基于Ability企业级工业互联网数据平台的危险源及能耗数据安全传输

张鹏军　张代华　訾旭华　闫小丽
内蒙古伊泰煤炭股份有限公司　内蒙古鄂尔多斯　017000

摘　要：随着煤化工流程行业工业互联网及大数据技术应用越来越广泛的数字经济发展背景下，结合公司运营实际状况，在跨区域的三地不同子公司之间建立统一的Ability企业级工业互联网数据平台，采集DCS、PLC、SCADA、GDS、SIS、ITCC等生产过程系统数据，并将数据归一化融合处理存储到平台，对这些数据分析应用与结果展示。与此同时，按照政府行管部门要求，将重大危险源、能耗双控等数据筛选出来上传至指定数据系统。在项目整体实施过程中，工业互联网数据平台系统实现了网络架构整体优化设计及信息网络安全可靠、数据简单方便传输与扩展应用。

关键词：工业互联网数据平台；生产过程系统；融合；重大危险源；能耗双控数据；网络架构优化设计；信息网络安全；数据传输与扩展应用

Based on Ability enterprise industrial Internet data platform Safe transmission of hazard and energy consumption data

Pengjun Zhang, Daihua Zhang, Xuhua Zhang, Xiaoli Yan
Inner Mongolia Yitai Coal Co., LTD., Ordos 017000, Inner Mongolia, China

Abstract: Under the background of digital economy development with more and more extensive application of industrial Internet and big data technology in coal chemical process industry, and combined with the actual operation situation of the company, the unified Ability enterprise-level industrial Internet data platform has been established between different subsidiaries in three places across the region. It collects DCS, PLC, SCADA, GDS, SIS, ITCC, and other production process system data, stores the data in the platform with normalized fusion processing, analyzes and applies these data, and displays the results. At the same time, according to the requirements of government administration departments, the data of major hazard sources and energy consumption dual control will be screened out and uploaded to the designated data system. In the overall implementation process of the project, the industrial Internet data platform system has realized the overall optimization design of the network architecture, the information network is safe and reliable, and the data is simple and convenient for transmission and extended application.

Keywords: industrial Internet data platform, production process system, fusion, major hazard, energy consumption dual control data, network architecture optimization design, information network security, data transmission and extended application

引言：

以伊泰煤制油、伊泰化工公司两个生产运营企业为依托，建成企业级工业互联网大数据平台，跨越东胜集团公司、杭锦旗伊泰化工公司、大路煤制油公司三地的大数据基础平台，采集伊泰煤制油、伊泰化工两运营工厂DCS、PLC、SCADA等生产过程实时数据以及视频信号等，集团公司收集SAP系统销售、库存等关系型数据进入大数据平台分类型存储，从而奠定大数据平台基础，然后根据生产业务需求实现跨地跨域跨类型数据融合。可以解决企业普遍出现的信息孤岛问题，通过统一的数据平台，融合各种自动化系统、信息系统数据，通过数据安全防控手段确保数据及信息网络安全，以此促进数

据口径的一致性，为数据应用专题提供强有力的数据支撑。在应用管理方面搭建数据平台与绩效分析应用，通过数据自动流转、数据分析传输自动化，减轻工作人员繁复的数据提报工作量。

1　跨地跨域数据采集与融合

数据平台作为智能工厂建设的基础，包括所有智能工厂建设过程中所需的数据采集与整合、数据分类与应用、数据开发、数据接口与集成等功能，是完成项目所需所有软件和与之配套的重要基础。考虑到数据平台需要从DCS控制系统、PLC控制系统、电气SCADA系统、视频监控系统进行数据采集与传输。

Ability工业互联网平台是实现智慧集团智能工厂的基础，所有智能工厂功能可在这个基础上实施。在数据平台基础上实现边缘智能应用模式，面向煤化工行业平台数据采集与开发的通用需求，依托工业互联网平台支持多源异构数据的归一化和边缘集成，利用协议转化，开展平台边缘侧数据预处理、存储以及智能分析，提供边缘设备实时异常检测、实时运行环境分析等应用服务，实现多工业通信协议兼容及数据间互通，增强平台实时分析能力，并与云端分析的协同集成。

Ability数据管理平台是一种基于Web的工具，支持Hadoop集群的创建、管理和监控。数据管理平台支持大多数Hadoop组件，包括HDFS、MapReduce、Hive、Pig、Hbase、Zookeeper、Sqoop和Hcatalog等；除此之外，数据管理平台还支持Spark、Storm等计算框架及资源调度平台YARN。数据管理平台从集群节点和服务收集大量信息，并把它们表现为容易使用的，集中化的接口。数据管理平台通过Web形式显示诸如服务特定的摘要、图表以及警报信息[1]。

数据平台采集生产过程DCS分散控制系统、PLC可编程控制系统、电力综合自动化数据采集系统SCADA、GDS有毒可燃气体检测系统、ITCC汽轮机压缩机集成控制系统、SIS安全仪表系统等不同过程控制系统的实时数据，采集视频监控信号，并根据业务需求整合ERP（Enterprise Resource Planning企业资源计划管理系统）SAP等关系型数据，实现数据跨域融合。项目实施过程中，数据平台对东胜集团公司总部、准格尔旗大路煤制油公司、杭锦旗伊泰化工公司三地联网，实现数据融合（如图1），统一管理与应用。

对于数据采集存储按集团公司统一制定的数据汇总规则执行。1）针对实时采集的数据，要求所提供的现场服务器或管理机实时采集的数据应通过工业标准协议（包括OPC Da，OPC Ua）或modbus TCP/IP modbus TCP/slave上传至智能工厂数据平台。2）针对离线采集的数据采集，结构化数据存储到关系型数据库，如myql、oracle、DB2等；非结构化数据支持json、xml格式；3）针对采集频率不高的数据，需要支持webservice、API等上层传输协议推送或拉取至智能工厂数据平台，同时支持数据EXCEL导入导出功能。

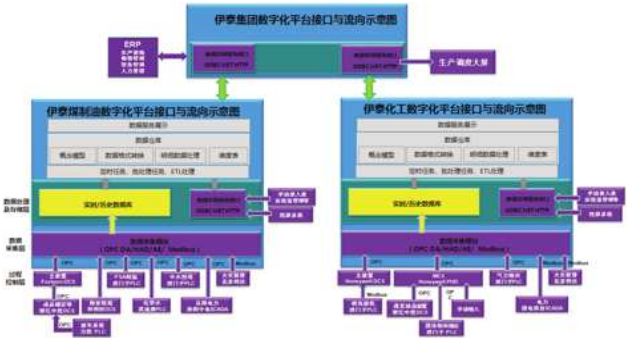
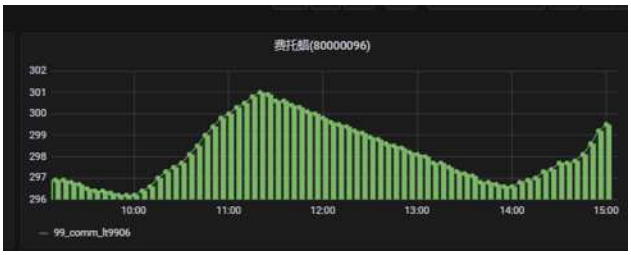


图1　三地多种协议数据采集与融合

伊泰煤制油公司通过数据平台采集生产过程主装置FOXBORO DCS系统、稳定轻烃浙江中控DCS系统、3套水系统PLC、PSA制氢PLC系统、深圳中电电力综合自动化SCADA系统等7套不同过程控制系统数据的采集，每秒采集实时数据达到19195多点，详见表1。



数据平台历史数据显示

表1　煤制油各PCS生产过程系统数据采集融合一览表

序号	系统名称	数据库部署点	通讯协议	采样频率
1	全厂FOXBORO DCS	12038	OPC Da	1次/S
2	电力SCADA系统	4794	modbus	1次/S
3	稳定轻烃和利时DCS	370	OPC Ua	1次/S
4	PSA制氢PLC系统	199	OPC Ua	1次/S
5	化学水PLC系统	338	OPC Ua	1次/S
6	中水回用PLC系统	1186	OPC Ua	1次/S
7	污水PLC系统	270	OPC Ua	1次/S
	总计	19195		

1.1 煤制油公司主生产装置Foxboro DCS系统数据采集

FOXBORO DCS系统是煤制油公司全厂底层过程控制中的主要数据来源，涉及水系统、锅炉、空分、气化、净化、合成、加工、罐区等各个装置或单元，在全厂范

围内统一管控底层生产设备的运行。将FOXBORO DCS OPC数据采集软件安装到数据平台服务器，在软件许可授权范围内把底层过程控制数据通过网闸、防火墙等网络安全防护设备采集到Ability数据平台，将全厂各装置生产过程数据抽取AI、AO、DI、DO、流量累计等点类型的实时值（1次/秒）共计12038点的采集部署工作。

成品罐区、新中间罐区等装置由浙江中控DCS系统控制，该系统数据通过OPC方式传输到Foxboro DCS系统，再通过Foxboro DCS主系统将数据平台。

数据平台与主装置Foxboro DCS系统通过OPC协议通讯连接，Foxboro DCS具有OPC授权软件、在数据平台采集节点服务器上安装Foxboro DCS系统的OPC专业软件，并配置OPC协议相关设置。通过硬件防火墙进行隔离。

传输方式：单向传输。Foxboro DCS系统→数据平台。

1）防火墙设置网络安全策略

防火墙外网到内外、内网到外网全部禁止访问。

2）防火墙设置内网到外网访问的白名单访问权限

设置防火墙内网到外网访问的具体的源主机和目地主机及目地服务。

3）防火墙设置外网网到内网访问的白名单访问权限

设置防火墙外网到内网访问的具体的源主机和目地主机及目地服务。

1.2 PSA制氢生产装置西门子S7-400控制系统数据采集

数据平台服务器采用OPC协议试着建立与PLC通讯时，并在其系统中配置了OPC协议，经测试通过Matricon OPC软件可读取到数据。然而，将防火墙安全隔离设备搁到系统中按系统说明配置好之后，却读不到数据。考虑服务器运行安全性，利用个人笔记本电脑模拟通讯场景，采用OPC与modbus两种不同通讯协议交换测试，经过反复测试获得成功，采用的测试方法与步骤是：

（1）设置PLC系统计算机操作系统的防火墙，将防火墙设置为关闭模式。

（2）DCOM设置用户，建立administrator，everyone。激活远程和启动权限，三个用户都增加权限。

（3）OPCEnum属性设置。在常规选项中将默认（原来）改为连接模式。

1.3伊泰化工数据采集

霍尼韦尔DCS系统涉及19套系统，主要有锅炉、水煤浆气化、粉煤气化、污水、化学水、净化、硫回收、合成、加工等装置，这些DCS系统已传输到MES系统。除了霍尼韦尔DCS系统，其余固体物料储运西门子S7-400 PLC系统、蒸发结晶浙江中控DCS系统通过OPC协议数据到实时数据库。

国电南自电力SCADA系统其数据采集不支持OPC协议传输，在电力侧需将电力数据转换为Modbus RTU协议，在数字平台侧再将Modbus协议转换为OPC协议。因SCADA系统有多套系统，将不同站号的设备串联后进行通讯，Modbus RTU设置为相同通讯参数；

2 信息网络安全

数据采集过程中，经网闸、防火墙双层硬件防护，实现企业级工业互联网大数据平台及底层控制系统的网络安全，并结合大数据软件安全防护功能，构成信息网络安全体系（如图2）。

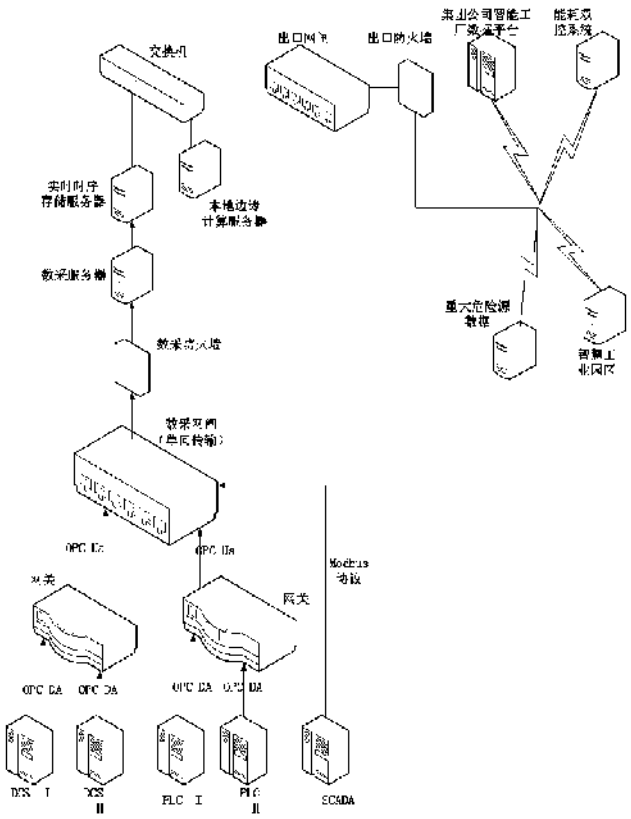


图2 信息网络安全架构

2.1硬件网闸

网闸采用摆渡功能，内外网主机与数据交换区之间采用非网络物理连接，通讯采用私有协议，彻底杜绝未经授权数据通过，保障内外网之间的通讯安全。防火墙设置网络白名单模式，设置端口白名单访问权限，对于底层控制系统设置为单向传输模式，只允许控制系统向上传输数据到系统平台，不允许系统平台反向传输数据。依次保证信息网络安全。

外网能耗端设备安全隔离传输。独立双主机“2+1”，即由外部处理单元、内部处理单元、隔离安全

数据交换单元构成网络隔离设备架构，内、外部主机通过专用隔离部件组成的安全隔离数据交互单元连接，安全隔离数据交互单元是两个网络之间唯一的可信物理信道。该内部信道裁剪了TCP/IP等功能网络协议，采用私有协议实现协议隔离，由此避免外界信息的侵入。

2.2 防火墙隔离防护

对于控制系统均采用单向传输，只允许控制系统向上传输数据到系统平台，不允许系统平台反向传输数据。同时采用防火墙思科CISCO FFP2110-ASA-K9进行硬件隔离。网络安全主要有硬件防护，具体为：

（1）防火墙设置网络白名单访问权限。只允许设计的白名单通过网络访问系统，如伊泰OA系统，DCS系统及数字化平台软件。

（2）防火墙设置端口名单访问权限。在防火墙网络端口设置各流入数据相互隔离，不允许相互访问，以此设置访问权限，保证网络安全。各流入数据中含有FOXBORO DCS系统、和利时DCS系统、PSA PLC系统等，通过防火墙设置将这些数据相互阻断。

（3）防火墙设置单端单向访问设置，只允许控制层（DCS或PLC系统）向上层（数据平台中数据采集服务器）传输数据，不允许数据平台向下层控制层传输数据，保证系统网络安全可靠。

2.3 系统网络架构的安全策略

2.3.1 单套控制系统如何阻止来至其它控制系统的入侵

各控制系统连接入三层交换机/防火墙，通过三层交换机/防火墙的端口隔离设置达到不能互相访问，只能和本地二层交换机连接的端口进行通讯。这意味着位于二层的各控制系统之间的网络访问权限被隔断了，不允许相互访问，以此保证各控制系统的独立性和安全性。

2.3.2 各控制系统和数字化平台本地服务器安全策略

通过防火墙的单向访问策略设置，连接控制系统三层交换机的防火墙端口仅被有限的、特定的几个IP访问，而且设置只读属性，以此来保证通讯的有限性。

2.3.3 各控制系统和数字化平台集团服务器安全策略

通过防火墙的单向访问策略设置，除了本地采集服务器有限的几个IP可以读取控制系统数据，其它IP访问均被屏蔽。以此保证控制系统数据的安全性。

3 能耗双控数据传输

按照国家节能中心数据采集上传的标准规范，对企业现场能耗数据采集接入、安全隔离、数据处理、加密上传[2]。借助企业工业互联网数据平台，它集成物联网多种应用技术，实现多协议数据安全采集生产过程数据，从中筛选出所需要的电力、水、煤、蒸汽、氮气、液化气、燃烧气、仪表风和凝结水等能耗相关数据（如图3）进行汇总，与DCS控制系统对比验证（如图4）、整理打包、数据加密，采用HTTPS通道保护传送至能耗在线监测系统接入端系统，上报企业能源消耗，为政府监管决策提供重要数据支撑，为重点用能单位的精细化能源供

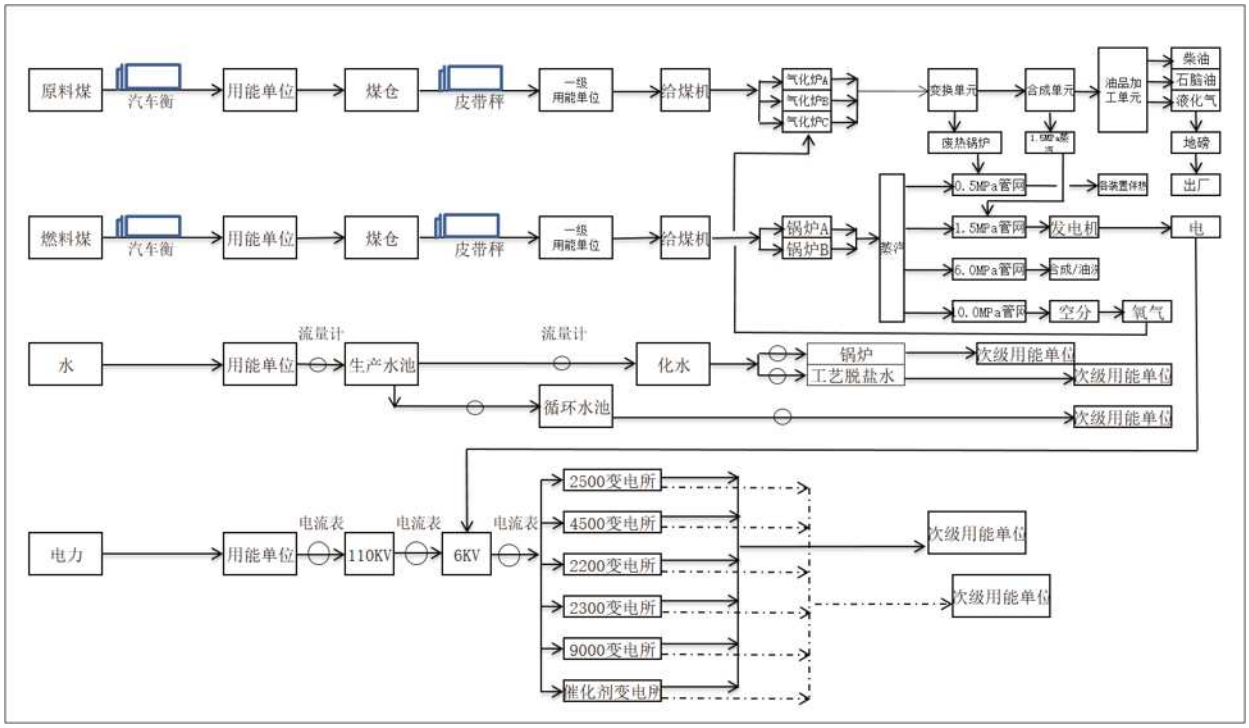


图3 能耗双控数据

图4　能耗双控数据传输界面

给与消耗管理提供依据。接入端系统通过网闸、防火墙网络安全隔离，确保系统网络自身安全和数据安全，还可进行平台版本校验、用能单位基础信息上传、用能单位采集数据上传、查看本单位用能数据采集和上传情况、查看本单位综合能源消费情况等。

4　重大危险源数据上传

按照应急管理部门意见[3]，危化品生产企业“两重点一重大”的关键装置重点部位的数据需接入安全生产风险监测预警系统（如图5）。通过Ability工业互联网数据平台所采集融合的数据，从中筛选出调和罐区、化学品罐区、液化气球罐区、液体石蜡罐区、气化炉、变换装置、净化装置、费托合成装置、油品加工装置、稳定轻烃装置（如图7）等危险源设备的温度、压力、液位感知数据经过网络安全通道接入安全风险监测预警系统。

图5　重大危险源危化品生产风险检测预警系统总览图

图6　重大危险源感知数据上传

5　结束语

通过建设企业级工业互联网数据平台，整体统筹设计信息网络架构、落实国家关于工业互联网信息网络安全管理及能耗双控、重大危险源数据上传要求要求，提升工业互联网数据平台及DCS、PLC、SCADA等底层控制系统安全防御能力及安全防护水平，为煤化工流程行业工业互联网建设摸索出一条符合企业实际发展路线的数字化发展路子。

参考文献：

[1]Ability数据平台及接口用户手册，2021年

[2]《危险化学品安全生产风险监测预警系统数据接入规范》中华人民共和国应急管理部危险化学品安全监管司&科技和信息化司，2020年3月

[3]《关于进一步推进重点用能单位能耗在线监测平台数据对接工作的通知》内蒙古自治区发展和改革委员会，2021年3月9日