审计

5.4.2.5.1 安全审计包括下列要求：

a） 应启用安全审计功能，审计应覆盖每个用户，对重要的用户行为和重要安全事件进行审计。

b） 审计记录应包括事件的日期和时间、用户、事件的类型、事件是否成功及其他与审计相关的信息。

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

d） 应对审计进程进行保护，防止未经授权的中断。

e） 应在可配置的频率下，对各系统的时钟进行同步，以便于对审计记录的集中分析。

5.4.2.5.2 安全审计的不同等级保护系统有下列要求：

a） 等级保护一级系统无要求。

b） 等级保护二级系统应满足 5.4.2.5.1 中 a）～c）的要求。

c） 等级保护三级系统应满足 5.4.2.5.1 中 a）～e）的要求。

5.4.2.6 软件容错

5.4.2.6.1 软件容错包括下列要求：

a） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定的要求。

b） 在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施。

c） 应提供自动保护功能，当故障发生时自动保护当前所有状态，以保证系统能够进行恢复。

5.4.2.6.2 软件容错的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.2.6.1 中 a）的要求。

b） 等级保护二、三级系统应满足 5.4.2.6.1 中 a）～c）的要求。

5.4.2.7 资源控制

5.4.2.7.1 资源控制包括下列要求：

a） 当通信双方中的一方在一段时间内未作任何响应时，另一方应能自动结束会话。

b） 应能对系统的最大并发会话连接数进行限制。

c） 应能对单个账号的多重并发会话进行限制。

d） 应能对并发进程的每个进程所占用资源的最大限额进行分配。

5.4.2.7.2 资源控制的不同等级保护系统有下列要求：

a） 等级保护一级系统应满足 5.4.2.7.1 中 c）的要求。

b） 等级保护二、三级系统应满足 5.4.2.7.1 中 a）～d）的要求。

5.4.2.8 数据完整性

5.4.2.8.1 数据完整性包括下列要求：

a） 应采用校验技术保证重要数据在传输过程中的完整性。

b） 应具备检测、记录和报告机制，防止对软件和信息未经授权的更改。

c） 应对发电厂监控系统的输入或直接影响控制系统动作的输入内容和语法的合法性进行校验。

d） 对于采用工业无线或现场总线网络通信的联网设备，应保护其传输信息的完整性。

e） 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，至少包括鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要视频数据等。

f） 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，至少包括鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要视频数据等。

g） 在完整性验证过程中如发现差异，应提供自动化工具通知给一组可配置的接收者。

h） 对于采用工业无线或现场总线网络通信的联网设备，应能使用密码学机制识别信息在通信过程中是否被篡改。

5.4.2.8.2 数据完整性的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.4.2.8.1 中 a）～d）的要求。

b） 等级保护三级系统应满足 5.4.2.8.1 中 a）～h）的要求。

5.4.2.9 数据保密性

5.4.2.9.1 数据保密性包括下列要求：

a） 在信息传输时，应对有明确的“读”权限的信息提供保密性保护。

b） 在进行加密时，应按照国家相关保密部门的要求采用合适的加密算法、密钥长度和密钥管理机制。

c） 应支持国家密码管理部门批准使用的密码算法，使用国家密码管理部门认证核准的密码产品，遵循与密码相关的国家标准和行业标准。

d） 应采用密码技术保证重要数据在传输过程中的保密性，至少包括鉴别数据和重要业务数据。

e） 应采用密码技术保证重要数据在存储过程中的保密性，至少包括鉴别数据和重要业务数据。

5.4.2.9.2 数据保密性的不同等级保护系统有下列要求：

a） 等级保护一、二级系统应满足 5.4.2.9.1 中 a）、b）的要求。

b） 等级保护三级系统应满足 5.4.2.9.1 中 a）～e）的要求。

5.4.2.10 数据备份和恢复

5.4.2.10.1 数据备份和恢复包括下列要求：

a） 应提供重要数据的本地备份与恢复功能。
b） 对于监控系统和设备，包括采用工业无线或现场总线网络通信的设备在内，应在不影响正常设备使用的前提下，识别和定位关键文件，以及备份用户级和系统级的信息（包括系统状态信息）。
c） 对于监控系统和设备，包括采用工业无线或现场总线网络通信的设备在内，应定期记录一个安全状态，在系统受到破坏或发生失效后，能够恢复和重构控制系统到一个已知的安全状态。
d） 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
e） 对于监控系统和设备，包括采用工业无线或现场总线网络通信的设备在内，应提供备份机制的可靠性验证能力。
f） 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。
g） 应提供重要数据处理系统的热冗余，以保证系统的高可用性。
h） 应具备可配置频率的自动备份能力。

5.4.2.10.2 数据备份和恢复的不同等级保护系统有下列要求：
a） 等级保护一级系统应满足 5.4.2.10.1 中 a）～c）的要求。
b） 等级保护二级系统应满足 5.4.2.10.1 中 a）～e）的要求。
c） 等级保护三级系统应满足 5.4.2.10.1 中 a）～h）的要求。

5.4.2.11 剩余信息保护

5.4.2.11.1 剩余信息保护包括下列要求：
a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
b） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
c） 应清除不再使用的组件上具有明确“读”权限的访问信息。
d） 应防止通过易失性共享内存资源进行的未授权和无意的信息传输。

5.4.2.11.2 剩余信息保护的不同等级保护系统有下列要求：
a） 等级保护一级系统无要求。
b） 等级保护二级系统应满足 5.4.2.11.1 中 a）、c）的要求。
c） 等级保护三级系统应满足 5.4.2.11.1 中 a）～d）的要求。

5.5 安全管理中心

5.5.1 系统管理

5.5.1.1 系统管理包括下列要求：
a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。
b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

5.5.1.2 系统管理的不同等级保护系统有下列要求：等级保护一、二、三级系统应满足 5.5.1.1 中 a）、b）的要求。

5.5.2 审计管理

5.5.2.1 审计管理包括下列要求：
a） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。
b） 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

5.5.2.2 审计管理的不同等级保护系统有下列要求：等级保护一、二、三级系统应满足 5.5.2.1 中 a)、b）的要求。

5.5.3 安全管理

5.5.3.1 安全管理包括下列要求：

a） 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。

b） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

5.5.3.2 安全管理的不同等级保护系统有下列要求：

a） 等级保护一、二级系统无要求。

b） 等级保护三级系统应满足 5.5.3.1 中 a)、b）的要求。

5.5.4 集中管控

5.5.4.1 集中管控包括下列要求：

a） 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。

b） 应能建立安全的信息传输路径，对网络中的安全设备或安全组件进行管理。

c） 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。

d） 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律、法规的要求。

e） 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

f） 应能对网络中发生的各类安全事件进行识别、报警和分析。

5.5.4.2 集中管控的不同等级保护系统有下列要求：

a） 等级保护一、二级系统无要求。

b） 等级保护三级系统应满足 5.5.4.1 中 a）～f）的要求。

6 监控系统信息安全评估

6.1 基本要求

6.1.1 应对发电厂监控系统的脆弱性、面临的威胁及其信息安全防护能力进行分析评估，以确保监控系统的信息安全防护满足国家相关法律、法规、标准及本文件的安全防护要求。应通过评估，掌握监控系统的脆弱性和面临的威胁，并提出相应的措施，以消除风险或将风险控制在可接受的范围。发电厂监控系统的脆弱性及主要威胁见附录 A。

6.1.2 监控系统信息安全评估不应影响系统原有的实时性、可用性、可靠性和安全性。对监控系统的各项评估工作，宜在离线或模拟环境下完成。对监控系统的评估，若包括通信网络，宜在网络结构完整的监控系统环境下进行。应加强安全评估工作的风险控制，预防安全评估工作本身引入的安全风险，评估工作开始前应做好应急预案。监控系统的信息安全评估工作应常态化定期进行。

6.2 评估对象

6.2.1 监控系统信息安全评估所涉及的对象包括监控系统的各组成部分，以及相关的操作与管理人员，是客观存在的设备、网络、人员和文档等。

6.2.2 具体实施评估的对象可以是单个的设备、网络、人员和文档，也可以是由多个设备、网络、人员和文档构成的集合。

6.3 评估方法

6.3.1 文档查阅

6.3.1.1 评估查阅的文档应包括监控系统规划设计方案、网络拓扑图、系统安全防护计划、安全策略、架构、要求、标准作业程序、程序作业过程管理文件，授权协议、系统互连备忘录和事件响应计划等，评估其准确性和完整性。

6.3.1.2 评估发电企业在信息安全政策及技术方面是否保持最新；验证相关文档是否符合法律、法规和标准；验证过程文档，评估企业信息安全政策和技术措施是否有效实施；查找企业政策的缺陷、过时或不合理的内容。

6.3.2 现场访谈

6.3.2.1 对涉及监控系统的管理人员、运行人员、维护人员、供应商、工艺工程师、开发人员和系统集成商等进行面对面的交流。

6.3.2.2 交流收集客观材料，作为对文档查阅工作的补充。

6.3.3 现场核查

6.3.3.1 在现场生产环境下，应对已确定的评估内容进行现场核查。

6.3.3.2 一般情况下，现场核查应包括以下评估内容：

a） 监控系统的现场物理环境。

b） 监控系统的配置、系统架构、防护措施和系统日志等。

c） 监控系统的安全管理工作。

6.3.4 工具检测

6.3.4.1 对涉及评估对象功能、性能和安全性的评估内容，可采用专用的检测软件或工具，在现场检修或运行环境下对其进行信息安全风险评估。

6.3.4.2 在采用工具检测时，应注意避免因检测给监控系统带来不可预测的风险，并确保在风险发生时，可根据合适的应急预案，消除风险及其后续的影响。

6.3.4.3 工具检测的具体操作，应严格按照所采用检测工具的操作规范和普遍认可的工作实践进行。

6.4 评估方案与结论

6.4.1 评估方案

6.4.1.1 实施评估应编制评估实施方案。评估方案应至少包括评估项目、评估方式、检测对象、操作流程和风险预控等内容。

6.4.1.2 根据普遍接受的评估实践，评估项目可包括“必做项”和“选做项”两类。

6.4.1.3 具体的评估工作中，宜根据监控系统的实际情况，在满足“合规性”的前提下，确定评估项目是否合适，并在实施评估工作前做好必要的应急措施。

6.4.2 评估结论

6.4.2.1 评估人员在执行评估操作并得到各种评估依据之后，应对各评估实施单元给出评估结果。

6.4.2.2 根据普遍接受的评估实践，通过计算得出被评估系统的分值，并给出被评估系统是否满足信息安全防护技术要求的结论。

附 录 A
（资料性）
发电厂监控系统的脆弱性及主要威胁

A.1 概述

随着时间的推移和系统研发技术、信息安全攻防技术的变化和发展，对发电厂监控系统的脆弱性及面临的主要威胁，不断会有新的发现。一般来讲，发电厂监控系统的脆弱性可以归为策略管理类、平台类和网络类，也可能有一些特殊的脆弱性未包括这三类之中。发电厂监控系统所面临的威胁可来自多个方面，主要可分为两类：一类是对抗性来源，另一类是自然来源。

A.2 脆弱性

A.2.1 策略管理类

常见的策略管理类脆弱性主要包括：

a） 监控系统安全策略不当。
b） 员工安全培训和意识不足。
c） 安全架构和设计不足。
d） 对于监控系统没有明确的、书面的安全策略和管理文件。
e） 安全措施的保障机制缺失。
f） 监控系统缺乏安全审计机制。
g） 缺乏实用的应急响应预案或预案缺乏演练。
h） 缺乏明确的配置变更管理机制或管理不到位。

A.2.2 平台类

常见的平台类脆弱性主要包括：

a） 平台配置方面：系统漏洞被发现后，系统厂商没有及时开发相应的补丁；漏洞补丁不能及时安装；漏洞补丁缺乏广泛而有效的测试；系统使用厂家的默认配置；关键配置文件没有可靠的备份；没有有效的访问控制策略；密码策略设置不当，、没有密码或密码不当。
b） 平台硬件方面：安全环境变更时没有充分的测试，未授权用户可接触设备，允许远程访问，双网卡跨接不同的网络环境，未注册设备，使用无线传输的设备，关键设备无冗余，关键设备无备用电源。
c） 平台软件方面：使用不安全的协议，采用明文传输，开启不必要的服务，存在缓冲区溢出的可能，自身的安全功能未开启，无日志或日志维护不当。
d） 恶意软件防护方面：未安装防恶意软件的工具，防恶意软件的工具的版本或特征库未更新，防恶意软件的工具安装前未进行有效的广泛测试。

A.2.3 网络类

常见的网络类脆弱性主要包括：

a） 网络配置方面：未实施数据流控制，安全设备配置不当，网络设备配置文件保存不当，网络设备密码修改周期过长，访问控制措施不充分。
b） 网络硬件方面：网络设备物理防护不足，不安全的物理接口，物理环境控制缺失，非授权人员

对设备和网络连接的访问，关键网络设备没有冗余备份措施。

c） 网络边界方面：未定义网络边界，边界未安装适当的防护设备或设备的防护策略配置不当，专网中存在非法流量，专网运行非专用的协议和应用。

d） 网络监控和日志方面：网络设备和安全设备未开启日志或日志保存不当，没有安装信息安全监控系统或监控设备。

e） 网络通信方面：采用未加密的通用协议，未识别关键监测点和控制路径，用户、数据与设备的认证手段不足，网络通信数据完整性校验不足。

f） 无线连接方面：无线客户端和接入点的认证措施不足，无线客户端和接入点的传输保护措施不足。

A.3 威胁来源

A.3.1 自然威胁来源

自然威胁来源主要包括系统的复杂性、人为的错误、意外事故、设备故障和自然灾害，它们均属于传统的生产安全范畴。

A.3.2 对抗性威胁来源

发电厂监控系统面临的对抗性威胁主要来源于：

a） 犯罪集团：一般性的犯罪分子，利用网络攻击来获取经济利益。有组织和有特定目的的犯罪团伙则利用网络来破坏国家的关键基础设施，通过造成经济损失和人员的伤亡来威胁国家安全。

b） 工业间谍：利用网络秘密获取知识产权和技术秘密，目的是打击竞争对手和获取经济利益。

c） 恶意的黑客：掌握了网络渗透能力的个人或组织，通过制作、使用和扩散恶意软件和间谍软件对用户形成威胁，他们的动机各不相同。

d） 心怀不满的内部员工：内部员工对目标系统很了解，往往能够不受限制地访问系统，所以他们如果要对系统造成损害或窃取系统数据，往往并不需要大量的计算机入侵知识。

参 考 文 献

[1] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求
[2] GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南
[3] GB/T 36047—2018 电力信息系统安全检查规范
[4] GB/T 36466—2018 信息安全技术 工业控制系统风险评估实施指南
[5] GB/T 37138—2018 电力信息系统安全等级保护实施指南
[6] GB 50660—2011 大中型火力发电厂设计规范
[7] 中华人民共和国国家发展和改革委员会令 2014 年第 14 号 电力监控系统安全防护规定
[8] 国能安全〔2014〕317 号 电力行业网络与信息安全管理办法
[9] 国能安全〔2014〕36 号 电力监控系统安全防护总体方案
[10] 中网办发文〔2016〕3 号 关于开展关键信息基础设施网络安全检查的通知