# 安全可信智能电厂控制系统构建方案*

王 翔,申志伟,朱肖曼,郭 烁,李 玲
(华北计算机系统工程研究所,北京 100083)

**摘 要**:随着火电厂信息化建设的快速推进,工控系统将实现高度数字化和智能化,对传统控制系统的计算、存储以及安全防护能力提出了较高的要求。基于中国电子 PK 体系,提出一种自主安全可信的智能电厂控制系统构建方案,通过云边协同机制,有效提高工业控制系统的边缘计算能力和基于自动预判、自主决策的智能化水平;进一步基于网络安全防护规定,提出了云-网-端一体化的积极防御体制。

**关键词**:工业控制系统;安全可信;智能电厂;边缘计算;云平台
**中图分类号**:TN914 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.212018

**中文引用格式**:王翔,申志伟,朱肖曼,等. 安全可信智能电厂控制系统构建方案[J].电子技术应用,2022,48(5):56-60.
**英文引用格式**:Wang Xiang,Shen Zhiwei,Zhu Xiaoman,et al. Method of constructing a secure and trustable industrial control system in smart power plant[J]. Application of Electronic Technique,2022,48(5):56-60.

# Method of constructing a secure and trustable industrial control system in smart power plant

Wang Xiang,Shen Zhiwei,Zhu Xiaoman,Guo Shuo,Li Ling
(National Computer System Engineering Research Institute of China,Beijing 100083,China)

**Abstract**:With the rapid advancement of informatization construction of power plants, industrial control systems will achieve a high degree of digitization and intelligence, which puts forward higher requirement for the calculation, storage and safety protection capabilities of traditional control system. Based on the PK system of China Electronics Corporation (CEC), this paper proposes a secure and trustable industrial control system in smart power plant. The cloud edge collaboration can effectively improve the capability of edge computing and the level of intelligence based on automatic prediction and independent decision-making mechanism. Besides, based on the network security protection regulations, a cloud-network-end integrated active defense system is proposed.

**Key words**:industrial control system;secure and trustable;smart power plant;edge computing;cloud platform

## 0 引言

随着火电厂信息化、数字化、智能化技术的快速发展,移动互联网、云计算、大数据、人工智能和物联网等新型互联网技术广泛渗透并应用到现代化数字电厂的建设中[1-2],智能发电技术已成为全面提高电力系统运行效率、推动能源革命的必然趋势。目前,智能电厂的建设主要集中在将先进互联网技术在非生产侧应用层进行适配、推广和应用(如通信系统实时性升级改造、电厂数字孪生、人员定位、智能巡检、设备故障诊断和工业大数据平台[3-5]);而运用先进互联网技术对生产侧控制系统智能化升级改造,用来指导调度、决策和运维的应用案例较少。随着火电厂智能化技术的推进,现有火电厂控制系统的带宽和计算能力无法满足智能化工业场景下高实时、大宽带、强安全的信息通信要求,难以从整体提升平台的协作能力和智能化水平[6]。

本文提出一种基于飞腾(Phytium)芯片和麒麟(Kylin)操作系统(PK 体系)的自主安全智能电厂控制系统构建方案。该方案将传统的 3 层控制系统模型优化为 5 层模型结构,在现场设备层和平台层之间增加既能提供边缘计算能力又具备多协议解析、区块链、可信计算、密文传输、数字签名等多技术属性的边缘层。该方案通过云边协同互补,有效提高电厂控制系统的智能化运行能力和整体安全防御能力,有效提升火电厂自动化控制系统自动预判、自主决策和自我演进的能力。

## 1 电厂工控系统模型

### 1.1 火电厂工控系统模型

现有火电厂工控系统模型如图 1 所示,由设备层、控制层和监控层 3 层模型结构构成基本模型[7]。

设备层主要包括现场各种仪表、传感器、变送器和执行器。该层靠进被控工艺生产过程,将生产过程的各

* 基金项目:北京市科技计划项目(Z191100004619003)

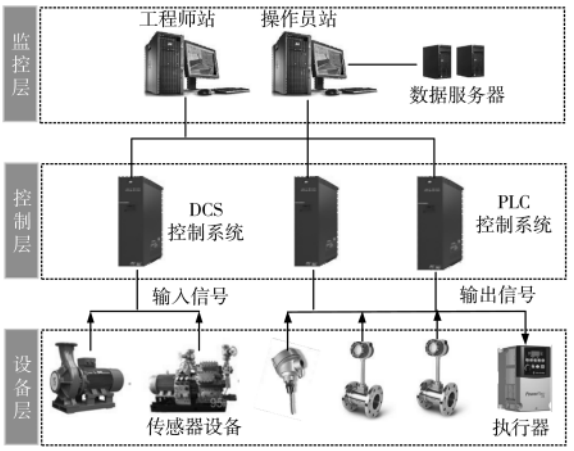


图 1 传统工控系统模型

种物理量转换为电信号。

控制层主要由现场控制站和数据采集站构成，用以完成数据采集与处理和分散控制任务。一般在火电厂中，现场控制站和数据采集站集中安装于主控室后面的电子设备室中[8]。现场控制站通过现场仪表直接与生产过程相连接采集过程变量信息，并进行转换和运算等处理，产生控制信号以驱动现场的执行机构，实现对生产过程的控制。现场控制站可控制多个回路，具有极强的运算和控制功能，能够自主地完成回路控制任务，实现反馈控制、逻辑控制、顺序控制和批量控制等功能。数据采集站接收大量的过程信息，并通过监控级设备传递给运行人员，数据采集站不直接参与控制。

监控层的主要设备包括操作员站、工程师站和数据服务器等附属设备[9]。监控层构成控制系统的人机接口，用以完成集中监视、操作、组态和信息综合管理等任务。

### 1.2 火电厂安全可信智能控制系统模型

依托飞腾芯片和麒麟操作系统，提出一种安全可信智能控制系统构建方案。该方案在传统的设备层和控制层之间增加了边缘层，控制层之上增加了云平台层和应用层。将传统的 3 层控制系统模型改为设备层、边缘层、控制层、平台层和应用层 5 层模型结构，如图 2 所示[10-11]。

设备层、控制层和监控层主要功能与现有火电厂工控系统一致。安全可信控制系统模型中边缘层既可以提供边缘计算能力，又具备多协议解析、区块链、可信计算、密文传输、数字签名等多种技术属性，实现设备泛在连接。云平台层融合大量的基础工艺技术原理与行业知识，集成可重复使用的组件，是一个可扩展的操作系统，为应用软件开发提供一个基础平台。边缘层和云平台之间协同互补，实现云边协同，有效提高火电厂控制系统的智能化和整体安全防御能力[12]。

## 2 安全可信智能电厂控制系统模型

安全可信智能电厂控制系统主要流程示意如图 3 所示。

现场设备层靠近被控生产过程附近，主要包括各种

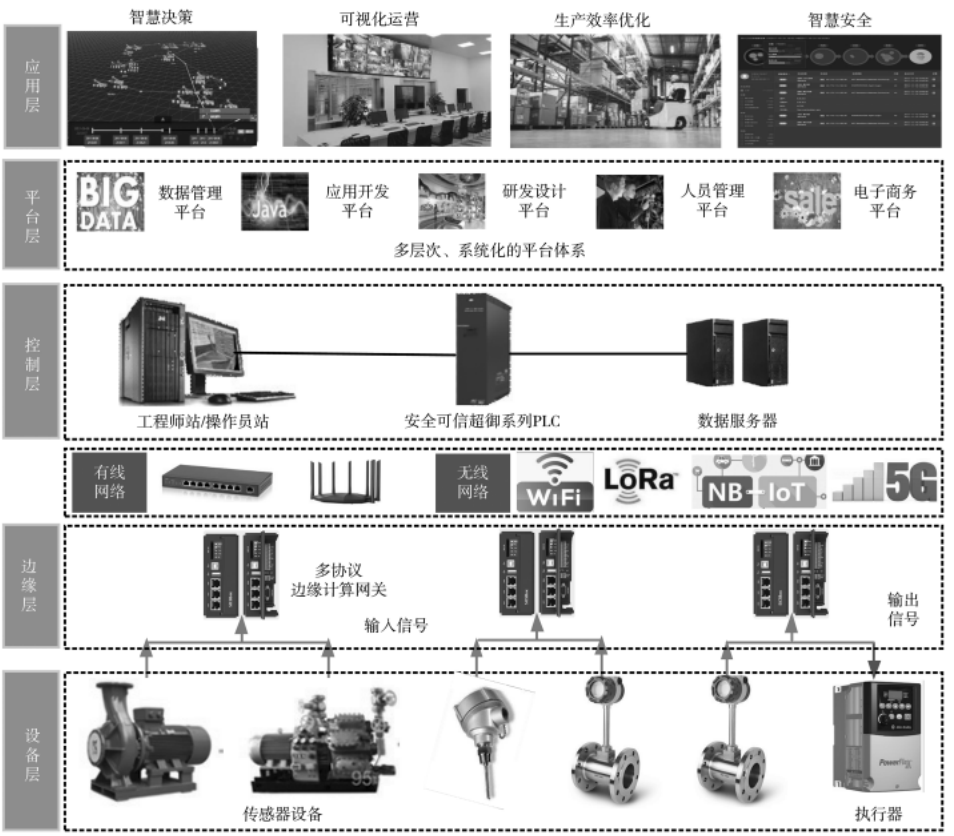


图 2 传统工控系统模型


《电子技术应用》http://www.chinaaet.com

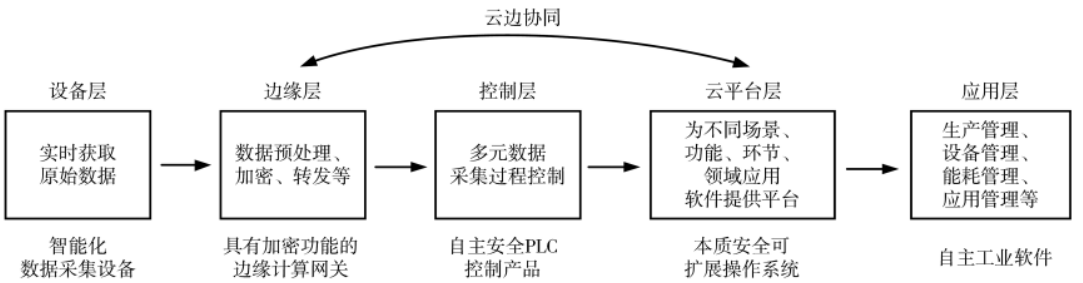


图 3 安全可信智能电厂控制系统流程图

智能化的数据采集设备，实时获取原始数据。与传统设备层的主要区别在于：由数字量及模拟量为主的数据模式转变为以图像、视频为主的多元数据模式[13]。

边缘层设备靠近网络边缘侧，主要设备为一系列高性能的边缘计算网关，实现多元数据接入以及处理、转发、安全防护等边缘功能[14]。该网关支持有线和无线通信模式，包含 100 多种工控协议解析模块，具有防解析、防篡改的数据加密功能。边缘层设备将计算任务从云计算中心迁移到数据原头，基于实时的大数据形成自主决策分析能力，有效解决了智能化控制系统数据量大、处理能力不足、传输时延大的问题。

控制层设备主要为一系列自主安全可编程逻辑控制器(Programmable Logic Controller，PLC)。自主安全 PLC 融合可信启动模块，实现控制系统的本质安全，具备逻辑顺序控制、定时和计数等功能[15]。系统启动时，先执行只读存储器中相关验证逻辑，对操作系统软件进行完整性度量，只有通过验证才能正常执行启动操作系统。

云平台层将生产环节中涉及的技术原理和知识，规则化、软件化和模块化处理，为不同的应用场景、功能、环节、领域应用软件的二次开发提供一个可扩展的操作系统。云平台可实现不同设备间数据信息的相互嵌套、集成、调用、交互和深度融合，完成边缘层无法胜任的计算任务。除此以外，云平台层可直接接入互联网“云安全”病毒库，构建“云－网－端”一体化的控制系统防御体系。

应用层主要是面向特定的应用场景，以各种软件的形式提供特定的服务。基于软件系统分析结果，构建全厂域内的数字孪生系统，建立集中显示指挥中心，实现分析预测、态势感知、智慧调度、智慧决策和智慧运维等功能。

## 3 典型应用案例分析

汽轮机冷端系统是火电厂热力系统中重要的系统，为了维持发电系统较高的能量转化效率，其必须时刻控制在一恰当的背压。由于实际运行中影响该系统运行状况的因素众多且复杂，因此传统的调节手段很难做到精细化调节，影响发电效率。

基于智能电厂控制系统建设方案，在原有控制逻辑基础之上，增加与汽轮机抽真空系统结合的具有边缘计算能力的网关设备，实时收集风机集群流量和环境温度、风速、风向等参数，从而使空冷岛具备自我学习、调节优化的功能。基于冷端智能优化，可以实时调整机组背压，如图 4 所示。

将人工智能技术与控制机理模型结合，优化抽气风机的运行流程，建立从结果到原因的先进反向控制逻辑，有效解决 PID 逻辑算法无法精准卡边控制的问题，使机组实时运行在最佳背压，节能增效，为企业带来可观的收益。

## 4 智能电厂控制系统安全防护方案

能源企业是我国经济社会稳定运行的重要基础设施，因此火电厂工控系统安全是网络安全的重中之重。早期的火电厂工控系统完全隔离于互联网，很少受到信

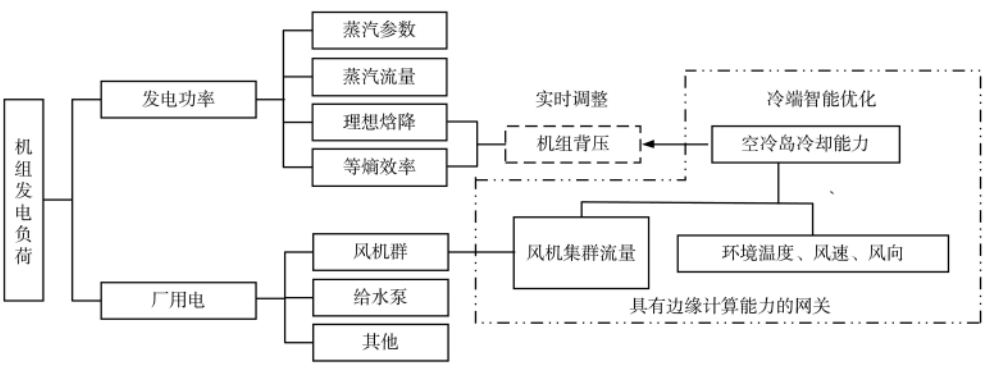


图 4 基于边缘计算网关的汽轮机冷端系统

息安全方面的威胁。智能电厂控制系统融合大量新一代信息技术，打破了工控系统与互联网之间的物理界限，所面临的网络安全问题更加严峻。

针对智能电厂控制系统边缘侧和网络侧面临的攻击、渗透等新型风险问题，提出基于入侵防御系统、主机安全防护系统、网络安全防护网关、检测与审计系统和统一管理平台为核心的云-网-端一体化工控网络安全积极防御整体方案，如图 5 所示。

网络安全防护网关：在火电厂生产网(主控设备、辅控设备)与办公网间以及工控网络出口位置处部署网络安全防护网关产品。其具有阻止来自外部系统攻击、系统间的越权访问、恶意软件扩散和入侵攻击和保护控制系统安全运行的功能。

主机安全防护系统：在工控系统的关键主机和服务器中安装主机安全防护系统。主机安全防护系统主要有统一身份认证和主机白名单类两类产品。其中：统一身份认证可保障主机和服务器不被非法用户控制；主机白名单可有效阻止非授权软件或进程的安装和运行，变被动为主动，杜绝信息非法窃取、数据和系统遭受非法破坏的行为发生。

入侵防御系统：在网络出入口核心交换机旁路部署入侵检测类产品，实时检测来自办公网及其他网络区域恶意软件的入侵，帮助客户及时采取应对措施，避免发生事故。

网络检测与审计系统：在工控网络旁路部署网络监测与审计类产品，监测网络中的恶意攻击、误操作、违规行为、非法设备接入以及恶意软件的传播，并详实记录网络通信流量，为安全事故调查取证提供技术支撑。

态势感知平台：借助大数据分析技术，建立态势感知平台，实时监控网络运行状况，对工控系统内引发安全态势变化的多种因素进行分析处理，建立威胁信息共享机制，把握网络安全事件发展趋势，确保网络系统运行的安全稳定，大大提升网络风险防控能力。

云-网-端一体化的工控网络安全积极防御方案贯穿设计、运行、服务等全生命周期，从设备安全、控制安全、网络安全、数据安全、应用安全、管理安全等多个方面全面提高了关键基础设施行业工控系统的体系化防御能力。

## 5 结论

面向火电厂信息化、智慧化建设的新需求，本文提出一种安全可信的智能电厂控制系统构建方案。该系统引入了云-边协同机制，从设备侧提高了工控系统边缘计算能力和智慧化水平；建立数据平台，实现工控系统内数据深度交互与融合，形成基于自动预判、自主决策的智能化水平。鉴于智能电厂控制系统面临的新型攻击、渗透等风险问题，基于自主安全的工控设备，提出云-网-端一体化工控网络安全积极防御整体方案，从硬件、软件和数据等方面提高了工控系统的整体安全防御能力。

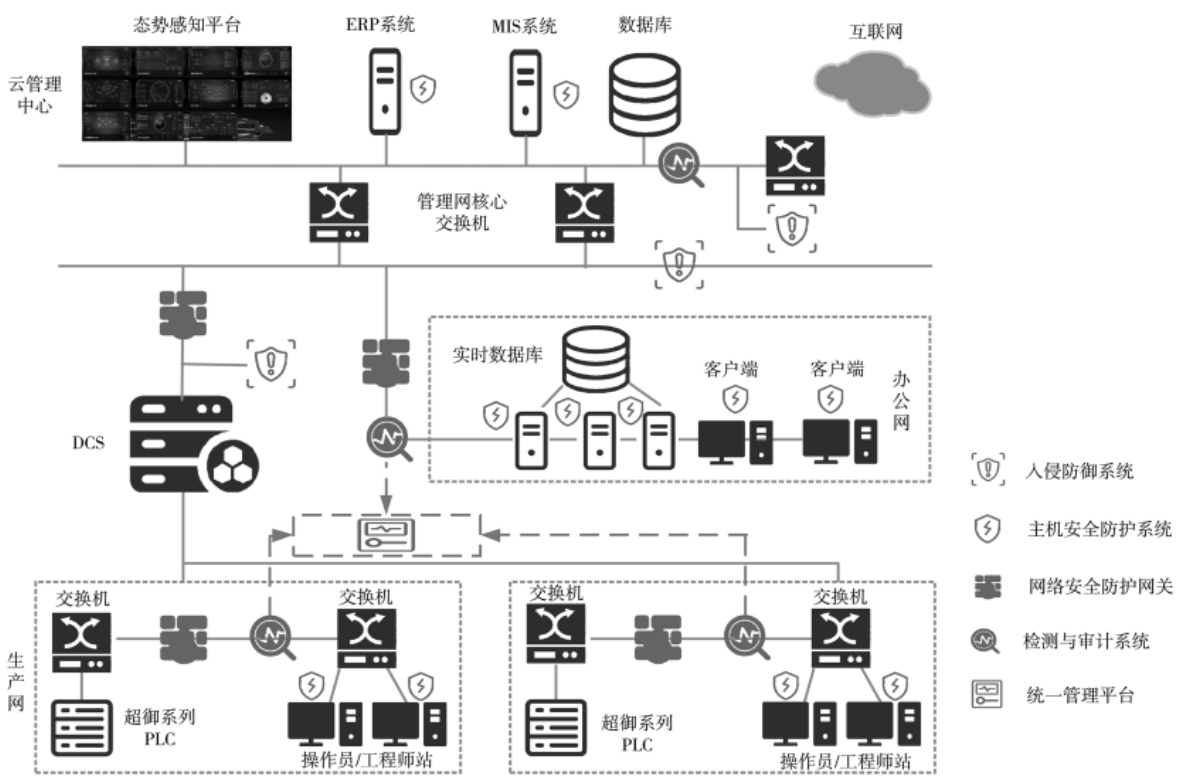


图 5 智能电厂控制系统安全防护方案


《电子技术应用》http://www.chinaaet.com

参考文献
[1] 马振涛,李奇颖.基于数据湖的智慧电厂 IMS 平台建设及应用[J].中国信息化,2020(12):84-85.
[2] 赵东.火力发电厂中智慧电厂存在的问题和优化对策研究[J].电气技术与经济,2020(6):9-11.
[3] 梁涛,李宗琪,姜文.火电厂智能化远程管理云平台系统设计[J].中国测试,2020,46(2):103-109.
[4] 杨新民,曾卫东,肖勇.火电站智能化现状及展望[J].热力发电,2019,48(9):1-8.
[5] 王瞳,杨爽.火电机组智能发电控制系统架构简述[J].东北电力技术,2021,42(3):44-46.
[6] 赵志楠.电厂热控自动化系统稳定性研究[J].技术与市场,2021,28(1):144-145.
[7] 王志纲,范秋香,马高衔.火电厂燃料智能化采制样系统平衡风装置研究[J].电力科技与环保,2020,36(6):58-59.
[8] 王邓.基于数字化形势下的火电厂智能化转型分析[J].中国新通信,2017,19(2):81.
[9] 黄刘松.浅析大数据平台在火电机组的应用前景[J].科学技术创新,2019(32):58-60.
[10] 李林枫,黄晶晶,李琳.工业控制系统安全分析及渗透测试经验分享[J].自动化博览,2021,38(1):48-53.
[11] 刘蔚棣,郭乔进.工业控制系统安全发展综述[J].信息化研究,2021,47(1):1-9.
[12] 赵悦琪,赵德政,林浩.工业控制系统安全防护体系研究[J].电子技术应用,2021,47(1):69-72.
[13] 邵诚,钟梁高.一种基于可信计算的工业控制系统信息安全解决方案[J].信息与控制,2015,44(5):628-633.
[14] 倪旻,范菁,李晨光.工业控制系统信息安全防护技术研究综述[J].云南民族大学学报(自然科学版),2020,29(6):619-627.
[15] 丰大军,张晓莉,杜文玉,等.安全可信工业控制系统构建方案[J].电子技术应用,2017,43(10):74-77.

(收稿日期:2021-08-10)

作者简介:
王翔(1989-),男,博士,工程师,主要研究方向:工控信息化建设、网络安全等方面咨询设计。
申志伟(1980-),男,博士,正高级工程师,主要研究方向:云计算、网络安全、人工智能、大数据应用、移动互联网等产品研发。
朱肖曼(1979-),女,硕士,高级工程师,主要研究方向:网络安全、通信网络等。

扫码下载电子文档

(上接第 55 页)

[12] CHEN C,LIU Z.Broad learning system:an effective and efficient incremental learning system without the need for deep architecture[J].IEEE Transactions on Neural Networks and Learning Systems,2018,29(99):10-24.
[13] 张红斌.电力系统负荷模型结构与参数辨识的研究[D].北京:华北电力大学,2003.
[14] LE T,KANG H,KIM H..Household appliance classification using lower odd-numbered harmonics and the bagging decision tree[J].IEEE Access,2020,8(1):55937-55952.
[15] 江帆,杨洪耕.基于广义回归神经网络的非侵入式负荷识别方法[J].电测与仪表,2020,57(3):1-6,18.
[16] TAVEIRA P,MORAES C,LAMBERT-TORRES G.Non-Intrusiveidentification of loads by random forest and fire-works optimization[J].IEEE Access,2020,PP(99):1.

(收稿日期:2021-11-15)

作者简介:
王毅(1981-),男,博士,副教授,主要研究方向:宽带电力线载波通信、智能电网用电信息采集系统。
王萧阳(1996-),通信作者,男,硕士研究生,主要研究方向:非侵入式负荷监测,E-mail:tha031076@163.com。
李松浓(1980-),男,博士,高级工程师,主要研究方向:用电信息采集系统。

扫码下载电子文档

# 版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所