

第 11 卷

信息系统及安全防护部分 说明书

中国电力工程顾问集团西北电力设计院有限公司

Northwest Electric Power Design Institute Co., Ltd. of China Power Engineering Consulting Group

2024年 11 月 西 安

目 录

1	概述	1
1.1	工程概况及设计依据	1
1.2	规范及标准	1
1.3	信息化水平	2
1.4	设计原则	2
2	信息系统规划	3
2.1	系统规划	3
2.2	基础设施规划	6
2.3	机房规划	11
3	信息系统设计	12
3.1	全生命周期数据管理系统	12
3.2	生产信息一体化管控平台	13
3.3	厂区管理系统	23
3.4	燃料一体化管控系统	25
3.5	高级智能应用系统	25
4	接口设计	30
4.1	与生产实时控制系统之间	31
4.2	与集团公司信息系统之间	31
4.3	与广域网的接口	31
5	网络安全防护	31
5.1	安全目标	错误！未定义书签。
5.2	安全范围	错误！未定义书签。

5.3	安全防护原则	错误！未定义书签。
5.4	安全标准	错误！未定义书签。
5.5	网络安全规划	错误！未定义书签。
5.6	控制系统网络安全规划	错误！未定义书签。
5.7	信息系统网络安全规划	错误！未定义书签。

1 概述

1.1 工程概况及设计依据

1.1.1 工程概况

1.1.1.1 建设单位

甘肃能化股份有限公司。

1.1.1.2 建设地点

本工程位于甘肃省庆阳市宁县。

1.1.1.3 建设规模

本项目为新建项目，新建 2×660MW 超超临界空冷燃煤发电机组，同步建设脱硫系统、脱硝系统等。

1.1.1.4 建设进度

项目于 2024 年 12 月开工，第一台机组计划 2027 年 5 月建成投产，第二台机组计划 2027 年 6 月建成投产。

1.1.2 设计依据

1.1.2.1 可行性研究报告及可研审批文件。

1.1.2.2 甘肃能化庆阳 2X660MW 煤电项目工程勘察及初步设计招标文件。

1.1.2.3 国家法律法规、国家标准、建设标准强制性条文。

1.1.2.4 《大中型火力发电厂设计技术规范》（GB 50660-2011）

1.1.2.5 《火力发电厂初步设计文件内容深度规定》（DL/T 5427-2009）及有关设计标准、规程、规范、技术规定等。

1.1.2.6 《电力勘测设计技术管理制度》（DLGJ159.1-9，中国电力规划设计协会）

1.1.2.7 院三标管理体系文件、有关企业标准。

1.2 规范及标准

本工程信息系统设计及安全防护部分应遵循以下规范及标准：

《大中型火力发电厂设计规范》 GB 50660-2011

《智能建筑设计标准》 GB 50314-2015

《综合布线系统工程设计规范》 GB 50311-2016

《数据中心设计规范》 GB 50174-2017

《计算机信息系统 安全防护等级划分准则》 GB/T 17859

《火力发电厂厂级监控信息系统技术条件》 DL/T924-2016

《火力发电厂信息系统设计技术规定》 DL/T5456-2012

1.3 信息化水平

利用新一代信息技术、人工智能技术、检测、控制、工程、管理技术，以发电厂为载体，在其关键环节或过程，形成具有一定自主性的感知、学习、分析、决策、通信与协调控制能力，实现安全、可靠、绿色、经济、灵活的智能化电厂。

1.4 设计原则

信息系统的规划应兼顾现状、立足本期、考虑发展。

1.4.1 本工程拟建设数字智能化电站运营平台。

1.4.2 数字智能化电站运营平台建设原则

- 整体规划：数字智能化电站运营平台是电厂的管理运营中心，在设计与实施时，立足全局进行综合考虑与规划，既要考虑全面又要避免重复投资造成不必要的浪费，尽最大可能避免出现信息孤岛或者蜘蛛网。

- 分步实施：根据整体规划，将数字智能化电站运营平台建设划分为

多个阶段，分步实施，分步使用，同时利用已有应用系统的经验完善后续应用系统的设计。

第一阶段：构建电厂全生命周期的数据集成平台、生产信息一体化管控平台、智慧厂区管控系统，打造以全生命周期数据为基础、涵盖基本智能应用功能的数字化智能电站。

第二阶段：根据自身需求，充分调研市场上成熟的智能化应用模块，部署高级智能应用。

- 先进性与经济性兼顾：设计与数字智能化电站运营平台时，在经济适用的基础上充分考虑技术的先进性与前瞻性，为系统扩展提供一定的空间。

- 安全可靠：安全性涵盖硬件设备容错能力、数据资源访问策略、用户验证机制和系统备份策略等多个方面。

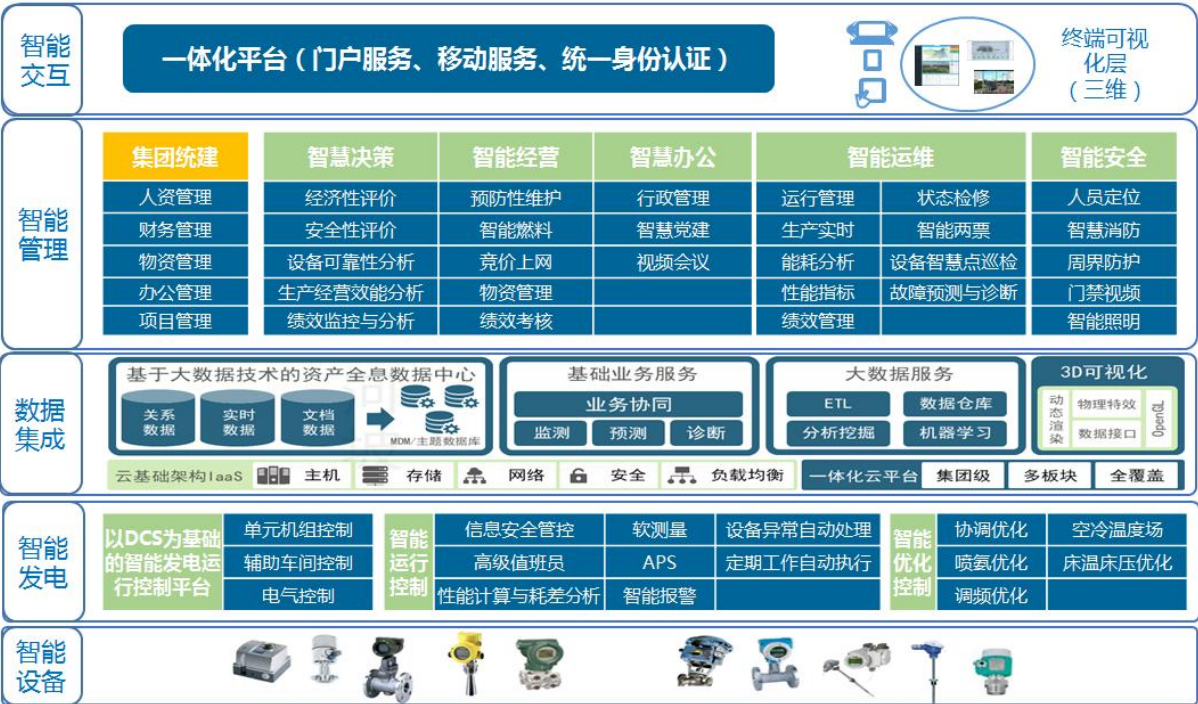
- 符合通行标准：应用系统设计与实施必须符合相应的国际标准、国家标准和行业标准等。

- 充分考虑开放性和可扩展性：考虑硬件设备的可扩展性和软件模块的灵活性与开放性，以适应系统将来可能的发展。其中数字智能化电站运营平台的整个硬件基础设施建设统一考虑、统一部署。

2 信息系统规划

2.1 系统规划

数字智能化电站运营平台的应用架构图如下：



（1）智能设备层：智能设备层在电厂传统运行设备层的基础上，采用先进的测量传感技术，对电厂生产过程进行全方位检测和感知，并将关键状态参数、设备状态信息及环境因素转换为数字信息，对其进行相应的处理和高效传输，为智能发电层及智能管理层提供基础数据支持。

①智能设备层中嵌入高精度的机组重要参数软测量信号，包括：锅炉热量、入炉煤质、锅炉入炉煤粉流量、烟气含氧量、汽轮机排汽焓、锅炉蓄能、蒸汽流量等，为智能控制层中的优化控制、在线经济性分析及诊断系统提供重要数据保证。

②智能设备层中嵌入现场总线设备技术，其不仅可以有效减少现场电缆数量，提高系统信号传输的抗干扰能力和可靠性，而且可以为智能发电层与智能管理层提供海量数据，通过对数据处理实现设备可靠性分析及故障预警，并以智能管理层为基础构建现场总线和智能设备的在线智能管理系统，将被动的管理模型改变为可预测性的管理维护模式。

③智能

设备层中嵌入先进的测量设备，如采用红外检测设备以热图像形式反映设备的三维温度场信息，可有效的对设备故障进行实时预警及诊断；利用火焰图像频谱分析法，对电厂锅炉煤质进行有效的计算和分析；使用智能机器人，完成一些工作人员无法实现的操作，如对高危区域进行巡检、探伤等。通过先进的检测设备对生产现场进行全方位检测和感知，提高设备运行可靠性，有效提升风险防控水平。

（2）智能控制层：智能发电层主要包括智能控制及智能生产监管，是智能电厂控制的核心。智能发电层以智能DCS为核心，扩展智能优化库、开发服务器等资源，实现智能监测、智能控制、智能诊断与优化运行。由于燃煤电厂机组对象特性复杂且需不断适应外界工况的变化，传统DCS控制功能已不能满足多样化生产需求，因此在智能控制中需结合先进控制算法及智能控制策略、多目标优化、数据分析等技术手段，来满足对象多样化的需求。①智能控制中嵌入更丰富、更先进的实时控制与优化算法模块，包括预测控制、自抗扰控制、内模控制、鲁棒控制等先进控制算法模块，同时包含多目标寻优算法以及机器深度学习等实时优化算法模块功能。②智能控制中嵌入更具针对性、实用性的节能优化控制系统解决方案，包括基于精准能量平衡的智能机炉协调优化控制、脱硝优化控制、一次调频优化控制等算法，以满足机组快速、经济、环保等多目标柔性优化控制需求。③智能生产监管中嵌入机组实时经济性分析与诊断系统，结合智能设备层提供的高可靠、高精度的测量信息，应用锅炉核心计算方程、汽轮机热经济状态方程、机组性能耗差分析等工程分析方法，实现对电厂设备及系统性能的实时计算，全面、精确、直观的反应当前机组性能指标和能损分布情况，指导机组运行人员进行合理性的调整，达到提高机组运行效率、

降低煤耗的目的。④智能控制层中嵌入自启停控制系统，将全程自动控制与顺序控制有机结合，融合设备运行状态监督技术，具备自学习、自校正等能力，可显著增加机组控制系统的自动化水平，最大限度的减少运行人员的操作强度和人员数量，实现减员增效。⑤智能生产监管根据智能控制层提供的节能优化控制系统解决方案、机组经济性分析及诊断结果、设备状态监测与智能预警、自启停控制系统提供用户界面、柔性多目标决策、模型的更新与深度学习、故障自切换与恢复等监督功能；同时向智能管理层提供机组的全面分析诊断报告，为智能管理的决策提供依据。此外，在智能生产监管层中配备厂级负荷优化系统及高级值班员决策支持系统，为机组的高效运行及安全管理维护提供支持。

(3) 智能管理层：智能管理层中提供自组织的精细化管理解决方案，通过厂级能效对标与考核系统、运行管理系统、智能巡检、精密点检与设备远程管理、设备定期轮换管理、可视化技术监督智能管理、可视化三维作业指导书及检修培训、缺陷管理、全局成本利润分析与决策、移动应用、远程诊断、三维虚拟电厂与安全管控、三维建档等管理系统，设计基于数据共享的管理一体化平台，实现发电厂的闭环、自组织的精细化管理系统。

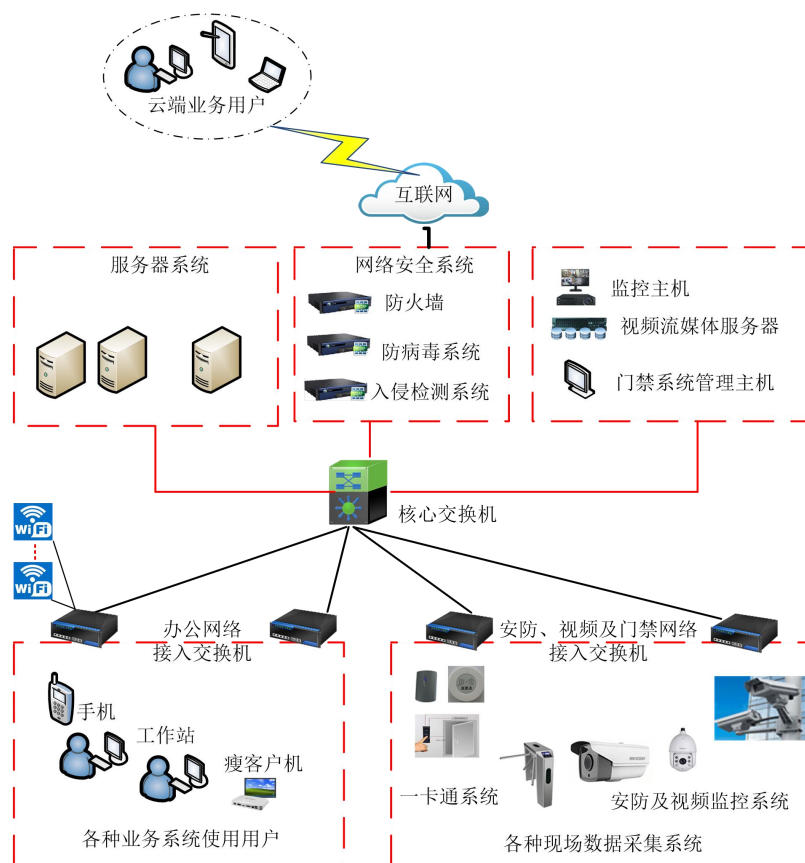
2.2 基础设施规划

2.2.1 基建阶段基础设施规划

基建阶段网络基础设施包括办公网络、安防及视频监控网络、门禁一卡通网络的建设，为基建阶段的项目管理应用、造价物料、安防管理等提供服务。

在基建办公楼设置信息机房。服务器、核心交换机、防火墙、安防监控服务器等设备布置在信息机房。

网络系统图如下：



服务器配置：设置项目管理系统、档案管理系统、财务管理系统服务器，设置流媒体服务器等。

网络配置：设置1台核心交换机作为办公网络和安防监控网络公用的核心服务交换机，通过虚拟网段划分隔离不同的应用系统网络。办公网络根据现场信息点数量设置相应的汇聚交换机数量，选择48口网络交换机作为接入交换机。安防监控网络根据现场监控点的布置位置及数量配置相应的接入交换机数量、监控摄像头、门禁读卡器、通道闸机等设备。

2.2.2 全厂基础设施规划

网络设计为两级，即网络主干级和工作组级。所有楼宇间为主干网段，

全部采用光缆和千兆以太网技术。建筑物内为工作组级，采用六类非屏蔽双绞线和快速以太网技术，采用TCP/IP通讯协议。为每台工作站提供独享的100M带宽，同时通过VPN（虚拟专用网）连接至相关单位。

本工程设计规划两套独立的综合布线系统，一套用于全厂管理信息系统办公业务网络，简称办公网络，另一套用于厂区所有智能化系统设备的数据传输网络，简称设备网络。

管理信息系统的业务办公网络中，每个工位设置一组信息点（一个数据点、一个语音点），重要的工位或者区域设置2组信息点，面板采用六类非屏蔽数据模块。智能化系统的设备网络中，每个设备至少一个信息点，重要的区域的重点设备设置2个信息点，为了减少中间节点造成断点，因此，设备与交换机之间不设置信息面板，直接用六类非屏蔽双绞线通过水晶头连接。

办公网络主干网采用12芯单模铠装光纤作为传输介质，工作区域采用六类非屏蔽双绞线作为传输介质。设备网络主干网采用12芯单模铠装光纤作为传输介质，工作区域采用六类非屏蔽双绞线作为传输介质。

建筑物的设备间内统一采用24芯光纤配线架、24口RJ45模块式配线架、110对110型语音配线架等作为连接件，网络交换机采用48口、24口、16口，接入层交换机可堆叠，堆叠数量不超过2个。

建筑物之间采用光纤冗余配置，重要建筑物之间采用光缆冗余配置（信息机房到脱硫综合楼、输煤综合楼、材料库等）。

2.2.2.1 网络设计

办公网络核心交换机采用冗余配置，与建筑物之间采用双链接。设备网络核心交换机也采用冗余配置，与建筑物之间采用双链接。

建筑物之间主干网采用万兆，桌面百兆。

2.2.2.2 网络交换机

核心交换机采用冗余配置，与建筑物之间采用双链接。

每个建筑物按照汇聚层配置设备，整个网络按照2级设置连接。

2.2.2.3 虚拟化主机系统

数据中心主机存储建设实现数据中心的绿色节能和虚拟化，除了底层的关系型数据库和实时数据库各配置独立的冗余物理服务器，其它各类应用服务器均采用虚拟化服务器。虚拟化服务器以及数据集中存储模式大大降低了数据中心建设成本、提升数据中心的运营效率和管理能力。

所有服务器均通过万兆双链路连接接入交换机。集中存储设备实现数据IP SAN存储和文件NAS存储。

各类应用服务器进行虚拟化设计，满足智慧电厂信息化系统各个应用系统的需要，包括厂级监控、设备管理、智能巡检、智能操作票、设备状态检修、燃料一体化管控、三维移交管理、三维可视化、可视化安全管理、智慧厂区管理、生产经营分析、智能采集上报、数据集成、门户及综合管理系统、移动终端、档案等业务系统。

2.2.2.4 网络安全

配置防火墙、路由器、防病毒设备、入侵检测设备、上网行为管理机、隔离网闸、堡垒机。

生产过程以及实时数据采集接口机以及接口机防火墙设备，约10套。

2.2.2.5 网络系统图



2.2.2.6 虚拟化主机系统

实时数据库服务器配置2台组成冗余配置，安装实时数据库系统，用于存储生产实时数据，与其他系统用网闸进行单向隔离。

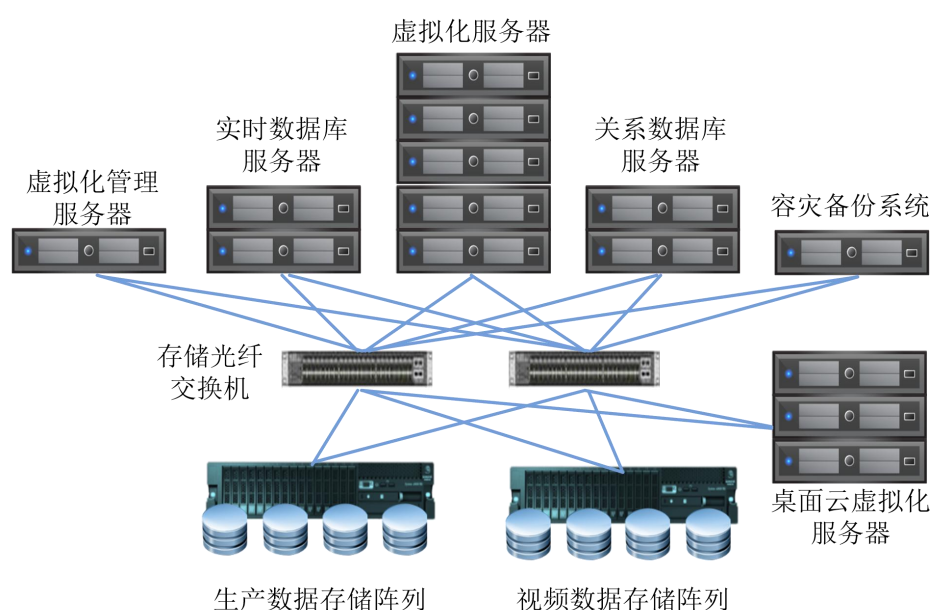
关系数据库服务器配置2台组成冗余配置，安装关系型数据库，用于管理数据。

虚拟化服务器配置7台物理服务器，为全生命周期的数据管理平台、电厂管控一体化业务系统、数字可视化安全管理系统、智慧厂区管控系统、

数字化煤场等等系统的应用提供服务。

桌面云虚拟化服务器配置3台物理服务器，为全厂所有桌面系统提供服务。

配置2套存储系统，一套用于储存生产管理数据，容量30T，另一套用于存储安防视频多媒体数据，容量300T。



2.2.2.7 无线网络

搭建一套LTE无线网络作为生产办公无线网，采用信息技术、5G移动通信技术和管理手段，实现对生产装置和厂区环境的全面感知和监控；同时实现各岗位的协同工作，紧密连接生产经营的各个环节。达到降本增效、协同响应、移动化作业和管理的效果。

2.3 机房规划

信息机房按照B级机房标准进行建设，保证计算机设备对温度、湿度等的要求，机房装修由建筑专业安排考虑。机房防静电地板高度不低于300mm。

3 信息系统设计

3.1 全生命周期数据管理系统

全生命周期数据管理平台用来装载设计单位、设备厂家、工程建设单位等的工程信息，并通过数据模板扩展为运营期使用的数据，成为企业的工程数据仓库，其中包括：三维模型、工程位号、工程文档等。

全生命周期数据管理平台是将电厂概念与设计、施工、运营、维护直至退役阶段内的工程信息进行整合、共享、存储以及管理的解决方案载体。在不同的阶段内，该平台系统具有不同的功能来满足设计、施工、运营阶段不同的业务需求。

全生命周期数据管理平台将三维模型与现场各系统间数据关联，实现三维模型和数字化文档综合展示；具备应用服务集成接口，可与智能发电运行控制系统、生产视频监控、三维资产全生命周期管理等系统进行数据关联，实现信息与资产的一体化管理，为电厂生产运行的全寿命周期管理提供形象、直观、真实的三维图形和数据依据。

全生命周期数据管理平台同时是一个以数据为中心的系统，能抓取对象并建立它们之间的多种关系，以便直观导航。

此外，全生命周期数据管理平台还将电厂在运行、维护过程中需要进行的各类活动进行定义和实时可视化管理，同时，利用强大的数据分析功能，根据专家知识库，提供实时最优化决策建议。

三维模型作为全寿命周期数据平台的信息载体，应涵盖全厂所有需要承载其它关联信息（设计、运营、管理、安全等）的模型，具体涵盖范围包括汽机房及锅炉房结构、建筑模型，厂区建筑模型，电气、热控桥架及相关设备模型，工艺专业各系统烟风道、管道以及相应支吊架模型，工艺

专业设备模型等。

3.2 生产信息一体化管控平台

通过研究发电企业的管理需求和解决策略，分析企业信息化管理状态及信息化建设需求，建立包含集团统建部分及智能决策、智能经营、智慧办公、智能运维、智能安全等的管控一体化业务系统。生产信息一体化管控平台功能以生产经营业务为主体，实现对安全、运行、资产、检修、经营、成本等进行全过程精细化管理，由设备供应商完成设备标识编码的编制。本方案中，由一体化管控平台统一构建企业门户，与全生命周期数据管理平台、数字化工程、智慧厂区等实现交互，完成各类管理功能界面设计以及相关功能的三维可视,使企业各类业务之间的关系达到高度协调统一，控制流、物流、资金流、信息流需得到完整、清晰体现。生产经营管控一体化系统具备下述的具体功能。

3.2.1 应用模块

应用模块要在甘肃能化集团统筹规划下进行，甘肃能化集团侧已有的模块，电厂侧就不用重复建设。

系统功能应包括：集团统建部分、智慧决策、智能经营、智慧办公、智能运维、智能安全等部分。见下图：

智能管理	集团统建	智慧决策	智能经营	智慧办公	智能运维		智能安全
	人资管理	经济性评价	预防性维护	行政管理	运行管理	状态检修	人员定位
	财务管理	安全性评价	智能燃料	智慧党建	生产实时	智能两票	智慧消防
	物资管理	设备可靠性分析	竞价上网	视频会议	能耗分析	设备智慧点巡检	周界防护
	办公管理	生产经营效能分析	物资管理		性能指标	故障预测与诊断	门禁视频
	项目管理	绩效监控与分析	绩效考核		绩效管理		智能照明

3.2.1.1 集团统建部分

人力资源管理主要包括：劳动管理、干部管理、人事档案管理、工资及奖金管理、劳动合同管理、劳动保险管理、教育培训管理、基础信息管理及劳资统计；

财务管理主要包括：账务管理、工资管理、成本管理、固定资产管理、资金管理、税收管理、财务综合管理；

资产管理包括：设备基础管理、预防性维护、缺陷管理、项目管理、标准工作、排班管理、工单管理、采购管理、库存管理、资源管理、停机管理、可靠性维护、作业预算、成本核算。

3.2.1.2 决策与经营管理

经营管理系统包括：计划统计管理、全面预算管理、财务管理、成本与报价管理、燃料管理、粉煤灰综合利用。分述如下：

计划统计管理主要包括：生产计划统计管理、技术经济指标管理、生产统计管理、制定工程、材料、资金等各项计划等；

全面预算管理主要包括：预算编制、预算控制、预算调整、预算报表、预算分析；

成本与报价管理主要包括：成本计算、成本分析、成本预测、报价策略；

燃料管理主要包括：燃料的计划管理、采购管理、装运管理、接收管理、库存管理、结算管理、统计与报表；

粉煤灰综合利用主要包括：对电厂生产副产品的进行单项管理。如灰，渣，石膏等物品及综合利用的情况。

3.2.1.3 生产管理系统

生产管理系统包括：运行管理、安全管理、技术监督管理、生产实时管理。分述如下：

运行管理主要包括：定期工作管理，日志管理，运行分析，交接班管理，运行生产调度管理，运行规程管理，安全管理，指标管理，生产计划管理，机组性能优化管理；

安全管理主要包括：人身事故管理、设备事故管理、交通事故管理、综合管理、安全教育培训、两措管理；

技术监督管理主要包括：节能监督管理，绝缘监督管理，电测监督管理，继电保护监督，化学监督管理，金属监督管理，热控监督管理等；

生产实时管理主要包括：管理与机组的效率有关的信息，与机组发电质量有关的信息，与机组安全运行有关的信息，机组运行管理方面的信息。

3.2.1.4 行政管理部分

行政管理系统包括：办公事务子系统、档案资料子系统、人力资源子系统、综合查询子系统。分述如下：

办公事务管理主要包括：收文管理、发文管理、文书档案管理、文档管理；

档案管理主要包括：科技档案、文书档案、财务档案管理等。

综合查询和企业网站主要包括：建立电厂内部局域网（Intranet）和国际互联网（Internet）的站点。并提供电厂综合查询功能，主要包括：实时监视管理、通用查询管理、数据分析管理。

3.2.1.5 系统维护部份

按照目前软件的开发水平，软件的维护应采用集中维护的方式，即应用软件在中心机房进行处理和修改。同时，系统应具备较完善和自适应的

应用支撑平面。

系统维护子系统功能主要包括权限维护、数据安全维护、代码维护、数据字典维护。

3.2.1.6 统一门户网站建设与管理

建立统一的网络门户，帮助员工实现对不同应用系统的单点登录，实现个性化主页配置。建设综合查询系统，以满足决策层、管理层和执行层的各种决策和管理需要。

3.2.2 生产实时

生产实时监视是生产实时数据的采集、监视、分析和优化，主要包括数据采集、实时画面监视、耗差分析、性能计算、指标考核、运行优化、设备状态监测、事故报警、实时数据库、趋势分析、指标对标、历史回放等内容。

3.2.2.1 实时/历史数据库

数据库支持标准的B/S（浏览器/服务器）和C/S（客户/服务器）结构，具有良好的开放性和可扩展性，支持多服务器结构，当扩建机组的数据接入时，只需增加数据库服务器即可。

对于数据的采集应包括所有生产监控系统的实时数据，所采集的每个点的精度应可按电厂的要求定义。

提供点数10万点的实时数据库，采取有效的压缩方式保证电厂所有生产过程实时信息和计算、分析结果数据的保存时间至少达到6年。

实时数据库系统应有和与其联网的数据源系统的标准接口，它们至少应包括目前国内外主流DCS。目前认可的主流标准是OPC V2.0。

实时数据库不仅作为监控信息系统所有计算分析程序和打印、报表所

需数据的来源，还有和生产管理系统上关系型数据库的标准接口。服务器和客户端的硬件应采用标准的第三方产品，软件模块应完全支持和兼容微软的体系结构。实时数据库对外提供OPC、API等接口，供第三方软件读取数据。

3.2.2.2 数据采集与存储

主要功能包括远程维护，接口状态可视化监视，数据链路异常报警，网络中断数据本地缓存，断点续传，时间同步。

1) 数据采集

数据采集服务通过特定通道按照既定的规约格式和方式，采集DCS数据以及其他外部系统的数据，存储到实时/历史数据库。

2) 数据传输

数据处理服务对采集到的各类数据进行转换、压缩、校验和检查，并完成物理存储。具体功能如下：

数据包压缩：在不影响数据刷新周期的条件下对传输的数据包进行压缩，减少对网络带宽的占用，提高传输效率，提供数据包压缩方法的详细说明和压缩效率说明。

数据有效性校验：根据一定的校验规则，对各类业务数据的格式自动进行分析，以确认数据传输的有效性。

数据合理性检查：根据各业务数据的有效数据范围、突变范围等物理属性，自动识别数据的合理性。

数据存储：对传输到集团的数据存储到集团的实时/历史数据库中，确保数据准确、完整。

3.2.2.3 全厂生产过程监视

厂级生产过程监视与管理可以按用户要求进行实时画面组态，并使系统的生产模拟图与各生产控制系统的监控画面一致。以Web方式显示全厂各生产系统实时信息，这些画面包括机组DCS、各辅网等所有实时监控系统的画面。

生产过程画面以趋势图、棒图、相关参数组等多种形式进行画面显示，显示生产过程数据、设备状态、报警状态、经济指标等信息，参数显示能显示实时值、历史趋势查询，在定义时段内的最大值、最小值以及平均值等。

生产过程画面应实现历史数据回放功能。

3.2.2.4 趋势分析

能访问实时/历史数据库中所有Tag，方便地将趋势数据导出，方便其他报告引用。

3.2.2.5 综合报表

提供一套完整的、灵活的、可视化的综合报表组态平台，对全厂生产实时数据进行综合处理、统计分析，可以很方便的进行数据组合和计算生成报表，形成机组或全厂生产运行报表。

提供的综合报表平台基于实时数据库中的实时/历史数据和性能计算、运行考核等其它功能中的数据，同时可采集各种外部数据，如手工输入的数值型和文本型数据。

综合报表平台提供自动生成班报、日报、周报、旬报、月报、季报、年报以及事件报表等各种报表类型。

3.2.2.6 事故回放

以更加直观的图形方式全面展现机组工况，对运行人员提供事故培训

指导，提高运行人员的事故处理能力。

生产过程回放能采集所有的控制系统图形，并且图形和控制系统完全一致。

可结合历史数据和监视画面，以控制系统过程图形的方式直观再现过去某一时刻机组的运行状况，以便对机组过去某段时间内的运行情况进行分析和事故追忆。

3.2.2.7 事件与报警管理

跟踪生产运营中发生的生产事故和有较大影响的紧急事件，并及时向相关职责岗位报告。事件跟踪与管理功能提供对该业务的支持，利用该功能，可以对事件/报警进行定义和设置，在电厂发生事故和紧急事件时，能迅速报警提示；同时，提供对历史事件的查询功能。包括：报警定义、实时事件报警、事件报警的存储、查询和打印、导出功能等。提供专用工具完成报警相关的管理和维护功能。

3.2.2.8 小指标考核

运行小指标考核通过对实时采集数据或人工输入数据的统计、计算和分析，获得企业不同部门、不同层次的小指标数据，为企业生产经营决策、班组考核等提供依据，具备以下功能：

班组运行数据分析：对各个班组的生产运行数据进行横向和纵向的比较分析，并以各种图形方式进行显示（包括直方图、曲线图等）。

全厂综合指标分析：由计划统计部门在各车间日常生产运行数据的基础上进行全厂综合性指标数据的统计、计算和分析。对分析结果以各类报表的形式显现（包括生产日、月、年报等），并需要经过审批流程。

根据用户要求按班、值、峰/谷/平或其它任意时间段定制并形成各类小

指标核算日、月、年报表。

提供专用工具配制和管理，指标考核按用户定义运算法则，将运行指标转化为量化考核指标，用户可自定义需要考核的指标，考核的方式，运算法则，提供有好的界面方便操作；

3.2.3 信息编码

3.2.3.1 信息分类与编码

管理信息系统中的信息类别特别多，数据量大，为了方便用计算机进行处理和保持数据一致性，必须对信息按照统一的标准进行编码。信息编码对管理信息系统的建设有重大影响，只有建立科学、规范的信息编码体系，才能方便信息处理、加快处理速度和节省存储空间，也有利于保持数据的一致性。

3.2.3.2 重要信息编码

部门编码：本厂部门编码采用2位无实义码。保持编码的唯一性，一个部门撤销后，它的编码即行作废，不再赋予其它部门，新设部门按顺序赋予新的编码。

职工编码：本厂职工编码采用4位无实义顺序码，保持编码的唯一性，当一名职工的档案取消后，他的编码不再赋予其他人，新职工按顺序赋予新的编码。

设备编码：本工程数字化智能电厂系统使用电厂标识系统编码。

其它代码：其他代码应采用符合中华人民共和国国家代码标准的国家标准代码。

3.2.3.3 电厂标识系统编码实施方案

本方案主要提出电厂标识系统编码在编制和实现方面需要采用的步骤

和承担任务角色的参考意见：

（1） 编制《全厂标识系统》编码原则

由工程设总根据工程设计要求负责制订总的原则和编码编写说明及规则，各专业据此提出本专业详细的编码定义。

上述内容在总图阶段完成。

同时，各专业应在总图设计阶段完成之前，作为一项工作内容，把编码原则专门告知相关设备提供厂商（包括前期已签署协议的厂商），使电厂标识系统编码能够统一，避免制造厂与设计院在电厂标识系统编码上出现差异。

（2） 电厂标识系统编码的编制

在施工图总图阶段完成系统图编码的编制，同时在施工图阶段完成其余编码的编制。

以上工作由设计单位负责完成。

（3） 电厂标识系统编码的实施

在实施过程中，组织机构的安排通常有两种做法：一种是由软件开发商主导完成，电厂组织人员进行一定的配合；一种是电厂组织人员主导完成，必要时软件开发商作相应的配合。

数据准备

由电厂在设计图纸及图上所标识电厂标识系统编码的基础上，收集电厂标识系统电厂设备安装布置图等建立标识系统所需的设备资料，并提出电厂的管理需求：要求电厂标识系统编码管理到设备元件级，相关的资料也要做到设备元件级。

实践中发现，图纸上的编码与实际应用尚有差距，例如部分编码编到

设备级，而应用需要到达元件级；部分设备的编码与厂家所标识的不一致；编制方法与管理要求有差异；电厂标识系统代码应覆盖电厂的所有设备等。因此，需要在对已有的编码进行核实、补充、完善、审核。

人员组织

电厂指派项目技术负责人，要求其对电厂的所有系统和设备较熟悉，通常由运行总工负责，参与此项工作。

配合人员的要求：指定机、炉、灰、化学、燃料等机务专业人员各1名，电气、仪控（包括燃料、化学）每专业各1名，土建专业人员1名。提供必要的系统图并参与编码核实和完善等工作。基础数据相关的资料准备要做到设备元件级。

编制人员的要求：应是专业技术人员或者业务骨干，在电厂标识系统编码原则学习和编码核实、补充、完善、审核期间脱产工作，服从电厂专家的现场管理，按时完成提交的相关工作计划。

对协调人员的要求：能代表电厂协调解决电厂标识系统编码期间出现的各种问题。

电厂审查标识系统方案

编制结束进入审核阶段，审核期为20个工作日/机组。

编制人员的培训

分为高级培训和编码培训。其中高级培训对象主要为电厂的系统专家，要求对电厂的所有系统和设备较为熟悉，一般由电厂指定一到两名值长或者运行总工负责；编码培训主要对象为电厂的每个专业技术人员或者业务骨干。采用集中培训的方法，培训期分别为7个工作日。聘请软件开发商在现场进行培训及辅导。

编码录入

由电厂的数据录入人员将标识系统代码完整地录入电厂所使用的信息管理系统代码库中；经过录入数据与书面数据的再校核后提供信息管理系统使用。

提交电厂标识系统的全部文件

内容包括：

- (1) 电厂标识系统设计说明书；
- (2) 电厂标识系统指南；
- (3) 电厂标识系统索引表；
- (4) 电厂标识系统编码手册；
- (5) 电厂标识系统编码数据库。

使用人员的培训

使用户熟练掌握和运用电厂标识系统，使其在电厂标识系统设计原则，标识构成，编码方法等方面有全面的了解和掌握。聘请软件开发商在现场进行培训及辅导。

验收

对电厂标识系统编码的验收主要包括如下的内容：编制原则验收；设备编码验收；零件编码验收；项目验收等。由电厂组织专业人士进行。

电厂标识系统实施结束后，随整个数字化智能电厂营运平台试运行进行整个系统验收。

电厂标识系统编码在应用过程中还要不断进行数据维护。

3.3 厂区管理系统

智慧厂区管控系统是电厂全生命周期的数据集成平台的一个子系统，

与电厂全生命周期的数据集成平台间设有数据接口，最终纳入平台统一管理。

智慧厂区管控系统将建立统一的智慧厂区共享平台，对各类分散的安全子系统进行有机的互连，在可视化的三维场景监控画面下，综合处理各项厂区业务，从而实现智慧厂区的协调联动、安全防护。

主要集成系统如下：

1) 生产视频监视系统：采用全数字高清摄像头，用于生产区域的可视化监控。全厂闭路工业电视主系统按照#1~#2机组（含升压站）区域、水系统区域、脱硫系统区域、除灰区域、输煤区域，尿素区、安保区域等监控子系统进行设置，设置400个摄像头。全厂工业电视系统是由监控子系统为基础联网组成一套全厂范围数字化监视系统。显示器和控制主机分别设在集控室和各子系统控制室中。集控室设置液晶显示器，可以监控全厂区域所有摄像探头的图像，各子系统控制室分别设置1台数字主机及液晶显示器，监控本子系统内的摄像探头。值长台设置闭路电视管理终端，负责闭路电视系统的集中管理及维护。

2) 门禁一卡通系统：记录并管理楼宇人员出入情况，对强行开门、超时未关门等行为进行记录并报警。

3) 安防系统：安防系统由周界报警系统和安防视频系统组成，周界报警系统主要通过安装在厂区围墙安装红外对射探头和电子围栏，探测非法进入厂区或者试图非法进入设防厂区的行为，并进行声光报警，并显示周界位置及相关视频信息。

4) 火灾报警报警：通过感温、感烟、可燃气体等探测异常，自动定位、高亮显示火灾报警点。

5) 人员定位：通过UWB、视频联动等技术，对于进入工作现场的人员，

在厂区三维模型里进行定位及监控。

6) 三维电子地图系统：基于三维环境的厂区电子地图系统，包含厂区内各个建筑物、厂区道路、厂区围墙、厂房内/厂区主要设备的三维数字化模型。

3.4 燃料一体化管控系统

电厂燃料智能管控系统是一套独立运行的系统，有专属的软件和硬件设备，接入数字化智能电站运营平台，是数字化智能电厂的一个独立组成部分，能够实现与上级公司燃料管理系统的无缝衔接。

通过燃料管理系统控制及协调，保证燃料系统采、制、化工作自动有序进行，减少人为干涉。通过自动控制、操作采样机、汽车衡等验收设备，且设备工作流程不能随意修改，减少人工操作的项目、频次，提高工作效率，减少人为影响；降低人力成本、提高管理效率和管理质量；

验收业务流程公开、透明、可追溯，防止作弊使假的发生，减少管理漏洞，减少煤炭供需双方的矛盾。系统直接和验收的仪器设备相连，现场实时采集、自动处理各种数据，减少手工抄录环节，且数据不能随意修改，提高数据的准确性、安全性和透明度；

实现燃料管理业务的整合，实现内部数据资源的高度共享。决策层能实时了解基础数据，调整、控制燃料采购、存储计划；依据完善的统计报表、科学的分析模型，为管理部门的数据对比和管理决策提供辅助支持；以精细化管理来降本增效。

对所有工作点视频监控，设立视频监控中心，记录验收过程的所有工作，并提供远程监察，形成完善的监控网。

3.5 高级智能应用系统

3.5.1 设置设备状态检修功能

设备是电厂最重要的资产，设备状态好坏直接影响到电厂运营质量。因此，设备检修也从：

已发生问题的纠正性维修==》定期的计划检修==》按等级的预防性检修 发展到了基于大数据分析来预测的状态检修。

1) 要实现状态检修，首先要有“设备智能预警”，它能够提前发现可能影响系统和设备的早期故障特征并发出预警(它与传统SIS中的“设备早期预警”的最大区别是：SIS中的是按设计或实验给出的固定阈值来判断，不具有按实际工况按设备模型自我分析能力)；

2) 要实现状态检修，核心是要有“专家知识库”，这是集合研究院、热工院、同类机组厂家、同类型兄弟单位的综合经验及智慧的知识库，它体现出技术共享及传承，将个人经验予以信息化编排，使得专家的价值最大化；

3) 要实现状态检修，还有一个背景是要实现设备全寿期管理，全面整合以KKS编码串联的设备数据，而不能是孤岛一样分散于各专业系统，实现厂级数据标准化和集中管控/利用。

3.5.2 设置智能巡检功能

在传统视频监视基础上，充分开发利用视频新技术，包括：

——视频融合技术：将多摄像头监拍的多幅画面予以智能融合，构成立体全息监控画面；

——视频分析技术：实现人员定位及跟踪，并与后端各专业系统进行融合，将信息展示在视频周边；

——红外热成像技术：对于温度敏感设备，通过红外热成像及时发现

设备异常状态；

可构建发展出“智能巡检系统”，实现：

（1）减少巡检次数。充分利用高新技术，通过视频移动监视现场环境及设备，实现无人化日常巡检。

（2）规划巡检路线。对于必需的一些巡检，自动实现巡检路线规划，有效规避危险点。

（3）人员跟踪定位。对于巡检人员通过位置定位，随时了解工作情况。

（4）应用系统融合。将实时运行信息、设备动态信息等集成到视频监视画面中。

（5）移动终端应用。将巡检功能作为一个移动App子应用，集中到移动平台上。

（6）设备检测诊断。将设备状态的异常变化推送给相关人员和其他综合性应用。

设置智能机器人系统，主要在输煤栈桥、煤场设置智能巡检机器人，减少巡检人员数量，降低巡检人员工作强度。

3.5.3 智能报表

智能报表模块是一套集成发电运行静态知识、统计辅助分析、动态因果关系辅助推理的智能化应用，智能报表功能的实现具有以下多方面的有益效果：

- 1) 自动生成报表，减少人工填报工作；
- 2) 及时响应报送要求，避免人为干预；
- 3) 统一指标库，方便管理人员对机组状况的掌握；
- 4) 报表可以自由定制，满足不同报表使用人员的需求。

3.5.4 智慧消防

针对火力发电厂火灾的特点（火焰温度高、蔓延速度快、设备相互威胁大、设备易爆裂、建筑结构易变形倒塌、易造成人员伤亡等），结合物联网、云计算等新技术发展，全方位监控电厂区域内的消防安保状况，实现预防预警、精确防控、及时处理，达到省时、省力、省钱的目标。将电厂内消防相关系统和DCS系统，通过物联网的方式，将数据信息化，上传至智慧消防系统，让消防工作各个部分深度融合、有机联动，提高消防处置效率。同时，结合人员日常巡检和数据分析等功能，建立“人防、物防、技防”三防结合，全面提升电厂消防隐患安全管理水平。系统主要功能包括在线监测、巡查检擦、智能分析、数据分析、事件中心和仿真培训。

3.5.5 汽轮机与大型转机可视化监测与诊断系统

根据电厂实际运维行情况，可在智能发电系统平台设置汽轮机与大型转机可视化监测与诊断系统功能模块，该功能模块分为两部分。一是汽轮机可视化监测与诊断系统，二是大型转机可视化监测与诊断系统。

汽轮机可视化监测与诊断系统通过对汽轮发电机组振动和轴系各种动静间隙的实时计算，在主控室运行员站屏幕上，以透视的方式实时监视汽缸内高速转动的各转子的运行状态；高精度显示各转子的动态间隙变化，包括各轴颈处的油膜厚度，盘车状态下的大轴顶起高度，各轴封间隙，各隔板汽封间隙等，根据间隙变化和机组的振动情况确定密封和机组的状态，并以不同的颜色显示。从运行员站上可以直观地判断机组常见的不平衡、不对中、油膜涡动、汽流激振、部件脱落、松动和碰摩等故障，具有形象生动，易于理解和准确可靠的特点。

大型转机可视化监测与诊断系统能够设置、采集、自动分析处理机械

设备的振动、超声波、红外探测等数据，在运行员站画面进行实时监视，自动给出分析诊断结果，及时报告机械设备的运转状态，并提供维护检修建议，协助设备管理工程师，做出科学的检修计划决策。大型转机的监测对象主要是一次风机、二次风机、引风机等。

对汽轮机及大型转机的可视化监测与诊断系统的合理使用，保守估计可延长主机大修时间1~3年，减少辅机检修费用30%以上；同时有效降低非停、降负荷和恶性事故的发生几率。

3.5.6 智能两票

在两票管理业务中融合人员定位、手机APP、二维码、声像监控等以及三维等技术，可实现两票管理三维升级。利用移动端替代传统纸票，实现无纸化操作，节省了打印和回填环节，运行人员在现场即可完成操作票的执行过程记录，提高工作完成的效率。工作票在开出后，由工作票的许可时间和结束时间作为时间要素，工作票的设备信息即设备的工艺位置作为空间要素，在系统监视环境中以时间要素和空间要素自动生成电子围栏。

电子围栏将形成自动报警区，借助人员定位和移动手机技术，对两票的工作负责人和工作班成员长时间离开电子围栏区域进行手机的振动或短信等报警提醒，对非工作成员的闯入，不但对闯入人员，同时对工作负责人和值班成员等进行手机的报警提醒，防止非工作人员误入设备间造成误操作。

3.5.7 数据集成、决策智能

分散在各个专业系统的数据通过“数据集成平台”可被清理整合为厂级公共数据，但如何有效利用这些数据成为企业难题（空有宝山而不知自用）。根据智能电站的发展趋势结合当前各种上层应用的特点，数据利用路线为：

(1) 统一数据模型。基于业务目的，根据要利用的数据信息，构建相应的分析模型。(杜绝私搭乱建，避免某些上层应用把自己建成了新的信息孤岛)

(2) 两大核心应用：智能采集上报系统+生产经营分析系统。这两系统恰恰体现出厂级数据利用的两个面，其一是将数据扁平化，通过对数据进行钩稽关联计算，直观展现某指标的值，常体现为二维报表；其二是将数据立体化，通过对数据的各个维度延展，表达同比、环比、占比等特性，常体现为分析图表；

(3) 数据共享复用。两大核心应用已经基本将厂级数据进行了覆盖加工，它们已产生了大量可被深层利用的分析数据（例如能耗指标、可靠性指标），这些数据可被“实时利润预测系统”和“竞价上网分析系统”等所持续利用，实现数据共享和价值再造。而深度利用的结果可回馈到电厂决策层，指导企业营销决策。

3.5.8 移动应用

现在移动应用在日常管理和办公过程中体现的重要越来越大，通过移动应用可以实时掌握企业生产经营情况，可以及时处理各项工作任务，实现随时随地都可以快速办公。移动应用提供业务流程实时审批（应该包括公文审批、任务审批、会议回执等）、关键指标即时查看（应该包括发电量、上网电量、供电煤耗、厂用电率等）等功能。移动应用通过统一门户应能实时推送实现事件与报警等。移动应用采用跨平台技术，能够同时支持苹果IOS和安卓手机及PAD等平台。

4 接口设计

4.1 与生产实时控制系统之间

机组DCS系统、辅助车间DCS系统、电网远程发送单元(RTU)等实时控制系统或装置通过单向隔离网闸接入实时数据库服务器，通过该服务器向数字化智能电厂运营平台提供所需的生产过程数据信息。

4.2 与集团公司信息系统之间

配置路由器与集团公司专网进行接入；

4.3 与广域网的接口

采用电信专线与互联网相连，光纤到信息机房。

采用VPN方式进行互联网连接，实现管理信息系统的远程管理功能。

5 网络安全防护

5.1 安全目标

信息安全的最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。

5.2 安全防护范围

信息安全主要包含物理安全、网络安全以及计算机系统安全。

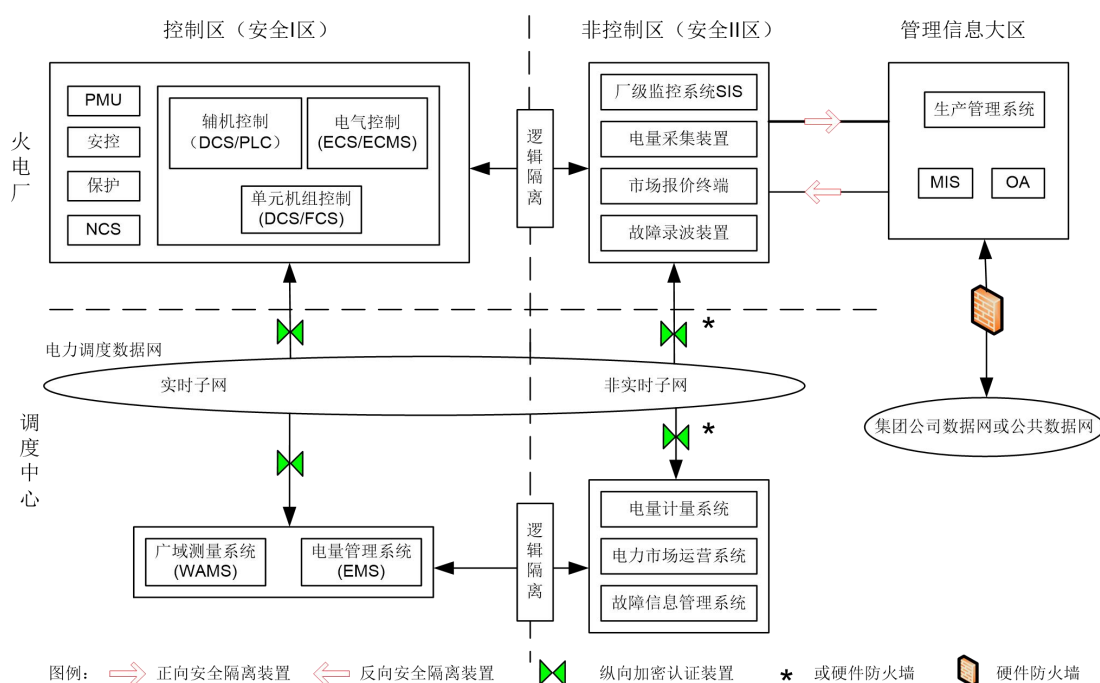
本工程信息安全主要指智能电厂信息系统、机组分散控制系统或现场总线控制系统（DCS/FCS）、可编程控制系统（PLC）等系统内部、相互之间以及与集团公司或公共数据网的接口在计算机硬件、软件、系统、网络、应用、数据等方面的信息安全。

5.3 安全防护原则

火力发电厂控制系统与信息系统安全防护的总体原则是“安全分区、网络专用、横向隔离、纵向认证”。重点强化边界防护，提高内部防护能力，保证生产控制系统及重要数据的安全。

5.3.1 安全分区

根据《电力二次系统安全防护总体方案》(国家电监会 2006 年 34 号令),火力发电厂控制系统与信息系统信息安全区域原则上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(又称安全区I)和非控制区(又称安全区II)。控制系统与信息系统信息安全分区以及边界防范措施拓扑图如下图所示:



5.3.2 网络专用

各控制系统网络应当在专用通道上使用独立的网络设备组网,采用基于不同通讯介质或者不同通道、不同光波长、不同纤芯等方式,在物理层面上实现各个控制系统的网络专用,并且与电力企业其它数据网及外部公共信息网的安全隔离。

同一控制系统业务类型（例如DCS/FCS）的控制网络应按单元机组以及机组公用部分划分不同的专用网络,全厂公用应采用独立的专用网络,用以实现同一控制系统业务类型在不同机组的网络专用。

5.3.3 横向隔离

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。

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、防火墙或者相当功能的设施，实现逻辑隔离。

控制区与非控制区之间应采用国产硬件防火墙、具有访问控制功能的设备或相当功能的设施进行逻辑隔离。

5.3.4 纵向认证

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。

对于重点防护的发电厂在生产控制大区与广域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或者加密认证网关及相应设施，实现双向身份认证、数据加密和访问控制。

5.4 安全定级

目前，国内应用的信息安全评价标准是国家质量技术监督局颁布的《计算机信息系统安全保护等级划分准则》GB 17859-1999。该标准将计算机信息系统安全保护能力划分为用户自主保护、系统审计保护、安全标记保护、结构化保护和访问验证保护 5 个安全等级。

国家质量技术监督局2001年颁布的《信息技术-安全技术-信息技术安全性评估准则》国家推荐标准GB/T 18336-2001。该标准定义了7个评价保证等级（Evaluation Assurance Levels, EAL）。以及按危害程度划分的标准《信息安全技术网络安全等级保护定级指南》GB/T 22240-2020。

标准等级越高，信息系统和技术产品的安全可信度就越高，几个标准等级的对应关系如下表（由低到高）：

GB/T 22240-2020		GB 17859-1999	GB/T18336-2001
安全等级	等级名称	保护能力	
			EAL1
第一级	自主保护	用户自主保护	EAL2
第二级	指导保护	系统审计保护	EAL3
第三级	监督保护	安全标记保护	EAL4
第四级	强制保护	结构化保护	EAL5
第五级	专控保护	访问验证保护	EAL6
			EAL7

根据【2022】471号国家能源局综合司关于印发《电力行业网路安全等级保护定级指南》，本工程管理信息系统安全按第二级执行，智能发电按第三级执行。

应严格根据《信息安全技术 信息系统安全等级保护测评要求》GB/T 28448-2019的要求周期进行等级测评。

5.5 网络安全规划

为满足等级保护要求，本工程拟采取的网络安全措施如下：

安全层次	项目	采取的安全措施或遵循标准	
安全物理环境	物理位置选择	1、机房场地建筑应具有防震、防风 and 防雨等能力 2、机房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。	
	物理访问控制	电子门禁系统	
	防盗窃和防破坏	设置防盗报警系统或视频监控系统。	
	防雷击	各类机柜、设施和设备等通过接地系统安全接地；设置防雷保安器或过压保护装置等。	
	防火	设置火灾自动消防系统、机房建设采用耐火材料等	
	防水和防潮	防水检测、报警；窗户、屋顶、墙壁采用防水方法；	
	防静电	防静电地板或采用静电消除器、防静电手环等	
	温湿度控制	机房空调/精密空调	
	电力供应	稳压器+UPS	
	电磁防护	应对关键设备实施电磁屏蔽；屏电源线和通信线缆应隔离铺设	
安全通信网络	网络架构	防火墙（基础级）/路由器/交换机；负载均衡、行为管理、综合网管系统	1. 干路设备、边界设备、汇聚层以上的设备、安全设备等设备性能冗余空间充足（路由器、交换机和防火墙提供网络通信功能的设备） 2、带宽在设计要求上满足需求上要有一定比例的冗余 3、划分 VLAN，业务系统网段合理划分、有效隔离，保护重要网段 4. 关键网络设备及安全设备要求冗余配置（如核心交换机、负载均衡、防火墙、行为管理等）

	通信传输	VPN	客户端到服务器、服务器到服务器之间要使用 SSL 等通信
安全区域边界	边界防护	防火墙（基础级）网闸、路由器和交换机、态势感知、终端管理系统、行为管理	端口级访问控制；控制非法联入内网；控制非法联入外网；无线的准入；边界访问控制策略
	访问控制	防火墙（增强级）、上网行为管理、网闸、路由器和交换机	边界访问控制策略（网闸、防火墙、路由器和交换机等提供访问控制功能的设备）；防火墙对应用识别，并对应用的内容进行过滤
	入侵防范	入侵防御、态势感知 抗 APT 攻击、抗 DDoS 攻击和网络回溯等系统	检测网络入侵行为；新型网络攻击的检测和分析
	恶意代码和垃圾邮件防范	防火墙（增强级）+防病毒模块；邮件安全网关	（防病毒网关和 UTM 等提供防恶意代码功能的设备或系统）防御网络恶意代码；垃圾邮件进行检测和防护
	安全审计	日志审计系统、堡垒机、行为管理、防火墙（基础级）、SSL VPN	（综合安全审计系统、路由器、交换机和防火墙等设备）启用日志功能；开启审计用户行为策略
安全计算环境	身份鉴别	主机配置项+VPN\运维堡垒主机+CA	1. 设备设置登录认证功能；用户名不易被猜测，口令复杂度达到强密码要求 2. 启用设备自身策略 3、使用 SSH、HTTPS 加密 4、双因素认证：用户名口令、动态口令、USBkey、生物特征等鉴别方式
	访问控制	主机配置项+防火墙（基础级），VPN,运维堡垒主机水印系统	主机配置项；主机配置项（权限分离）；基于应用的访问控制策略
	安全审计	防火墙（基础级）、日志审计系统	启用安全审计
	入侵防范	主机配置项+入侵防御,行为管理,漏洞扫描系统,态势感知、终端检测与响应平台	1、操作系统遵循最小安装原则 2、操作系统配置终端接入方式、网络地址范围；操作系统配置终端接入方式、网络地址范围 3、系统配置项（如登录对输入框输入的内容进行长度、位数及复杂度验证等）
	恶意代码防范	终端检测与响应平台	安全杀毒软件并及时更新库
	数据完整性	VPN; CA	系统使用 HTTPS, SSL
	数据保密性	VPN, 数据加密软件	
	数据备份恢复	数据备份软件+容灾备份系统, HCI, XYClouds	双活热备
	剩余信息保护	应用配置项	
	个人信息保护	行为管理	应用配置项
安全管理中心	系统管理	运维堡垒主机、APM、网管系统、SOC 平台等	
	审计管理	数据库审计、日志审计、运维堡垒主机	
	安全管理	运维堡垒主机、SOC 平台等	
	集中管控	运维堡垒主机、网管平台、终端	1、划分运维管理域，安全设备或安全组

		检测与响应平台管理平台、补丁分发系统、态势感知、SOC 平台、SOC 平台等	件集中管理 2、建立一条安全的信息传输路径 3、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 4、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 6 个月以上; 5、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 6、能对网络中发生的各类安全事件进行识别、报警和分析。
--	--	--	--

5.6 控制系统网络安全规划

5.6.1 安全物理环境

为满足等级保护要求，生产控制网络设置以下物理与环境安全措施：

- （1）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；
- （2）机房应设置防盗系统或专人值守的视频监控系统；
- （3）机柜、设施和设备等通过接地系统安全接地，做好防止感应雷措施；
- （4）机房及相关的工作房间做好防雷、防火、防水、防潮、防静电措施；
- （5）配备维护机房电力稳定供应的相关设备和冗余电力线路；
- （6）做好电磁防护，对关键设备实施电磁屏蔽。

5.6.2 安全通信网络

生产控制网络按照国家网络安全等级保护要求，接入网络的终端应进行合法性检查，对网络数据进行详细记录并可溯源分析，网内主机终端需进行安全防护，充分考虑智能发电平台的业务多样性，细化安全单元，严控边界防护，整体提升生产控制网络主动防御能力。

生产控制大区内个别业务系统或其功能模块需要使用公用通信网络、无线通信网络以及处于非可控状态下的网络设备与终端等进行通信时，应设立安全接入区。安全接入区与生产控制大区中其他部分的联接处应设置电力专用横向单向安全隔离装置。

5.6.3 安全区域边界

根据安全区划分，控制区网络边界主要有以下几种：生产控制大区内控制区（安全区 I）与非控制区（安全区 II）之间的边界；生产控制大区内部不同业务系统之间的边界；厂内生产控制大区 NCS 与电力调度数据网之间的边界。生产控制大区内控制区与

非控制区之间应采用电力专用正向隔离装置，其功能、性能、电磁兼容性需经过国家相关部门的认证和测试，隔离强度应达到或接近物理隔离，且满足火电厂对业务数据的通信要求。NCS 与电力调度数据网的纵向连接处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，与调度端实现双向身份认证、数据加密和访问控制。纵向加密认证设备配置要明确源 IP、目标 IP、端口等。

5.6.4 安全计算环境

对于发电厂 DCS、NCS 等人机交互站，生产云等关键应用系统的服务器，以及高级应用计算站、网络边界处的接口站等，应使用安全加固的操作系统，加固的技术标准和管理策略符合电力行业网络安全等级保护三级要求。加固方式包括但不限于：安全配置、安全补丁、采用专用软件或采用强化操作系统访问控制能力的安全操作系统以及配置安全的应用程序。

对登录网络设备、安全设备的用户进行身份鉴别及权限控制，设备应设置系统管理员、审计管理员、安全管理员，实现设备特权用户的权限分离。管理员登陆地址也应进行限制，口令复杂度满足安全要求。

生产控制大区的各主机应当关闭或拆除不必要的软盘驱动、光盘驱动、USB 接口、串行口、无线、蓝牙等，确需保留的需通过安全管理及技术措施实施严格监控。可通过主机加固等技术措施实现对 USB 外设进行管控，对移动介质的插入、拷贝、写入等操作进行审计。

应用系统应提供用户身份标识唯一和鉴别强度检查功能，保证系统中不存在重复用户身份标识；设置密码复杂度检查，禁止明文存储密码；配置登录失败处理功能，采取结束会话、限制非法登录次数和自动退出等措施。

生产控制大区内主机应采用免受恶意代码攻击的技术措施。对不适宜部署恶意代码防护的主机，可通过部署主机白名单软件进行安全防护。

关键主机设备、网络设备或关键部件应进行相应的冗余配置。对关键业务的数据定期进行备份。

5.6.5 安全管理中心

在关键生产系统内至少应部署一套安全审计系统。安全审计系统对生产控制大区内生产实时网络进行流量审计，包含对工控协议进行深度包协议解析，实时检测针对工业

协议的网络攻击、违规操作、非法接入等异常行为，及时发现隐藏在系统网络流量中的异常数据包。同时，安全审计系统还需对生产控制大区内操作系统、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、黑客的攻击行为。

5.7 信息系统网络安全规划

5.7.1 安全物理环境

数据中心机房满足以下要求：

(1) 根据 GB50174-2017《数据中心设计规范》要求，数据中心机房应至少按照 C 类机房进行建设。

(2) 数据中心机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

(3) 机房应设置火灾自动消防系统，能自动检测火情、自动报警、自动灭火。

(5) 应配置机房环境监控系统，包括温湿度、漏水检测、强制排水设备、机房专用空调、UPS 系统、视频、门禁、烟感等设备自身应配带监控接口，监控的主要参数宜纳入设备监控系统，通信协议应满足设备监控系统的要求。

5.7.2 安全通信网络

网络安全机构的核心交换、云平台的接入交换和存储设备设置冗余，满足接入终端实名要求，对终端访问进行详细记录并可溯源分析，充分考虑云平台、安全监测、安全运维的安全防护需要，整体提升管理信息网的网络安全主动防御能力。

核心网络设备采取 IP 和 MAC 地址绑定、动态 ARP 检测、DHCP 监听等技术，防止 IP 地址欺骗和 ARP 中间人攻击等威胁行为，防止数据在传输过程中被监听。管理信息网与互联网边界除硬件防火墙基本防护外，增加上网行为管理、入侵检测系统提升安全防护能力。

5.7.3 安全区域边界

(1) 管理信息网与广域网、无线网络、外委承包商等网络连接处需划分边界，边界至少部署硬件防火墙进行安全防护。

(2) 管理信息网与互联网边界除硬件防火墙基本防护外，还应增加上网行为管理、入侵检测系统提升安全防护能力。

(4) 网络边界入口实行入网安全规范技术，部署网络准入系统，对接入网络的系统设备进行入网合规性检查，防止非法入网，提高网络边界安全保护能力。

(5) 部署一套网络入侵防护系统，并合理设置检测规则，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。

5.7.4 安全计算环境

办公终端部署统一的病毒防护系统，集中监控终端准入管理、系统安全加固、终端安全审计等功能，能有效抵御已知病毒、未知恶意代码和 APT 有效攻击。服务器终端同样部署统一的病毒防护系统，同时对服务器操作系统进行主机加固。

服务器操作系统安装防病毒系统，并对所有服务器操作系统进行主机加固，提升操作系统安全级别，统一网络安全保护平台实现对主机加固及运行状态进行实时监测，确保相关服务器操作系统主机加固有效符合操作系统安全级别标准要求。服务器主机系统应采取数据安全保护措施，提高数据安全应急能力，满足数据应急恢复需求。

应用系统提供用户身份标识唯一和鉴别强度检查功能，保证系统中不存在重复用户身份标识；系统应设置用户首次登录时修改初始密码；禁止明文存储密码；配置登录失败处理功能，采取结束会话、限制非法登录次数和自动退出等措施。严格限制默认帐户的访问权限，授予不同帐户为完成各自承担任务所需的小权限，并在它们之间形成相互制约的关系。

建立自动备份系统，实现重要数据备份与恢复。定期进行备份数据恢复测试，测试应在测试环境中进行，确保实际备份数据的异机可恢复性，测试过程应做好记录及分析。

5.7.5 安全管理中心

部署一套安全审计系统，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、黑客的攻击行为。特别对于远程用户登录到本地系统中的操作行为，应进行安全审计。同时部署一套堡垒机，并采用双因素认证，能够对设备系统的运维操作进行全面记录，具备运维审计自查询功能。