工业互联网密码应用发展白皮书

（2021 年）

工业互联网产业联盟（AII）

2021 年 8 月

工业互联网产业联盟
Alliance of Industrial Internet

声　　明

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

工业互联网产业联盟
Alliance of Industrial Internet

编写说明

随着近年来工业互联网的快速发展，工业互联网的安全形势日益严峻。工业互联网攻击事件逐年增加、网络攻击级别不断提高，然而我国的工业互联网自主化程度偏低，安全防护建设比较弱，尤其是密码应用建设匮乏。密码技术作为保障网络与信息安全最有效、最可靠、最经济的关键核心技术，能够从根本上解决部分工业互联网的安全问题，所以工业互联网的密码应用建设亟需加强。当前国际关系紧张，网络安全形势严峻，我国先后颁布实施《网络安全法》和《密码法》，密码应用上升到国家法律和战略高度，工信部发布的《工业互联网创新发展行动计划（2021-2023 年）》将深化商用密码应用列为重要工作之一。

鉴于工业互联网密码应用发展的迫切性与重要性，**工业互联网产业联盟密码应用研究特设组**组织编写本白皮书，旨在梳理工业互联网密码应用背景，构建工业互联网密码应用技术体系，总结我国的工业互联网密码技术、产品、服务地供给能力，介绍工业互联网密码应用的典型实践，分析密码应用推广面临的痛点，以及提出工业互联网密码应用发展建议。

牵头编写单位：中国信息通信研究院

参与编写单位：傲林科技有限公司、海尔卡奥斯物联生态科技有限公司、江苏徐工信息技术股份有限公司、中国电子科

技网络信息安全有限公司、工业信息安全（四川）创新中心有限公司、长春吉大正元信息技术股份有限公司、北京信安世纪科技股份有限公司、长扬科技（北京）有限公司、郑州信大捷安信息技术股份有限公司、苏州三六零智能安全科技有限公司、深圳奥联信息安全技术有限公司、北京海泰方圆科技股份有限公司

编写组成员（排名不分先后）：

中国信息通信研究院：徐秀、马聪、何阳

傲林科技有限公司：任飞、王潮阳

海尔卡奥斯物联生态科技有限公司：唐宇、余涛、汪燕锋

江苏徐工信息技术股份有限公司：王焕、谢海红

中国电子科技网络信息安全有限公司：刘波、李智林、肖远军

工业信息安全（四川）创新中心有限公司：张文科、罗影、敖麒

长春吉大正元信息技术股份有限公司：韩璇、刘岵

北京信安世纪科技股份有限公司：付军、汪宗斌

长扬科技（北京）有限公司：汪义舟、赵华、张亚京

郑州信大捷安信息技术股份有限公司：刘为华、康亮、廖正赟

苏州三六零智能安全科技有限公司：韩涛

深圳奥联信息安全技术有限公司：蔡先勇

北京海泰方圆科技股份有限公司：薛静、许世波

目　录

一、工业互联网密码应用背景

（一）工业互联网面临严峻的安全威胁

1. 全球工业互联网安全问题

随着新一轮工业革命的快速推进，工业互联网成为大势所趋。工业互联网通过将工业体系与互联网体系深度融合，将工业领域中的人、机、物等生产经营要素全面联通，形成了影响工业和经济发展的关键信息系统。从封闭的工业环境到开放互联网的网络环境，工业互联网正面临网络安全与工业安全带来的双重风险。随着近年来工业互联网的快速发展，全球工业互联网安全形势严峻。

工业互联网攻击事件逐年增加，工业互联网成为新的网络攻击重点目标。近年来，随着工业平台信息化水平的不断提升，针对工业网络攻击的事件也频繁发生：委内瑞拉大停电、美国东海岸断网、台积电遭受勒索病毒导致停工、美国最大成品油运营商科洛尼尔（Colonial Pipeline）遭俄罗斯 Darkside 勒索病毒攻击被迫关闭关键燃油网络等。大量工业控制设备暴露在互联网上，工控协议的私有化严重且协议安全保护较弱，导致攻击门槛极大降低；工控系统漏洞逐年爆出，大量漏洞被攻击者利用。作为关系国家工业命脉和关键基础设施的重要系统，工业互联网已成为网络攻击新的重点目标，存在巨大的外部攻击风险。

国际竞争日益激烈，网络安全风险加剧，工业互联网的网

络攻击级别不断提高。近年来，国际竞争日益激烈，国际规则逐渐失序，外部环境震荡不安，极大增加了来自外部的高级别网络攻击的威胁等级。针对工业互联网的攻击者越来越专业化、组织化，攻击行为也正在不断升级。目前已经从传统的攻击工具利用，逐步向 0-day 漏洞利用、嵌套式攻击、木马潜伏植入等更高级的攻击形态演变，这些行为掺杂了大量的人工智能、躲避手段、情报手段、社会工程等多维度的变化。这些变化无一不在向我们透露：针对工业互联网的网络攻击不是普通的攻击行为，而是高级别的国家级网络对抗。

2. 我国工业互联网安全问题

在国家新基建战略的推动下，工业互联网进入快速发展阶段，形成了新技术加速融合、新生态加速形成、新模式加速推广的良好局面，但同时，我国的工业互联网也面临前所未有的安全威胁和挑战。一旦遭受网络攻击，可能会威胁国家安全、国计民生和社会公共利益。

我国工业基础和自主化能力较弱，带来巨大安全隐患。近年来，虽然我国制造业得到了快速的发展，但是相比于经历过三次工业革命的西方欧美国家，我国工业基础依然较为薄弱，关键基础材料、核心基础零部件、元器件、先进基础工艺等工业基础能力依然存在个别不足之处，关键核心技术短缺局面尚未完全改变。大量核心部件、PLC 等依赖进口，给我国工业互联网安全带来了极大隐患。无论是在供应链各个环节上可能被注入的后门、恶意代码，还是断供等问题，都直接影响我国工

业互联网的安全发展。据《2020 年上半年我国互联网网络安全监测数据分析报告》数据显示，我国暴露在互联网上的工业设备高达 4630 台。其中存在高危漏洞隐患的设备占比约 41%，电力、石油天然气、城市轨道交通等重点行业暴露的联网监控系统达 480 套，存在信息泄露、跨站请求伪造、输入验证不当等高危漏洞隐患的系统占比约 11.1%。这些暴露在互联网上的工业系统和设备一旦被攻击，将直接威胁重点行业的运行安全。

工业互联网发展迅猛，但是安全防护建设投入较低。近年来，在产业、政策的多方推动下，我国建成超过 70 个有影响力的工业互联网平台，连接工业设备的数量达到 4000 万套，工业 APP 突破 25 万个，工业互联网产业规模达 3 万亿元。虽然工业互联网产业经济发展迅猛，但工业互联网安全产业在工业互联网核心产业中占比始终较低，近年来基本维持在 0.5%[1]的水平，这个数值距离欧美国家 5%-10%的安全投入依然存在巨大差距。据《2020 年上半年我国互联网网络安全监测数据分析报告》数据显示，境内工业控制系统的网络资产持续遭受来自境外的扫描嗅探，包括美国、英国、德国等 90 多个国家，日均扫描超过 2 万次。能源、制造、通信等重点行业的关键信息基础设施及系统成为嗅探目标。利用嗅探到的资产信息和相关漏洞进行攻击会导致相关行业安全事件的发生，将给我国基础设施带来威胁性、破坏性甚至是毁灭性的打击。对于工业互联网安全的忽视，将会给工业互联网安全带来巨大隐患。

[1] 数据来源：前瞻产业研究院整理.

（二）国家出台工业互联网安全政策体系

1. 法律法规

在网络安全形式严峻的大环境下，国家出台了多项相关法律、法规和政策标准，为工业互联网安全产业注入“强心剂”。

《网络安全法》将网络安全上升为国家战略。“没有网络安全就没有国家安全，没有信息化就没有现代化。”在中央网络安全和信息化领导小组第一次会议上，习近平总书记提出网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。《网络安全法》的出台，是将已有的网络安全实践上升为法律制度，通过立法织牢网络安全网，为网络强国战略提供制度保障。作为我国第一部全面规范网络空间安全管理方面问题的基础性法律，《网络安全法》是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

《密码法》正式颁布执行，密码应用有法可依。密码是我们党和国家的“命门”、“命脉”，是国家重要战略资源。2020 年 1 月 1 日，《中华人民共和国密码法》正式开始实施，作为总体国家安全观框架下的国家安全法律体系的重要组成部分，其颁布实施将极大提升密码工作的科学化、规范化、法治化水平，有力促进密码技术进步、产业发展和规范应用，切实维护国家安全、社会公共利益以及公民、法人和其他组织的合法权益，同时也将为密码部门提高“三服务”能力提供坚实的法治保障。

网络安全等级保护制度 2.0（简称等保 2.0）新增工业控制场景扩展要求，明确密码应用。等保 2.0 标准在对等保 1.0 标准进行优化的同时，针对云计算、物联网、移动互联网、工业控制、大数据新技术应用提出了新的安全扩展要求。其中，也明确了工业控制系统在各个防护环节中的密码应用，如：数据加密技术、完整性检验技术、数字签名技术、身份鉴别技术等。等保 2.0 系列标准将推动《网络安全法》对于等级保护要求的落地，明确密码的具体应用场景和需求，指导密码技术在工业控制场景的应用落地。

这期间，网络安全等级保护和商用密码安全性评估作为《网络安全法》和《密码法》落到实处的两项重要工作，也在不断发展和完善中。

2. 政策红利

随着国家相关法律法规的制定和政策指南的相继出台和执行，各项措施将逐步细化，加快推进我国工业互联网安全“**顶层纲领+行动计划+实施指南”政策体系**的形成。

党中央国务院高度重视工业互联网的安全、有序发展。党的十九大报告指出，“加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合”。以党的十九大精神为指引，深入贯彻落实习近平新时代中国特色社会主义思想，以供给侧结构性改革为主线，以全面支撑制造强国和网络强国建设为目标，明确了我国工业互联网发展的指导思想、基本原则、发展目标、主要任务以及保障支撑，提

出了“立足国情、面向未来，打造与我国经济发展相适应的工业互联网生态体系”。

2017年10月30日，国务院常务会议审议通过了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，这是指导和规范我国工业互联网发展的纲领性文件。其中发展目标中明确指出：到2025年“基本建立起较为完备可靠的工业互联网安全保障体系”，到2035年“安全保障能力全面提升”。

为落实《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，工信部发布了《工业互联网发展行动计划（2018-2020年）》和《工业互联网创新发展行动计划（2021-2023年）》，目前，《工业互联网发展行动计划（2018-2020年）》已执行完成，新发布的《工业互联网创新发展行动计划（2021-2023年）》中将“深化商用密码应用”作为重要工作内容，指出“加快密码应用核心技术突破和标准研制，推动需求侧、供给侧有效对接和协同创新，推动密码技术深入应用。”

二、工业互联网密码应用体系

经过近几年的快速发展，工业互联网架构日渐清晰，主要由网络、平台、设备等不同层级构成，同时也涵盖贯穿多层级的产业链资源、数据要素等。上述环节均不同程度涉及与工业生产或管理紧密相关的身份鉴权、传输安全、敏感信息保护等个性化需求，需要使用密码技术持续增强安全支撑能力，构建

工业互联网密码应用体系。

（一）搭建融合开放灵活的工业互联网络

工业互联网络体系是工业互联网的基础承载，由网络互联、数据互通和标识解析三部分组成。网络互联实现要素间的数据传输，数据互通实现要素间传输信息的相互理解，标识解析实现要素的标记、管理与定位。工业互联网网络体系架构如下图所示：

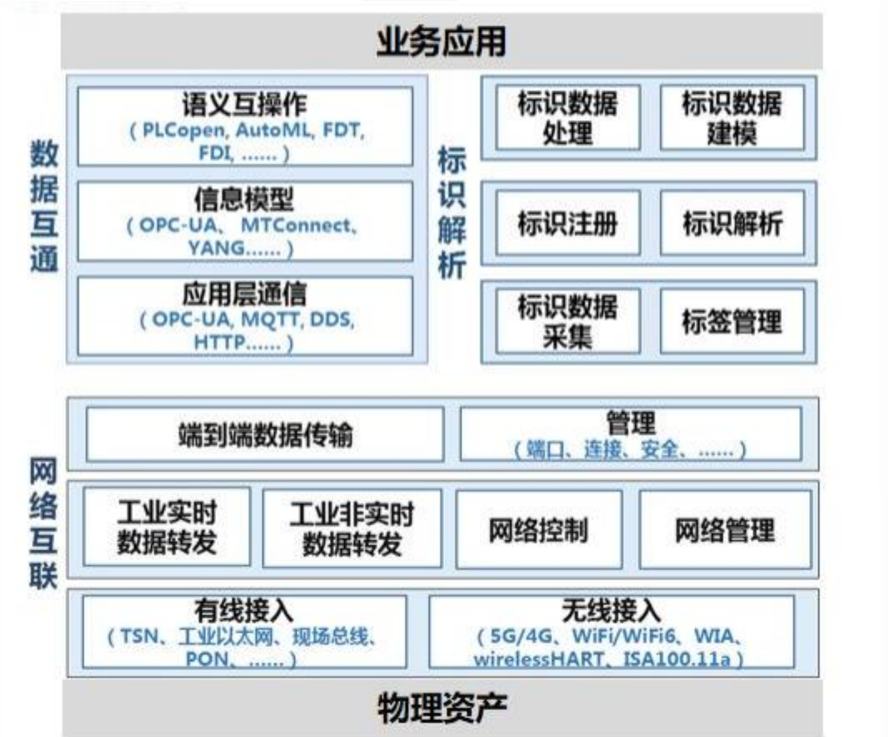

图 2.1　工业互联网络体系[2]

工业互联网业务发展对网络基础设施提出更高要求，工业互联网的网络体系发展呈现出开放、融合、灵活的三大发展趋势。在整体发展过程中，5G 新型基础设施的部署及标识解析系统的深度应用，将为工业互联网发展奠定重要基础，也对密码

[2] 图片来源：工业互联网产业联盟《工业互联网体系架构（版本 2.0）》.

应用提出新的要求。

1.5G+工业互联网密码应用

5G+工业互联网的融合应用，主要是将 5G 的多接入边缘计算（MEC）、5G 切片技术应用到工业超高清视频、AR/VR、云端机器人、远程控制、机器视觉、云化自动导引运输车（AGV）等场景中，满足各类型的工业互联网应用需要。

由于 5G 网络已然具备了完整的接入域安全、网络域安全、用户域安全、管理域安全的安全防护能力，本报告主要从接入端、边缘侧、行业专网三个方面分析 5G 与工业互联网融合对商用密码应用的新需求。

5G 终端密码应用需求分析。在“5G+工业互联网”应用场景中，覆盖了 eMBB、mMTC、uRLLC 三大类典型的行业终端形态，也给终端密码应用带来了新的要求。在工业互联网中，高清工业摄像头等 eMBB 类终端，需要提供有效的终端可信计算保护和 Gbps 级别的高速密码运算处理；常见工业传感器等 mMTC 类终端，需要轻量级的密码算法和协议、低成本的密码实现以及便捷化的设备认证与密码资源部署；远程低时延要求的控制类终端等 uRLLC 类终端，需要低时延、端到端的密码认证与数据保护机制，保障数据安全可靠。

5G MEC 密码应用需求分析。5G 多接入边缘计算(MEC)一方面将云计算环境部署在移动网络的边缘侧，满足低时延、高带宽的关键应用；另一方面支持更广泛的连接协议，满足更复杂的应用场景，工业企业可以通过 MEC 的部署快速构建园区专网，

在无需自建网络的情况下，获取高速、安全的网络服务。工业互联网与 5G 网络结合，需要考虑对接入企业 MEC 的设备实现基于密码的二次认证、对传输数据提供机密性及完整性保护、MEC 与企业内网间的安全隔离与交换，保障 MEC 在工业互联网中部署应用的合理性。

5G 切片专网密码应用需求分析。利用 5G 网络切片能力可以基于 5G 网络快速构建行业专网，从而打通孤立的网络节点和平台，实现产业链间的数据共享与业务协同，满足产业数字化转型需要。5G 行业专网的密码应用需求，包括网络资源的加密隔离、切片内的强身份鉴权与访问控制、业务数据的端到端加密保护，确保工业互联网行业专网应用的安全、可控。

综上需求分析，5G+工业互联网的密码应用需要充分利用 5G 网络的已有安全设计和元素，实现安全机制与 5G 模组、网元的融合设计，通过企业用户、运营商的多元化密码保障服务，支撑 5G+工业互联网商用密码应用落地。

2. 标识解析系统密码应用

工业互联网标识解析体系是工业互联网实现互联互通的“中枢神经”，工业互联网标识解析网络体系包括终端、节点、协议、软件、组织机构以及配套基础设施多类对象，其密码应用需求可分别从各类对象本身和体系架构进行分析。

从对象需求角度分析。终端是标识解析服务的入口，节点是标识解析体系的关键组成，协议是标识解析通信的基础，软件直接提供标识解析服务，组织机构是标识解析软件硬件的管

理与操作者，配套基础设施是标识解析服务的重要支撑，上述对象都可能成为标识解析体系的脆弱点。

从体系结构角度分析。首先，标识解析体系的树形分层体系结构为拒绝服务攻击提供了可能，一旦上层节点被破坏将造成子节点之间不可达。其次，当其节点数据被篡改时，将为整个标识解析体系带来不同程度的影响。例如，国际根服务器被篡改可能会误导客户端请求，将其引导至错误的顶级、二级或企业节点，被破坏节点授权的下级节点也将不可信。企业节点服务器被篡改可能会返回错误的标识解析结果。中心节点数据被篡改可能导致更大范围的污染扩散。

综上需求分析，密码应用需要保障工业互联网标识解析终端、节点、组织机构身份可信，防止伪造身份的中间人攻击、重放攻击以及越权访问，应从组织机构、终端、协议、平台系统等方面采取防护措施，保证身份可信、记录可信。在标识注册环节、标识数据同步环节、标识解析环节，保证传输数据的机密性和完整性。

a）组织机构方面，加强机构实体身份认证，对于新申请加入的组织机构做好相关身份与资质审查，建立身份信息标识，保证操作过程身份可校验，防止机构身份伪造。

b）终端方面，一是加强标识载体安全，通过防伪、标识绑定等技术防止被动及主动标识载体中的标识编码被篡改、伪造；二是提升客户端安全，通过基于硬件安全模块的安全防护技术，防止客户端被破坏，避免其身份被篡改、伪造、恶意利用。

c）通信协议方面，采用具有认证机制的通信协议，在各级节点间、客户端与服务端间等通信过程中，对主体身份、消息进行安全认证，支持配套的认证密钥建立。同时保证数据在网络通信过程中的数据机密性、完整性和不可抵赖性。

d）平台系统方面，建设支持多种认证方式的身份与权限管理平台，对工业互联网标识解析涉及的多主体对象的身份及权限进行统一管理，对用户访问的全过程实行严格的权限控制，包括从登录到退出的全过程。

（二）构建安全可信的工业互联网平台

为实现数据优化闭环，驱动制造业数字化转型，工业互联网平台需要具备海量工业数据与各类工业模型管理、建模分析与智能决策、工业应用敏捷开发与创新、工业资源集聚与优化配置等一系列关键能力。从功能体系上看工业互联网平台包括边缘层、IaaS 层、PaaS 层及 SaaS 层。不同的功能层级，对应不同的密码应用需求。同时，不同层级之间的安全传输以及跨平台之间的身份互认均需要密码技术来实现。

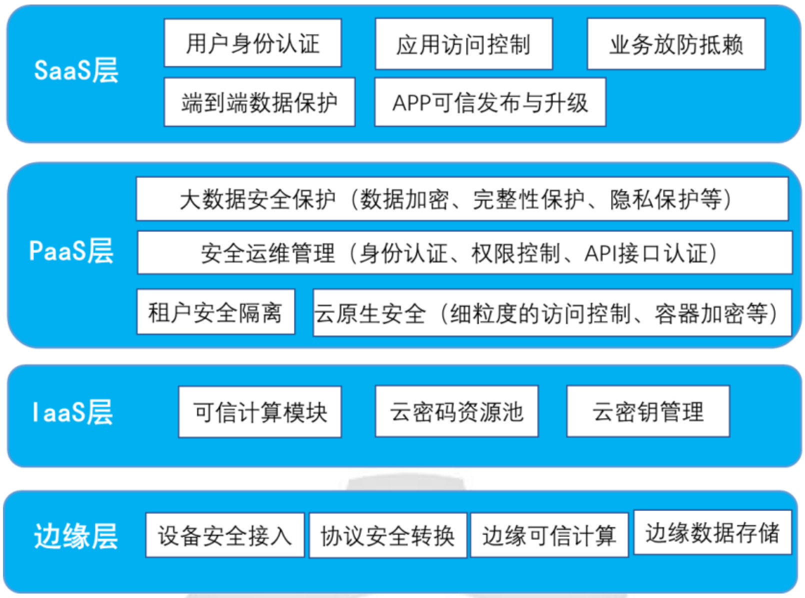

图 2.2　工业互联网平台密码应用架构图

1. 边缘层密码应用

边缘层是工业互联网相较传统互联网络的主要特征之一，其本质是利用泛在感知技术对多源设备、异构系统、运营环境、人等要素信息进行实时高效采集和云端汇聚。边缘层提供海量工业数据接入、转换、数据预处理和边缘分析应用等功能。

边缘层计算设备往往分散于各个产线、库房等现场环境中，边缘终端设备计算资源有限，安全防护能力薄弱，工业互联网平台在接入、转换、传输的过程中，数据易被侦听、拦截、篡改、丢失等，攻击者利用边缘终端设备漏洞可对平台实施入侵或发起大规模网络攻击。因此，对边缘层设备实施以密码技术为基础的安全防护变得十分重要。

边缘层对商用密码应用主要有以下需求：

工业设备安全接入。边缘层具备对机器人、机床、高炉等工业数据的接入能力，需提供有效的接入认证手段和数据传输

加密保护机制，确保数据来源的真实可信及数据的机密性与完整性。

协议安全转换与数据多安全级保护。边缘层负责对采集的异构数据源进行格式统一和语义解析，需考虑利用密码机制对异构安全协议进行转换，满足数据加密传输需要，同时对接入的隐私数据与敏感数据进行安全标识与多安全等级的加密处理，满足数据分级分类需要。

边缘可信计算处理。在工业互联网场景下，工业边缘计算往往用于产线设备在线检测、预测性维护等重要场景，对数据分析、计算处理的可靠性要求很高，需要考虑在边缘计算环境本身不完全可控的情况下，利用基于密码的可信计算技术，保障数据计算处理的安全可信。

边缘数据存储安全。在工业互联网场景下，边缘计算节点需要实时跟踪物联设备的状态变化，并按照时间序列存储完整的历史数据，存储的数据中可能存在生产端的敏感数据，需要利用密码技术进行加密保护，同时利用密码的时间戳技术，保障存储数据不可篡改。

由于部署环境的特殊性，边缘层对密码实现的高并发、轻量化有较高的要求，同时由于部署环境的开放性，需要采用更强的密钥保护、防丢失技术，满足无人值守环境下的密码应用安全需要。

2. IaaS 层密码应用

工业互联网 IaaS 是指基于虚拟化、分布式存储、并行计算、

负载调度等技术，实现网络、计算、存储等计算机资源的池化管理，根据需求进行弹性分配，并确保资源使用的安全与隔离，为用户提供云基础设施服务。

从技术架构来看，工业互联网 IaaS 与一般的云 IaaS 并没有差异性，但是制造企业出于企业知识产权、商业机密保护、业务系统安全等方面考虑，企业自建云方式部署 IaaS 依然是主流，部分工业互联网平台采用租用公有云方式或者混合云方式部署 IaaS。

IaaS 层对商用密码应用主要有以下需求:

- 可信计算环境: 在等保 2.0 标准体系中，将"可信计算"列为核心防御技术，对于工业互联网应用中涉及的等保三级及以上系统，要求所有计算节点都应基于可信根实现开机到操作系统启动，再到应用程序启动的可信验证，并在应用程序的关键执行环节对其执行环境进行可信验证。上述要求对 IaaS 平台中的 TCM 模块部署、可信计算密码支撑及响应的可信密码应用提出了较高的要求。
- 用户身份鉴别: 对 IaaS 平台上的云租户，要求有效的用户/账号体系实现主体对虚拟机、数据库、云网络、云存储等基础资源的访问; 在用户鉴权过程中需采用两种或两种以上组合的身份鉴别机制，且必须有一种采用密码技术; 对用户身份鉴别数据需采用密码技术实现机密性与完整性保护。
- 云存储加密: 在 IaaS 层实施存储加密，主要有两方面

的考虑：一方面，由于云计算是基于 API 而非物理访问来管理的，导致系统管理人员往往具有管理级的访问权，存在用户非知情情况下获取数据的可能；另一方面，由于 IaaS 平台往往具备多租户的特点，存储加密可以有效避免其他用户访问底层数据和系统，更有利地使用云平台资源。

- 云通信加密：云通信安全主要解决单一计算环境允许多租户同时共享网络时，网络隔离、数据通信加密和完整性保护问题。可采用 SSL 或 IPsec 实现虚拟机之间、虚拟机与控制台之间的数据加密保护。

IaaS 层特定的商用密码支撑需求：

- 可信云平台：可信云平台是指关键服务器上采用了系统可信和应用可信功能，通过度量和验证来保障计算环境安全，以及应用运行安全的云环境。可信云平台构建需采用符合国家密码局要求的可信计算模块，并通过对 BIOS、Bootloader、操作系统内核、关键系统模块和应用的逐层哈希验证，来保障系统运行环境未被篡改。
- 云密码资源池：云密码资源池是指将密码计算单元进行统一管理，实现随机数产生、密钥管理、密码计算等能力的柔性调度，以支持弹性伸缩、按需分配，动态部署的密码应用需求，满足公有云、私有云等不同场景下的密码应用需要。
- 云密钥管理：云密钥管理服务是一类为云上不同层级用

户提供密钥全生命周期管理的支撑类服务，通过云密钥管理服务可以快速的创建和管理各型密钥，提供托管式密钥管理服务，为端、边、云上的各类密码应用需求提供统一的密钥管理支撑，符合监管和合规要求。

3. PaaS 层密码应用

PaaS 层提供资源管理、工业数据与模型管理、工业建模分析和工业应用创新等功能。PaaS 平台提供了统一的 IT 资源调度与运维管理能力，同时为数据的治理、分析、服务、应用提供了集约管理平台，支持工业数据的统一建模，为研发、生产、运营环节提供统一的数字化工具与服务。

随着中台概念的兴起，中台能力成为工业 PaaS 平台发展的主要技术方向。通过大数据、微服务、持续集成、低代码交付能力的深层应用，使得工业 PaaS 平台更加易于实现数据的一体化管理和业务的灵活化支持。

PaaS 层对商业密码应用有以下需求:

- 大数据安全: 大数据安全指 PaaS 平台对结构化数据、半结构化数据、非结构化数据采集、存储、处理、分析、应用等全生命周期中面临的安全风险，包括传输安全、存储安全、计算安全、隐私保护等，需要采用密码技术来解决。
- 租户安全隔离: PaaS 平台往往涉及多个企业或者一个企业的多个业务部门，需要有效的密码保护机制进行隔离保护，保障数据和业务逻辑的隔离性。

- 云原生数据安全：云原生技术主要指以容器、持续交付、DevOps 以及微服务为代表的技术体系，在使用云原生技术后，开发者无需考虑底层的技术实现，可以充分发挥云平台的弹性和分布式优势，实现快速部署、按需伸缩、不停机交付等。在云原生架构下，以微服务为场景需要更细粒度的访问控制与加密保护，包括微服务间通信加密和证书管理、容器数据加密、服务间相互调用的访问控制，需要利用密码技术实现精细化管控。
- 运维管理安全需求：运维人员身份管理，远程数据传输安全加解密。相关密码应用主要包括平台账户身份认证、多租户权限控制、数据访问与处理环境的安全，同时包括边云协同过程中的数据、资源使用与应用部署层面的加密保护，也包括应用层开放 API 的接口认证与加密。

4.SaaS 层密码应用

应用层以工业 APP 为主要形态提供针对研发设计、工艺优化、能耗优化、运营管理的各类创新应用，同时提供开发者社区和应用商店，构建更加完整易用的工业互联网应用生态，提供二次开发及定制化能力满足用户个性化需求。

工业 APP 生态的构建，是工业互联网平台能够支撑工业经验知识的软件化封装，加速共性业务组件的沉淀复用，实现低门槛的工业应用创新，吸引第三方能力的有效聚合，支撑企业快速满足社会化协作和市场需要的关键。而基于商用密码的安全能力是开展应用创新和商业模式创新的重要基础。

应用层对商业密码应用有以下需求:

- 统一身份认证与单点登录：应用层需要提供统一的应用登录认证机制，便于用户在不同应用间的无缝跳转。需要采用基于密码技术的多因子认证，来构建统一的身份管理与用户认证体系，保障用户对应用、服务、数据访问身份的一致性。
- 应用鉴别与访问控制：工业 APP 的鉴别与访问控制涉及用户对 APP、APP 对 PaaS 平台、用户对数据的多级访问控制要求，实现基于角色的、字段级访问控制要求。
- 端到端数据保护：工业 APP 中涉及大量企业敏感数据的存储与展示，需要采用端到端的加密保护机制，保障数据在中间处理与存储环节不可见，保障用户数据安全。
- APP 可信发布与升级：利用基于密码的证书体系，构建 APP 开发者、发布者、审核者的信任体系，实现工业 APP 的可信升级，保障工业 APP 生态安全。

（三）打造具有内嵌安全的工业智能设备

工业智能设备广泛应用于关键信息基础设施，其稳定可靠运行不仅关系到人们日常生活的方方面面，还会对国家安全产生重要的影响。工业互联网的设备层主要实现工业数据采集、连接、转换和数据预处理功能，主要设备包括数据采集、集中控制、数据远程传输和控制等智能机器、专用设备、成套设备、仪器仪表等。

为确保终端设备的真实性，传输数据的机密性、完整性和

不可否认性，防止伪造终端接入和数据被篡改，现场终端侧需要部署密码安全模块，密码安全模块和边缘层的安全设备交换设备证书，实现双向的身份认证和密钥协商。

（1） PLC 控制器中的密码应用

PLC 控制系统（可编程逻辑控制系统）是以 PLC 控制器为中心、控制技术和信息技术结合的基本工业控制系统，是工作在现场控制层的基础系统。

PLC 控制器中包括芯片、操作系统及运行环境、PLC 控制功能模块和密码模块。PLC 控制功能模块用于运行用户逻辑组态，实现业务控制流程；密码模块嵌入到 PLC 控制系统的各组成设备中，可以是物理模块，也可以是逻辑模块，主要实现密码算法、密码安全功能和安全管理功能，对外提供密码计算服务接口，用于存储敏感数据、提供密码安全功能、密钥等敏感数据管理、安全策略管理以及和后台安全管理服务器的交互。

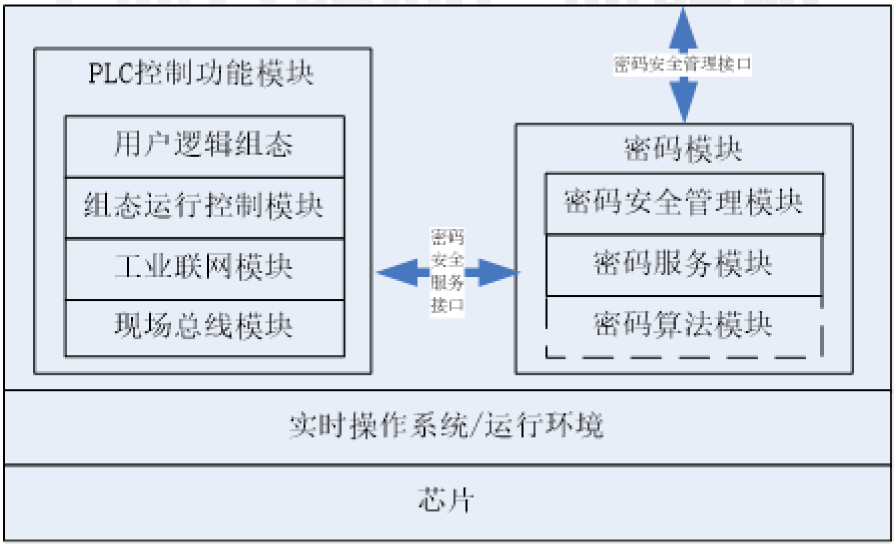

图 2.3 PLC 控制器密码应用组成

（2）SCADA 系统中的密码应用

SCADA 系统(数据采集与监视控制系统)可实现对测控点分散的各过程或设备的实时数据采集，本地或远程的自动控制，以及生产过程的全面实时监控，并为安全生产、调度、管理、优化和故障诊断提供必要和完整的数据及技术手段。

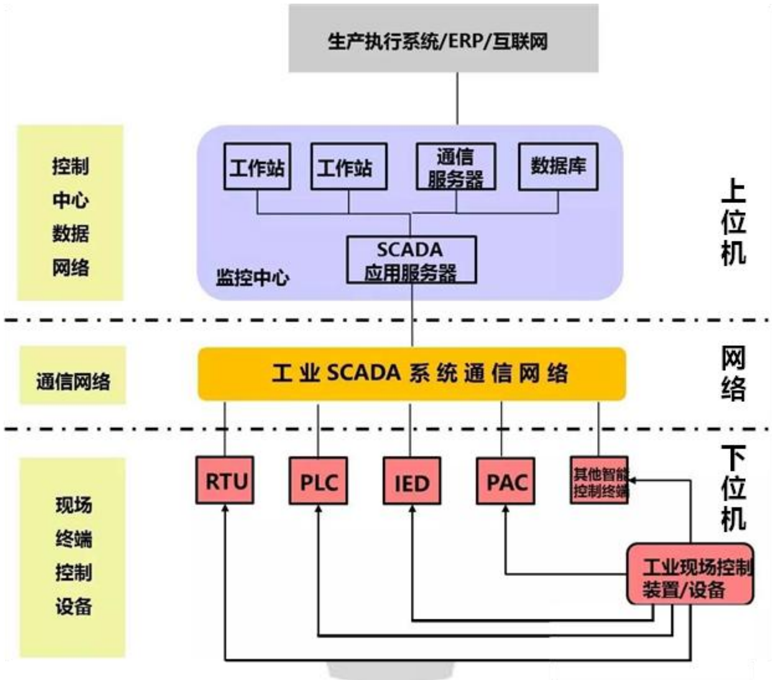

图 2.4　SCADA 系统分层架构示意图

SCADA 系统架构可分为三个层次，包括上位机层、下位机层和网络层。密码应用有如下需求：

- 上位机层的安全保护：业务功能安全主要是通过在上位机层部署采用商用密码的密码安全设备，实现业务功能及数据安全，包括对上位机终端的身份认证、控制指令和数据的加解密等；SCADA 系统的管理功能涉及到上位机层所有的操作用户应使用基于非对称密码算法的身份认证机制、所有针对 SCADA 系统的远程访问都需要验证数字证书，基于数字证书实现角色权限的管理。

- 通信网络的安全保护：主要是指上位机层与下位机设备之间的数据通信的链路安全，通信内容为关键控制信息或回传数据，传输时容易被截获或被篡改，因此应对其进行加密，考虑到执行效率，可采用对称密码算法进行数据加密。
- 下位机层的安全保护：下位机设备是 SCADA 系统的关键部件，具体采集相关数据上传到上位机及执行 SCADA 系统的控制指令，对下位机设备应采用基于非对称密码算法的数字证书进行保护，实现基于数字证书的用户权限管理，保证下位机设备远程访问及身份识别的安全；下位机设备回传数据到上位机时应使用自身的私钥进行签名并使用对称加密算法加密，以保证数据来源的合法性和安全性；同时，上位机发送给下位机设备的信息也需要使用私钥进行签名并使用对称加密算法进行加密。

（四）支撑智能制造产业链价值协同

产业链的本质是用于描述一个具有某种内在联系的企业群结构，它是一个相对宏观的概念，存在两维属性：结构属性和价值属性。产业链中大量存在着上下游关系和相互价值的交换，上游环节向下游环节输送产品或服务，下游环节向上游环节反馈信息。产业链的实质就是不同产业的企业之间的关联，而这种产业关联的实质则是各产业中的企业之间的供给与需求的关系。产业链协同是指如何通过价值链、企业链、供需链和空间链的优化配置和提升，使产业链中上下游间实现提高效率、降

低成本的多赢局面。产业链协同的核心目的就是打通上下游间各个环节，实现企业竞争力的提升。

密码技术对于产业链间的协同，主要提供四个方面的能力：一是以数字证书为基础，建立真实、可信、分布化的企业数字身份体系和信用体系；二是利用电子签名等技术支撑业务流、资金流、物流和信息流数据的线上流转、可控共享与有效溯源；三是以基于隐私保护的数据安全共享为前提，加深产业链内企业间的供需协同、资源协同、能力协同，实现生产制造模式创新；四是以区块链技术为重点，支持以真实业务为核心的产业链金融，解决产业链属企业融资难融资贵难题。以下列举五个典型应用：

（1）证照电子化

在工业产业链中，存在着多个生态合作伙伴，包括原材料商、零部件商、渠道商、贸易商、物流企业等等。面对着整体规模、技术水平、资源实力各不相同的企业，如何识别出优质的合作伙伴，确保产供销活动的有效开展，是产业链生态发展的基础。对于合作伙伴的身份确认、资质确认、信用画像是发展优质合作伙伴的关键。

电子证照作为具有法律效力和行政效力的专业性、凭证类电子文件，已经成为市场主体和公民活动办事的主要电子凭证，是支撑政府服务运行的重要基础数据。2021 年政府工作包括，推动电子证照扩大应用领域和全国互通互认，将进一步扩展电子证照在企业端的使用。目前，以电子营业执照为代表的企业

电子证照已经在国内广泛使用。电子营业执照与纸质营业执照具有同等法律效力，是市场主体取得主体资格的合法凭证，电子营业执照以国家市场监督管理总局为统一信任源点，记载了市场主体的身份信息，能够证明企业身份的合法合规性，同时市场主体使用电子营业执照可以对数据电文进行电子签名，符合《电子签名法》第十三条规定条件的，电子签名与手写签名或者盖章具有同等法律效力。

在密码技术的应用上，电子证照主要具有以下几方面的应用需求：

一是电子证照的合法性验证，通过电子印章、电子签名等基于密码的防护技术手段，对电子证照内容进行签名，保障证照合法使用；

二是电子证照的全生命周期管理，从电子证照制作、发放、查询、核验等各个环节，建立电子证照数据安全传输、安全存储、防篡改、防抵赖等安全保护机制，确保电子证照的安全管理；

三是电子证照的安全应用，利用数字证书技术进行电子证照的安全核验，以及基于电子证照的电子签名，满足企业到企业、企业到个人、企业到政府等多元化的使用要求。

电子证照对密码产品的应用需求包括以下几个方面：

一是灵活安全的电子证照载体：证书是电子证照的基础，需要合规的商用密码介质进行存放。传统采用 USB-key 等硬件介质进行证书存放，但难以满足移动化时代的应用需求，需要

考虑手机盾、软 Key 等新型密码载体形态，通过 APP、小程序等方式，更好的提供电子证照的各种应用服务；

二是以数字证书系统为核心的电子证照应用支撑平台：电子证照应用支撑需要证书管理系统、安全接入系统、数字签名系统、电子印章系统的支持，从而实现统一身份认证、统一电子印章，以及电子证照的多元化应用。

三是推进区块链+电子证照的新型应用：通过区块链与电子证照的融合应用，将电子证照及电子证照的颁发使用环节在区块链上存证，保障电子证照应用全过程的可信可查、可追溯，同时实现多中心环境下电子证照的互信与共享。

（2）合同数字化

合同是企业间达成合作的基础，是保障企业间有效协作的关键。随着《合同法》与《电子签名法》的陆续出台，电子合同逐步取代传统的纸质合同，成为了企业与个人、企业之间签约的主要形态。对于工业企业之间的电子合同而言，除了利用电子签约方式提升合同签署效率、降低签署成本之外，对合同的全方位、全过程数字化管理，已经成为了发展的新趋势。

合同的数字化管理，将合同从电子化升级到知识化、智能化的新阶段，紧密围绕企业销售、招投标、采购等业务活动，实现合同起草、审批、签订、履行等过程工作的信息化管理，并结合合同的风险预警、履约监控等手段，将合同数字化管理延伸到企业数字化转型的各个方面。

在合同数字化方面，密码技术主要满足以下需求：

一是确保电子合同签署的安全合规：在电子合同签署的流程中，需要使用密码技术进行身份核验、电子签名、数据传输保护以及时间戳服务，从而保障电子签名过程的有效性。

二是实现电子合同的安全存证：对第三方存证的电子合同，应采用加密机制保障合同安全存储，防止合同内容被非法获取，同时需要提供有效的加密手段、完整性鉴别手段来保障电子合同在签约方、公证机构以及存证平台之间的传输安全。

三是完成电子合同的内部可控流转：在企业内部，应当对敏感合同内容进行全生命周期的存储加密保护和完整性保护，并建立基于数字签名的合同审批流程，保障合同生命周期的安全可控、可追溯。

合同数字化管理对密码产品的应用需求包括以下几个方面：

一是电子印章：电子印章技术以先进的数字技术模拟传统实物印章，其管理、使用方式符合实物印章的习惯和体验，其加盖的电子文件具有与实物印章加盖的纸张文件相同的外观、相同的有效性和相似的使用方式。电子印章将电子签名技术完全隐藏在电子印章的后面，降低电子文件的使用成本，并易于与主要流式、版式文件格式集成。

二是数据存证平台：数据存证系统通过将身份、信息、资产、行为上链，使得存证无法篡改，便于被各方共享，并作为纠纷发生时的电子证据，实现全流程留痕，全链路可信，全节点见证，高效解决企业纠纷，降低企业风控成本，结合区块链技术和数据加密技术，可以保障电子合同等关键数据的安全存

证。

（3）供应链溯源

商品从原材料、零部件到达最终消费者受众，往往经过了多个生产制造企业、仓储企业、物流企业、各级分销商、零售商、电商等多个环节。在产品的生产、流通、消费等环节中，存在着假冒伪劣、以次充好等扰乱市场秩序的行为发生，影响最终产成品质量和消费者权益，供应链溯源体系的建立，将打通采购、生产、销售、仓储、物流等各个环节，实现货品全过程的来源可查、去向可追、责任可究。

供应链溯源中，密码技术主要满足以下的应用需求:

一是建立“一物一码”的信息标识:结合密码技术与 RFID 技术，构建可信的商品溯源码，保障商品信息的唯一标识，防止篡改。

二是基于区块链技术实现全过程管理:利用区块链分布式、不可篡改的特性，实现商品在生产流通的各个环节进行全过程上链存证和可控流转，实现全过程可追溯，实现有效的责任认定。

在供应链溯源中，对于商用密码产品的需求包括以下两个方面:

一是利用轻量化、低成本的密码标识方案，满足货品标识的隐私性、不可篡改性需要。

二是建立具有隐私保护、强确权的区块链平台，实现商品流转信息的安全保密和抗抵赖。

（4）制造协同化

协同制造指利用先进网络技术与信息技术，将串行制造过程转变为并行制造过程，实现供应链内部及跨供应链间的设计、制造、管理、商务等合作的生产模式，最终通过改变经营模式达到资源高效利用的目的。

当今，越来越多的工业企业通过工业互联网平台建立了与上下游供应商、合作伙伴和客户的直接连通，集聚供应信息并进行深度挖掘分析，提高了供应链的反应速度、匹配精度和调运效率，降低了采购成本，减少了成品和在制品的库存，缩短了对客户服务的响应时间。

然而随着数据在企业生产经营中的重要性日益体现，协同制造也给安全带来了更高要求：

一是需要保障企业间生产过程数据的安全可控共享。产业链上下游企业共享仓储数据、生产数据、订单数据，可以更好的制定采购计划、排产计划，更快的满足客户使用需求，但是由于企业间本身的竞合关系，以及不同的供应商、不同客户间错综复杂的关系，需对数据共享的范围、内容以及共享方式进行基于密钥的细粒度管理与访问控制，避免企业自身核心数据及其他合作伙伴数据的失泄密。

二是需要建立工厂现场可信可证的远程诊断与服务模式。工业互联网使得设备商能够更好的了解设备的工作状态开展远程故障诊断、维护升级甚至是预测性维护服务，从而更好的响应客户需求。然而在此过程中，也可能导致客户数据的非授权

访问以及外部入侵的可能。需要利用密码技术进行远程访问授权、通信传输保护和升级固件的可信验证，保障工厂服务安全。

在制造协同化过程中，需充分分析共享的数据内容，建立包含机密性、完整性、不可否认性相结合的数据保护方案，结合细粒度的密钥管理机制，保障数据在企业间可控共享。

（5）产业链金融

产业链金融是指金融机构以产业链上的核心企业为依托，以真实的业务场景为基础，为整个产业链上的链属企业提供金融服务的一种模式。在一条产业链上，中小微企业往往处于劣势，且缺乏足够的信用和资产抵押获得足额的贷款满足生产活动需要，而产业链金融依靠真实业务场景及核心企业信用的传导，化解中小企业融资难、融资贵问题，加速整个产业链条上的资金流转。

在产业链金融中，密码技术主要满足以下应用需求:

一是利用区块链技术，实现核心企业信用的多级流转，解决上游中小企业的融资难题。通过构建线上化的产业链金融平台，建立具有区块链唯一标识的核心企业付款凭证，实现多级分拆与流转。利用密码的完整性、不可否认性，实现金融机构对核心企业应付凭证的快速核验，从而提升审批与放款效率。

二是建立基于密码的设备远程管控手段，助力线上化的机械设备融资租赁。利用加密安全传输，实现高价值工程机械设备的远端控制，结合真实有效的地理位置信息、使用状态信息，进行设备的有效管控，当租户没有按期付款时，实现设备的远

程停机，保障设备租赁企业的合法利益。

三是实现黑名单客户信息的隐私共享，化解产业链金融风险。利用隐私计算“可用而不可见”的特性，利用同态加密、安全多方计算等隐私计算技术，实现黑名单客户信息在银行、企业及政府机构间可信共享，实现智能化动态风控，化解产业链金融风险。

在产业链金融中，对于商用密码产品的需求包括以下三个方面:

一是基于区块链的数字凭证及流转体系，实现可确权、可分拆、可流转，全过程可查可证。

二是基于可信计算的安全物联模块，实现对远程指令的安全验证和可信操作，有效控制高价值设备使用。

三是基于隐私计算的安全风控模型，实现风险名单的可控共享，保障资金安全。

（五）推动数据要素市场化流通

数据是工业互联网的核心驱动力，也是工业互联网的本质要素之一。来源于传感器或监控系统的数据不断被采集、积累，形成了具有巨大价值的数据资产。而在协同、柔性、智能等工业生产模式的驱动下，数据在更大范围内加速流通、共享和交易，以数据为中心的工业生产成为了一种新业态。

2020 年 4 月 9 日，中共中央国务院公布了《关于构建更加完善的要素市场化配置体制机制的意见》，并明确要加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价

值、加强数据资源整合和安全保护，第一次将数据与土地、劳动力、资本、技术一起作为生产要素纳入市场化的配置体系之中。

数据要素市场化建设有三个阶段：“数据资源化”、“数据资产化”和“数据资本化”，通过渐进式的“三化”工作，使得数据具有通用性、全局性、价值性和流通性等多种属性之后，数据才可以成为“生产要素”。而在这三化的过程中，密码都将起到极其重要的作用。

（1）数据资源化层面

数据资源化是将来自于不同信息系统、控制系统、物联设备的信息，通过加工处理，形成可见、可采、互通、可信的高质量数据资源的过程。

但是在企业的实际生产经营中，由于信息化能力参差不齐、底层设备接口标准化程度低、信息系统互联互通差、数据自采率低、通信协议不兼容等一系列原因，造成了数据来源混乱、数据失真、统计口径不一致等一系列问题，给后续的数据应用带来了严峻的挑战。

通过密码技术在数据源头的部署与应用，可以有效解决数据来源可信的问题：

一是通过密码能力在 IoT 终端中的泛在化部署，对数据采集来源进行可信标识，实现“一数一源”;

二是通过基于密码的安全接入能力构建，构建海量数据的安全接入通道，实现“可信汇聚”；

三是通过来源数据的安全标识、多属性加密、完整性保护，构建端到端加密、细粒度访问控制的数据保护能力，实现“一源多用”。

以密码技术为基础，从来源可信、接入可信、内容可信三个层面，构建安全、可信、规范、易用的数据资源体系。

（2）数据资产化层面

数据资产化是指通过元数据管理、主数据治理、知识图谱构建、数据挖掘等一系列活动，将数据与企业生产、经营等实际业务场景相结合，为企业带来实际价值的过程。

对企业数据的充分应用，涉及跨应用、跨部门、跨组织间的数据打通，企业数据资产在信息化部门、数据运营部门和业务部门间高效流转，数据安全已经远远超出了传统数据库审计、灾备、敏感文件流转监控的防护范围，需要构建新的防护能力。

通过密码体系与工业大数据架构的融合设计结合动态的密钥分配管理体系，有助于打造数据安全治理新范式：

一是结合结构化数据、非结构化数据、时序数据、图数据等不同数据的存储形式，构建安全存储、可信计算的基础环境，打造数据资产的安全计算平台；

二是结合数据体系和数据血缘关系，建立基于密钥的数据资产隔离防护模型，打造多级安全的数据资产加密保护体系；

三是对数据的访问与可控共享，部署端到端加密与基于策略的访问控制能力，实现对数据调用的细粒度管控，确保数据资产可控调用。

从数据存储与计算处理、数据资产管理与治理、数据服务三个层面，嵌入相应的密码保护机制，实现基于策略确保数据资产安全可控。

（3）数据资本化层面

数据资本化是指通过数据交易、流通等实现数据要素市场化、社会化配置的过程。通过市场化的交易手段，将企业在生产运营中沉淀的大量数据从企业的经营成本转化为产业链高效协同的价值点和新的利润点，已经成为了数字经济发展过程中产业界的一种共识。

然而随着数据价值的不断挖掘，越来越多的企业和个人认识到数据泄漏对个人隐私安全、企业商业秘密乃至国家安全可能构成的严重威胁；国家也在通过《个人信息保护法》、《数据安全法》等一系列法律法规的出台来约束数据使用的合规性。如何通过可证明安全的技术手段，保障数据价值的可控、可信流动，支持数据要素的共享与增值，已经成为数据要素资本化的重要前提。

以密码技术为基础，构筑数据要素的共享与增值服务，将是实现数据价值共享与增值的重要手段:

一是基于信任服务基础设施，通过数据指纹、数字签名与时间戳技术，构建数据资产的“产权证”，实现数字资产确权;

二是利用同态加密、多方安全计算等隐私计算技术，实现密文状态下的数据运算处理，实现数据价值的可控共享;

三是通过区块链技术，构建基于共识的价值互联网络，为

数据价值的流转、交易与变现提供底层能力支持。

密码技术从资产确权、隐私利用、价值流通三个方面，帮助实现数据价值的有效交易，实现基于工业互联网密码应用的创新发展。

三、工业互联网密码能力供给

工业互联网密码应用的发展依赖于密码相关产业链的供给能力。当前，我国密码产品种类齐全，初步形成了从密码芯片、板卡、整机到系统和服务的完整产业链，面向工业互联网等特定领域需求的密码应用产业链供给能力基本具备，但部分环节个性化能力仍有待提升。以下对工业互联网中密码应用相关产业链供给能力做了简要梳理。

（一）密码理论支撑

1. 通用的商用密码算法和协议

我国的商用密码算法主要包括 ZUC、SM2、SM3、SM4 和 SM9。以 ZUC 算法为核心的加密算法 128-EEA3 和完整性保护算法 128-EIA3，与美国 AES、欧洲 SNOW 3G 共同成为 4G 移动通信密码算法国际标准，主要用于 4G 移动通信中移动用户设备和无线网络控制设备之间的无线链路上通信信令和数据的加解密和完整性校验，适用于工业互联网的网络通信安全防护。SM2 算法可以满足应用中的身份鉴别和数据完整性、信息来源真实性的安全需求,与 RSA 算法相比，SM2 算法具有以下优势：一是安全性高，二是密钥短，三是签名速度快。利用 SM3 杂凑算法可生成 HMAC，用作数据完整

性检验和消息鉴别，检验数据是否被非授权修改以及保证消息源的真实性。SM4 算法主要用于加解密，实现起来较为简单，不仅适用于软件编程实现，更适合硬件芯片实现。SM9 算法是一种标识密码（Identity-Based Cryptography, IBC)，用户的公钥就是用户的唯一身份标识，该算法解决了 PKI 需要大量交换数字证书的问题，使安全应用更加易于部署和使用。

密码协议是指两个或以上参与者使用密码算法时，为达到加密保护或安全认证目的而约定的交互规则，一般包括密钥交换协议、实体鉴别协议和 IPSec、SSL 等综合的密码协议。我国国家标准 GB/T 15843 系列规定了进行实体鉴别的机制，包括采用对称加密算法的机制、采用数字签名技术的机制、采用密码校验函数的机制、采用零知识技术的机制以及采用人工数据传递的机制。IPSec 和 SSL 支持采用多种密码技术为通信交互中的数据提供安全防护，IPSec 工作在网络层，一般用于两个子网间的通信，SSL 工作在应用层和传输层，一般用于终端到子网间的通信，我国于 2014 年先后发布了密码行业标准 GM/T 0022-2014《IPSec VPN 技术规范》和 GM/T 0024-2014《SSL VPN 技术规范》。

2.基于标识的密码体制

随着工业互联网、物联网技术的快速发展，终端设备激增已经成为必然趋势。基于证书的公钥加密体制将面临严峻的证书管理问题。为了便于工业互联网实现终端设备快速、便捷的无线接入，基于标识的密码体制受到广泛关注。IBC 是一种基于实体身份标识生成密钥的密码体制，实体公钥可由其身份标识得到，相

应的私钥由可信第三方密钥服务器产生，无需颁发公钥证书，解决了基于证书的公钥加密体制在证书存储和管理过程中开销过大的问题。

在工业互联网系统中，IBC 的应用能够提供简洁的密钥管理、极低的带宽和存储开销、高效密码算法实现、同时支持强不可抵赖的身份认证能力。IBC 以设备 ID、用户手机号等为标识公钥，分发专属私钥，不需要预先注册数字证书及认证，实现可信的身份认证。也不需要建设证书中心，仅需要使用密钥管理中心，避免了工业互联网巨大的设备数字证书及存储问题，极大地减少了平台维护、管理和使用成本。在系统设计上，可以支持国产 SM9 算法，保证了密钥产生、分发及运算的安全。在工业互联网安全应用扩展上，可以和 RFID 等技术相结合。

3. 适用于物联网的轻量级算法

物联网的应用组件是计算能力相对较弱的嵌入式处理器，计算可使用存储往往较小，且考虑到各种设备的功能需求，能耗必须限制在某个范围之内。传统的密码算法无法很好地适用于这种环境，适用于资源受限环境的密码算法就是所谓的轻量级密码，包括轻量级的分组密码、流密码、数字签名等。目前资源受限环境的硬件缺乏统一的国际标准，而且轻量级密码还处于发展阶段，所以对于轻量级密码算法并没有统一的衡量和评价的标准体系。

轻量级密码与传统密码相比有几个特点：首先，资源受限的应用环境通常处理的数据规模比较小，因此，对轻量级密码吞吐量的要求比普通密码要低的多；其次，RFID 和传感器等应用通常

对安全性的要求不是很高，适中的安全级别即可；再者，轻量级密码大多采用硬件实现，由于实现环境条件的限制，除了安全性之外，轻量级密码算法追求的首要目标是占用空间小及实现效率高。简单的说，就是应用环境对轻量级密码硬件实现的芯片大小有严格的限制。在这些环境下，为了实现目标，轻量级密码有的不实现密钥扩展算法而是采用机器内置密钥；有的不提供解密算法。这些特点使得轻量级密码的密钥长度多为 64 比特和 80 比特。随着普适计算、物联网技术的发展，轻量级密码会被应用在工业互联网的多种场合。

典型的轻量级算法有 PRESENT 算法、LBlock 算法（又称鲁班锁）、Grain 系列算法、SM7 算法等。其中，SM7 算法是我国商用密码算法系列的分组密码算法，适用于非接触式 IC 卡，常见的门禁卡即可基于 SM7 算法实现身份鉴别；LBlock 是中国科学院软件研究所的密码专家团队设计的，具有很高效的性能；Grain v1 是 eSTREAM 计划最后的 7 个胜选算法之一，具有很高的安全特性。

4.适用于隐私保护的密码技术

工业互联网是云计算平台的延伸，继承了云计算平台的特性，同态加密和多方安全计算等密码技术是云环境下的隐私保护问题的重要解决手段。

（1）同态加密

同态加密是一类加密算法，有同态的性质，用户对密文进行运算后再解密得到的结果与直接对明文进行运算得到的结果一致。同态加密已经运用在云计算平台，但是全同态加密的效率很低，

目前尚未实用。在云计算环境中，该协议可以充分利用云服务器的计算能力，实现对明文信息的运算，而不会有损私有数据的私密性。可用于构建安全多方计算协议、零知识证明协议等。可用于基于云的数据共享平台，数据拥有者可以对存储在云端的资源进行计算。

（2）安全多方计算

安全多方计算解决的是独立数据拥有者可以在不信任对方以及第三方的情况下进行隐私协同计算。不同于传统的计算场景，工业互联网云平台用户需要把数据和计算外包给云，因此用户将失去对资源和数据的完全控制，安全多方计算的特点对于云计算的安全保障有得天独厚的优势。多方安全计算可用在工业互联网资源共享计算环节，在无信任中心情况下，执行协同计算，使数据真正达到可用不可见。

（二）密码产品供给

1. 通用类

（1）密码安全模块

密码安全模块支持国产密码算法，可以提供高性能的数据签名/验签、加密/解密的要求，以及简单的密钥管理功能，部署在工业互联网的设备层，为工控现场设备、控制器提供传输加密、身份鉴别、访问控制等功能，需要与工控加密网关配套使用。嵌入式密码安全模块适用于具备集成能力的部分现场设备层智能终端和现场控制层控制器。非嵌入式密码安全模块适

用于不具备集成能力的现场设备和控制器，以外接的形式部署在现场设备和控制器侧。

（2）工控加密网关

工控加密网关配套密码安全模块使用，部署在工业互联网边缘层，适用于通过广域网进行数据传输的场景。工控加密网关与密码安全模块通过设备证书进行双向身份认证，采用 IPSec VPN 隧道技术，与密码安全模块在不可信信道上，构建安全可靠的虚拟专用数据通道，为传输数据提供机密性、完整性保护以及数据源鉴别和抗重放攻击等安全保障。工控加密网关采用内外双主机系统架构，内、外端主机间通过非网络方式隔离进行通信，实现上层工控系统与广域网之间的物理隔离。

（3）SSL VPN 安全网关

SSL VPN 安全网关基于密码运算、访问控制、协议代理等安全技术手段，为工业互联网的业务系统提供实现对用户的身份识别及其访问应用系统的权限管控，并对应用数据的机密性、完整性进行保护，对网络边界进行安全防护。

（4）数据库加密系统

数据库加密系统用于保证工业数据在存储过程中的安全性和完整性。在敏感数据写入历史数据库之前，根据不同数据库的表结构组织形式，数据库加密系统对敏感数据进行部分或全部加密，用户在读取对应的敏感数据时，通过数据库加密系统将数据解密后读取。

（5）IPSec VPN

通过 IPSec VPN 在各层之间建立安全通道，对所有进出网络的信息进行基于策略的访问控制，并完成对通信双方的身份认证、通信数据的加密/解密，满足用户网络跨区域互联互通私密性、完整性和抗抵赖的安全需求。

（6）密钥管理系统

密钥管理系统支持完善的对称密钥和非对称密钥管理应用体系，提供对称密钥和非对称密钥全生命周期在线和离线管理，包括密钥产生、密钥分发、密钥更新、密钥撤消、密钥恢复、密钥归档等功能。系统提供三权分立策略，对管理人员身份鉴别及登录控制，杜绝非法用户登录访问系统。

（7）数字证书认证系统

数字证书认证系统基于 PKI 技术，实现了用户注册、审核，密钥产生、分发，证书制证、签发、发布、下载、查询等一系列完整的证书中心服务功能，使应用系统能够方便的使用加密和数字签名技术，从而保证网络信息传输的机密性、真实性、完整性和不可否认性，为应用和用户建立起一个安全的网络运行环境。

2. 云服务类

（1）云服务器密码机

云服务器密码机采用虚拟化技术，按需生成多台虚拟密码机(以下简称 VSM)并提供密钥管理和密码运算服务，满足云计算环境、传统计算环境中数据加密保护、金融支付、密钥管理及身份认证等安全需求。云服务器密码机采用安全隔离技术实

现各 VSM 密钥在存储和使用过程中的安全，支持管理通道和业务通道的安全防护，支持多台 VSM 组建集群，并具有负载均衡，可提供高可用的密码服务，保障用户业务的连续性。

（2）云密码资源池管理平台

云密码资源池管理平台基于 OpenStack 云平台，将原本静态分配的密码机作为密码资源池的抽象集合，以池化机制为云密码机对外提供可按需分配、弹性伸缩的云密码服务资源；通过对密码资源池的统一管理实现密码资源的申请、共享、调度、按需分配，为运维人员提供密码资源监控、部署、回收等云密码资源池运维功能，可降低运营成本，提高管理效率。

（3）云密钥和云证书管理系统

云密钥管理是在密码资源池基础设施的基础上，为平台服务商、用户提供密钥托管相关的支持活动，如密钥托管服务、密钥安全隔离和存储服务、密钥安全访问服务、密钥的策略控制服务等。基于云计算的弹性计算特点和 CA 系统的特点，把包括远程用户注册管理系统、 OCSP 及 CRL 证书状态查询服务、LDAP 证书发布系统等服务层的子系统迁移到云上，可有效提升 CA 的服务性能，并能满足安全管理要求。

（三）创新密码服务

1. 高安全切片

网络切片是指根据不同的业务对网络的需求不同，通过网络资源进行灵活分配，按需组网。作为 5G 网络关键技术，网络

切片是在虚拟化技术的基础上，将多个虚拟网络功能进行动态裁剪、编排并部署，形成相互独立的虚拟网络，每个虚拟网络可根据用户需求提供定制化。随着 5G 技术在工业互联网领域的应用探索，对网络功能虚拟化技术也提出了更高的安全要求。

网络切片在支撑多样化工控场景的同时，也提供不同的安全服务，从而确保工控数据与网络信令的机密性和完整性，保障终端设备安全入网，保护厂商和用户的隐私。高安全切片要求网络切片可按需定制安全保护机制，从而提供相应的安全服务，包括身份管理、权限管理、切片识别、切片配置、密码算法和安全协议更新、运行周期管理、切片实例化安全和用户数据安全传输等功能。

2. 云访问安全代理

云访问安全代理（Cloud access security broker， CASB）是内部部署或基于云的安全策略实施点，位于云服务使用者和云服务提供商之间，以在访问基于云的资源时合并和插入企业安全策略。 CASB 整合了多种类型的安全策略实施。示例性安全策略包括身份验证、单点登录、授权、凭据映射、设备配置文件、加密、令牌化、日志记录、警报、恶意软件检测/预防等。

云访问安全代理提供如下功能:

（1）可见性: 能够对所有的云服务进行业务风险的发现和评估，并提供集中化的视图展示;

（2）合规性: 遵照地方性的法律法规或行业性的规定，从而为企业规避法律或政策风险;

（3）数据安全：通过了解云上数据的状态，通过数据防泄漏、数据加密等数据保护措施，保护数据安全；

（4）威胁防护：通过建立威胁情报库，不断更新威胁情报，并对进出云计算平台的数据进行检查和比对，及时发现威胁并采取相应的安全措施。

3. 区块链即服务

区块链即服务（Blockchain as a Service，BaaS）是一种帮助用户创建、管理和维护企业级区块链网络及应用的服务平台。它具有降低开发及使用成本，兼顾快速部署、方便易用、高安全可靠等特性，是为区块链应用开发者提供区块链服务能力的平台。BaaS 通过把计算资源、通讯资源、存储资源，以及上层的区块链记账能力、区块链应用开发能力、区块链配套设施能力转化为可编程接口，让应用开发过程和应用部署过程简单而高效。同时通过标准化的能力建设，保障区块链应用的安全可靠，对区块链业务的运营提供支撑，解决弹性、安全性、性能等运营难题，让开发者专注开发。

BaaS 可用于保障工业互联网中各类数据的真实性与完整性，实现数据权益保护。将工业互联网采集数据存储在 BaaS 上，能够从源头保护工业互联网数据完整性，方便对工业互联网数据的取证、鉴定、保全以及出证，保障数据在全生命周期的证明力。将工业互联网标识数据存储在 BaaS 上，方便对标识身份进行分布式验证，支撑对标识数据进行全生命周期的可信管理，包括注册、主体身份信息变更、属性数据更新、注销回收等。

BaaS 可用于实现工业互联网中的信息可信共享协作，通过智能合约实现工业互联网信息的多方共识验证，防止信息的篡改，同时结合匿名隐私保护技术，实现信息的安全共享与可信的价值交换，提升工业互联网安全可信生产能力。BaaS 可打通跨企业、跨平台的可信数据交互渠道，实现可信、可追溯的数据录入和基于身份认证及访问控制的数据共享，保障企业及平台方的数据权属，支撑工业互联网数据治理，促进工业互联网企业及平台的互联互通。

传统的信息化模式对于已经形成的数字化文件信息在各个节点的传递过程中，缺乏强大的数据保护措施，会出现数据文件的失窃和篡改的可能性。利用区块链多方参与的特性，在区块链网络中接入监管节点，可以在不影响原有生产及操作流程的基础上，快速同步区块链存储数据，支撑监管部门对工业互联网数据进行柔性监管与合规审计。

4. 隐私计算平台

隐私计算平台指面向隐私保护的计算系统，涵盖数据的产生、存储、计算、应用、销毁等信息流程全过程，想要达成的效果是使数据在各个环节中“可用不可见”。从技术角度出发，和隐私计算相关联的技术包括多方安全计算、可信执行环境、联邦学习、差分隐私、区块链等。目前业内采用的主流技术包括三类：多方安全计算、联邦学习和可信执行环境。

隐私计算平台应用于工业领域，可保障工业数据在共享流通过程中不被数据拥有者之外的任何人获取，同时通过隐私计

算平台又可以实现不同企业间进行数据的任意计算、查询等操作。

5. 统一身份认证服务

工业互联网环境下,用户在多个不同的系统上完成业务工作将成为一种新常态。因而,如何在保障系统安全性的情况下简化用户的登录操作、提高工作效率、提高系统的易用性成为工业互联网应用系统和平台的重要使命之一,这使得统一身份认证系统的地位变得愈加重要。

通过证书、指纹认证、扫码登录 PC 应用等方式，实现统一身份认证和单点登录，在提升安全等级的同时，也大大提高用户工作效率，降低工业企业管理成本。

6. 统一密码服务平台

统一密码服务平台密码技术结合云架构、虚拟化、多租户等技术，实现密码功能以云服务形式提供给业务系统或用户。统一密码服务平台支持全栈式密码功能，以应对不同模式的业务系统。对基础设施即服务（IaaS）形式部署的应用，统一密码服务支持以虚拟密码模块、虚拟密码机或虚拟密码系统的形式提供；对平台即服务（PaaS）形式部署的应用，支持以开放平台即可使用密码云所提供的密码能力，业务系统通过 SDK 完成密码功能调用；对于软件即服务形式的应用，支持各种密码功能的业务化封装，形成若干逻辑上独立的业务单元，完整交付用户。

同时，密码云通过统一配置管理提供先进的实时自动化智能化的运营管理能力。支持密码服务创建、发布、上线、下线、销毁等环节的全流程全自动部署，在不影响业务实时运转的情况下，实现灰度部署，密码服务快速发布上线，自动回滚、自动备份。

（四）体系化密码保障

1. 密钥管理

工业互联网场景下的工业系统和设备使用大量的工业专有协议，产生了大量加解密密钥。密钥管理成为实现工业互联网数据加密传输、存储的关键能力。密钥管理中心（KMI）是实现密钥管理的主要手段，覆盖了密钥自产生到最终销毁的全生命周期,包括系统初始化,密钥的生成、分配、存储、备份、恢复、吊销、销毁、保护、丢失等。作为一种安全基础设施，PKI 可以为工业互联网应用和平台提供电子认证服务基础，实现各类用户证书的申请、审核、颁发、注销、更新等服务，同时实现数字证书的生命周期管理。采用基于密码的 PKI/CA 机制可以有效保障工业互联网的身份认证、授权管理。

2. 密码态势感知平台

密码态势感知平台可采用不同的架构方式，根据业务类型提供规范的数据接口，SDK 客户端以被动+主动的方式采集密码应用相关数据，并实时将分散在各种密码设备的多源异构数据集中聚合，服务端将数据存储在数据库中，集中管理。平台监

控引擎实时分析各项监控指标的数据，发现异常问题并以告警和公告的方式通报各密码设备的安全问题。

3.密码监管平台

通过分析引擎多维度业务数据统计以及业务趋势预测深度感知密码应用状况。向上级监管部门提供管理引擎，自动化输出各种类型的密码应用统计报告，支撑运维、审计、业务分析等。通过可视化技术将密码资产数据、密码设备监控数据、业务应用密码合理性，合规性，安全性数据、分析数据、运维数据通过交互图表、地理信息等形式向监管部门提供全面的密码应用监管信息。

4.密码应急响应平台

对密码应用系统自身进行安全预警，提供利用流量分析平台、第三方流量探针、IISOC、云监测等系统接收上报的安全事件，并对安全事件从业务角度进行汇总分析，其内容包括数据查询（行业、时间、IP 地址）、安全事件分布、安全态势、安全事件类型排名、源地址排名、目的地址排名、攻击类型排名、行业攻击分布、DDOS 攻击方式分布、DDOS 攻击行业分布、DDOS 攻击站点排行、DDOS 攻击单位列表、安全事件态势、风险和安全事件等以及利用地图直观展现辖区监测单系统安全事件的分布情况并实现可视化呈现。

四、工业互联网密码应用实践

（一）海尔卡奥斯平台

1. 密码应用需求及痛点

海尔在数字化转型过程中，在密码应用方面产生了如下几点需求：

（1）设备安全认证

海尔的工厂、园区遍布国内，在海外也有覆盖，每个园区、厂区、生产车间内有众多工业制造及相关业务的机器设备（传感器、机器、控制器、执行器、监视器等等）。这些机器设备种类繁多、数量巨大，如何进行海量设备身份标识、认证、鉴别，这是当前海尔数字化转型的一大难点和痛点。

（2）数据通信加密

对于海尔来说，数据通信涉及到多个层面：设备与设备之间、设备与控制器之间、控制器与平台之间、平台之间、车间之间、厂区之间、园区之间。在任意两个实体之间进行通信时都需要考虑数据的加密保护、防泄漏、防篡改。离生产设备越近，设备对数据实时性要求越高，设备对数据传输的性能要求也就越高，进而对数据加密的性能要求也越高。如何在生产设备端提供轻量级、高安全的通信数据加密方案，并且在不同层次提供不同性能的加密方案，是海尔在数字化转型过程中的另一大难点和痛点。

（3）敏感数据加密保护

工业生产数据属于企业核心机密，具体涉及客户信息、订单数据、库存信息、产量数据、图纸、配方、流程、参数等等，这些数据涉及专利、软著等知识产权保护或者其他商业利益，

一旦这些数据发生泄露、篡改、丢失，将会给企业带来巨大利益损失，因此必须对此类数据进行加密存储、严格防护。如何对此类数据进行敏感性分类、分级，并制定不同类别、级别的数据加密方案，也是海尔当前数字化转型过程中的一大难点和痛点。

（4）密码产品替换成本高、周期长

密码技术产品一旦投入使用，其升级成本极高，且国产密码的市场接受周期长，导致企业重新更换密码产品的成本非常高。尤其是在工业控制系统中更是如此。一方面，传统工控系统应用程序和协议最初在设计开发时并未采用认证和加密机制以及其他安全策略来防护系统安全。另一方面，工控系统本身具有关键性和敏感性，产品、技术、算法升级可能导致未知风险。再者，工控系统对于实时性的要求高，集成密码算法会消耗设备的计算能力，影响系统的功能性、实时性。

2. 密码应用现状

卡奥斯云平台密码应用安全解决方案结合云计算架构的特点（计算资源虚拟化、数据集中化、应用服务化）以及云的应用场景，通过与统一身份认证与数字证书等安全保障应用集成，形成全方位、多层次、多维度、立体纵深的以密码为核心的云计算安全保障体系，对卡奥斯内部提供通用与典型密码应用。

从资源层、服务层、云业务平台密码应用、云安全管理密码应用、云平台可信接入密码应用、安全通信网络、用户层安全密码应用等几个层面分别对不同层次中的主机、网络、数据

存储、用户身份、终端身份等进行基于密码的安全性验证。

（1）IoT 安全网关建设

卡奥斯目前正在建设安全网关认证系统，该系统主要解决的是 IoT 终端身份可信认证问题。该系统包含网关设备和云端设备管理平台两部分。网关设备部署在工控终端的网关位置，负责采集各工控终端信息后上送至云端管理平台进行工控终端身份信息的验证、查询。

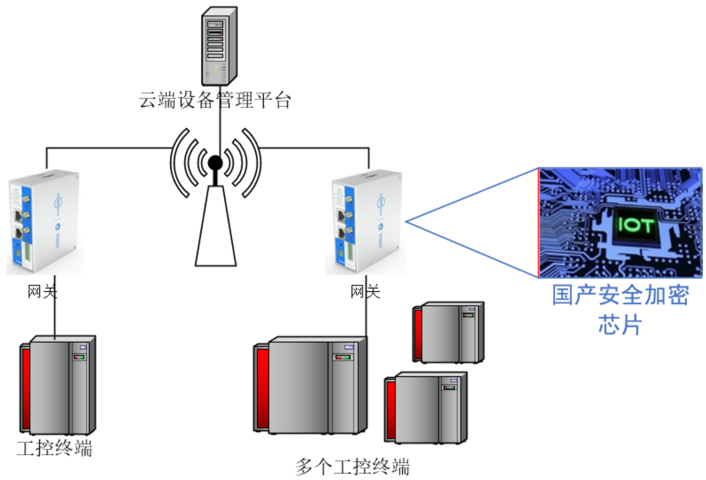

图 4.1　IoT 安全网关部署

网关设备采用安全加密芯片，芯片已经固化设备自身身份信息，每次与管理平台通信时都需要从芯片中获取已经加密的设备身份信息并随通信数据发送。同时，加密密钥也存储在芯片中。

（2）数据安全建设

卡奥斯从数据内容本身层面着手，有效防护数据泄露的风险。首先，采用自建数据加密平台进行数据加密，解决数据与云平台服务商之间的信任问题；其次，对数据采用国密加密算法进行加密，最大限度符合安全法律法规要求，并且切实确保

数据在存储阶段不被泄露。

卡奥斯数据存储安全逻辑架构如下图所示：

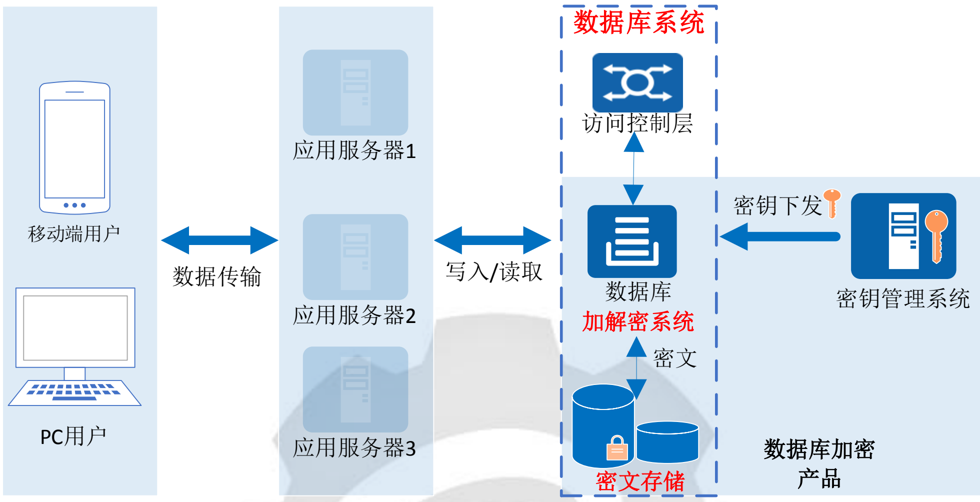

图 4.2　数据存储安全逻辑架构

存储加密业务时，业务系统数据传输到数据库中，直接通过加解密系统自动加密，加密后数据以密文的形式存储，用户层面无感知，在不修改原有数据库应用程序的情况下实现数据存储加密。

卡奥斯传输加密方案采用标准的国密 SM2、SM3、SM4 加密算法，严格遵循国密局商用密码产品有关密码算法的使用要求和技术规范。建立了终端用户到服务端的数据传输安全防护体系，终端动态加载透明加密模块，强化身份合法鉴别、保证终端数据传输安全。

（3）态势感知平台建设

卡奥斯通过建设态势感知平台，结合漏洞扫描、日志审计、APT 发现等产品能力，发现密码漏洞等安全风险并进行整改；同时，利用态势感知的综合关联分析能力感知密钥泄露、加解

密接口滥用等相关的威胁行为，并进行威胁通报预警和安全事件实时处置，以及对安全事件的事后取证、追踪溯源，最终实现为卡奥斯工业互联网平台密码应用进行综合防护的目的。

（4）密码应用与零信任架构深入融合

传统的网络边界日渐模糊，传统的安全架构被打破，以智能身份访问控制平台为核心的零信任安全架构体系逐渐成为网络安全的主流。在零信任体系的实践中，海尔卡奥斯将密码与用户、设备和服务的身份识别紧密结合，构建增强的身份管理机制，形成策略制定的关键组成部分，为卡奥斯提供更为可靠的安全基础设施，并保障卡奥斯云平台高效达成等保 2.0、密评的相关测评要求。

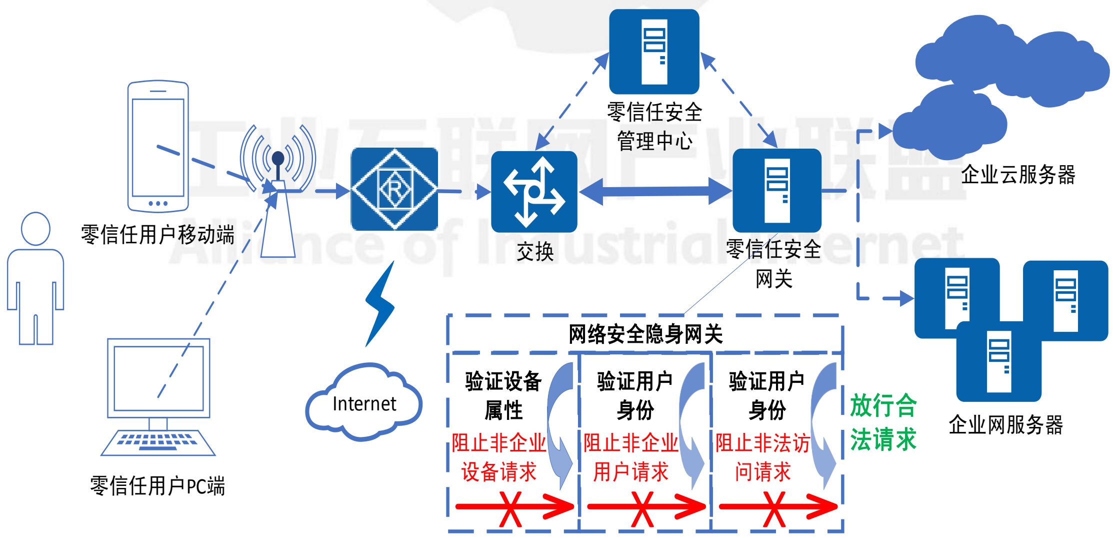

图 4.3　零信任安全架构体系

（二）徐工汉云平台

1. 密码应用需求及痛点

由于工业互联网终端主体身份及归属不同，所以要在交错的网络节点间通信确保身份合法性，同时满足不同终端形态的计算能力和硬件属性，保证相互之间的身份合法性和高效认证。需要分析工业互联网的业务形态和技术特点，利用现代密码技术原理，搭建通用的身份识别与信任体系架构，以适用于不同业务体系，不同终端形态及技术形态的身份安全认证。

2. 密码应用现状

汉云通过对工业互联网平台终端设备注册接入、网络通信、数据传输、数据存储、服务器等方面的密码应用，构建了汉云工业互联网平台密码软硬件服务设施。总体架构如图：

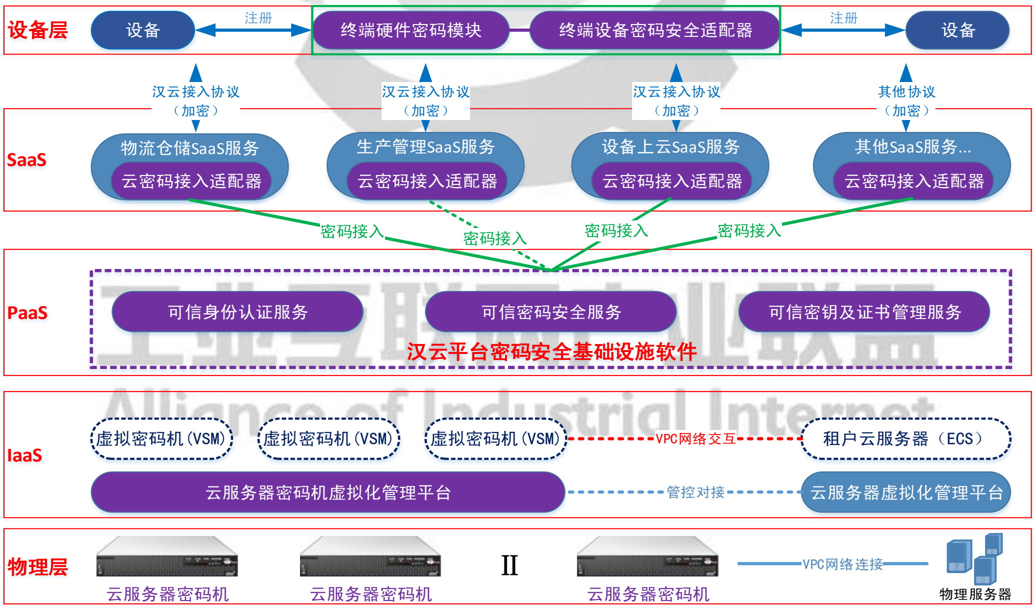

图 4.4　徐工汉云平台密码应用总体架构图

（1）物理层部署云服务器密码机提供密码的硬加密最高安全等级的密码安全运算能力；

（2）IaaS 层基于物理层云服务器密码机构建租户（工业应用企业）虚拟密码机服务，通过云服务器密码机虚拟化管理

平台完成物理密码机和租户虚拟密码机的统一管控，实现密码运算资源的虚拟化，提供弹性硬件密码运算资源动态调配能力；

（3）PaaS 层构建可信密码安全服务、可信密钥及证书管理服务、可信身份认证服务，基于多租户的方式提供工业互联网应用场景下的各类密码服务；

（4）SaaS 层基于虚拟密码机、可信密码安全服务、可信密钥及证书管理服务、可信身份认证服务构建工业应用系统的密码接入适配器，通过密码安全适配中间件为各类控制系统提供密码安全接入能力以及数据安全传输、存储能力；

（5）设备层基于终端硬件密码模块和终端密码安全接口中间件为各类终端提供终端密码安全注册接入能力。

（三） 工业无线网 WIA-FA 安全组网

1.密码应用需求及痛点

WIA-FA 技术规范是面向离散制造业工厂自动化应用中高并发、高实时、高可靠的现场传感器/执行器接入需求而研制开发的一种工作在 2.4GHz/5GHz ISM 频段的工业无线网络解决方案。工厂自动化属于高速控制应用，WIA-FA 无线网络设备的数据更新周期小于 10ms、可靠性高达 99.99%以上。WIA-FA 技术与 2011 年完成的面向过程自动化的 WIA-PA 技术标准（IEC62601），构成了全面覆盖流程工业和离散制造业的工业互联网基础技术体系，标志着我国在工业互联网技术领域的研究取得重大进展。

如果将工业控制系统比作国家关键基础设施的“中枢”，

无线传输信号就是保证其顺畅、高速、稳定连接的神经，其安全问题将直接影响关键基础设施的正常运行。无线信号传输中需要考虑数据的加密保护、防泄漏、防篡改，确保数据的机密性、完整性和不可篡改性。

2.密码应用现状

工业无线网 WIA-FA 安全组网为增强星型拓扑结构，包括一个中心及若干现场设备。中心由一个网关设备（可存在冗余网关设备）及一个或多个接入设备组成。WIA-FA 网络中共有四类设备：网关设备（GW，Gateway Device），接入设备（AD，Access Device），现场设备（FD，Field Device），手持设备（HD，Handheld Device）。网络拓扑图如下：

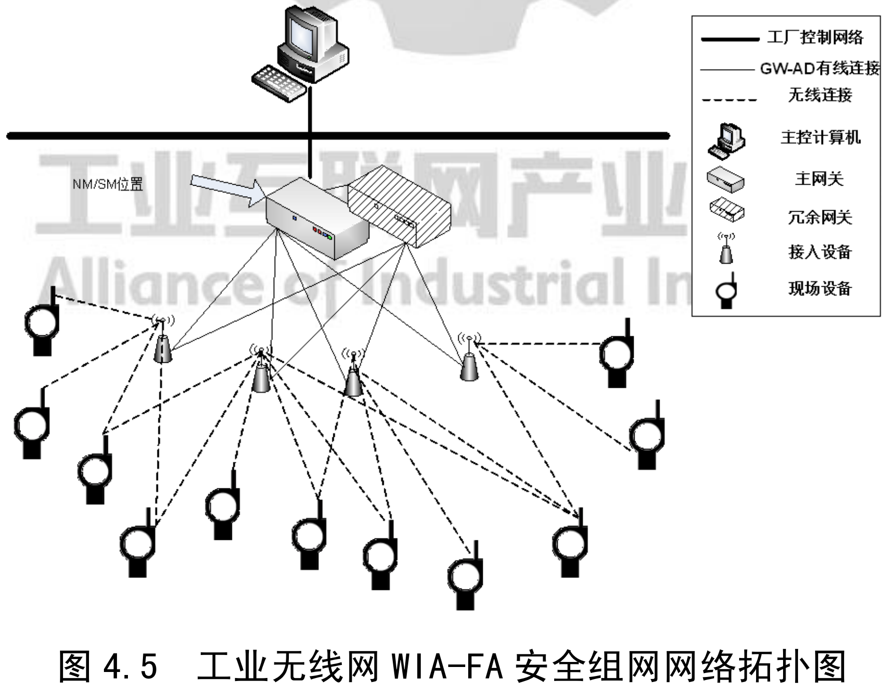

图 4.5　工业无线网 WIA-FA 安全组网网络拓扑图

（1）网关设备是连接 WIA-FA 网络与其他网络的设备，网关设备包括以下主要功能：

- 提供 WIA-FA 网络与现场总线等外部网络连接的接口，利用数据映射和协议转换功能实现 WIA-FA 网络与现场总线等外部网络的互连;
- 负责网络管理和安全管理功能;
- 通过接入设备与 WIA-FA 网络中的其他设备进行通信，交换设备间的信息;
- 作为全网唯一的时钟源，实现网络时间同步。

（2）接入设备安装在工业现场，与网关设备之间以有线方式连接，负责将现场设备上的传感器数据、告警及网络管理相关信息转发到网关设备，或将网关设备的控制信号、管理信息和配置信息转发给现场设备。

（3）现场设备即无线节点，是安装在工业现场，连接生产设备或传感器、执行器，负责发送现场数据和接收控制命令。

网关设备、现场设备均内嵌有基于国产密码算法的硬件密码模块产品，通过密码模块对数据包进行加密，保证数据包即使被截获也无法还原数据。每个无线信号收发的数据报文都有密钥加密，密钥不定期更新，密钥产生算法和更新的周期都可以配置选择，从而保证通信过程中的数据安全。

五、应用推广面临的痛点

（一）密码技术支撑不足，适配产品品类较少

我国商用密码起步较晚，目前大部分工控系统已集成国外密码算法，工控系统国产化水平不高，全面应用商用密码具有

一定难度。而且工业互联网对业务实时性要求较高，集成密码算法可能会影响系统的功能性，消耗设备的计算能力。从密码基础技术的角度来说，满足工业互联网中轻量级、低时延加密认证需求的密码算法和密码产品尚未成熟，相关密码算法和产品标准尚未出台，与工业互联网适配的密码应用产品较少，无法完全满足工业互联网特殊场景下的密码需求。

（二）政策驱动有待强化，实施台账尚未制定

我国相继出台了《网络安全法》、《密码法》等法律政策，为推动密码技术特别是国产密码的商业化应用起到了至关重要的作用。其中，《密码法》明确了密码在网络信息安全中的支撑保障作用；等保 2.0 增加了对物联网、云计算、工业控制系统的安全防护要求。但是，由于工业互联网在我国出现时间尚短，尚未形成针对工业互联网领域应用密码技术的顶层指导性政策文件和具体实施指南，尚未制定工业互联网密码部署的时间台账，这也导致密码技术在工业互联网中应用时缺乏统一的政策指导，虽然依据等保 2.0 和 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》可以指导各个部分的密码建设，却无法形成统一的整体化建设指导。

（三）商用密码认知薄弱，接受程度依然不高

虽然密码技术广泛应用于各类信息系统之中，但是由于密码技术本身较为艰深晦涩，用户通常对密码的原理了解不深，且由于密码技术通常承担着底层防护的功能，导致用户对于密

码技术的感知也较为薄弱，这在很大程度上使用户忽略了密码发挥的巨大作用。因此，在现有的工业互联网系统中，用户往往忽视了密码技术的重要作用，导致用户缺乏为密码产品买单的意愿。另外，大多工业企业缺少网络安全、信息安全人员，应用密码来保障安全的意识淡薄，最初在设计开发时并未采用认证和加密机制以及其他安全策略来防护相关系统、设备的安全。

（四）投资成本有所增加，后期收益无法预判

商用密码应用是系统化、体系化的密码应用改造和升级。对于工业互联网用户，需要增加部署 PKI 系统、添置加解密硬件资源（安全芯片、加密机、安全网关、云密码设备等）、应用软件改造升级等，这需要投入额外的时间、人力和物力。对于密码企业，开发一款工业互联网密码产品的投入较高，要与业务系统进行反复的联调测试以保证适配业务系统的需求。因此，在市场需求和商业模式尚不清楚的情况下，密码厂商很难投入大量成本进行新产品的开发，往往使用现有的产品勉强应付各种工业互联网场景的需求，这也导致了对于工业互联网场景的适配性差，影响了密码技术在工业互联网中的应用。

六、发展建议

（一）监管合规

应遵照《网络安全法》、《密码法》、《数据安全法》等相关法律的要求，尽快从国家层面出台密码技术在工业互联网

中应用的指导性政策，围绕工业互联网的密码应用需求，加大对工业互联网密码应用的支持力度，监督工业互联网服务企业、应用企业对密码技术的应用情况，定期开展工业互联网密码应用的安全性评估，推动工业互联网密码应用合规有效，保障工业互联网密码应用相关工作的开展和有效实施落地。

（二）标准制定

应尽快制定工业互联网领域相关的密码标准，包括密码技术、密码产品、密码管理等标准，通过标准化活动促进接口统一、产品兼容、服务互认，逐步形成工业互联网密码应用标准体系，指导密码技术、产品及服务在工业互联网中应用推广，促进密码应用生态健康有序。工业互联网涉及的行业较多，如电力、能源、水利、矿山、机械、交通运输等，对于具体的行业场景有不同的业务需求，所以需要结合行业的具体业务需求和适用场景，定制对应的密码应用的技术要求、测试方法、管理要求等标准。

（三）试点示范

建议持续加大对工业互联网密码技术和产品的支持力度，开展工业互联网密码应用试点示范工作，鼓励密码厂商和工业互联网相关企业开展应用试点。通过有效的开展工业互联网密码应用的试点工作，落地并验证标准和对应的产品、系统、方案等，并通过实践有效地检验密码应用的效果。对密码应用前后的系统进行安全风险分析、评估和对比，对试点效果、经验

进行梳理和总结，并选取优秀的试点案例进行示范和扶持推广。通过试点示范和政策扶持工作，在实践中进一步推动密码应用的顺利发展和良性循环，通过试点示范打造优秀标杆，加强行业指导和引领，推动密码应用规模发展。

（四）技术攻关

建议持续加大对工业互联网领域密码技术和产品研发创新的支持力度，鼓励密码技术创新，在已有商用密码算法的基础上，进行技术攻关，拓展自主密码技术的应用场景。尽快突破云上虚拟环境加密、时延敏感网络加密、轻量级密码等工业互联网中密码技术应用的难题，建立适用于工业互联网的统一密码管理体系，支撑密码技术在工业互联网领域的广泛应用和快速发展。

（五）生态构建

充分发挥产业内企业的力量并联合高校、研究院，建立工业互联网领域商用密码技术专家团队，遴选或由各成员单位推荐密码技术专家、学者，对企业在工业互联网中的密码应用给出指导。通过产业内企业的不断合作，提出具有高可行性的工业互联网密码应用解决方案，构建相对完善的工业互联网商用密码产业生态。