附件 4:

发电厂监控系统安全防护方案

1 总则

1.1 为了加强发电厂电力监控系统安全防护，抵御黑客及恶意代码等对发电厂监控系统发起的恶意破坏和攻击，以及其它非法操作，防止发电厂电力监控系统瘫痪和失控，和由此导致的发电厂一次系统事故和其他事故，制定本方案。

1.2 本方案是《电力监控系统安全防护总体方案》配套的系列文件之一，其它文件包括:《省级以上调度中心监控系统安全防护方案》、《地（县）级调度中心监控系统安全防护方案》、《变电站监控系统安全防护方案》、《配电监控系统安全防护方案》和《电力监控系统安全防护评估规范》。

1.3 本方案适用于火电厂、水电厂、核电站、风电场、光伏电站、燃机电厂等各种类型发电厂。

2 基本原则

2.1 安全分区

按照《电力监控系统安全防护规定》，原则上将发电厂基于计算机及网络技术的业务系统划分为生产控制大区和管理信息大区，并根据业务系统的重要性和对一次系统的影响程度将生产控制大区划分为控制区（安全区 I）及非控制区（安全区 II），重点保护生产控制以及直接影响电力生产

(机组运行)的系统。

2.2 网络专用

电力调度数据网是与生产控制大区相连接的专用网络，承载电力实时控制、在线生产交易等业务。发电厂端的电力调度数据网应当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力企业其它数据网及外部公共信息网的安全隔离。发电厂端的电力调度数据网应当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。

2.3 横向隔离

横向隔离是电力监控系统安全防护体系的横向防线。应当采用不同强度的安全设备隔离各安全区，在生产控制大区与管理信息大区之间必须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，隔离强度应当接近或达到物理隔离。生产控制大区内部的安全区之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的设施，实现逻辑隔离。防火墙的功能、性能、电磁兼容性必须经过国家相关部门的认证和测试。

2.4 纵向认证

纵向加密认证是电力监控系统安全防护体系的纵向防线。发电厂生产控制大区与调度数据网的纵向连接处应当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，实现双向身份认证、数据加密和访问控制。

2.5 综合防护

综合防护是结合国家信息安全等级保护工作的相关要求对电力监控系统从主机、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防护的过程。

3 安全区的划分

3.1 控制区（安全区Ⅰ）

火电厂和水电厂的控制区主要包括以下业务系统和功能模块：火电机组分散控制系统（DCS）、火电机组辅机控制系统、自动发电控制系统（AGC）、自动电压控制系统（AVC）、火电厂厂级信息监控系统的监控功能、水电厂集中监控系统、梯级调度监控系统、网控系统、相量测量装置（PMU）、继电保护、各种控制装置(调速系统、励磁系统、快关汽门装置等)、五防系统等。

核电站的控制区主要包括以下业务系统和功能模块：核电站厂级分散控制系统（DCS）、自动电压控制系统（AVC）、厂级信息监控系统的监控功能、网控系统、继电保护、辅机控制系统、相量测量装置（PMU）和自动控制装置（安控、电力系统稳定器等），其中辅机控制系统包括三废处理系统、循环水处理系统、凝结水精处理系统和除盐水系统等。

风电场的控制区主要包括以下业务系统和功能模块：风电场监控系统、无功电压控制、发电功率控制、升压站监控

系统、继电保护和相量测量装置（PMU）等。

光伏电站的控制区主要包括以下业务系统和功能模块：光伏电站运行监控系统、无功电压控制、发电功率控制、升压站监控系统、继电保护等。

燃机电厂的控制区主要包括以下业务系统和功能模块：燃机电厂厂级分散控制系统（DCS）、燃气轮机控制系统（TCS）、厂级信息监控系统的监控功能、自动发电控制系统（AGC）、自动电压控制系统（AVC）、相量测量装置（PMU）、火警探测系统、升压站监控系统、继电保护等。

对于没有分散控制系统（DCS）的小型发电厂的监控系统，其生产控制大区可以不再细分，可将各业务系统和装置均置于控制区，其中在控制区中的故障录波装置和电能量采集装置可以通过调度数据网或拨号方式与相应的调度中心通信。

3.2 非控制区（安全区Ⅱ）

火电厂和水电厂的非控制区主要包括以下业务系统和功能模块：火电厂厂级信息监控系统的优化功能、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、电能量采集装置、电力市场报价终端、故障录波信息管理终端等。

核电站的非控制区主要包括以下业务系统和功能模块：厂级信息监控系统的优化功能、电能量采集装置和故障录波

装置等。

风电场的非控制区主要包括以下业务系统和功能模块：风功率预测系统、状态监测系统、电能量采集装置和故障录波装置等。

光伏电站的非控制区主要包括以下业务系统和功能模块：光伏功率预测系统、电能量采集装置和故障录波装置等。

燃机电厂的非控制区主要包括以下业务系统和功能模块：厂级信息监控系统的优化功能、电能量采集装置和故障录波装置等。

对于将电能量采集装置置于发电厂控制区内的情况，可以只将计量通信网关置于非控制区。

3.3 管理信息大区

火电厂和水电厂的管理信息大区主要包括以下业务系统和功能模块：火电厂厂级信息监控系统的管理功能、雷电监测系统、气象信息系统、大坝自动监测系统、防汛信息系统、报价辅助决策系统、检修管理系统和管理信息系统(MIS)等。

核电站的管理信息大区主要包括以下业务系统和功能模块：厂级信息监控系统的管理功能、检修管理系统和管理信息系统（MIS）。

风电场的管理信息大区主要包括以下业务系统和功能模块：天气预报系统、检修管理系统、测风塔系统和管理信

息系统（MIS）等。

光伏电站的管理信息大区主要包括以下业务系统和功能模块：天气预报系统、检修管理系统和管理信息系统(MIS)等。

燃机电厂的管理信息大区主要包括以下业务系统和功能模块：厂级信息监控系统的管理功能和管理信息系统（MIS）等。

发电厂管理信息大区的业务主要运行在发电企业数据网或公共数据网，各发电企业可以遵照安全防护规定的原则，根据各自实际情况，自行决定其安全防护策略和措施。

此外，核电站的辐射监测系统、地震监测系统、环境监测系统、实物保护系统、应急分析与指挥系统等信息系统，与电力生产没有直接关系，不属于电力监控系统，不在本规定的防护范围内。建议核电站应尽可能将上述系统划分在管理信息大区，并按照相关主管部门的要求进行安全防护。

4 边界安全防护

4.1 横向边界防护

4.1.1 生产控制大区与管理信息大区边界安全防护

发电厂生产控制大区与管理信息大区之间通信应当部署电力专用横向单向安全隔离装置。

4.1.2 控制区（安全区Ⅰ）与非控制区（安全区Ⅱ）边界安全防护

安全区Ⅰ与安全区Ⅱ之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的设备，实现逻辑隔离、报文过滤、访问控制等功能。所选设备的功能、性能、电磁兼容性必须经过国家相关部门的认证和测试。

发电厂（DCS）系统部署在安全区Ⅰ，与运行在安全区Ⅱ的发电厂厂级监控系统（SIS）优化功能进行信息交换应当采用逻辑隔离的安全防护措施。

4.1.3 系统间安全防护

发电厂内同属于安全区Ⅰ的各机组监控系统之间、机组监控系统与控制系统之间、同一机组的不同功能的监控系统之间，尤其是机组监控系统与输变电部分控制系统之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等。

发电厂内同属于安全区Ⅱ的各系统之间、各不同位置的厂站网络之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等。

发电厂内同属于管理信息大区的各系统之间、各不同位置的厂站网络之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等。

发电厂电力市场报价终端部署在非控制区，与运行在管理信息大区的报价辅助决策系统信息交换应当采用电力专用横向单向安全隔离装置。发电企业的市场报价终端与同安全区内其它业务系统进行数据交换时，应当采取必要的安全措施，以保证敏感数据的安全。

4.2 纵向边界防护

发电厂生产控制大区系统与调度端系统通过电力调度数据网进行远程通信时，应当采用认证、加密、访问控制等技术措施实现数据的远方安全传输以及纵向边界的安全防护。发电厂的纵向连接处应当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，与调度端实现双向身份认证、数据加密和访问控制。

参与系统 AGC、AVC 调节的发电厂应当在电力调度数据网边界配置纵向加密认证装置或纵向加密认证网关进行安全防护。对于没有 DCS 系统，或不参与 AGC、AVC 调节的发电厂，其电力调度数据网边界配置的安全防护措施可以根据具体情况进行简化。

对于不具备建立调度数据网的小型发电厂可以通过拨号、无线等方式接入相应调度机构的安全接入区，其他发电厂禁止使用远程拨号方式与调度端进行数据通信。

4.3 第三方边界安全防护

如果发电厂生产控制大区中的业务系统与环保、安全等

政府部门进行数据传输，其边界防护应当采用生产控制大区与管理信息大区之间的安全防护措施。

管理信息大区与外部网络之间应采取防火墙、VPN 和租用专线等方式，保证边界与数据传输的安全。

禁止设备生产厂商或其它外部企业（单位）远程连接发电厂生产控制大区中的业务系统及设备。

5 综合安全防护

5.1 入侵检测

生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计。

5.2 主机与网络设备加固

发电厂厂级信息监控系统等关键应用系统的主服务器，以及网络边界处的通信网关机、Web 服务器等，应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专用软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当经过测试。

非控制区的网络设备与安全设备应当进行身份鉴别、访问权限控制、会话控制等安全配置加固。可以应用电力调度数字证书，在网络设备和安全设备实现支持 HTTPS 的纵向安全 Web 服务，能够对浏览器客户端访问进行身份认证及加密传输。

应当对外部存储器、打印机等外设的使用进行严格管理。

生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备；管理信息大区业务系统使用无线网络传输业务信息时，应当具备接入认证、加密等安全机制。

5.3 应用安全控制

发电厂厂级信息监控系统等业务系统应当逐步采用用户数字证书技术，对用户登录应用系统、访问系统资源等操作进行身份认证，提供登录失败处理功能，根据身份与权限进行访问控制，并且对操作行为进行安全审计。

对于发电厂内部远程访问业务系统的情况，应当进行会话控制，并采用会话认证、加密与抗抵赖等安全机制。

5.4 安全审计

生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为以及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。

可以采用安全审计功能，对网络运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全设施运行日志等进行集中收集、自动分析。

5.5 专用安全产品的管理

安全防护工作中涉及使用横向单向安全隔离装置、纵向加密认证装置、防火墙、入侵检测系统等专用安全产品的，应当按照国家有关要求做好保密工作，禁止关键技术和设备的扩散。

5.6 备用与容灾

应当定期对关键业务的数据进行备份，并实现历史归档数据的异地保存。关键主机设备、网络设备或关键部件应当进行相应的冗余配置。控制区的业务系统（应用）应当采用冗余方式。

5.7 恶意代码防范

应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应当经过测试。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。

5.8 设备选型及漏洞整改

发电厂电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞和风险的系统及设备；对于已经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统及设备的运行管理和安全防护。生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备。

附录 1　各类型电厂安全分区表

表 1 火电厂、水电厂监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	火电机组分散控制系统 DCS	DCS			A2
2	火电机组辅机控制系统	辅机 PLC/DCS			A2
3	火电厂厂级信息监控系统	监控功能	优化功能	管理功能	A2
4	调速系统和自动发电控制功能 AGC	调速、自动发电控制			A1
5	励磁系统和自动电压控制功能 AVC	励磁、自动电压控制			A1
6	水电厂监控系统	水电厂监控			A1
7	梯级调度监控系统	梯级调度监控			A1
8	网控系统	网控系统			A1
9	相量测量装置 PMU	PMU			B
10	自动控制装置	PSS、汽门快关等			B、A1
11	五防系统	五防系统			A2
12	继电保护	继电保护装置及管理终端			B
13	故障录波		故障录波装置		B
14	梯级水库调度自动化系统		梯级水库调度自动化		A1
15	水情自动测报系统		水情自动测报		A1
16	水电厂水库调度自动化系统		水电厂水库调度自动化		A1
17	电能量采集装置		电能量采集		B、A1
18	电力市场报价终端		电力市场报价		B
19	管理信息系统 MIS			MIS	A2
20	雷电监测系统			雷电监测	A2
21	气象信息系统			气象信息	A2
22	大坝自动监测系统			大坝自动监测	A2
23	防汛信息系统			防汛信息	A2
24	报价辅助决策系统			报价辅助决策	A2
25	检修管理系统			检修管理	A2
26	火灾报警系统	火灾报警			A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

与调度中心无关的电力监控系统不接入调度数据网。

表 2 核电站监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	核电站厂级分散控制系统 DCS	DCS			A2
2	自动电压控制 AVC	自动电压控制功能			A1
3	厂级信息监控系统	监控功能	优化功能	管理功能	A2
4	相量测量装置 PMU	PMU			B
5	网控系统	网控系统			A1
6	火警探测系统	火警探测系统			A2
7	辅机控制系统	辅机控制系统（三废处理系统、循环水处理系统、凝结水精处理系统、除盐水系统）			A2
8	继电保护	继电保护装置及管理终端			B
9	自动控制装置	安控、电力系统稳定器 PSS 等			A1、B
10	故障录波		故障录波装置		B
11	电能量采集装置		电能量采集装置		A1、B
12	管理信息系统 MIS			管理信息系统	A2
13	检修管理系统			检修管理系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

与调度中心无关的电力监控系统不接入调度数据网。

表 3 风电场监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	风电场监控系统	风机监控 风电场监控			A2
2	无功电压控制	无功电压控制功能			A1
3	发电功率控制	发电功率控制功能			A1
4	升压站监控系统	升压站监控功能			A1

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
5	相量测量装置 PMU	PMU			B
6	继电保护	继电保护装置及管理终端			B
7	故障录波		故障录波装置		B
8	电能量采集装置		电能量采集装置		A1、B
9	风功率预测系统		风功率预测		A1、A2
10	状态监测系统		风机状态监测		A2
11	测风塔系统			测风塔	A2
12	天气预报系统			数字天气预报	A2
13	管理信息系统 MIS			管理信息系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

表 4 光伏电站监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	光伏电站运行监控系统	电站运行监控			A2
2	无功电压控制	无功电压控制功能			A1
3	发电功率控制	发电功率控制功能			A1
4	升压站监控系统	升压站监控功能			A1
5	相量测量装置 PMU	PMU			B
6	继电保护	继电保护装置及管理终端			B
7	故障录波		故障录波装置		B
8	电能量采集装置		电能量采集装置		A1、B
9	光伏功率预测系统		光伏功率预测		A1
10	天气预报系统			数字天气预报	A2
11	管理信息系统			管理信息系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

表 5 燃机电厂监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	燃机电厂厂级分散控制系统 DCS	机组单元控制、自动发电控制、机组保护、辅机控制、公共系统等			A2
2	燃气轮机控制系统 TCS	燃气轮机控制功能			A2
3	自动电压控制 AVC	自动电压控制功能			A1
4	厂级信息监控系统	监控功能	优化功能	管理功能	A2
5	升压站监控系统	升压站监控功能			A1
6	相量测量装置 PMU	相量测量功能			B
7	自动发电控制 AGC	自动发电控制功能			A1
8	火警探测系统	火警探测系统			A2
9	变电站综合自动化系统	变电站监控、继保、故障录波 RTU			A1
10	继电保护	继电保护装置及管理终端			B
11	故障录波		故障录波装置		B
12	电能量采集装置		电能量采集装置		A1、B
13	管理信息系统			管理信息系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

附录 2　各类型电厂监控系统安全防护示意图

火电厂监控系统安全分区及边界防护如图 1 所示。

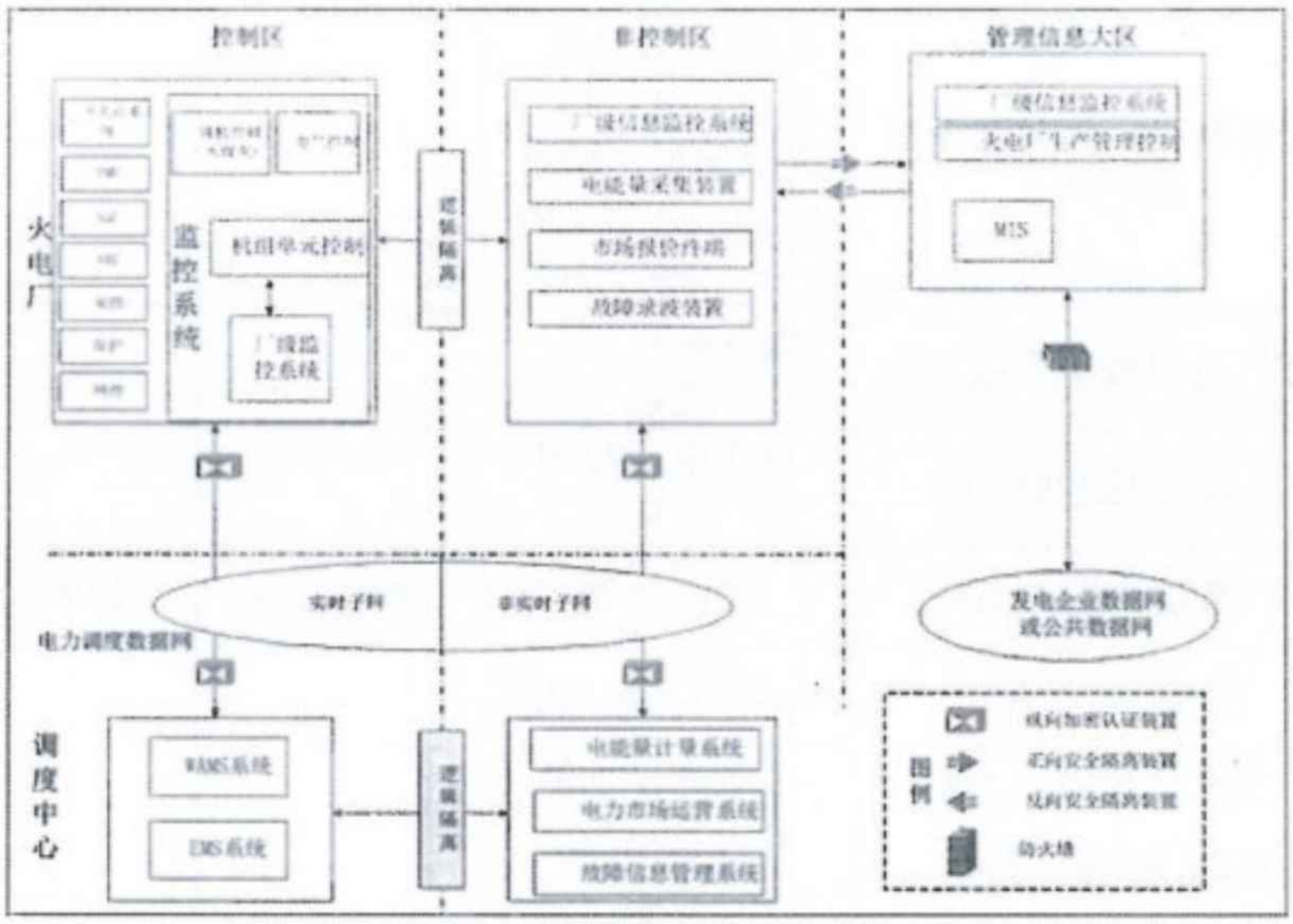

图 1 火电厂监控系统安全部署示意图

水电厂监控系统安全分区及边界防护如图 2 所示。

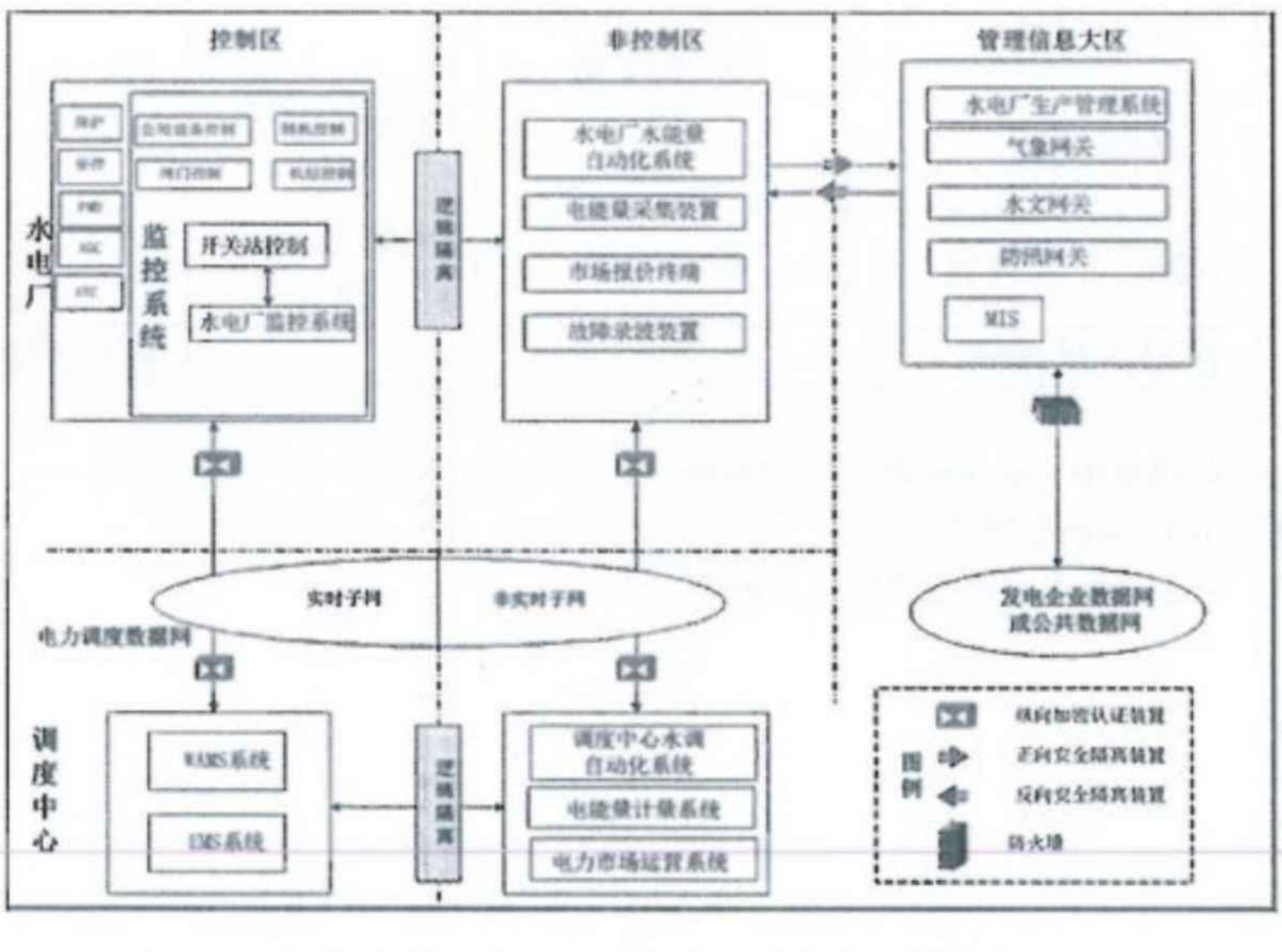

图 2 水电厂监控系统安全部署示意图

当水电厂监控系统与监控中心或梯级调度中心之间通过广域网络连接时，应当采取纵向加密认证措施进行安全防

护。梯级水电厂的安全防护部署如图 3 所示。

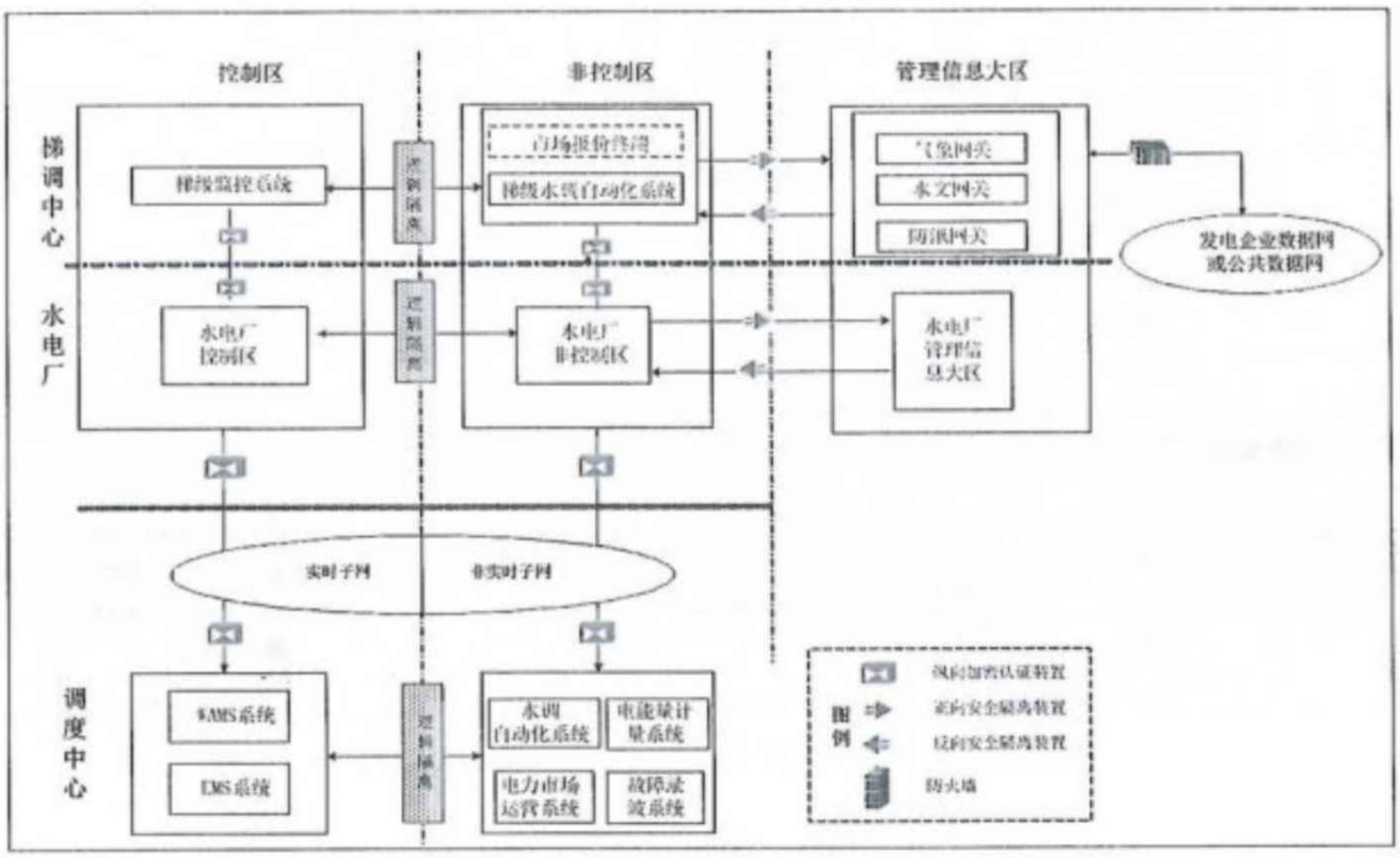

图 3 梯级水电厂监控系统安全部署示意图

核电站监控系统安全分区及边界防护如图 4 所示。

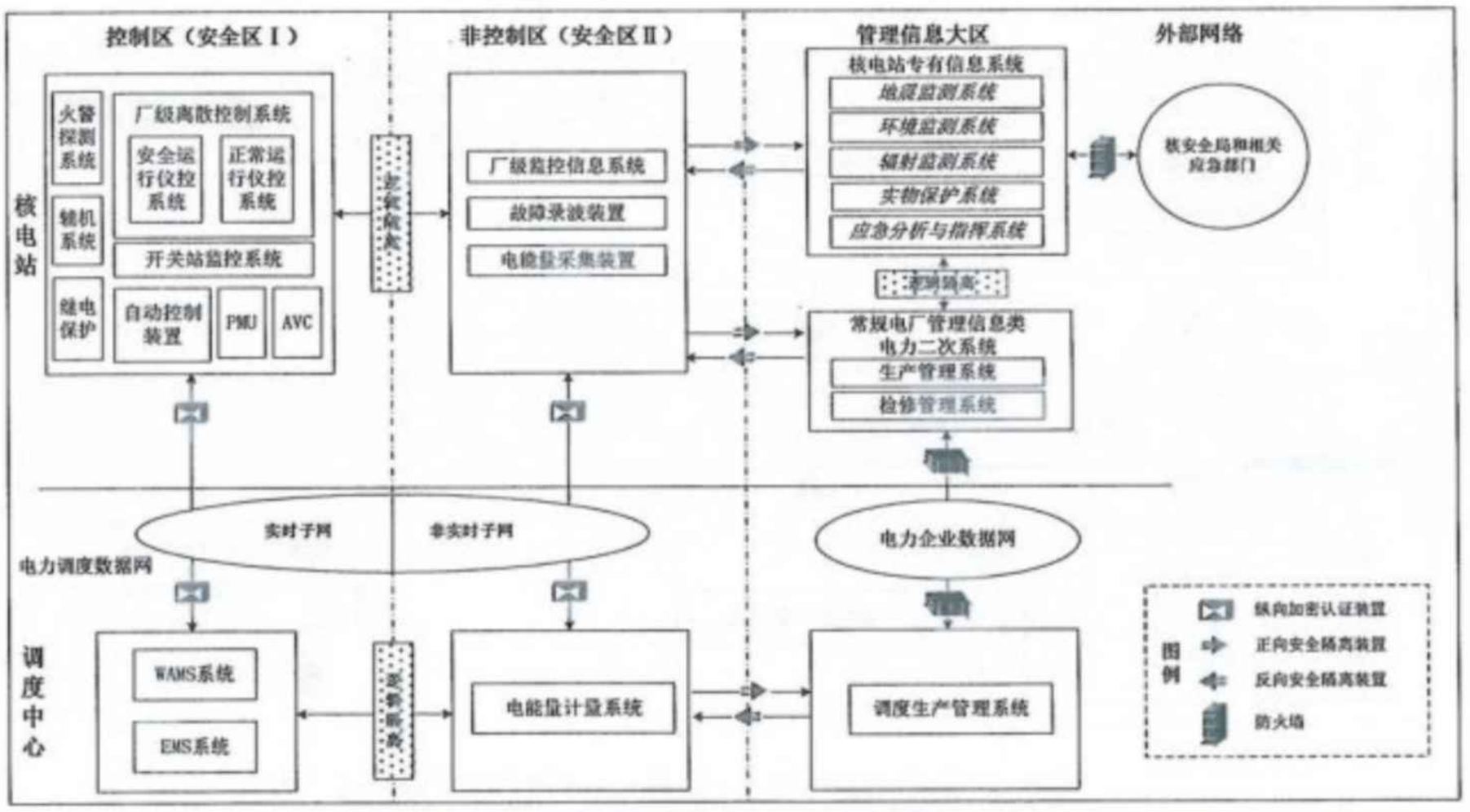

图 4 核电站监控系统安全部署示意图

风电场监控系统安全分区及边界防护如图 5 所示。

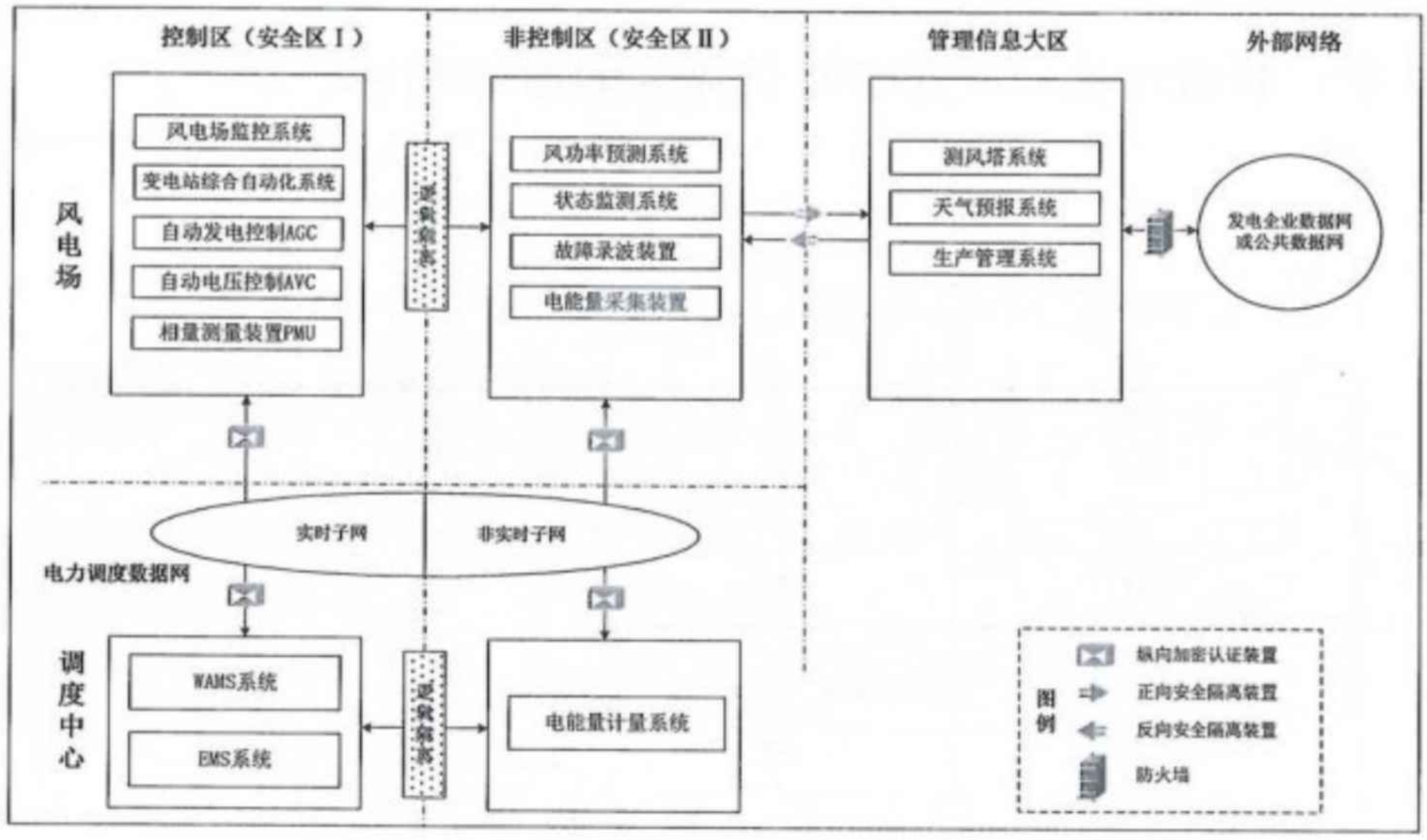

图 5 风电场监控系统安全部署示意图

光伏电站监控系统安全分区及边界防护如图 6 所示。

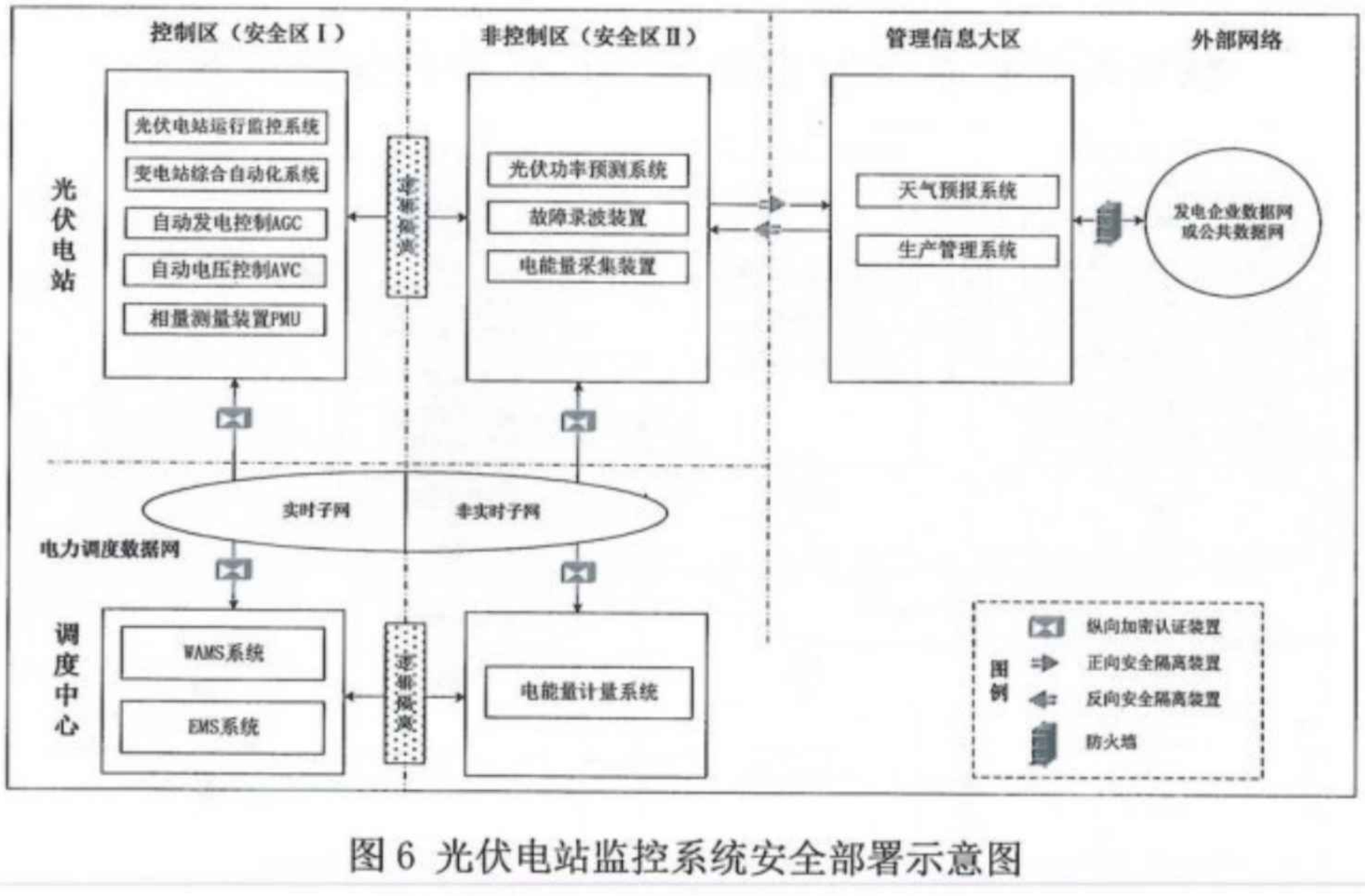

图 6 光伏电站监控系统安全部署示意图

燃机电厂监控系统安全分区及边界防护如图 7 所示。

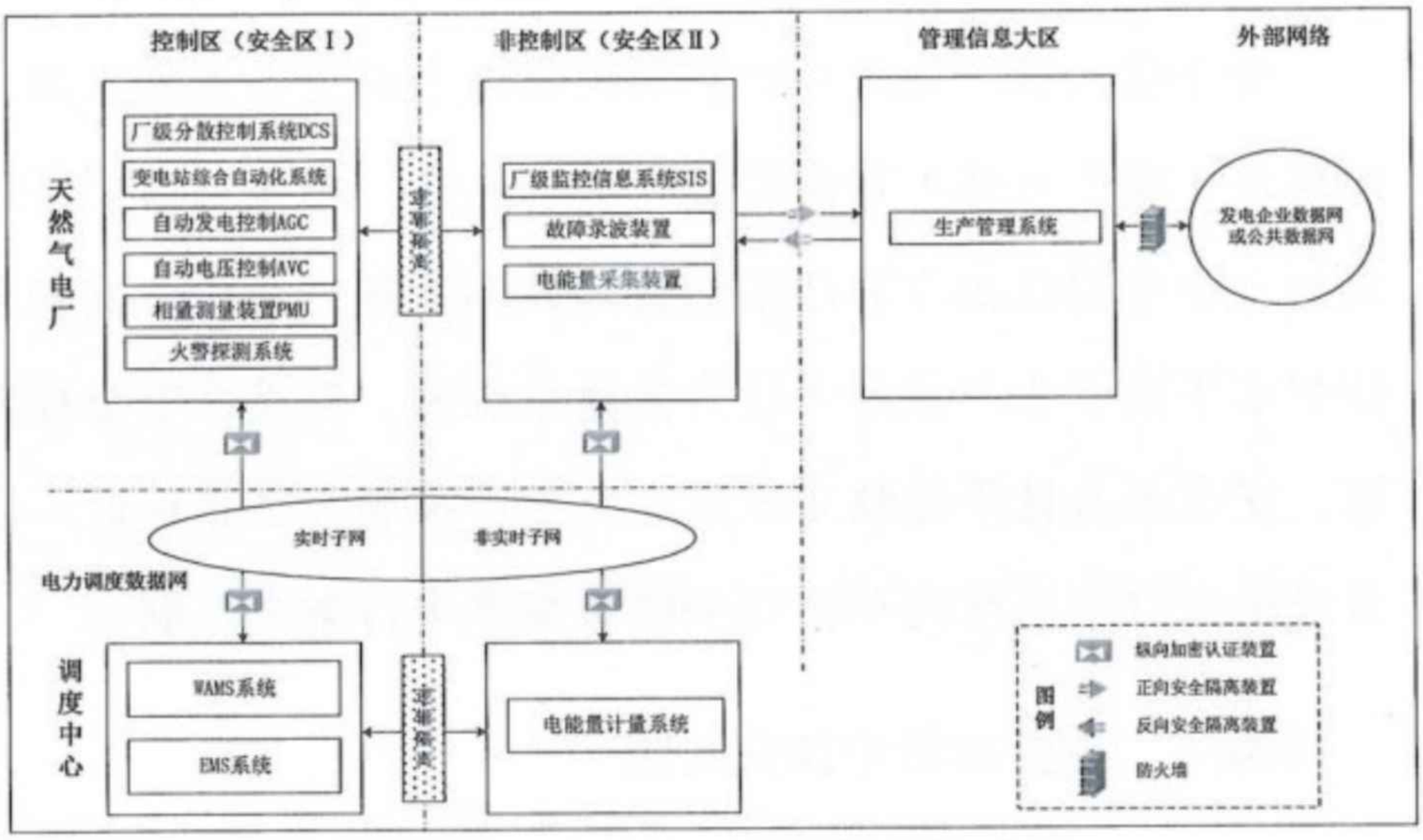

图 7 燃机电厂监控系统安全部署示意图