基于“边缘智能+网络安全”的一体化工业互联网边缘计算系统应用探讨

Discussion on the Application of Integrated Industrial Internet Edge Computing System Based on "Edge Intelligence + Network Security"

★ 丁文勇 英赛克科技（北京）有限公司

摘要： 本文首先对工业互联网进行总结概述，分析了边缘计算在工业互联网体系中的重要作用，并就5G技术、网络安全保障、数据分析拓展应用等新技术、新场景赋予边缘计算的新需求、新趋势进行分析讨论。然后，基于未来趋势和当前边缘计算应用需求，通过边缘计算与网络安全深度融合创新，提出了基于“边缘智能+网络安全”的一体化工业互联网边缘计算系统，并从系统架构、软件系统、硬件平台、功能应用四个维度，对一体化系统进行论述，最后对工业互联网生态圈建设进行探讨。

关键词： 边缘计算；工业网络安全；工业互联网；大数据分析

Abstract: This article first gives an overview of the Industrial Internet, analyzes the key role of edge computing in the industrial Internet system, and analyzes and discussed the new demands and new trends brought by 5G technology, network security assurance, and data analysis and expansion applications to edge computing. Then, based on the future trend and the current application requirements of edge computing, through the deep integration and innovation of edge computing and network security, an integrated industrial Internet edge computing system based on "edge intelligence + network security" is proposed, and the integrated system is discussed from the four dimensions of system architecture, software system, hardware platform and functional application. Finally, the construction of the industrial Internet ecosystem is discussed.

Key words: Edge computing; Industrial network security; Industrial Internet; Big data analysis

1 引言

工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。工业互联网旨在使用传感器数据、M2M通信及自动化技术，融合泛在互联、大数据和机器学习等先进技术，提升工业和制造业总体效率，构建覆盖全产业链、全价值链的全新制造和服务体系，推动生产方式、产品形态、商业模式、产业组织的深刻变革，是中国先进制造业向数字化、网络化、智能化升级转型的主要方向。

工业互联网应用涉及工控自动化和管理信息化等基础设施改造、应用系统架构升级、商业模式创新三大环节，如图1所示，需要工控网络技术、边缘处理技术、工业大数据技术、互联网技术和网络安全技术等多技术的融合创新，并且工业互联网因其特殊的应用场景，以及在“边缘处理”与“网络安全”技术和产品层面，与消费/商业互联网应用具有质的差异，是当前工业互联网技术融合创新的重点发展领域之一。

图1 工业互联网应用环节

2 边缘计算在工业互联网体系中的作用

2020年4月，工业互联网产业联盟发布《工业互联网体系架构2.0》，将工业互联网划分为网络、平台、安全三大功能体系，如图2所示，为工业互联网产业发展提供了框架和方向指引。

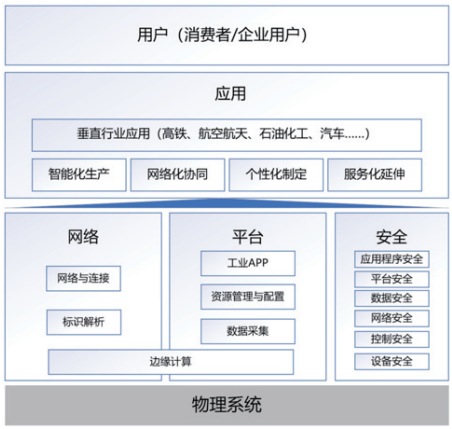

图2 工业互联网功能体系

网络为工业互联网的基础，通过边缘计算（网络侧）语义互操作、应用层通信等功能，结合网络互联、标识解析等技术将数字空间扩展到工业全系统、全产业链，并实现产品需求、设计、研发、管理、服务全过程以及生产资料、现场设备、过程控制、生产管理等各生产环节的泛在互联。平台为工业互联网的中枢，借助弹性载体以及边缘计算（平台侧）工业数据接入、预处理、协议解析等功能，为海量资源泛在连接、分析处理、模式应用提供支撑。安全为工业互联网的保障，通过安全技术、安全管理、安全服务等综合措施，着力控制、边缘（内外边缘、工艺边缘）、网络、平台、数据等关键环节，保障工业互联网支撑基础设施以及智能应用、智能装备等关键要素安全。

基于工业互联网体系架构，结合工业互联网“云管边端”建设实践，边缘计算因作为网络和平台体系中的重要支撑技术，以及其在工业互联网企业内网与企业外网互联、纵向数据集成、网络安全防护等领域的重要作用，已经成为工业互联网“云边端”协同的关键枢纽环节和网络安全保障的关键节点。

3 新技术新场景促进“智能、安全”在边缘侧深度融合

随着对工业互联网技术的不断探索与发展，边缘计算在数据接入、转换、预处理等经典功能应用的基础上，通过与5G、网络安全保障、数据分析拓展应用等方面的融合发展，逐渐被赋予新的内涵，并呈现出边缘智能与网络安全融合发展的趋势。

3.1 “5G+工业互联网”边缘计算，加速促进边缘智能

“5G+工业互联网”是利用5G构建满足工业智能化发展的，具有大带宽、低时延、大连接特点的无线网络基础设施。当前，“5G+工业互联网”终端、“5G+工业互联网”边缘计算等融合创新发展迅速，但受工业设备设施数字化和自动化程度的限制，面对工厂复杂的生产环境和特殊生产要求，采用“5G+终端”方式从工业终端或控制底层，推进企业工业互联网建设还存在较多困难，当前可行且正在广泛尝试的是从边缘计算设备或设施入手，构建以“5G+边缘计算”为基础的网络互联和数据互通体系，增强云边、边端连接，借助云平台和大数据实现数据价值的深度挖掘，并通过边缘设备实现与现场设备、现场数据的垂直整合，促进云端计算、数据、分析、服务、管理等能力向下传递，加速促进边缘智能。

3.2 历史性存量网络安全问题与新型技术安全风险叠加，促进安全边缘发展

工业行业普遍存在历史性、系统性的存量网络安全问题，如工业协议设计缺陷、工业数据明文传输、工业控制装备漏洞、网络计算资源不足、网络安全防护缺失等，与云计算、大数据、人工智能等新兴技术应用带来的工业互联网平台安全、云计算安全、数据安全、算法与模型安全等新风险新问题相互作用相互影响，形成更为复杂严峻的网络安全挑战。边缘计算设备作为工业互联网平台与企业内部生产装备系统协同的桥梁，是工业数据和连接的汇聚点，也是存量网络安全问题与新型安全问题的叠加点，进一步促进边缘设备由原来的边缘智能向安全边缘智能方向发展。

3.3 信息安全+边缘数据融合分析，促进安全保障由“网络安全”向“业务安全”迈进

企业工业控制系统是工业互联网体系的重要组成部分，是包含生产数据采集、数据传输、数据处理、生产控制、设备动作、物理生产状态或物理环境改变等过程的融合基础设施，其涉及信息的一系列处理、存储、应用过程和生产控制与物理状态改变过程。因此，与传统信息安全相比，工业网络安全是信息安全、工业控制安全、功能安全、物理环境安全等多个交叉领域的结合体，面临传统Security和Safety双重安保挑战。随着工业网络安全研究的逐渐深入，企业工业安全防护正由传统“网络安全”视角向融合物理安全、功能安全、信息安全的“大安全”业务视角转变。基于边缘计算技术，实现工业生产业务数据、工业装备全生命周期数据、物理环境数据、功能安全数据的主动实时采集、解析与转换，构建完整、真实、切实有效的工业系统业务安全分析模型。结合网络安全技术，从全局视角，面向关键装备和系统全生命周期安全管理，构建基于工业业务模型的安全态势感知等大数据平台，综合考虑工业控制系统信息安全、功能安全、物理安全等安全运营活动，最终形成以“安全设备+边缘计算”为节点、以大数据安全能力为支撑、以业务安全为核心、涵盖关键工业装备系统全生命周期的业务安全运营体系。

4 基于“边缘智能+网络安全”的一体化边缘计算系统

针对“边缘智能”与“网络安全”的融合发展趋势，以及信息安全与边缘数据融合分析等新场景新应用，一体化边缘计算系统分别在系统架构、软件系统、硬件平台、功能应用等方面进行了创新设计和实践。

4.1 系统架构

一体化边缘计算系统基于“轻量计算系统+5G无线融合通信+边缘智能+深度安全”等核心技术，采用系统能力资源“柔性”集成架构，借助系统工程方法，将各类计算、连接、智能处理，以及行为检测、基线学习、协议分析等计算与安全能力标准化为能力组件，并根据应用场景和功能需求进行动态集成，保证了系统服务的柔性利用和各类能力资源的动态匹配。如图3所示。

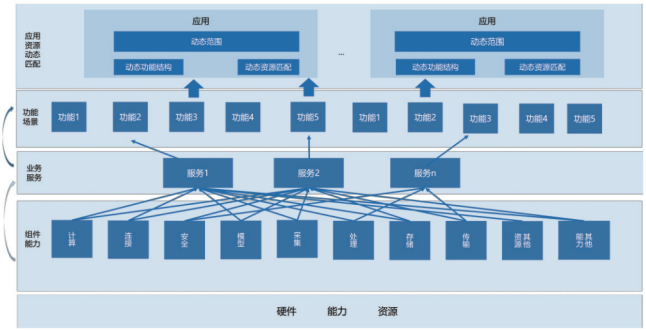

图3 系统能力资源“柔性”集成架构

4.2 支撑系统与软件平台

在系统层面，结合工业互联网应用场景连接对象多样性、硬件规格多样性等特点，参考移动互联系统开发模式，采用操作系统技术路线，将硬件的差异性与软件功能解耦，同时将工业网络安全和边缘计算共性技术需求，如工业数据接入、工业协议解析、网络安全防护、工业数据处理、人机智能交互、自身安全防护等融入操作系统中，形成了独具特色的工业互联网安全操作系统及其支撑应用软件开发平台，可快速构建不同性能的工业网络安全标准产品和客制化边缘计算节点产品，保证了系统平台对各类应用场景的快速响应。一体化边缘计算系统结构如图4所示。

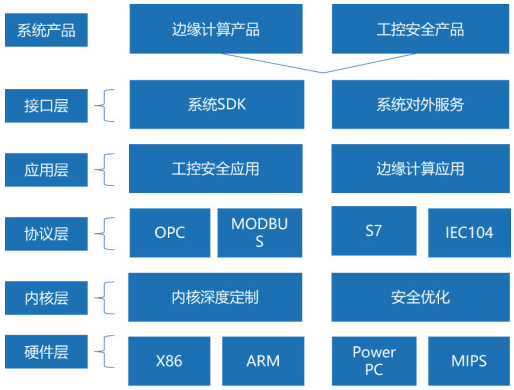

图4 一体化边缘计算系统结构图

系统特点：

（1）工控硬件广泛兼容。安全操作系统广泛适应于多种工业级硬件架构，可为不同的工控场景提供低功耗、高可靠、轻量级的解决方案。

（2）工业协议灵活组态。支持多种协议栈和工

业协议的深度解析，可实现N:N型协议与数据的任意转换，并支持网口与串口设备的异构接入。

（3）安全能力深度集成。依托工业协议指令级深度防护技术和操作系统内核级安全加固方法，使安全贯穿操作系统的应用于底层。

（4）工业应用高效定制。安全操作系统作为平台系统，可适应各种场景下不同工业互联网应用的定制，形成完整生态。

4.3 模块化硬件计算平台

在硬件层面，通过“All in one”策略，以高性能嵌入式工业计算机为计算平台，有机融合工业以太网技术、工业现场总线技术、工业时序数据库技术、工业数据处理技术以及工业网络安全技术，为工业互联网提供模块化硬件计算平台，如图5所示。

图5 模块化硬件计算平台

平台特点：

（1）网络。支持各种传统总线型工控网络、工业以太网和单点工业设备的接入，支持4G、5G双路冗余通信。

（2）存储。采用动态存储扩展技术，内置工业大数据应用定制型时序数据库，可满足生产线、复杂设备和系统各类数据的汇聚和存储。

（3）计算。提供Python计算引擎，内置数据过滤、平滑和降噪、数据特征提取等基础数据处理算法，具备通用的计算能力。

（4）应用。提供工业大数据智能告警、系统和设备性能检测与预警、工业数据过滤脱敏、工业安全检测分析等基础智能应用，并提供各种工业云平台接口，便于接入各类私有云和公有云平台。

（5）安全。提供基于逻辑隔离或物理隔离的不同形态组件，确保工控网络、设备和系统安全。

4.4 功能应用

（1）网络安全隔离防护

一体化边缘计算系统可根据网络应用环境，提供逻辑隔离和物理隔离等多种网络隔离防护形态。逻辑隔离，即采用工业防火墙式安全防护方法，通过工业协议的深度解析、工业指令控制、工业行为监测、病毒检测、入侵检测、内容过滤等规则，形成“白+黑”网络安全防护能力。物理隔离，即采用工业网闸式安全防护方法，通过“2+1”硬件级网络隔离，结合应用层工业数据安全过滤、工业指令安全检测等规则，形成物理级网络安全防护能力。

在网络安全防护场景中，一体化边缘计算系统对内实现安全的数据采集、协议转换、实时计算与控制反馈，对外提供网络连接、数据传输、平台接入，同时借助内外侧异构协议、数据代理、安全检测等机制，隐藏内部网络和安全缺陷，形成工业互联网缓冲安全区，成为企业工业网络与数据安全防护的第一道防线。

（2）边缘计算与安全应用协同分析

面对传统安全数据分析平台运营效率低下、安全运营效果不佳，以及新型威胁、隐蔽威胁等网络安全问题，急需借助边缘计算、业务数据分析等工业互联网技术，集成行业丰富的技术与数据资源，充分发挥工业AI优势，融合工业系统功能、业务、物理环境以及关键工业装备全生命周期数据的工业互联网安全分析平台与安全运营体系。

一体化边缘计算系统作为工业数据与工业连接的汇聚点，可提供全量的工业业务与装备系统运行保真数据，并可根据上层安全平台数据规范，提供工业数据解析、过滤、脱敏、本地化分析等预处理功能，通过“PaaS”模式，协助上层平台理解、建立并完善工业业务安全分析模型，使安全分析系统开发者专注于安全分析和感知预测场景开发，将网络安全保障由“网络保障”上升至“业务保障”，有效改善态势感知等安全数据分析系统在工业系统内“水土不服”等问题。

（3）协议解析与异构设备安全接入

从底层技术维度来看，工业互联网之所以成为一个独立的技术领域，其中重要原因在于工业协议与商用/消费互联网相比具有协议种类多、协议开发无序、协议私有化严重等特点，使得工业协议深度解析能力成为衡量工业互联网安全防护产品和边缘计算产

品技术能力的关键指标。

一体化边缘计算系统支持CDT、GPC、Modbus TCP/ASCII/RTU、SNMP、IEC 101、IEC 103、IEC 104、OPC、EIP(CIP)、S7、ABPLC、DLT645、OneWayTrans、MQTT、DNP3、MMS、GOOSE等数十种工业协议的指令级深度解析，结合系统工业数据可信采集机制，可有效保障接入数据安全，并支持Modbus TCP/ASCII/RTU等同类异构工业协议的数据采集和转换。

（4）云边协同

为满足工业生产实时性、连续性等方面的需求，边缘计算除具备广泛的数据接入和网络连接能力外，还需将工业互联网平台功能在靠近数据源的边缘侧进行映射，以实现生产现场数据实时处理与业务快速优化，满足工业在实时性、可靠性、确定性、低时延数据感知、边云协同、轻量级边缘应用等方面的需求。一体化边缘计算系统在协议解析、数据边缘处理、数据存储等能力基础上，借助4G、5G等通信技术，对外提供资源协同、应用协同、服务协同、数据协同、边云协同等标准化接口，保障系统高效“就近”提供边缘智能服务。

以上应用场景和功能已在民航飞机、高铁动车组、智能制造等装备或系统的智能维修、设备优化运营、工业安全分析等工业互联网场景中取得良好应用。

以高铁动车组预测性运维系统为例。通过构建独立的列车中央维护计算机（CMC），即一体化边缘计算系统（主要实现边缘智能、云边协同、网络安全隔离防护），对车载各子系统的传感器监测数据和报警信息进行全面采集，通过内置的虚警过滤、性能计算、智能测试等应用，对机车数据进行预处理和边缘侧智能分析，将关键数据传输至随车机械式移动手持客户端，并通过5G网络实现与地面中心系统的协同分析。另外，中央维护计算机采用“网闸”网络安全防护模式，通过“2+1”硬件级网络隔离机制，实现机车与地面网络的安全隔离和数据内容的安全检测，为无人控制列车、智能列车提供可靠网络安全保障，如图6所示。

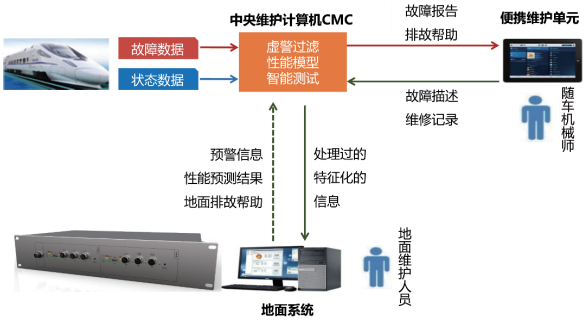

图6 高铁动车组预测性运维

5 结语

我国工业互联网产业发展正处在“边建设边完善、边应用边优化”的培育阶段，5G、工业AI等技术为工业互联网发展注入了新动能，不断促进工业互联网相关技术的快速发展，并加速向网络安全、物联网等其他领域外延渗透，为相关领域解决有关问题提供了新的途径和思路。但新技术的应用必然伴生新的安全问题，面对工业互联网及其相关技术“OT”与“IT”的双重属性，需以伴生思维综合考虑“工业”和“互联网”中不同属性及其衍生安全问题，结合工业互联网融合创新和工业系统“本体安全”思路，为工业互联网快速发展持续提供安全保障。AP

作者简介

丁文勇（1990-），男，山东德州人，高级工程师，硕士，现就职于英赛克科技（北京）有限公司，主要研究方向为工业网络安全、云计算安全。

参考文献：

[1] 工业互联网产业联盟. 工业互联网体系架构（版本2.0）[Z]. 2020-4-23.

[2] 工业互联网产业联盟. 工业互联网标准体系（版本2.0）[Z]. 2019-2-25.