ICS XX.XXX.XX
CCS X XX

ZJSEE

浙 江 省 电 力 学 会 标 准

[状态]

火电机组分散控制系统安全防护技术规范

Technical specifications for safety protection of decentralized control systems in thermal power units

（与国际标准一致性程度的标识）

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

浙 江 省 电 力 学 会　发 布

目　　次

[状态]

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。

本文件（或本部分或本指导性技术文件）由浙江省电力学会提出并解释。

本文件（或本部分或本指导性技术文件）起草单位（包括第一承担单位和参加起草单位，按对标准的贡献大小排列）：

本文件（或本部分或本指导性技术文件）主要起草人（按对标准的贡献大小排列）：

本文件（或本部分或本指导性技术文件）首次发布（或本文件×年×月首次发布，×年×月第一次修订，×年×月第二次修订）。

引　　言

××（特定部分）××。

[状态]

XXXX 技术规范

1 范围

本文件规定了火电机组分散控制系统安全防护技术规范等要求。

本文件适用于浙江省火电机组分散控制系统安全防护。

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。

GB17859　　计算机信息系统安全保护等级保护划分准则

GB/T25069 信息安全技术 术语

GB/T22239 信息安全技术　网络安全等级保护基本要求

GB/T22240 信息安全技术　网络安全等级保护定级指南

GB/T36572 电力监控系统网络安全防护导则

DL/T2614　电力行业网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

分散控制系统　Distributed Control System

分散控制系统是以微处理器为基础，采用控制功能分散、显示操作集中、兼顾分而自治和综合协调的设计原则的新一代仪表控制系统。它采用控制分散、操作和管理集中的基本设计思想，采用多层分级、合作自治的结构形式。其主要特征是它的集中管理和分散控制。DCS 在电力、冶金、石化等各行各业都获得了极其广泛的应用。

3.2

网络安全　cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于 稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源： GB/T 22239—2019,3.1]

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。

[来源： GB/T36572—2018,3.3]

3.4

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。

[来源：GB/T36572—2018,3.6]

3.5

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。

[来源： GB/T36572-2018,3.4]

3.6

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。

[来源： GB/T36572—2018,3.5]

3.7

横向单向安全隔离装置　horizontal one-way security isolation device

在不同安全区间禁止通用网络通信装置，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。

[来源： DL/T 2614,3.9]

3.8

纵向加密认证装置　vertical encryption authentication device

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装置。

[来源： DL/T 2614,3.10]

3.9

安全域　security　domain

由一组具有相同安全保护需求并相互信任的系统组成并共享安全保护策略的逻辑区域。

[来源： DL/T 2614,3.11]

3.10

基本要求　Baseline

[状态]

相应等级系统所应满足的对应级别的最基本安全防护要求。

3.11

增强要求 enhanced requirements

因技术或条件限制，可能需要长期逐步改进的安全防护要求。

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

DCS：分散控制系统（Distributed Control System）

FTP：文件传输协议（File Transfer Protocol）

IP：互联网协议（Internet Protocol）

IT：信息技术（Information Technology）

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

USB：通用串行总线（Universal Serial Bus）

5 安全防护技术规范

5.1 第二级防护要求

5.1.1 安全物理环境

5.1.1.1 物理位置选择

基本要求

a) 机房场地应选择在具有防震能力的建筑内，建筑物的防震等级应满足该建筑建设时所明确的抗震设计要求。

b) 机房场地应具备防风和防雨能力，机房应尽量不设置窗户，有窗户的则应采用双层密封玻璃并保证窗户的密封性，机房的墙体门窗等应及时进行检查加固，确保不存在破损开裂情况。

c) 机房场地应尽量避免设在建筑物的顶层或地下室，同时应避开用水设备或设施，如避免机房顶部或墙体有水管经过。确因条件限制，无法选择最佳位置的机房，应加强防水和防潮措施：位于顶层的机房，机房顶层应进行有效的防水保护，如粉刷防水涂料等；位于地下室的机房，则应设置防水淹措施，如在通往机房的过道上设置防水淹闸门，同时配备湿度调节设施用于防潮。

5.1.1.2 物理访问控制

基本要求

a) 机房出入口应安排专人值守，用于控制、鉴别和记录进入的人员，如登记进入机房的人员、进出时间以及相关事由等。

5.1.1.3 防盗窃和防破坏

基本要求

a) 应将设备或主要部件通过螺丝等方式固定在机架或机柜中，所有设备应设置明显的不易除去的标识，如镶嵌金属铭牌或粘贴纸质标签等。

b) 应将通信线缆铺设在隐蔽安全处，如铺设在桥架或防静电地板下的固定线槽中。

5.1.1.4 防雷击

基本要求

a) 机房应设置接地系统，并将各类机柜、设施和设备等通过接地线连接接地系统进行安全接地。

5.1.1.5 防火

基本要求

a) 机房应设置火灾自动消防系统，配备烟感、温感等火情自动检测和自动报警装置，并通过联动灭火装置实现自动灭火。

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料，应选择不低于B1级别的材料。

5.1.1.6 防水和防潮

基本要求

a) 应采取窗户密封、刷防水涂层等措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b) 应通过配备精密空调、除湿设备或墙面粉刷特殊涂料等措施防止机房内水蒸气结露，通过在空调下方设置地漏或防水坝等措施防止地下积水的转移与渗透。

5.1.1.7 防静电

基本要求

a) 应采用防静电地板或地面（如防静电地板胶），并采用必要的接地防静电措施，如机柜、设施和设备防静电接地。

5.1.1.8 温湿度控制

基本要求

a) 应设置精密空调（或机房专用空调+湿度控制设备）自动调节温度和湿度，使机房温湿度的变化在设备运行所允许的范围之内，夏季温度应保持在22℃-26℃，冬季温度应保持在18℃-22℃，湿度应保持在35%-65%。

5.1.1.9 电力供应

基本要求

a) 应在机房供电线路上配置稳压器和过电压防护设备，如UPS；

b) 应提供短期的备用电力供应，如配备UPS、发电机等设备，至少满足设备在断电情况下的正常运行要求。

5.1.1.10 电磁防护

基本要求

[状态]

a) 机房内的电源线和通信线缆应隔离铺设，如通信线缆按桥架铺设，电源线铺设在防静电地板下管道中，强电弱电铺设在不同的管道中等，避免互相干扰。

5.1.1.11 室外控制设备物理防护

基本要求

a) 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、防雨和防火能力等；

b) 室外控制设备放置应远离强电磁干扰、强热源等环境，也应尽量避免放置在雷电、风沙频发的环境中，如无法避免应及时做好应急处置及检修，保证设备正常运行。

5.1.1.12 硬接线防护

增强要求

a) 当DCS及配套设施采用硬接线方式进行采集控制时，宜采用带螺丝固定的DB9、DB15接口、航空插头等经加固的连接端子或工业连接器进行连接，确保数据传输的稳定性和可靠性，避免因接触不良问题导致业务异常；同时宜采用带有电磁屏蔽功能的线束，避免因电磁干扰导致业务异常；

b) 当DCS及配套设施接线柜存在室外暴露时，应充分考虑防尘和防水，采用具备防尘防水功能的机柜；同时还应考虑防盗窃和防破坏，采用带锁的机柜，并在相关区域配备闭路电视监控设施；

c) 当DCS及配套设施采用硬接线方式进行数据采集时，宜采用具备信令控制功能的RTU网关设备与DCS进行交互，实施必要的访问控制，并禁止对DCS及配套设施进行写入操作。

5.1.1 安全通信网络

5.1.1.1 网络架构

基本要求

a) DCS应部署在生产控制大区的控制区（安全区I）内，生产控制大区的控制区（安全区I）与非控制区（安全区II）之间应采用防火墙等具有访问控制功能的设施实现逻辑隔离；生产控制大区与管理信息大区之间应部署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，并禁止E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越生产控制大区和管理信息大区边界。

b) 应避免将DCS网络区域部署在边界处，DCS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。

c) DCS应按照系统安全保护等级将其部署在相应安全保护等级的安全域内，不同安全保护等级的DCS应部署在不同的安全域。

d) DCS网络不应与公共网络连接，不应存在互联网出口链路。

5.1.1.2 通信传输

基本要求

a) 应采用校验技术或密码技术保证通信过程中数据的完整性，采用密码技术的应按照国家密码管理部门与行业有关要求使用密码算法。主要涉及鉴别数据、重要业务数据、重要审计数据和重要配置数据等。

5.1.1.3 可信验证

增强要求

a) 可基于可信根对DCS通信设备的系统引导程序、系统程序、重要配置参数和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并将验证结果形成审计记录送至安全管理中心。

5.1.2 安全区域边界

5.1.2.1 边界防护

基本要求

a) 应保证跨越DCS网络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。

5.1.2.2 访问控制

基本要求

a) 应在DCS网络边界及区域之间设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b) 应删除多余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；

c) 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；

d) 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；

5.1.2.3 入侵防范

基本要求

a) 应能够在DCS关键网络节点处监视网络攻击行为。

5.1.2.4 恶意代码防范

基本要求

a) 应能在DCS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，应以离线方式及时更新，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。

5.1.2.5 安全审计

基本要求

a) 应部署专用审计系统，或启用设备或系统审计功能，对DCS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，审计记录的留存时间应符合法律法规要求（6个月以上）。

5.1.2.6 拨号使用控制

基本要求

[状态]

a) DCS应禁止使用拨号访问服务。

5.1.2.7 无线使用控制

基本要求

a) DCS应禁止使用无线通信，并禁止选用具有无线通信功能的设备。

5.1.2.8 可信验证

增强要求

a) 可基于可信根对DCS边界设备的系统引导程序、系统程序、重要配置参数和边界防护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，并将验证结果形成审计记录送至安全管理中心。

5.1.3 安全计算环境

5.1.3.1 身份鉴别

基本要求

a) 应对登录DCS相关设备、软件的用户进行身份标识和鉴别，身份标识应具有唯一性，禁止多人共用同一个账号，身份鉴别信息应具有复杂度限制，口令长度应不小于8位，且为字母、数字和特殊字符混合组合，口令应实现定期更换，更换频率应不大于90天，账户和口令应不相同，禁止明文存储口令；

b) DCS相关的设备、软件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措施；其中非法登录次数的限制应不大于10次，登录连接超时时间不高于20分钟。该安全设置应基于不对安全生产产生不利影响的前提下进行，如可能产生不利影响的，可采取其他替代措施进行一定的风险控制，如人员7*24小时值守，实时监控等。

c) DCS相关的设备、软件进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；如采用安全的RDP协议、SSH协议、HTTPS协议等，禁止使用telnet等明文传输协议。

5.1.3.2 访问控制

基本要求

a) 应对登录的用户分配账户和权限；账号的分配和权限设置应满足实际业务需要并符合安全要求，不允许存在所有账号都是最高权限的情况。

b) 应重命名或删除默认账户，修改默认账户的默认口令；此处默认账户的定义应当是广义的，对于常见的admin、root、test、manager等也可以视作为默认账号，这些常见账户应当进行删除或重命名，无法删除或重命名的默认账户，则应重点设置强口令进行保护。

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；可通过定期排查或定期巡检等方式，及时发现并清除多余、过期账户，并杜绝账户共享行为。

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，且特权用户管理员无权对审计记录进行操作；

5.1.3.3 安全审计

基本要求

a) 应启用安全审计功能或利用生产控制大区专用安全审计系统进行安全审计，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，至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作(如用户登录、退出)等；

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，审计记录的留存时间应符合法律法规要求（6个月以上）；宜通过日志审计系统的方式进行日志备份。

5.1.3.4 入侵防范

基本要求

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；最小安装以实际业务需要为依据，不允许安装明显影响系统安全的软件，如远程控制软件等。

b) 应关闭不需要的系统服务和安全风险高的通用网络服务功能（如网络打印服务、网络存储服务、FTP等）；如需使用SNMP服务，应采用安全性增强版本，应设定复杂的 Community控制字段，禁止使用 Public 、Private 等默认字段。

c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；可通过设备本身策略或者网络层设备实现，限制地址一般为固定IP或者少量地址段。

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。如无法实现该功能，可通过增强DCS网络管控措施降低该类漏洞被利用的可能性，从而降低该问题所带来的风险。

e) 应通过相关测试工具发现可能存在的已知漏洞，对于无法开展测试的系统，可通过版本比对的方式发现相关漏洞。发现的漏洞应结合DCS整体网络环境、现有防护措施等多方面因素综合评估漏洞风险，经评估后明确漏洞风险是否可接受，对风险不可接受的漏洞应及时进行修补，修补前应经过安全性、兼容性和稳定性等方面充分测试评估后再执行修补动作，同时保留相应记录。

5.1.3.5 恶意代码防范

基本要求

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。防恶意代码软件版本和恶意代码库更新前应进行安全性和兼容性测试。对于DCS等涉及实时控制的系统，推荐使用白名单管理软件进行恶意代码防范。

5.1.3.6 可信验证

增强要求

a) 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和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，并将验证结果形成审计记录送至安全管理中心。

5.1.3.7 数据完整性

[状态]

基本要求

a) 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，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据等；其中，鉴别数据传输完整性保护主要涉及设备远程登录和系统远程访问等相关场景。重要业务数据传输完整性保护主要涉及应用系统访问及数据跨边界传输等相关场景。重要审计数据传输完整性保护主要涉及审计数据通过网络进行收集保存等相关场景。重要配置数据传输完整性保护主要涉及配置数据通过网络进行备份等相关场景。

5.1.3.8 数据备份恢复

基本要求

a) 应提供重要数据的本地数据备份与恢复功能，备份数据能够完全恢复至备份执行时状态，数据保存期限应符合国家相关规定，备份频率及备份方式应结合实际业务情况，确保数据丢失时能够及时恢复。

b) 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。对于管控较为严格的DCS网络，如无法直接利用通信网络传输重要数据的，可通过人工或其他等效方式将重要数据定时备份至备用场地。

5.1.3.9 剩余信息保护

基本要求

a) 应保证操作系统、数据库管理系统、应用系统、中间件、系统管理软件等的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。如登录界面不应保留前一次登录的用户名信息，不应记住历史登录的账号密码、账户注销退出后应不能访问登录后才能访问的页面、登录过程中产生的缓存文件应在账户注销退出后及时清除等等。

5.1.3.10 个人信息保护

基本要求

a) 应仅采集和保存业务必需的用户个人信息，对于不涉及个人信息采集和保存的系统，此项可不适用。

b) 应禁止未授权访问和非法使用用户个人信息，对于不涉及个人信息访问和使用的系统，此项可不适用。

5.1.3.11 控制设备安全

基本要求

a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制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) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

c) 应关闭或拆除主机的光盘驱动、软盘驱动、USB 接口、串行口、无线、蓝牙或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理。

5.1.4 安全管理中心

5.1.4.1 系统管理

基本要求

a) 应通过提供集中系统管理功能的系统（如堡垒机、集中管控终端等）对系统管理员进行身份鉴别，只允许系统管理员通过提供集中系统管理功能的系统对网络设备、安全设备、服务器、数据库等进行系统管理操作，并对这些操作进行审计。

b) 应通过系统管理员（该系统管理员权限不得与审计管理员和安全管理员的权限重叠）使用提供集中系统管理功能的系统，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；

c) 应定期及在配置发生变动前、后分别对设备的系统管理相关配置文件进行备份。其中定期备份的频率不得低于每季度一次。

5.1.4.2 审计管理

基本要求

a) 应通过综合日志审计系统对审计管理员进行身份鉴别，只允许审计管理员通过综合日志审计系统对被集中管理的日志进行审计管理操作，并对这些操作进行审计；

b) 应通过综合日志审计系统的审计管理员对被集中管理的日志进行分析，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；

c) 应严格限制审计数据的访问控制权限，实现审计用户与其他用户的权限分离；审计记录的访问控制权限应由审计管理员掌握,且审计管理员权限不得与系统管理员和安全管理员的权限重叠；

d) 应定期及在配置发生变动前、后分别对设备的审计管理相关配置文件进行备份。其中定期备份的频率不得低于每季度一次。

5.1.5 技术安全管理

5.1.5.1 安全管理层面

a) DCS应满足DL/T 2614-2023《电力行业网络安全等级保护基本要求》中的总体管理要求；

b) DCS应满足DL/T 2614-2023《电力行业网络安全等级保护基本要求》中第二级电力监控系统安全保护要求中的相关管理要求。

5.2 第三级防护要求

5.2.1 安全物理环境

5.2.1.1 物理位置选择

基本要求

a) 机房场地应选择在具有防震能力的建筑内，建筑物的防震等级应满足该建筑建设时所明确的抗震设计要求。

b) 机房场地应具备防风和防雨能力，机房应尽量不设置窗户，有窗户的则应采用双层密封玻璃并保证窗户的密封性，机房的墙体门窗等应及时进行检查加固，确保不存在破损开裂情况。

[状态]

c） 机房场地应尽量避免设在建筑物的顶层或地下室，同时应避开用水设备或设施，如避免机房顶部或墙体有水管经过。确因条件限制，无法选择最佳位置的机房，应加强防水和防潮措施：位于顶层的机房，机房顶层应进行有效的防水保护，如粉刷防水涂料等；位于地下室的机房，则应设置防水淹措施，如在通往机房的过道上设置防水淹闸门，同时配备湿度调节设施用于防潮。

5.2.1.2 物理访问控制

基本要求

a） 机房出入口应配置指纹、人脸、门禁卡等方式的电子门禁系统，用于控制、鉴别和记录进入的人员，电子门禁系统应具备完备的门禁日志记录功能，门禁日志记录信息应至少包括进出人员的身份、进出时间等。

5.2.1.3 防盗窃和防破坏

基本要求

a） 应将设备或主要部件通过螺丝等方式固定在机架或机柜中，所有设备应设置明显的不易除去的标识，如镶嵌金属铭牌或粘贴纸质标签等。

b） 应将通信线缆铺设在隐蔽安全处，如铺设在桥架或防静电地板下的固定线槽中。

c） 应设置红外、门磁、声光或电子围栏等类型的机房防盗报警系统，确保能够及时发现机房被非法闯入的行为；无法设置机房防盗报警系统的，应设置专人7*24小时值守的视频监控系统，视频监控应不存在监控死角，同时视频监控记录留存应大于三个月。

5.2.1.4 防雷击

基本要求

a） 机房应设置接地系统，并将各类机柜、设施和设备等通过接地线连接接地系统进行安全接地。

b） 应采取措施防止感应雷，例如设置防雷保安器（防浪涌保护器）或过压保护装置（电器保护器）等。

5.2.1.5 防火

基本要求

a） 机房应设置火灾自动消防系统，配备烟感、温感等火情自动检测和自动报警装置，并通过联动灭火装置实现自动灭火。

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料，应选择不低于B1级别的材料。

c） 应对机房划分区域进行管理，如划分设备区、UPS区、操作间等，区域和区域之间设置隔离防火措施，如设置防火玻璃、墙体等。

5.2.1.6 防水和防潮

基本要求

a） 应采取窗户密封、刷防水涂层等措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b） 应通过配备精密空调、除湿设备或墙面粉刷特殊涂料等措施防止机房内水蒸气结露，通过在空调下方设置地漏或防水坝等措施防止地下积水的转移与渗透。

c) 应安装漏水检测绳或对水敏感的检测仪表或元件，并通过配套的环境控制系统对机房进行防水检测和报警。

5.2.1.7 防静电

基本要求

a) 应采用防静电地板或地面（如防静电地板胶），并采用必要的接地防静电措施，如机柜、设施和设备防静电接地。

b) 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、防静电服、防静电手套等。

5.2.1.8 温湿度控制

基本要求

a) 应设置精密空调（或机房专用空调+湿度控制设备）自动调节温度和湿度，使机房温湿度的变化在设备运行所允许的范围之内，夏季温度应保持在22℃-26℃，冬季温度应保持在18℃-22℃，湿度应保持在35%-65%。

5.2.1.9 电力供应

基本要求

a) 应在机房供电线路上配置稳压器和过电压防护设备，如UPS；

b) 应提供短期的备用电力供应，如配备UPS、发电机等设备，至少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，输入电源应采用双路自动切换供电方式，如设备配置了双电源，并分别接入到不同的供电线路中。

5.2.1.10 电磁防护

基本要求

a) 机房内的电源线和通信线缆应隔离铺设，如通信线缆按桥架铺设，电源线铺设在防静电地板下管道中，强电弱电铺设在不同的管道中等，避免互相干扰。

增强要求

a) 应对关键设备实施电磁屏蔽，如使用电磁屏蔽机柜、建设屏蔽机房、机房墙体喷涂电磁屏蔽涂料等。

5.2.1.11 室外控制设备物理防护

基本要求

a) 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、防雨和防火能力等；

b) 室外控制设备放置应远离强电磁干扰、强热源等环境，也应尽量避免放置在雷电、风沙频发的环境中，如无法避免应及时做好应急处置及检修，保证设备正常运行。

5.2.1.12 硬接线防护

[状态]

增强要求

d) 当DCS及配套设施采用硬接线方式进行采集控制时，宜采用带螺丝固定的DB9、DB15接口、航空插头等经加固的连接端子或工业连接器进行连接，确保数据传输的稳定性和可靠性，避免因接触不良问题导致业务异常；同时宜采用带有电磁屏蔽功能的线束，避免因电磁干扰导致业务异常；

e) 当DCS及配套设施接线柜存在室外暴露时，应充分考虑防尘和防水，采用具备防尘防水功能的机柜；同时还应考虑防盗窃和防破坏，采用带锁的机柜，并在相关区域配备闭路电视监控设施；

f) 当DCS及配套设施采用硬接线方式进行数据采集时，宜采用具备信令控制功能的RTU网关设备与DCS进行交互，实施必要的访问控制，并禁止对DCS及配套设施进行写入操作。

5.2.2 安全通信网络

5.2.2.1 网络架构

基本要求

a) DCS应使用独立的网络设备和传输介质组网，保证网络设备的资源（如CPU、内存和背板带宽等）满足DCS高峰期需要，同时保证网络各个部分的带宽资源满足高峰期需要；

b) DCS应部署在生产控制大区的控制区（安全区I）内，生产控制大区的控制区（安全区I）与非控制区（安全区II）之间应采用防火墙等具有访问控制功能的设施实现逻辑隔离；生产控制大区与管理信息大区之间应部署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，并禁止E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越生产控制大区和管理信息大区边界。

c) 应避免将DCS网络区域部署在边界处，DCS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。

d) DCS应按照系统安全保护等级将其部署在相应安全保护等级的安全域内，不同安全保护等级的DCS应部署在不同的安全域。

e) DCS网络不应与公共网络连接，不应存在互联网出口链路。

f) 应提供DCS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。

5.2.2.2 通信传输

基本要求

a) 应采用校验技术或密码技术保证通信过程中数据的完整性，采用密码技术的应按照国家密码管理部门与行业有关要求使用密码算法；主要涉及鉴别数据、重要业务数据、重要审计数据和重要配置数据等。

b) 应采用密码技术保证通信过程中数据的保密性，并按照国家密码管理部门与行业有关要求使用密码算法。主要涉及鉴别数据和重要业务数据等。

5.2.2.3 可信验证

增强要求

a) 可基于可信根对DCS通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

5.2.3 安全区域边界

5.2.3.1 边界防护

基本要求

a) 应保证跨越DCS网络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。

a) 应采用网络准入、终端控制、身份认证或可信计算等技术措施，对非授权设备私自联到DCS网络的行为进行检查或限制；

b) 应采用网络准入、终端控制、身份认证或可信计算等技术措施，对DCS网络中的资产非授权联到外部网络的行为进行检查或限制。

5.2.3.2 访问控制

基本要求

a) 应在DCS网络边界及区域之间设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b) 应删除多余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；

c) 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；

d) 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；

e) 应对进出DCS网络的数据流实现基于应用协议和应用内容的访问控制；

5.2.3.3 入侵防范

基本要求

a) 应能够在DCS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；

b) 应能够在DCS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；

c) 应采取技术措施对DCS网络边界处及内部网络中的网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

d) 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

5.2.3.4 恶意代码防范

基本要求

a) 应能在DCS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，应以离线方式及时更新，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。

b) 应在DCS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，应以离线方式及时更新，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。

5.2.3.5 安全审计

[状态]

基本要求

a) 应部署专用审计系统，或启用设备或系统审计功能，对DCS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，审计记录的留存时间应符合法律法规要求（6个月以上）。

5.2.3.6 拨号使用控制

基本要求

a) DCS应禁止使用拨号访问服务。

5.2.3.7 无线使用控制

基本要求

a) DCS应禁止使用无线通信，并禁止选用具有无线通信功能的设备。

5.2.3.8 可信验证

增强要求

a) 可基于可信根对DCS边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

5.2.4 安全计算环境

5.2.4.1 身份鉴别

基本要求

a) 应对登录DCS相关设备、软件的用户进行身份标识和鉴别，身份标识应具有唯一性，禁止多人共用同一个账号，身份鉴别信息应具有复杂度限制，口令长度应不小于8位，且为字母、数字和特殊字符混合组合，口令应实现定期更换，更换频率应不大于90天，账户和口令应不相同，禁止明文存储口令；

b) DCS相关的设备、软件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措施；其中非法登录次数的限制应不大于10次，登录连接超时时间不高于20分钟。该安全设置应基于不对安全生产产生不利影响的前提下进行，如可能产生不利影响的，可采取其他替代措施进行一定的风险控制，如人员7*24小时值守，实时监控等。

c) DCS相关的设备、软件进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；如采用安全的RDP协议、SSH协议、HTTPS协议等，禁止使用telnet等明文传输协议。

d) 应采用用户名口令、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，且其中一种鉴别技术至少应使用密码技术来实现。若条件允许，可结合指纹识别、动态令牌技术以增强身份鉴别的安全性。若集成存在困难，可采取同一种鉴别技术多次复用（每次鉴别信息不相同）的方式进行身份鉴别,例如登录时要进行两次口令认证，且两次的口令不相同，再结合登录地址限制、绑定管理终端等其他技术手段，以达到同等防护效果或降低风险。

5.2.4.2 访问控制

基本要求

a) 应对登录的用户分配账户和权限；账号的分配和权限设置应满足实际业务需要并符合安全要求，不允许存在所有账号都是最高权限的情况。

b) 应重命名或删除默认账户，修改默认账户的默认口令；此处默认账户的定义应当是广义的，对于常见的admin、root、test、manager等也可以视作为默认账号，这些常见账户应当进行删除或重命名，无法删除或重命名的默认账户，则应重点设置强口令进行保护。

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；可通过定期排查或定期巡检等方式，及时发现并清除多余、过期账户，并杜绝账户共享行为。

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，且特权用户管理员无权对审计记录进行操作；

e) 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；

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；如果访问控制粒度只能达到用户组级别的，应做到每个组内只设置一个用户，以此保证访问控制权限的粒度可以细分到每个用户。

增强要求

a) 应对重要主体和客体设置安全标记，主机不支持敏感标记的，应在系统级生成敏感标记，使系统整体支持强制访问控制机制，并控制主体对有安全标记信息资源的访问。

5.2.4.3 安全审计

基本要求

a) 应启用安全审计功能或利用生产控制大区专用安全审计系统进行安全审计，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，至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作(如用户登录、退出)等；

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，审计记录的留存时间应符合法律法规要求（6个月以上）；宜通过日志审计系统的方式进行日志备份。

d) 应对审计进程进行保护，防止未经授权的中断，如通过权限控制保护审计进程无法被非授权关闭，或通过部署进程监控软件方式进行进程监控保护。

5.2.4.4 入侵防范

基本要求

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；最小安装以实际业务需要为依据，不允许安装明显影响系统安全的软件，如远程控制软件等。

[状态]

b) 应关闭不需要的系统服务和安全风险高的通用网络服务功能（如网络打印服务、网络存储服务、FTP等）；如需使用SNMP服务，应采用安全性增强版本，应设定复杂的 Community控制字段，禁止使用 Public 、Private 等默认字段。

c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；可通过设备本身策略或者网络层设备实现，限制地址一般为固定IP或者少量地址段。

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。如无法实现该功能，可通过增强DCS网络管控措施降低该类漏洞被利用的可能性，从而降低该问题所带来的风险。

e) 应通过相关测试工具发现可能存在的已知漏洞，对于无法开展测试的系统，可通过版本比对的方式发现相关漏洞。发现的漏洞应结合DCS整体网络环境、现有防护措施等多方面因素综合评估漏洞风险，经评估后明确漏洞风险是否可接受，对风险不可接受的漏洞应及时进行修补，修补前应经过安全性、兼容性和稳定性等方面充分测试评估后再执行修补动作，同时保留相应记录。

f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。如在关键的服务器节点上安装主机HIDS防范入侵行为。

5.2.4.5 恶意代码防范

基本要求

a) 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，并将其有效阻断。对于DCS等涉及实时控制的系统，推荐使用白名单管理软件进行恶意代码防范。

5.2.4.6 可信验证

增强要求

a) 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环长进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

5.2.4.7 数据完整性

基本要求

a) 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，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据等。其中，鉴别数据传输完整性保护主要涉及设备远程登录和系统远程访问等相关场景。重要业务数据传输完整性保护主要涉及应用系统访问及数据跨边界传输等相关场景。重要审计数据传输完整性保护主要涉及审计数据通过网络进行收集保存等相关场景。重要配置数据传输完整性保护主要涉及配置数据通过网络进行备份等相关场景。

增强要求

a) 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，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据等。

5.2.4.8 数据保密性

基本要求

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据等；其中，鉴别数据传输保密性保护主要涉及设备远程登录和系统远程访问等相关场景。重要业务数据传输保密性保护主要涉及应用系统访问及数据跨边界传输等相关场景。如无法实现DCS业务数据传输保密性要求的，可通过增强DCS网络管控措施降低数据被窃取可能性，并结合DCS业务数据保密性要求低的特性，降低该问题所带来的风险。

b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据等。如用户口令等鉴别信息应采用SM3等算法加密后保存，重要业务数据应采用SM4等算法加密后保存。如无法实现DCS业务数据存储保密性要求的，可通过增强DCS网络管控措施降低数据被窃取可能性，并结合DCS业务数据保密性要求低的特性，降低该问题所带来的风险。

5.2.4.9 数据备份恢复

基本要求

a) 应提供重要数据的本地数据备份与恢复功能，备份数据能够完全恢复至备份执行时状态，数据保存期限应符合国家相关规定，备份频率及备份方式应结合实际业务情况，确保数据丢失时能够及时恢复。

b) 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。对于管控较为严格的DCS网络，如无法直接利用通信网络传输重要数据的，可通过人工或其他等效方式将重要数据定时备份至备用场地。

c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

增强要求

a) 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。

5.2.4.10 剩余信息保护

基本要求

a) 应保证操作系统、数据库管理系统、应用系统、中间件、系统管理软件等的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。如登录界面不应保留前一次登录的用户名信息，不应记住历史登录的账号密码、账户注销退出后应不能访问登录后才能访问的页面、登录过程中产生的缓存文件应在账户注销退出后及时清除等等。

b) 应保证存有操作系统、数据库系统和应用系统用户敏感数据的存储空间被释放或重新分配前得到完全清除。如存储有敏感数据的存储空间另做他用时，应通过多次覆盖写入或其他有效方式，将敏感数据彻底清除，确保数据无法恢复后再进行存储资源的再分配或物理损毁。

5.2.4.11 个人信息保护

基本要求

a) 应仅采集和保存业务必需的用户个人信息，对于不涉及个人信息采集和保存的系统，此项可不适用。

b) 应禁止未授权访问和非法使用用户个人信息，对于不涉及个人信息访问和使用的系统，此项可不适用。

5.2.4.12 控制设备安全

[状态]

基本要求

a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制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) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

c) 应使用专用设备和专用软件对控制设备进行更新；

d) 应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序；

e) 应关闭或拆除主机的光盘驱动、软盘驱动、USB 接口、串行口、无线、蓝牙或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理。

5.2.5 安全管理中心

5.2.5.1 系统管理

基本要求

a) 应通过提供集中系统管理功能的系统（如堡垒机、集中管控终端等）对系统管理员进行身份鉴别，只允许系统管理员通过提供集中系统管理功能的系统对网络设备、安全设备、服务器、数据库等进行系统管理操作，并对这些操作进行审计。

b) 应通过系统管理员（该系统管理员权限不得与审计管理员和安全管理员的权限重叠）使用提供集中系统管理功能的系统，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；

c) 应定期及在配置发生变动前、后分别对设备的系统管理相关配置文件进行备份。其中定期备份的频率不得低于每季度一次。

5.2.5.2 审计管理

基本要求

a) 应通过综合日志审计系统对审计管理员进行身份鉴别，只允许审计管理员通过综合日志审计系统对被集中管理的日志进行审计管理操作，并对这些操作进行审计；

b) 应通过综合日志审计系统的审计管理员对被集中管理的日志进行分析，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；

c) 应严格限制审计数据的访问控制权限，实现审计用户与其他用户的权限分离；审计记录的访问控制权限应由审计管理员掌握,且审计管理员权限不得与系统管理员和安全管理员的权限重叠；

d) 应定期及在配置发生变动前、后分别对设备的审计管理相关配置文件进行备份。其中定期备份的频率不得低于每季度一次。

5.2.5.3 安全管理

基本要求

a) 应通过提供集中安全管理功能的系统（如堡垒机、集中管控终端等）对安全管理员进行身份鉴别，只允许安全管理员通过提供集中安全管理功能的系统对网络设备、安全设备、服务器、数据库等进行安全管理操作，并对这些操作进行审计。

b) 应通过安全管理员（该安全管理员权限不得与审计管理员和系统管理员的权限重叠）使用提供集中安全管理功能的系统，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；

c) 应定期及在配置发生变动前、后分别对设备的安全管理相关配置文件进行备份。其中定期备份的频率不得低于每季度一次。

5.2.5.4 集中管控

基本要求

a) 应划分出单独的网络区域，或单独的网段，或独立的带外管理网络，对分布在网络中的安全设备或安全组件进行管控；

b) 应能够建立一条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；如通过SSH、HTTPS等安全方式进行管理

c) 应通过部署网管软件等方式对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测，并应根据业务实际情况设定告警阀值，同时还应具备超过阈值后的告警功能，如弹窗告警或声光告警等。

d) 应对分散在各个设备上的网络运行日志、操作系统运行日志、数据库日志、业务运行日志、安全设施运行日志等通过综合日志审计系统进行收集汇总、集中分析，并保证审计记录的留存时间符合法律法规要求（6个月以上）；

e) 应能对网络中发生的各类安全事件进行识别、报警和分析。如在关键网络节点部署态势感知类设备，对各类安全事件进行识别和分析，并具备弹窗告警或声光告警功能。

增强要求

a) 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。

5.2.6 技术安全管理

5.2.6.1 安全管理层面

a) DCS应满足DL/T 2614-2023《电力行业网络安全等级保护基本要求》中的总体管理要求；

b) DCS应满足DL/T 2614-2023《电力行业网络安全等级保护基本要求》中第三级电力监控系统安全保护要求中的相关管理要求。

5.3 附加要求

a) DCS应满足《电力监控系统安全防护规定》中与DCS相关的要求；

b) 必要情况下，DCS应满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》；

c) 被认定为关键信息基础设施的DCS还应同时满足关键信息基础安全防护相关要求。

[状态]

附 录 A
（资料性）
DCS 防护重点参考

A.1 防护重点参考

火电机组 DCS 是通过控制单元实现对火电设备的远程控制和监测，通过传感器采集火电设备的运行数据，如温度、压力、流量等，然后根据采集的数据进行逻辑运算，实现对设备的自动控制。同时操作人员可通过 DCS 的人机交互应用界面进行火电设备的监测和控制。

根据 DCS 业务功能及数据流转过程，在对 DCS 进行安全防护时，应覆盖 DCS 业务流程中涉及到的所有对象，包括物理环境、网络架构、网络设备、安全设备、终端、服务器、数据库、DCS 软件、控制设备等。

根据目前火电机组的主流情况，DCS 通常需要将监测数据通过接口机传输至 SIS；还需要将监测数据通过硬接线方式传输至 NCS，同时要接收 AVC 和 AGC 的指令进行电压和功率的调整等。因此在安全防护时，需要重点关注上述两个边界的安全防护。

附 录 B
（资料性）
DCS 所在网络区域与其他网络区域间的安全隔离参考

B.1 链式拓扑结构安全隔离

链式结构中的控制区具有较高的累积安全强度，但总体层次较多，见图 A.1。

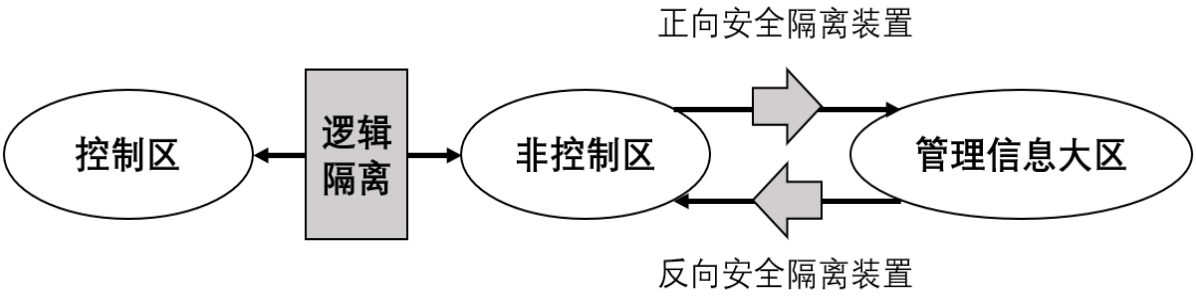

图 A.1 链式拓扑结构安全隔离示意图

B.2 三角拓扑结构安全隔离

三角结构各区可以直接相连，效率较高，但所用隔离设备较多，见图 A.2。

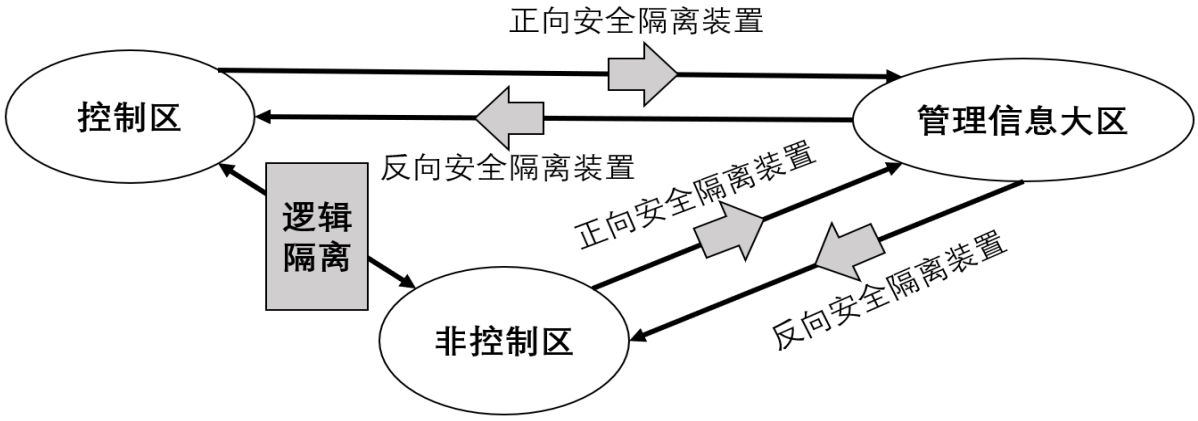

图 A.2 三角拓扑结构安全隔离示意图

B.3 星型拓扑结构安全隔离

星形结构所用设备较少、易于实施，但中心点故障影响范围大，见图 A.3。

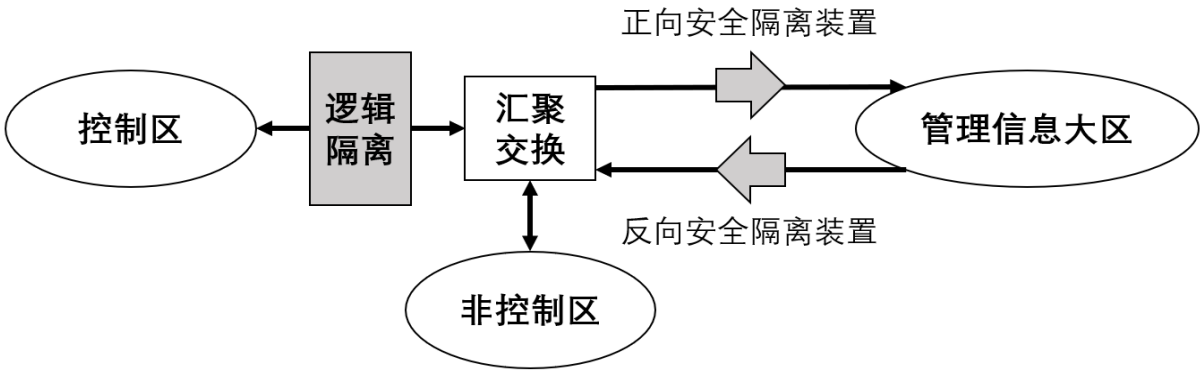

图 A.3 星型拓扑结构安全隔离示意图

[状态]

参 考 文 献

[1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[2] DL/T 2614-2023 电力行业网络安全等级保护基本要求

[3]《电力监控系统安全防护规定》(国家发展和改革委员会令 2024 年第 27 号)

[4]《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》(国能安全〔2015〕36 号)