5G 工厂网络安全白皮书

中国联通研究院

2023 年 5 月

版权声明

目 录

前 言

数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。二十大报告提出建设数字中国，加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。5G 应用的力度从“助力产业转型”演进成“推进新型工业化”。

5G 应用“扬帆”是推进 5G 赋能千行百业的着力点，在工业领域打造了 IT、CT、OT 深度融合新生态，实现重点领域 5G 应用深度和广度双突破。“5G+工业互联网”是 5G 应用“扬帆”的重要组成部分，5G 推动制造业从单点、局部信息技术应用向数字化、网络化、智能化转变。5G 工厂是推进“5G+工业互联网”高质量发展的关键抓手，加快“5G+工业互联网”新技术、新场景、新模式向工业生产各领域、各环节深度拓展，推进传统产业提质、降本、增效、绿色和安全发展。

随着 5G 工厂建设加速，工业网络边界也在不断的延伸。工业领域安全既面临来自互联网的外部威胁，又与工业生产的内部安全问题相互交织，安全风险更加严峻，体现在攻击路径增多、安全意识薄弱、数据安全等多个方面。传统的安全解决方案不能满足新的需求，必须建立 5G 工厂网络安全架构，助力新时期新形势下的工业信息安全能力提升，切实为制造强国和网络强国战

略的有效实施保驾护航。

本白皮书在深入研究 5G 网络、工控领域网络及工业企业数字转型遇到的安全问题，通过总结工业领域在新型工业化进程中的安全挑战，提出 5G 工厂网络安全参考架构，并对 5G 工厂安全所涉及的多种关键技术给出了详细介绍，为各行业、各企业开展 5G 工厂安全建设提供参考。

总策划：李红五　叶晓煜　李浩宇　梁　鹏　张建荣　范济安　张明山

主　编：周晓龙

副主编：柳　兴　冯冬芹　井　柯

编委会成员：

王　哲　王新宇　员晓雪　蒋美景　杨邦主　荆　雷　成　洁　王维治　胡文慧　蒋小燕　周　凯　潘松柏　万　刚　陈凤衍　张守华　谢武生　艾艳可　何　凯　聂智峰　孙振州　曾水祥　李　捷　范勇杰　赖羿明　柯　玮　林明峰　李剑锋　黄继烨　许毅鹏　庄　天　刘岩松　崔马剑　赵　磊　胡向亮　王晓翔　刘　峰

指导单位：中国联合网络通信有限公司政企客户事业群

中国联合网络通信有限公司网络与信息安全部

支持单位：浙江大学

杭州安恒信息技术股份有限公司

联通数字科技有限公司

浙江腾珑网安科技有限公司

中国联通(天津)工业互联网研究院

中国联通(江西)工业互联网研究院

中国联通(福建)工业互联网研究院

一、概述

（一）背景

工业制造是实体经济的基础，是国家经济的命脉所系，同时也是大国竞争中构筑未来发展战略优势的重要支撑，制造强国战略也成为中国实现伟大复兴的重要战略。工业互联网是新一代信息通信技术与工业经济深度融合的全新工业生态、关键基础设施和新型应用模式。5G 是实现人、机、物全面互联的新一代移动通信基础设施，是信息通信技术演进升级的重要方向。“5G+工业互联网”有利于推动工业化与信息化在更广范围、更深程度、更高水平实现融合发展，是经济社会高质量发展的有力抓手。“十四五”时期，通过实现金字塔式的“百千万”建设目标，推动全国 10000 家企业开展 5G 工厂建设，建成 1000 个特色鲜明 5G 工厂，遴选出 100 个 5G 工厂标杆。进一步加快“5G+工业互联网”新技术、新场景、新模式向工业生产各领域、各环节深度拓展，打造“5G+工业互联网”中国方案和 5G 工厂中国品牌。

5G 工厂为企业数字化转型提供了契机，数字化转型是企业利用数字技术彻底改变企业的运营效率、经营业绩，是企业提升竞争力的必由之路。5G 工厂是新一代信息技术与工业技术全方位深度融合所形成的产业和应用体系，是工业数字化和智能化发展的关键综合信息基础设施。其本质是以网络互联为基础，通过对工业数据的全面深度感知，实现智能控制、运营优化和生产组织方式变革，为企业数字化演进提供了技术保障和实践基础。5G 工厂的发展能够帮助企业快速实现数字化转型。

当前，我国“5G+工业互联网”创新发展进入快车道，5G 工厂在工业领域应用的重点将从生产外围辅助环节逐渐向生产中心控制环节迈进。作为数字经济的重要基础设施，新一代信息技术对制造业进行全方位、全角度、全链条的持续改造和优化，加速引爆工业格局的变革。5G 工厂作为新一代信息技术与制造业转型发展历史性融合创新期的新生事物，正在加速推进新型工业化进程。5G 工厂具有广阔的前景和无限的潜力，对于推动我国工业经济发展加快向更智能、更优质、更可持续的方向转型具有重要的价值和意义。

（二）事件及趋势

近几年，工控安全事件呈现高频率、高隐蔽、多样化特性。网络安全风险隐患向工业研发、生产、运行、管理、服务等产业链供应链各环节渗透，各类网络攻击事件层出不穷，有组织的、有针对性、国家级的网络攻击增多，后果影响日益严重。网络攻击带来的巨大利益和政治诉求让工业领域面临严峻的安全威胁，网络安全问题已经成为了一个全球性的问题，企业必须重视工业领域的安全，采取必要的措施来保护网络安全。

随着工业互联网应用范围的不断扩大，工控领域面临的安全风险不断增加。工业领域的安全事件频发，尤其在电力、石油、铁路运输、燃气、化工、制造业、能源、核应用等相关领域的关键网络一直都是全球攻击者的首选目标。据国家工信安全中心统计，2022 年公开披露的工业信息安全事件共 312 起；工业领域勒索事件共 89 起，较 2021 年增长 78%；工业领域数据泄漏事件共 338 起，比去年增长 25.2%。

这些攻击给个人、企业、国家带来了不同程度的损失。

工业领域的网络安全存在以下趋势：一是，第四次工业革命驱动工业数字化、网络化、智能化，使数据成为核心生产要素，因此工厂需要收集 IT、OT 等各领域数据，进而形成工厂 IT/OT 网络融合的趋势，使得工控安全与互联网安全交织在一起，安全问题变得更复杂；二是，合法指令的违规操作将成为常态，防火墙、数据网闸等传统 IT 网络安全措施难以有效形成防护，例如“震网病毒”可无视工业网络边界防护达成攻击目的；三是，工业数据交互、共享愈加频繁，数据共享和数据安全存在一定的冲突，使得工业数据存在较大的泄露、窃取、篡改等风险，单独的系统数据安全措施，难以形成有效的防护，需要通过对数据分类分级确权与授权，并辅以隐私计算、数据脱敏、数据清洗等技术手段予以保障；四是，勒索攻击等恶性事件显著增加，俄乌冲突更将网络战上升为实战，工业领域已成为网络攻防“新战场”，国家级战略打击“新命门”，保障新型工业融合领域网络安全成为新任务和新使命。因此，5G 工厂需立足于工业企业数字化转型实际，在发展中兼顾安全，建立健全工业企业网络安全保障体系，实现差异化、精准化的安全防护，为工厂建设筑牢网络和数据安全堤坝，力争做到工业企业高质量发展和高水平安全的动态平衡，为实现数字中国建设保驾护航。

二、工业领域安全政策与标准

（一）安全政策

网络安全作为我国经济社会数字化转型的关键驱动力，我国政府

从 2017 年至 2023 年，发布多个相关网络安全法律政策。《中华人民共和国网络安全法》自 2017 年 6 月 1 日正式施行，是我国第一部全面规范网络空间安全管理方面的基础性法律，对我国的网络空间法治建设具有重要的里程碑意义。工业企业网络安全关系到国家经济社会可持续发展，是事关国家长治久安的重大战略问题。为促使工业企业全面落实国家政策法规，持续打造基于自身核心竞争力的工业网络安全保障体系，筑牢企业安全基座，2021 年 9 月 1 日《中华人民共和国数据安全法》正式实施，2021 年 11 月 1 日《中华人民共和国个人信息保护法》正式实施。这两部法律分别聚焦数据安全与个人信息保护领域的突出问题，确立了数据分类分级管理、数据安全风险评估、数据安全审查、个人信息处理规则、个人信息处理者义务等制度。至此，中国网络安全与数据保护“三驾马车”法律体系正式形成，我国网络空间基本法律逐步成型。

在法律的指引下，国家部委针对工业领域网络安全发布系列政策文件。2017 年 11 月，国务院发布了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，成为推动工业互联网发展的纲领性文件，围绕制造强国和网络强国建设的安全保障需求，以“强化安全保障”和“安全可靠”为建设思路，以提升“安全保障能力”为发展目标。2019 年 7 月，工信部等十部门联合印发《加强工业互联网安全工作的指导意见》，成为推动工业互联网安全纲领性文件，指出了工业企业、监管部门和专业机构的能力建设方向，指出了明确责任和完善安全管理体系，指出了加快安全人才培养。2022 年 9 月，工信部

印发《5G 全连接工厂建设指南》中指出推进企业全面落实工业互联网企业网络安全分类分级管理相关政策与标准，提升设备、控制、网络、平台和数据等安全防护能力。

为更好地推动网络安全政策落地实施，工业和信息化部先后推动开展工业互联网安全深度行活动，深入宣贯工业互联网安全相关政策规范，推动在全国范围内深入实施工业互联网企业网络安全分类分级管理。开展工业互联网安全深度行活动典型案例和成效突出地区遴选工作，主要征集遴选一批安全防护举措有效、具备可复制可推广价值的分类分级管理典型案例，以及遴选一批做法创新有效、活动成效突出的先进地区。开展工业数据分类分级应用试点和工业领域数据安全管理试点等工作，在 5 个省市、9 个行业的 200 余家企业开展工业数据分类分级应用试点，同时在 15 个省市开展工业领域数据安全管理试点工作，促进工业数据分类分级在产业界应用落地。

无论是从工业数据分类分级试点情况来看，还是从企业自身网络安全分类分级工作来看，实施分类分级工作后，企业在网络安全和数据安全等方面都取得了明显的成效，提升了企业的硬实力，走在了行业的前列。企业通过分类分级提升数据汇聚能力、数据开放能力、数据治理能力，以安全策略为指导，构建起了全面、完整、高效的信息安全体系，为业务的创新发展提供了坚实的信息安全保障。随着国家顶层设计完善、底层落地得到大力支持、企业数据意识和安全意识等的不断提高、相关技术的不断进步，工业企业会更加认可 5G 在工厂中的安全应用，更多的企业开展 5G 工厂建设，帮助工业企业提质、

降本、增效、绿色、安全建设，从而提高整个行业的安全水平。

（二）安全标准

标准化工作是实现工业领域信息和网络安全的重要技术基础。各国政府高度重视工业领域的网络安全标准体系建设，以美国、欧盟为首的国家和组织纷纷出台政策，在原有的网络安全标准基础上，积极推动工业领域网络安全标准体系建设。美国国家标准与技术研究所（NIST）发布的《信息安全指南》（NIST SP800）是国际网络安全界广泛认可的工控标准纲领性文件，NIST SP800 定义了工业控制系统网络建设体系结构，目前已经发布近 90 项与信息网络安全相关的正式文件，形成了工控信息安全管理体系。国际标准组织 IEC 推出了《工业过程测量、控制和自动化网络与系统信息安全》（IEC 62443）为代表的工业控制系统信息安全系列标准，形成了包含电力、能源、机械、核工业等重工业领域的完整工控网络安全标准体系。针对 5G 网络安全，3GPP 发布了 TS33.501《5G 系统的安全架构和流程》，TR 33.813《网络切片增强的安全性研究》、TS 22.104《垂直领域中的网络物理控制应用的服务要求》等在 5G 网络安全和 5G 与工业互联网融合发展问题上提供了标准依据。

我国在工业领域网络安全标准体系建设相较于国外发达国家起步较晚，但发展迅速，至今已出台多部工业网络安全标准，涉及 5G 安全、工业互联网安全、工控安全等多个细分领域。据不完全统计，国内标准组织 CCSA、TC260 发布了 30 余项工业网络安全相关的国家标准，主要围绕工业自动化和控制系统、工业控制网络与信息两方面开

展研究，TC260 发布了《信息安全技术 工业互联网数据安全防护指南》、《信息安全技术 关键信息基础设施安全保护要求》、《信息安全技术 关键信息基础设施安全保护要求》、《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 工业互联网平台安全要求及评估规范》等一系列标准。CCSA 发布了《工业互联网网络安全总体要求》、《工业互联网平台安全防护要求》、《工业互联网数据安全保护要求》、《工业互联网安全态势感知系统技术要求》、《工业互联网数据安全分类分级指南》等安全标准。此外，在 5G 与工业互联网融合方面 CCSA 发布了《5G 移动通信网 安全技术要求》、《工业通信网络 网络和系统安全 系统安全要求和安全等级》等安全标准。

随着 5G 技术的成熟和推广，在《加强工业互联网安全工作的指导意见》等政策文件的助推下，工业互联网产业联盟、工业信息安全产业发展联盟、工业和信息化部商用密码应用推进标准工作组共同发布了《工业互联网安全标准体系（2021 年）》，提出要在各行业应用“5G+工业互联网应用安全技术”，使得 5G 技术逐渐纳入到工业领域网络安全标准体系的构建中。未来，随着 5G 工厂的逐步发展，工业网络安全标准体系与 5G 等新兴技术的联系越来越紧密。国家将重点布局工业 5G 网络安全标准，重点关注网络信息防护、工业 5G 网络设备的安全可靠性建设。

三、工业领域安全挑战

工业企业在数字化转型过程中，原本相互分割的 OT 和 IT 网络将逐渐交汇融合。OT 和 IT 网络的融合并非两张网络简单相连，而是以 5G、人工智能、物联网、云计算、大数据等为代表的新一代信息技术在工业领域中的应用，这将给工厂网络、数据、管理制度等带来诸多变化。与之而来的工厂信息安全变得复杂，安全风险呈现多元化特征，安全隐患发现门槛变得更高，安全形势进一步加剧。

（一）工厂终端

当前，我国大多数企业的工业现场设备存在种类繁多、新老设备参差不齐、系统漏洞升级更新慢、不同设备工业协议不同、联网难度大等特点。在传统工业生产中，现场设备是独立的个体，数字化、信息化、网络化程度较低，且网络安全防护建设落后于数字化信息化建设。虽然工业现场设备暴露于互联网上，极易被远程控制或者引发 DDoS 攻击，僵尸网络等问题，但是由于现场设备联网难度大使得设备相对独立，网络安全风险始终能得到有效控制。

工业企业完成数字化转型后，工业控制设备（PLC、RTU 等）、IT 终端设备（工作手机、工业 PAD 等）、智能终端设备（质检机器人、AGV 等）等设备将实现互联互通。当前现场设备自身的安全运行要求和规则尚不健全，终端设备彼此建立通信，设备的各种系统安全缺陷与漏洞也同样会引入到工业网络中，导致工业网络安全问题变得复杂。受工业特征的影响，现场终端设备的软件系统更新速度要远慢于工业企业完成数字化转型速度。大量含有漏洞的设备暴露于互联网上，一

旦这些终端被入侵者利用，容易形成规模化的设备僵尸网络，将成为新型高容量分布式拒绝服务（DDoS）攻击源，对工业应用、后台系统等构成巨大的安全威胁。

5G 工厂同样会面临含有漏洞的设备暴露于互联网上的问题，甚至会让传统不同域之间的终端设备彼此通信变得更加便捷，因此，需要设计有效的防护方式，减少终端设备的攻击面和攻击路径，将安全风险控制在可控范围内。

（二）AI 终端

5G 整合人工智能、数字孪生、云计算、AR、VR、边缘计算等各类新一代信息通信技术，在云、边、端统一架构平台上实现推理训练，支持快速的新模型迭代更新，有力的促进了 AI 技术在工业领域中的应用。近几年，AI 眼镜、AI 质检仪、AI 辅助决策仪、智慧分拣、智能 AGV 小车、智能环境监控仪等一批新 AI 终端和应用场景涌现，并不断向研发、生产等核心环节渗透赋能，在更大范围内发挥更核心的作用。AI 技术在工业领域成功大规模的应用，极大的提升了工业生产效率和企业管理效益，推动工业企业快速数字化转型。

人工智能会带来双刃剑效应，在赋能工业企业的同时，也给工业互联网带来了安全方面挑战。一是人工智能可被武器化，助力网络攻击。人工智能自我学习能力和自组织能力可用于寻找漏洞、破解密码等，提高网络攻击效率。二是人工智能可被滥用，威胁个人隐私。人工智能应用会增强信息采集和数据挖掘能力，加大了隐私泄露风险，甚至可能导致数据匿名化、数据脱敏等安全保护措施无效。三是人工

智能可决策失误，威胁人身安全。人工智能系统一旦出现感知、认知偏差或者受到网络攻击，系统就可能判断失误，并采取错误行动，甚至危及现场生产安全。

在工业领域大力发展人工智能的同时，必须高度重视 AI 技术可能带来的安全风险。5G 工厂作为工业企业数字化转型的信息基础设施，在促进人工智能技术在工业领域应用的同时，也应为人工智能应用提供防护，加强前瞻预防与约束引导，最大限度降低风险，确保人工智能技术在工业领域提供安全、可靠、可控的服务。

（三）工厂网络

传统工厂的网络架构以“两层三级”为主，包括了工业外网、工业 IT 网和工业 OT 网。IT 网络主要指基于互联网的网络应用，由管理业务数据、支撑管理流程的技术、系统和应用程序组成，常见的应用有 ERP、CRM、MES、OA 等。OT 网络是指传统工业控制网络，是由管理生产资产、保持顺畅运营的技术、系统和应用程序组成，常见的应用有 PLC、PCD、SCADA、SIS 等。传统工业网络中，IT 网络与 OT 网络相对独立，大部分工厂的 IT 与 OT 网络都物理隔离的，即便是需要连接都会采取网闸、防火墙等严格的安全隔离措施。

工业互联网以人、机、物全面互联为目标，实现工业设备及系统之间的数据流动，促使工厂围绕生产经营形成一个系统化的智能体系。工业互联网也会促进 OT 与 IT 网络融合，模糊并泛化了 OT 与 IT 网络的安全边界，让互联网领域的安全网络风险向工厂 OT 网络延伸。工业行业本身存在的网络工业协议设计缺陷、工业控制系统漏洞、网络

安全防护缺失等问题，工业企业虽然对传统工业网络采取了一定的安全防护措施，但其工业控制系统网络中存在的居多安全漏洞和风险隐患并未消除。融合带来的互联网安全风险，会与传统工业网络安全风险相互作用相互影响，形成了更为复杂严峻的工业网络安全挑战。工业互联网面临着攻击面广泛、攻击无处不在、平台网络风险日益严峻、物理安全威胁剧增等问题。

5G 工厂不仅会促进 IT 和 OT 网络走向融通，而且会扁平化传统工厂网络结构，使得工厂内的车间级和现场级网络的层级减少。5G 技术的开放特征将打破工业网络众多制式间的技术壁垒，实现网络各层协议间的解耦合，让工业网络重构成为可能。5G 工厂在重构工业网络同时，还会整合人工智能、物联网、云计算、大数据等为代表的新一代信息技术重构工业网络防护体系，为 IT 与 OT 网络融合带来的安全问题提供全新的防护方法论和策略。

（四）工业数据

工业数据贯穿于工业设计、工艺、生产、管理、服务等各个环节，是提升制造业生产力、竞争力、创新力的关键要素。传统工厂中的各个环节系统没有统一管理的体系，数据壁垒严重，跨系统和业务获取数据难，导致工厂的数据资料存在滞后性、分散性和复杂性的特点。由于传统工厂数据的滞后性大，缺少数据的联动和共享渠道，设备的运行状态没有实时的反馈，产线捕捉重要数据并没有形成系统化的监测，使得管理人员没办法通过零碎和复杂的数据来提升生产效益。

工业企业数字化转型是驱动工业数据融合的重要引擎。工厂在数

字化、网络化和智能化的发展进程中，会推动工业领域的数据加速融合。工业数据包含大量敏感信息，包括研发设计、开发测试、系统设备资产信息、控制信息、工况状态、工艺参数、系统日志、物流、产品售后服务等产品全生命周期各环节所生产的各类数据，这些数据往往属于工业企业的机密。随着工业企业数字化加速转型，传统工业控制闭环中沉没与消失的数据将被开放出来，生产全流程的数据将以标准化的形式供上层应用使用。数据被大规模收集和共享后，工业企业的数据安全风险也不断增加，数据泄露造成的安全问题也将变得更加严重。

从工业数据的特点来看，5G 工厂应解决以下三方面的数据安全问题。一是数据保密与低时延要求难以同时得到满足的问题。5G 工厂的很多工业应用场景，如 PLC 现场验证、SIS 工业应急、工业设备电源冗余切换等，对数据传输时延要求高，工业终端设备的计算能力相对较弱，很难使用传统高强度、低实时性的加密验证算法，数据保密性得不到保证。二是数据泄露、窃取以及被污染的风险增加问题。5G 工厂使得工业数据会跨部门、跨系统传输变得越来越频繁，当前数据有用即所得的现状未能得到有效控制，导致数据被污染、泄露或窃取后难以追踪溯源，数据安全性难以保障。三是当前大多数工业企业的数据安全能力无法满足新形势下的安全需求问题。大多数工业企业对工业数据的存储、使用和销毁的管理模式依然较为落后，未建立完善的数据安全管理制度，未落实授权访问机制和防篡改、防窃取、防误删等技术手段，没有规范完备的数据使用管理和销毁机制。

（五）安全设备

工业领域安全设备也可以分为三类，第一类是针对工业控制网络（OT）提供安全网关、网络行为与日志审计、入侵检测、主机加固、安全运维审计（堡垒机）、脆弱性检测、集中安全管理等；第二类是针对工厂和企业管理区网络（IT）提供传统信息安全等保要求的安全设备。第三类是融合自身自动化产品安全属性的安全设备。当前工业领域安全设备整体处于初级阶段，普遍存在两方面的问题。一是网络割裂，仅负责管辖范围的安全，无法实现跨域感知防护；二是功能单一，仅实现设置安全功能，不能与其他设备形成智能联防联控。

5G 工厂安全是工业生产安全和网络空间安全相融合的领域，涵盖工业领域中各个要素和各个环节的安全，需要专门的安全产品、技术和服务。当前，我国工业企业多采用传统的网络信息安全防护技术，以工控系统的“外建”安全防护产品和解决方案为主，尚没有工业 OT 方面的安全专用防护设备，整体安全解决方案还不成熟。随着新型工业化进程加速推进，现有安全设备将无法满足未来 5G 工厂的“数字化、网络化、智能化”应用要求。

安全设备正从产品及设备的基础应用，逐步向以系统化的安全设计、监测、防控一体化和智能化、信息化、平台化的综合工业安全能力方向转型。5G 工厂的发展促使定制化安全设备加速出现，满足客户不同产品形态、性能的需求。同时，国家高度关注信息安全设备的自主可控，将信息安全设备的国产化上升到国家安全的高度，依靠自主创新，积极发展具有自主知识产权的信息安全设备。近年来，在信息

安全产品国产化政策的推动下，信息安全设备的国产化替代趋势趋于显现。

（六）管理方式

传统工厂的信息系统可分为 IT 系统和 OT 系统两类，通常归属两个不同的部门管理。IT 部门是成本中心，他们的需求是安全，通过 IT 系统简化管理降成本。OT 部门是生产中心，其诉求是安全生产，提高生产效率，提高产品质量，降低浪费。他们对系统的考虑，是安全可靠，容易替换，操作简单，不改变原有习惯。IT 人员习惯从总体需求出发，采用自顶而下的方法，将系统划分为若干的子部件，且针对子部件提出和开发解决方案。OT 人员习惯于自下而上的思路，从个别的部件出发构建复杂的系统。在传统工厂，OT 和 IT 在逻辑上彼此独立，在物理上保持隔离或分割。因此，形成了两套无法复用的运营管理制度和体系。

工业企业数字化转型将使得 OT 和 IT 交汇融合，会促进 IT 与 OT 系统之间的数据交互、共享等，然而 IT 与 OT 系统的管理制度存在一定的差异。主要表现在两个方面，一是系统要素管理优先级问题，IT 与 OT 系统对保密性、完整性和可用性（CIA）的优先顺序不同，IT 系统将数据的保密性置于完整性和可用性之上，而 OT 系统将可用性置于完整性和保密性之上；二是管理团队的协调问题，随着智能技术在 IT 和 OT 系统中的深度应用，打破了 IT 与 OT 系统相对独立的工作环境，一些重要系统管理可能需要多个部门参与，每个部门都需要从不同视角相互监督、相互协作来履行各自的责任和义务，共同完成管理。

OT 和 IT 融合是一个长期的过程，在 5G 工厂下也不例外，因此需设计伴随者 IT 与 OT 网络融合的不断完善、不断更新的工厂安全管理制度。

执行制度靠人才，工厂 IT 网络与 OT 网络深度融合后，需要配备 IT/OT 复合型人才保障工厂安全运营。IT 与 OT 系统的信息安全属于两个不同学科，OT 系统信息安全人员主要关注 OT 系统的可用性，对 IT 系统知之甚少；OT 系统又存在很高的技术壁垒，使得 IT 系统信息安全人员无法深入了解 OT 系统。传统工厂中，IT 与 OT 网络长期的物理隔离，使得工厂缺乏培养 IT/OT 复合型的信息安全人才的需求和动力，造成该领域的复合型人才很少。随着 5G 工厂的大规模部署，为更好的执行工厂安全管理制度，因大规模培养 IT/OT/CT 复合型的信息安全人才。

四、5G 工厂安全参考框架

为了应对工业领域的终端、网络、数据和管理方式发生变化引起的安全挑战，针对当前存在的工业信息安全管理机制不健全、关键核心技术能力不足、产业发展基础薄弱、工业企业安全意识不强等问题和短板，综合安全与发展，提出 5G 工厂安全参考框架，助力新时期新形势下的工业信息安全能力提升，切实为制造强国和网络强国战略的有效实施保驾护航。

5G 工厂安全总体框架可以分为终端安全层、网络完全层、数据安全层、应用安全层和管理安全层。安全框架设计遵循融合、开放、灵活、前瞻的思想，提供终端、网络、数据、应用、管理等全方位的安全服务能力，基于网络安全和工控安全政策、法规及标准体系，构建工控安全和网络安全保障体系，充分发挥 5G 协同 AI、云计算、边缘计算、隐私计算等新一代信息技术，满足工业多场景的安全防护需求。参考架构如下图：

图 4-1 5G 工厂网络安全总体框架图

终端安全:5G 工厂终端类型众多,保障终端安全,可从资产安全、访问控制和 AI 终端安全三个方面入手，确保工厂内的终端安全。资产安全通过采取终端标识信息、工艺监控、协议解析、安全阻断等资产安全措施；访问控制主要涉及接入认证、零信任、操作权限管理和主机安全，确保只有合法的终端接入工业网络中。AI 终端安全主要应对后门攻击、对抗攻击、数据投毒和模型窃取攻击等安全威胁，及时发现安全风险和处置安全问题，保障终端安全运行。

网络安全：5G 工厂网络是以 5G 为核心的融合安全网络。针对 5G 网络承载不同业务的安全需求和安全风险，用“三同步原则”加强网络安全，在建设阶段，规划、设计和建设 5G 网络及信息安全保障机制，确保网络服务的安全性。在运营阶段，构建具有统一管理、智能防御和灵活部署的 5G 网络安全防护系统，提高对网络安全的响应能力。

数据安全：5G 工厂数据安全主要包含数据识别、数据保护和隐私计算等方面的技术。保障工业互联网数据安全，需要综合考虑工业数据的产生、传输、存储、处理、使用及销毁等全生命周期的安全问题，采取相应的安全防护技术手段，防止数据被泄露和篡改，主要技术手段包括数据分类分级、数据加密、可信计算等。

应用安全：5G 工厂应用安全层防护主要包含安全预警、安全分析、指令识别三个方面。保障工业应用安全，主要涉及漏洞修复、攻击识别、安全审计异常控制等方面，通过提升工业应用安全能力，能够大幅降低工厂遭受攻击的风险。

管理安全：5G 工厂通过人员管理、制度管理、供应链管理等方面保障工厂安全。以安全生产政策与法规为基础，构建工业企业综合安全管理能力，从而实现工业企业安全合规、生产安全、资产安全和业务安全的安全目标。

五、5G 工厂安全关键技术

未来，以 IT 安全为主的传统产品和服务已不能满足实际市场需求，应充分结合 OT 安全进行纵深发展。因此，5G 工厂安全技术应统筹考虑 IT 安全和 OT 安全需求，其中保障生产的连续性和可靠性是 5G 工厂网络安全的首要任务。本文主要介绍从终端、网络、数据、应用、管理等方面介绍 5G 工厂安全技术。

（一）终端安全

5G 工厂会促使现场终端设备由机械化向高度智能化转变，大量的智能设备容易暴露在互联网上，面临攻击范围大、扩散速度快等问题，如何保证终端设备安全是 5G 工厂网络安全的重要一环。

1. 资产安全

5G 工厂终端安全必须建立在“摸清家底”的基础之上，对网络中的所有业务资产进行信息收集及分析，预防攻击事件带来的危害。收集的方法及注意事项包括如下几项。

（1）无忧采集：主要是对工业系统终端进行信息采集，得到工业系统特征。值得注意的是，在采集过程中，要区分不必要的页面元素以进行过滤、减少不必要的请求。同时，增加采集节点，在进行大规模数据采集时，可以分散访问压力，提高采集效率。

（2）工艺监控：通过 5G 结合机器视觉、模式化识别等技术，进行在线检测监测，加强识别分析、远程诊断、智能预判，支持机器视觉质检、设备预测维护、无人智能巡检等应用场景，在保证生产质量

与安全的前提下，获取生产设备的多个工艺数据。将获取的工艺数据与拟合曲线进行对比，判断正常工艺数据或异常工艺数据。通过监控异常工艺数据，可提升异常工艺产品拦截效率。

（3）协议解析：面向 5G 工厂应用及其特征，针对各类终端进行全流量协议解析。通过对 5G 核心网信令面和用户面的监测与解析，对 COAP、MQTT、Modbus、OPC 等工控和物联网协议的深度解析，提升 5G 工厂终端应用的综合解析能力。

（4）安全阻断：主要是针对组态变更、操控指令变更、PLC 下装、负载变更等关键工艺行为进行监控，对特定过程状态参数、控制信号设定检测阈值，进行过程参数阈值监控。通过内置探针实时感知安全风险，自定义业务策略配置，对违规访问行为进行精准控制和阻断，实现精准安全防护。通过云网联动及时阻断终端非法接入、非法操作指令执行和工艺变更等违规行为。

2. 访问控制

在 5G 工厂中，以设备身份为中心进行细粒度的自适应访问控制，并定义设备接入规则，通过认证和密钥双重机制完成设备的接入鉴权，防止仿冒终端接入，提高终端接入过程的安全性。

（1）接入认证：工厂终端接入认证是工厂内部终端设备能够有效、稳定地连接到工厂网络的安全保障，实现数据共享和信息传递的重要安全措施之一。接入认证主要是对终端身份进行验证，如设备是否合法、接入权限等。5G 工厂终端设备可采用使用用户名和密码、数

字证书、生物识别等方式进行身份验证。身份验证的目的是为了确保工厂网络的安全性，防止未经授权的设备和人员接入网络，避免数据泄露和网络攻击等安全问题。

（2）零信任：对于 5G 工厂网络中所有的业务流量默认都是危险、不可信任的，让其信任的方式是不断的认证。“零信任”就是不信任任何人的策略，除非能明确知道接入者的身份。“零信任”可帮助 5G 工厂完成终端设备的多因素身份验证、持续监测、访问记录及跟踪，对终端每个环节产生的日志进行汇总、分析，实现终端接入可视化管理。

（3）权限管理：5G 工厂设备权限管理分访问控制和操作控制两种。访问控制可以控制设备能够访问的资源和数据，确保只有授权的设备才能够访问相关资源和数据；操作控制则可以控制设备能够进行的操作，从而防止设备进行非法的操作或者误操作，从而导致工厂设备的损坏或者安全漏洞。企业需要根据 5G 工厂实际需求制定权限管理办法，通过设定最小权限原则、实施角色权限管理、实施角色权限管理、强化审批机制、定期评估权限管理效果，实现 5G 工厂终端设备权限闭环管理。

（4）主机安全：5G 工厂设备主机安全策略包括防火墙、权限管理、数据备份、加密技术、漏洞扫描、安全日志、病毒防护等，企业可根据工业应用场景择取一种或多种安全策略，提升 5G 工厂设备主机的安全性。

3.终端安全防护

5G 工厂的终端安全防护需从终端管理、行为审计、业务流程管理等角度开展安全防护。

（1）终端管理：

终端管理主要从恶意代码防护、桌面标准化、终端外联、介质使用、系统加固等层面进行能力建设，确保终端安全合法合规。

（2）行为审计：

行为审计是对 5G 工厂终端系统、应用程序等进行监控和记录，对用户操作和系统行为进行追踪和分析，提高信息系统的安全性和可靠性。通过对终端操作时间点、操作频率、操作对象、操作合法性进行统计分析，判断操作是否合规、是否存在风险。终端行为审计不仅能够追踪用户行为、防止信息泄露和数据损坏，而且还能帮助企业和机构合规化管理，保护企业和机构的商业机密和重要信息。

（3）业务流程管理：业务流程管理包括业务流程设计、终端执行情况和工业生产业务流程管理。其中，业务流程设计管理需要充分考虑业务的特点、业务流程的复杂度、业务规则等，确保业务流程的合理性、有效性和可操作性；终端执行情况管理包括终端操作的正确性、操作的时效性、操作的异常情况等，通过监控终端的执行情况，可及时发现和处理业务流程中的问题和异常情况，提高业务流程的执行效率和准确性；工业生产业务流程管理考虑流程设计的合理性、终端执行情况以及终端在业务流程中操作数据的匹配，通过对业务流程

设计的审查和优化，确保流程的高效性和可行性。

（二）AI 终端安全

AI 终端及应用系统在业务场景中部署时，需要从架构安全、模型安全和攻防安全三个层面来开展防御。其中，架构安全是在 AI 终端及应用系统部署的业务中设计不同的安全机制，来保证架构安全；模型安全是通过模型验证等手段提升模型健壮性;攻防安全是对已知AI攻击设计有针对性的防御策略。

1.AI 安全架构

在工业领域中使用 AI 终端及应用，需要结合具体业务自身特点和架构，分析判断 AI 模型使用风险，综合利用隔离、检测、熔断和冗余等安全机制设计 AI 安全架构与部署方案，以增强工业 AI 应用场景的健壮性。为了保护用户利益，我们需要按照 AI 应用场景需求，在系统中合理运用如下安全机制确保 AI 终端及应用安全，如图 5-2 所示：

图 5-1 AI 引入业务决策的安全架构

（1）隔离：在满足工业应用场景的业务稳定运行的条件约束下，AI 终端及应用会分析识别最佳方案，然后发送至控制系统进行验证并实施。通常根据工业应用场景对各个功能模块进行隔离，并对模块之间设置访问控制机制。对 AI 终端及应用的隔离可以一定程度上减少针对 AI 推理的攻击面，而对综合决策系统的隔离可以有效减少针对决策系统的攻击。

（2）检测：在工业应用场景的主业务系统中部署持续监控和攻击检测模型，综合分析工业网络系统安全状态，并给出 AI 终端及应用威胁风险级别。当威胁风险较大时，综合决策可以不采纳智能系统的建议，并将最终控制权交回人员控制，保证在遭受攻击情况下的安全性。

（3）熔断：AI 终端及应用在进行关键操作时，如 AI 质检、智慧分拣等，通常要设置多级安全架构确保整体系统安全性。需要对 AI 终端及应用给出的分析结果进行确定性分析，并在确定性低于阈值时，将判断交回人工处理。

（4）冗余：大多数 AI 终端及应用决策、数据之间具有关联性，可以搭建业务“多模型架构”，通过对关键业务部署多个 AI 模型，避免单个模型出现错误时影响到业务最终决策，提升整个系统的强壮性。

2. AI 模型安全

针对未知攻击，需根据具体工业应用场景来增强 AI 模型本身的

安全性，避免可能遭受的攻击危害。图 5-3 给出了 AI 模型安全工作流程，可从模型可检测性、可验证性和可解释性开展研究。

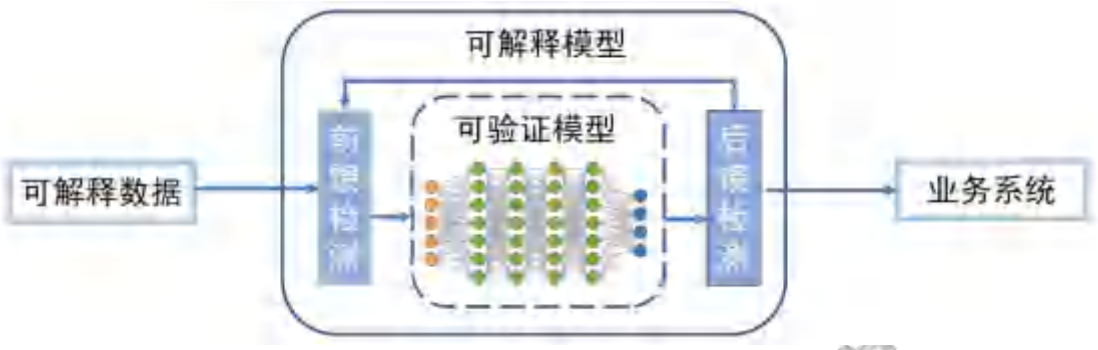

图 5-2 模型安全工作流程

（1）模型可检测性：AI 终端及应用部署运营前，需要对 DNN 模型做大量的安全测试，如前馈检测、后馈检测等，才能提升 AI 终端及应用的鲁棒性。其中，前馈检测是数据输入训练模型前所做的监测模型过滤恶意样本，后馈检测是模型输出评测结果后通过监测模块减少误判。

（2）模型可验证性：以 DNN 模型为例，DNN 模型具有高识别率、更低误报率等特性，广泛用于工业领域各种图像识别场景，如 AI 眼镜、AI 质检仪、智慧分拣等。通过 DNN 模型约束输入空间与输出空间的对应关系，验证输出在一定的范围内，来说明 DNN 模型在一定程度上具有安全性。

（3）模型可解释性：工业领域有些 AI 终端及应用是为了让操作员与工程设备之间有更好的互动，AI 系统具有不可解释性，给出最佳答案时，不会带来疑问，会给操作员带来困惑或操作风险。针对具体工业应用场景，通常要求数据可解释、模型可解释，以增强 AI 终端

及应用的可解释性，帮助我们分析 AI 终端及应用的逻辑漏洞或者数据死角，从而提升 AI 终端及应用的安全性。

当 AI 模型实现可检测性、可验证性和可解释性后，AI 终端及应用便具备了可解释性，输入/中间数据之间的逻辑关系会相对清晰。通过判断数据之间的自洽性可识别非法/攻击数据，甚至能清除恶意的攻击样本，提高 AI 终端及应用的健壮性。

3.AI 安全攻防

当前，很多 AI 应用已出现恶意机器学习、闪避攻击、药饵攻击以及各种后门漏洞攻击。业界已有很多针对已知攻击手段的对抗方法，表 5-1 列出 AI 应用在数据收集、模型训练及模型使用阶段的常见防御技术。

表 5-1 AI 安全防御技术

	数据收集阶段	模型训练阶段	模型使用阶段
闪避攻击	对抗样本生成	1、网络蒸馏 2、对抗训练	1、对抗样本检测 2、输入重构
药饵攻击	1、训练数据过滤 2、回归分析	集成分析	——
后门攻击	——	模型剪枝	输入预处理
窃取攻击	差分隐私	隐私聚合教师模型	——

（1）闪避攻击防御技术：

网络蒸馏：在多个 DNN 进行串联场景中，一种前一个 DNN 生成结果被用于训练后一个 DNN 的模型训练技术。网络蒸馏是未来智能制造生产线上常见的安全模型训练方法，该方法通过转移知识可以一定程度上降低模型对微小扰动的敏感度，提高 AI 终端及应用的鲁棒性。

对抗训练：一种利用已知攻击方法生成抵抗攻击扰动的训练技术，该训练技术能利用已知的各种攻击方法生成对抗样本，再将对抗样本加入模型的训练集中，然后对模型进行单次或多次重训练，生成可以抵抗攻击扰动的新模型。未来 5G 工厂，可综合全系统、全产业链的多类对抗样本，训练集数据丰富，不但可以增强新生成 AI 终端及应用模型的鲁棒性，还可以增强 AI 终端及应用模型的准确率和规范性。

对抗样本检测：对抗样本检测是模型使用阶段的一种监测技术，通过增加外部检测模型或原模型的检测组件来判断监测对象是否为对抗样本。不同的检测模型可能依据不同标准来判断输入是否为对抗样本。AI 终端可通过 5G 协同边缘计算、云计算上的外部检测模型，让输入样本和正常数据间确定性的差异、对抗样本的分布特征、输入样本的历史数据等作为对抗样本的判别依据成为可能。

输入重构：模型使用阶段的一种防御技术，通过将输入样本进行变形转化来对抗闪避攻击，变形转化后的输入不会影响模型的正常分类功能。在 5G 工厂中，AI 终端可在边缘计算、云计算的协助下，通过给输入样本加噪、去噪、自动编码器改变输入样本等方式，将输入样本进行变形来对抗闪避攻击，变形后的输入样本的正常功能不会受到影响。

以上防御技术都有适合的工业应用场景，并不能完全防御所有的对抗样本。

（2）药饵攻击防御技术：

训练数据过滤：通过对训练数据集的控制，利用检测和净化的方法防止药饵攻击影响模型。数据标签过滤和模型对比过滤常用的两种训练数据过滤方法。其中，数据标签过滤是利用数据的标签特性查找可能被药饵攻击的数据点，在重训练时过滤这些攻击点；模型对比过滤是减少可能被药饵攻击的采样数据，并借助数据标签过滤来对抗药饵攻击。在 5G 工厂中，可利用云计算的海量存储能力和超强计算能力帮助 AI 终端完成数据标签过滤和模型对比过滤，提升药饵攻击防御能力。

回归分析：一种基于统计学的检测数据集中的噪声和异常值的方法。常见的方法有对不同的损失函数来检查异常值、使用数据的分布特性来进行检测等。

集成分析：一种通过综合多个子模型的能力提升机器学习系统抗药饵攻击能力的方法。利用多个独立的模型共同构成 AI 终端及应用，通过 5G 网络将多个 AI 终端模型采用的不同训练数据集就行综合，实现降低整个系统被药饵攻击的概率。

（3）后门攻击防御技术：

输入预处理：一种模型使用阶段的防御技术，通过过滤触发后门的输入，降低输入触发后门的风险。

模型剪枝：一种模型训练阶段的防御技术，通过适当剪除原模型

的神经元，在保证正常功能一致的情况下，减少后门神经元的影响力。

（4）模型/数据防窃取技术：

隐私聚合教师模型：一种模型训练阶段的防窃取技术，该技术将训练数据分成多个集合用于训练一个个独立的 DNN 模型，然后基于这些独立 DNN 模型训练出学生模型。这种技术适合数据分散的工业应用场景，根据分散系统数据情况就地训练 DNN 模型，然后利用 5G 网络汇聚后训练出学生模型，这种方式可确保训练数据不会泄露，提高训练数据的隐私性。

差分隐私：一种数据收集阶段的防窃取技术，通过利用一些差分隐私的方法对数据或模型训练进行加噪，提高模型或数据的保护能力。在工厂 AI 质检、智慧分拣、智能环境监控仪等场景中，AI 终端可通过差分隐私获取其他 AI 终端的数据或模型的能力，但不会导致数据或模型被窃取。

（三）网络安全

5G 工厂会促进 IT 和 OT 融合，工厂网络结构也会出现不同程度的变化，但是传统 OT 网络仍会是 5G 工厂的核心网络。5G 技术作为打通 IT 和 OT 网络的重要工具，将普遍存在于工厂的各领域、各系统中。此外，IPv6 带来的新技术将 5G 工厂得到大规模应用。

1.OT 网络防护

OT 网络防护技术可以相当程度上阻止 IT 侧网络对工控系统的威胁，避免互联网攻击对工控系统造成破坏。其技术主要包括如下几项。

（1）网络安全检测

入侵检测：针对 OT 网络的入侵行为存在大量隐藏攻击，即攻击命令虽然符合协议规范，但违背了系统的生产逻辑，使系统处于危险状态，例如未授权的启动与停止指令、未授权的组态变更等。对于隐藏攻击的检测可以通过收集 PLC、RTU 等内部寄存器值、数字量及模拟量的输入和输出，为检测特征增加语义描述，最终通过关键状态发现检测隐蔽攻击。

漏洞扫描：OT 网络漏洞扫描是针对工业控制系统网络环境中存在的设备进行漏洞检测，进而对设备状态、漏洞信息进行分析，能够让工业控制系统管理者全面掌握当前系统中的设备使用情况、漏洞分布情况、漏洞风险趋势等内容，从而实现对系统内的核心组件进行有针对性的重点整治。

蜜罐技术：“蜜罐”是一种网络诱导技术，通过故意暴露网络漏洞诱骗网络攻击者发起攻击。在 OT 网络中，可以利用闲置的服务端口来充当蜜罐，采用增加蜜罐数量，增加蜜罐暴露几率的策略，起到“挡枪”的效果，达到保护目的。

（2）网络防护

网络隔离：作为工厂内部的传统网络安全手段，工控系统隔离技术通过在工控网络和企业网络之间部署防火墙等网络隔离设备，或者在工厂内网前方设置 DMZ 区域，控制外网与工控网络之间的数据交换，可以在很大程度上屏蔽外网带来的病毒感染风险，以及工业内部数据信息的泄露。

白名单技术：白名单技术有不同维度的分类。应用程序白名单，是用来防止未认证应用程序运行的一种措施，即只有允许的应用程序能被运行。资产白名单，是指对 OT 网络内的资产进行统计，区分权限后放入不同的白名单之中，如果有恶意设备接入，则基于资产白名单可以快速发现该威胁源。行为白名单，即将应用程序的合法行为进行定义，从而将合法访问与非法访问进行区别。

（3）拟态技术

网络空间拟态防御将会成为 5G 工厂的一种新型防御技术，该技术可以通过 5G 聚合 AI 终端、边缘技术、云计算等能力，提升工厂网络设备安全保障。

拟态路由器：在网络架构中引入多个异构冗余的路由执行体，对执行体维护的路由表进行共识裁决生成拟态路由器的路由表，行成拟态裁决机制。可实现不同执行体的防护能力互补，有效阻断恶意攻击，极大地提高路由器应对网络攻击的能力。

拟态 Web 虚拟机：利用云化部署优势，构建功能等价、多样化、动态化的异构虚拟 Web 服务器池，采用动态执行体调度、数据库指令异构化、多余度(共识)表决等技术，建立多维动态变换的运行空间，阻断攻击链，大幅增加传统 Web 服务和虚拟环境中的漏洞及后门利用难度，在不影响 Web 服务性能的前提下，保证服务的安全可信。

拟态算力服务：通过构建功能等价的云边拟态算力池的方法，采用动态执行体调度、异常发现、线上线下清洗等技术，可及时阻断工业软硬件漏洞后门攻击。

拟态防火墙：运用拟态防御技术，采用动态异构冗余架构设计，对传统防火墙架构进行改造，提升防火墙 Web 管理层面、数据流处理层面的防护能力，切实可信的准入控制保障。

2.5G LAN 安全

（1）5G 多层次隔离

5G 网络可以基于无线接入网、传输网与核心网等基础设施以及网络虚拟化技术构建面向不同业务特征的逻辑网络，能够根据 5G 工厂的安全需求支持各种差异化的业务场景，在不同安全分区或同一安全分区不同业务之间实现不同强度的隔离手段。

无线接入网隔离：面向无线频谱资源和基站处理资源的隔离方式。最高安全等级的工业控制类场景，通过独立基站或频谱实现安全隔离；安全等级低一些的应用场景，可通过物理资源块分配、数据资源承载参数配置、5G 服务质量特性优先级调度等多种方式实现。

传输网隔离：传输网隔离技术有硬隔离和软隔离两种方案。硬隔离通常采用 FlexE 技术，安全性能高，可更好的适应 5G 工厂网络中海量数据的安全区隔传输要求；软隔离最常见的策略是 VLAN 隔离，该方式是将切片标识作为 VLAN 标签，完成切片数据映射封装，实现切片的承载隔离。

核心网隔离：在核心网层面，可通过对 CPF 共享方式就行设计，实现安全隔离策略。目前有独享、部分共享、完全共享三种 CPF 共享方式，满足不同级别的安全隔离策略需求。

（2）5G 接入认证

当多种、海量终端接入 5G 工厂网络时，需要灵活的认证方式，在满足网络服务质量的同时，识别可信任终端，保证网络安全。常见的 5G 认证方式有切片认证和二次认证两种。

切片认证：5G 网络的切片技术，能考虑工厂的个性化需求，可以为 5G 工厂提供灵活的接入身份认证方法。例如加入限制，仅允许工厂认可的 IMSI 清单内的设备终端才能够接入到该业务的专属切片，保证网络切片分配给正确的用户，实现身份接入安全可靠。

二次认证：实现 5G 工厂对设备多重接入控制的需求，通过 5G 网络提供底层认证通道，由工厂自主制定认证算法和认证协议，实现灵活自主的二次认证。当 5G 主认证完成之后，在用户建立 PDU 会话时，由 SMF 发起二次认证，并由 DN-AAA 服务器对用户进行认证授权。在验证过程中，DN-AAA 服务器的部署有两种方案，一种是由工厂自主部署，通过 UPF 网元和 SMF 网元连接；另一种工厂以租户形式实现对入网终端的二次身份认证，由运营商直接部署在通信机房，与 SMF 网元连接，这时由运营商提供云上 AAA 服务。

（3）加密技术

在 5G 工厂中，对网络延时要求很高，PKI 等常规加密算法需要复杂计算，不适合工业应用场景。这种场景需要采用高速、低耗的加密技术。

轻量级加密技术：对称密码是一种运算速度较快的加密技术，可兼顾安全性和性能，能满足 5G 工厂超低时延和海量终端的加密需求。

能够更好地适用工业应用环境，尤其在芯片性能、能耗、存储空间、通信带宽、运行时间等软硬件条件受限情况下。

量子加密：量子加密通信是指利用量子密钥分发进行安全通信的网络，它主要利用量子密钥的不可抵抗、均匀、无界、零时延等特性，通过量子密钥进行加密传输，不但能够保证通信的安全性，而且还可以提高速率。随着量子相关技术的快速发展，目前量子加密已有零星应用。量子加密作为一种先进的加密技术，传输速度快、安全可靠性高的特点，在未来 5G 工厂中将得到广泛应用。

3. IPv6 安全

从 IPv4 到 IPv6，网络地址从 32 比特增加到 128 比特，足够长的网络地址使得“真实地址溯源”和“精细化网络管控”成为可能，也为 5G 工厂提供了前所未有的网络安全保障手段。

（1）SRv6 技术

通过分段转发 IPv6 数据包，可以实现网络切片的功能，每个网络切片都可以灵活定义自己的逻辑拓扑、SLA 需求、可靠性和安全等级，以满足不同业务、行业或用户的差异化需求。对于 5G 工厂而言，IP 层面网络切片的价值主要体现在以下两个方面：

负载均衡：通过切片的资源预留技术实现差异化 SLA 和不同等级的网络隔离诉求，精确预测网络上路由资源的分布情况，对路由策略进行动态调整，实现负载均衡的效果，合理分配网络资源。

高可靠收发：部分工业场景，如精密加工，对时延有严格的要求，

SRv6 技术可以通过路由策略的调度，实现网络传输时长的可控，通过确定性时延，保障安全生产。

（2）iFIT 技术

iFIT 将 OAM 指令携带在 IPv6 扩展报头中，根据染色比特经受的时延、误码等来获得链路实时性能，发现丢包、时延、抖动等异常现象，定位问题节点与路段。iFIT 在 5G 工厂网络安全中起到如下作用：

异常流量检测：利用 IPv6 扩展包头提供的数据空间，随流检测可为拥有海量终端的工业网络提供流量可视测能力，最高可对网络流量十万分之一的异动进行监控。利用精准的检测能力，既可以及时发现来自互联网的 DoS 攻击，也能自动地检测出工业设备潜在故障，实现了智能化网络运维。

静默故障感知：静默故障是指业务体验受损但没有达到触发告警门限且缺乏有效定位的故障。IFIT 可以真实还原报文的实际转发路径，实现网络 SLA 的实时监控，丢包检测精度可达 10^{-6} 量级，时延检测精度可达微秒级，能够进一步支撑对静默故障的完全检测、秒级定位。这种高精度丢包检测率可以满足工业控制“零丢包”业务的要求，保障业务的高可靠性。

分流数据审计：利用报头中存储的网络节点信息，获取数据包经过的路径，作为 5G 核心网 UPF 分流数据的审计。该技术可及时监测工厂内部数据非法外溢，避免恶意第三方访问或调用工厂保密数据。

（3）Multi Homing 技术

IPv6 Multi homing 是一种重要的网络服务，具有提高网络可靠

性、实现均衡负载、增加网络带宽、保证传输层存活性等优点。该技术可以区分同一个 PDU 会话中所含的多种服务质量要求、安全级别业务，为 5G 工厂网络提供不同的路由，并支持 UPF 分流企业敏感数据，与外网安全隔离。同时，还可实现 5G 终端按需连接公网或专网，为 5G 网络提供先建后断的业务连续性模式，减少切换中断时延，提高可靠性。

（4）IPv6 VPN 技术

与 IPv4 只能在数据链路层和网络层上建立 VPN 逻辑上的专线不同，IPv6 可以实现传输层的端到端专线。IPv6 VPN 的主要优势有：实现云网边端穿透、业务与连接解耦，一跳直达；协议简化，部署简单，不再需要隧道支持，可以直接运行；通过记录网络关键信息，可实现 VPN 专线路由的可管理、可溯源。IPv6 VPN 技术在 5G 工厂网络中应用，可兼顾网络的便捷性和安全性。

（四）数据安全

数据作为生产要素之一，能否做好数据深化应用、发挥数据价值是关乎工业企业能否迈过数字化转型门槛、站上更高发展台阶的关键，数据安全又是做好数据应用的前提保障。5G 工厂数据安全建设需从数据资产识别梳理、数据安全防护、数据安全风险评估、数据安全运营的安全框架进行考虑。

1.数据安全风险评估

数据安全风险评估是以数据为核心，通过现场调研和技术评估相

结合的方式对单位数据运行现状开展全面风险评估，了解数据管理相关控制的存在性及有效性，评估分析数据安全整体面上和点上的安全风险，作为安全体系规划建设的重要参照依据。在评估过程中，通常从数据环境风险分析、数据内容风险分析和业务流程相关的数据安全风险分析着手。

（1）数据环境风险评估：数据环境风险分析包括数据支撑环境安全风险分析（如主机安全、通信安全、数据库安全、大数据平台安全等）、数据使用环境安全风险分析（如终端准入、终端杀毒、用户组策略管理等）、数据运维环境安全风险分析（如授权与审批、危险操作识别与阻断、去标识化等）。例如：数据库安全风险分析，通过安全现状评估能有效发现当前数据库系统的安全问题，对数据库的安全状况进行持续化监控，保持数据库的安全健康状态。可采用数据库漏洞扫描、弱口令检测、配置核查与加固等方式展开工作。

（2）数据内容风险评估:数据内容风险评估可按照重要/敏感数据资产梳理、重要/敏感数据流动分析、重要/敏感数据流动风险检测的顺利进行。以重要/敏感数据流动风险检测为例，具体实施时可结合企业系统特点，快速对系统内部的敏感接口进行脆弱性评估，并结合后台脆弱性评估规则，自动发现并识别相关接口的脆弱性。检测包括登录接口脆弱性、接口权限评估、接口流动风险、数据暴露面、数据域流向等多个维度的风险检测项目，并对检测后问题开展风险评定等级，评定影响范围、并给出响应的整改意见。

（3）业务流程风险评估:在流程脆弱性分析过程中，围绕流程中

敏感数据的流转，编制数据流转视图。流转视图包含敏感数据确认、流转、业务风险等。

2. 数据资产识别

数据资产识别是数据安全的核心内容，通过对不同类型的数据进行甄别，识别其中存在的重要数据或敏感数据并对其进行分类定级处理，避免数据安全治理“眉毛胡子一把抓”的混沌状态，有针对性地对不同类别、不同级别的数据提供不同程度的安全防护提供依据。

（1）数据发现：通过扫描探测、网络流量分析、应用接口探测、业务锚点监测、调研访谈等方式发现各类数据源，如网络协议、应用接口、网页、文本、图片、视频、脚本、数据库、文件服务器等数据源。例如，对于数据接口。采用自动化接口发现技术，将网络流量中大量的 URL 等进行聚合归类，然后提取参数配置，还原接口的技术设计形式，并按照接口资源类型归类各类接口。同时，通过敏感数据识别、引擎识别接口，对业务系统和接口进行归类统计梳理。

（2）数据分类分级：对数据资源进行分类和分级，是实现数据有效管理和利用，保障数据安全的基础，也是促进数据开放和共享的关键环节。工业数据可分为结构化数据和非结构化数据两类，结构化数据可通过数据探测，对数据库服务进行数据资产盘点；非结构化数据需通过访谈、收集、调研等方式进行盘点。

（3）数据安全定级：数据完成分类后，便可对数据进行安全分级。数据安全定级主要根据数据的安全属性，如完整性、保密性、可

用性等，以及安全事件发生后的影响对象、影响范围、影响程度，对数据进行安全定级，通常将数据分为一般数据、重要数据、核心数据三级。

3. 数据安全防护

数据具有流动性，数据结构和形态会在整个生命周期中不断变化，需要采用多种安全工具支撑安全策略的实施，涉及到数据加密、秘钥管理、数据脱敏、水印溯源、数据防泄漏、访问控制、数据备份、数据销毁等安全技术手段。技术涉及面广、细节丰富。为此，本白皮书主要针对数据防泄漏、零信任数据安全、隐私计算等关键技术进行简要介绍。

（1）数据防泄漏：数据泄漏风险可通过数据网关、数据审计、数据脱敏、数据水印溯源、访问控制、身份认证等多种技术组合的方式来防护。结合数据分类分级结果，对重要数据、核心数据进行分级别、细粒度采取数据防泄漏保护，可得到更佳效果。

（2）零信任数据安全：零信任是一种安全模型，基于访问主体身份、网络环境、终端状态等尽可能多的信任要素对所有用户进行持续验证和动态授权。零信任模型通常采用身份管理基础设施、数据平面、控制平面三层架构，实现访问主体到目标客体的端到端安全控制。5G 工厂存在泛在异构终端连接，数据访问情况复杂，采用零信任数据安全方案是比较理想的解决方式。

（3）身份认证：在身份认证技术上，可对应用身份、设备身份进行高强度关联认证，如将应用程序自身签名、运行环境上下文摘要信息、应用内部用户身份、设备身份码、5G 通讯卡身份码、通讯网络地址信息、通讯链路信息进行整合，作为访问请求唯一主体进行认证。该认证信息可在零信任用户认证中心按需实时生成，具有即时性特征，适合 5G 工厂应用场景。这种采用多维度属性的身份认证方式，相比于单一属性授权方式，大大增强了安全属性。

（4）访问控制安全：基于传统访问控制策略列表，利用 UEBA 技术对数据访问交互管理能力进行深度分析研判，并能在过程中做出相应处置动作。UEBA 主要通过历史行为建模、实时行为分析，通过大数据分析、机器学习的方式优化判断阈值，解决传统规则方式存在安全盲区的问题。

（5）代理安全：常见的工厂代理技术有工厂应用系统的代理和关键 API 的代理。代理技术包括身份识别、权限识别、身份传递、数据脱敏、健康监控、流量管控、通道安全等多项核心技术，通过实施动态的访问者身份识别和权限识别操作，对服务健康状态进行实时检查，实现安全加固，并能通过统一的策略对服务的访问控制进行调整。

4.数据安全运营

数据安全运营是将技术、人员、流程进行有机结合的系统性工程，是保证数据安全治理体系有效运行的重要环节。数据安全运营遵循“运营流程化、流程标准化、标准数字化、响应智能化”的思想进行

构建，数据安全运营的需要实现流程落实到人，责任到人，流程可追溯，结果可验证等能力。数据安全运营需贯穿安全监测、安全分析、事件处置、安全运维流程，全面覆盖安全运营工作，满足不同类型、不同等级安全事件的监测、分析、响应、处置流程全域可知和可控。如图 5-3 所示，数据安全运营主要包含数据资源运营、数据安全策略运营、数据安全风险运营、数据安全事件运营和数据安全应急响应五个部分。

图 5-3：数据安全运营架构图

5. 隐私计算

隐私计算是一种保障数据在使用过程中“可用不可见”的安全技术，可在满足数据隐私安全的基础上，实现数据价值的流通。隐私计算可帮助 5G 工厂开展供应链上下游、产品销售全生命周期等管理，挖掘数据价值，解放数据要素生产力。隐私计算主要包括多方安全计算、同态加密、联邦学习、可信执行环境等。

（1）多方安全计算：多方安全计算是一种参与方不泄露各自数据以及中间计算结果的情况下，基于多方数据协同完成计算目标，可实现原始数据、计算模型等不被泄露。

（2）同态加密：同态加密是指对密文进行特定形式的代数运算得到的仍是加密的结果，将其解密所得到的结果与对明文进行同样的运算，二者结果相同。根据运算符不同，可分为乘法同态加密和加法同态加密，能够同时满足加法和乘法两个性质的算法称为全同态加密算法，只能满足其中之一的称为半同态加密算法。

（3）联邦学习：联邦学习是一种使多个参与方在不泄露其原始数据和隐私的前提下，能互相协作，构建和使用机器学习模型的系统或框架。通常需要一个汇聚方，每个参与方对自己的数据在本地训练模型的得到本地参数，然后将本地参数及部分信息提交给汇聚方，由汇聚方进行聚合计算得出全局参数，再发给所有参与方进行计算。

（4）可信执行环境：基于可信执行环境的安全计算是数据计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内部部署的代码和数据的机密性和完整性得到保护。

（五）应用安全

所谓应用安全，简单地说，是保护应用系统、应用程序的安全。为了保障应用安全，需要从安全预警、安全分析和指令识别三方面加强应用系统在安全性方面的设计和配置，防止在运行过程中发生应用系统不稳定、不可靠和资源被非法访问、篡改等安全事件。

1. 安全预警

安全预警主要针对工业应用系统，建立入侵攻击规则库、知识库、漏洞库等，综合利用入侵检测、攻击识别、漏洞扫描、异常报警管理等手段，对工业应用系统中发现的入侵攻击、漏洞利用、异常报警等进行安全预警。

（1）攻击识别：针对工业应用系统，建立工业入侵与攻击知识库、特征库，通过流量检测、入侵检测、安全态势监测等手段，精准识别工控系统中的异常接入、异常通信行为、IO 篡改、显示欺骗、控制篡改、固件异常提取、固件篡改、指令篡改以及异常报警、异常处置等行为，及时进行安全预警。

（2）漏洞扫描：在不影响工业应用系统正常安全运行的前提下，建立工业应用系统漏洞扫描机制，及时发现系统存在的漏洞，并对工业应用及时打补丁。

（3）入侵检测：在不影响工业应用系统正常安全运行的前提下，建立工控应用侵入检测机制，对工业应用系统中的全要素、全流量网络报文进行采集分析，对发现的入侵和攻击，及时预警。同时，结合工业应用系统入侵与攻击知识库、行为特征库，及时发现工业应用系统中的木马、恶意代码、非授权协议、非授权指令；结合工业生产业务逻辑与工况参数，及时发现利用工控系统自身机制和协议、指令发起的隐蔽攻击、隐性攻击。

（4）异常报警：建立工业应用系统报警管理机制，采用报警统

计分析、报警审计分析、关键工艺报警管理、多参数印证报警管理、测控指令与工况逻辑印证、上下文逻辑印证等技术手段，及时发现异常报警。

2. 安全分析

工业应用系统要求运维人员能够随时掌握工业业务应用运行的关键指标，及时发现安全风险、安全隐患，及时预警，实现主动运维、主动防御、主动管理。一旦发生攻击或安全事件，需要通过日志审计、威胁分析、关联分析、溯源分析等技术手段，实现有效地定位和取证。

（1）日志审计：工业应用系统的日志审计应该包括三个方面，一是对常规的安全设备、网络设备、数据库、服务器、应用系统、主机等设备所产生的系统安全事件、用户访问、系统运行（如文件的创建、删除、访问、更改等）、系统状态以及告警、操作、消息等记录进行审计分析；二是要结合工业应用系统的软件、硬件组件与网络配置实际，对工业应用系统中的登录接入、网络资产、通信过程、连接访问、网络流量等进行审计分析；三是要对工业应用系统中的组态、配置、操作、控制、报警指令和行为进行审计，及时发现与系统配置不相符的指令和行为。

（2）威胁分析：主要通过网络监测、入侵检测、漏洞扫描、防火墙应用、杀毒软件等技术手段，不仅要对工业应用系统的非授权访问、信息泄漏、流量劫持、数据篡改、拒绝服务、漏洞利用攻击等常规安全风险进行分析。还可结合工业应用系统的软硬件与控制方案实际，

和工业生产业务的运行工况参数、状态，对像“震网”病毒那样利用工业应用系统自身的运行机制、协议和指令，发起的系统侦察、指纹提取、指令劫持、指令伪造、操作篡改、控制篡改、配置篡改、数据篡改、IO 操控等行为安全风险进行分析。

（3）溯源分析：通过地址分析、日志监测、全流量分析、恶意文件、同源分析、攻击模型分析以及操作控制指令行为分析、组态配置行为分析、报警与处置信息分析、详情分析等手段，对工业应用系统受到攻击的攻击时间、攻击设备、攻击类型、攻击指令、被攻击设备、攻击行为以及对工业生产业务的攻击影响、可能的后果等进行分析，及时发现攻击源，并及时处置。

（4）关联分析：综合利用聚类分析、攻击场景、因果关系、序列分析等方法，结合工控系统软件硬件与网络配置实际，从网络资产、节点间通信关系、节点通信行为、系统管理、节点管理、网络管理等报文、流量等方面，对工控系统中的节点间通信过程进行关联分析。在 5G 工厂中可结合业务逻辑与控制方案，从时序逻辑、控制逻辑、指令上下文关系、指令与工况参数间的业务逻辑关系等，对工业应用系统组态配置、测量操作控制与报警处置指令、行为等进行关联分析，发现、识别利用工控系统运行机制、协议指令等发现的隐蔽式攻击。

3.指令识别

工业应用通过 SCADA、DCS、PLC、RTU 等工控系统的软件、硬件、网络的运行，采集传感器测量的工业生产过程运行状态参数，经过控

制算法运算后，向阀门、泵、电机等执行机构发送操作、控制指令，从而使工业生产的物理或化学过程安全、稳定、可靠运行在目标设计工艺状态。

工业应用系统的指令安全性，决定了其所控制的工业业务安全。指令安全性，是指工业应用系统的操作控制业务指令，符合其所控制的工业生产物理过程、化学过程向目标设计工艺状态趋近稳定并确保安全的调节规律。相反，如果工业应用系统所发出的操作控制业务指令，使工业生产调节过程中的工况与目标设计工艺状态的偏离安全阈值；即将触发安全事故，这样的指令即为非安全指令。非安全指令既包括工业应用系统不支持的指令，也包括系统支持但是由于系统遭到入侵、攻击发起或篡改过的指令，还包括操作人员误操作、违规操作触发的指令。

指令识别直接与业务系统相关，因此，5G 工厂应用系统首先要对系统中的测量、操作、控制指令点位进行精准识别；其次，需要结合 SCADA、DCS、PLC、RTU 等工控系统所控制的工业生产业务、操作规程和控制逻辑，对指令的安全性进行精准识别，及时发现使工业生产业务偏离安全调节域的异常控制指令、违规指令、误操作指令、指令篡改；最后，对可能引发的风险提前预警、提前处置，确保工业业务安全、生产安全和装置安全。

（六）管理安全

工业领域 IT 和 OT 深度融合，工厂的人员管理、制度管理和供应链管理需求出现了不同程度的变化，5G 工厂应站在 IT、OT 充分融合

的角度，来设计相应的管理制度。

1. 人员管理

面向 5G 工厂的各种应用场景，需要对人员的录用、资质、离岗、操作、访客、考核、培训等方面制订管理流程，并严格执行。

（1）资质审查：人力资源管理部门对于重要岗位应进行人员背景调查，可以采用电话、电子邮件、纸质材料和公函等方式进行。通常需要调查身份查验、学历和履历的真实性、学术及专业资格、犯罪记录、竞业禁止等。

（2）离岗审计：员工办理岗位调动和离岗手续过程中，相关部门应及时完成账号权限的调整、变更和注销等，并对该员工在各系统内的账号权限处理情况进行审核与检查。同时针对离职人员相关数据进行智能风险分析，设计安全技术加流程管理的模式，对有泄密风险的人员进行重点审计，预防离职时泄漏大量企业敏感数据，降低员工离职阶段泄漏数据风险。

（3）操作审计：记录所有与系统安全相关的事件和活动，通过 5G 网络传到云端进行长期保留，以便在需要时进行审计和调查。同时，对往来的邮件进行实时检测防护，降低通过邮件泄漏企业数据的风险。

（4）访客管理：进行访客管理时，应该做好访客信息完整登记、访客权限描述等工作，以确保只有授权的访客才能进入特定的区域。同时，帮助组织追踪访客的活动，以便在需要时进行调查。

（5）人才培养：针对 5G 工厂信息安全需要来培育人才，通过高等院校和科研机构加强学科建设和专业化培养，加强科研院所、安全厂商以及 5G 工业企业的联合培育模式，大力培养懂技术、会管理、能实操的 IT/OT/CT 复合型人才。

2. 制度管理

传统工厂涉及 OT 和 IT 两套运营管理制度，5G 工厂可率先在权限审批、风控管理和三同步方面开展融合管理制度设计。

（1）授权审批：企业根据常规授权和特别授权的规定，明确各岗位办理业务和事项的权限范围、审批程序和相应责任。5G 工厂可在企业日常管理活动中按照既定的职责和程序进行的授权，针对融合领域的特殊情况，进行特定条件下的授权。

（2）风控管理：企业风险管理主要包括规范流程管理、访问权限管理、数据安全性管理、供应商管理和监督追责机制管理。5G 工厂在技术层面做好访问权限管理、数据安全性管理、供应商管理之外，还需做好规范流程管理和监督追责机制管理。规范流程管理主要是明确员工的安全责任和义务，并定期进行培训，熟悉相关的规范流程，提高员工的安全意识和防范能力。监督追责制度主要是对违反安全规定和制度的人员进行惩处，并加强对安全管理工作的监督和管理，确保安全管理工作的有效性和可持续性。

（3）三同步制度：是指在 5G 工厂的规划、设计、建设和运行中做到网络安全的“同步规划、同步建设、同步运行”，要求在新建 5G

工厂的各个阶段中，根据国家、行业、集团及公司相关安全管理和技术规范要求，结合工厂实际面临的安全风险以及企业自身业务管理上的需要，同步落实相关安全防护措施，达到 5G 工厂网络安全防护的最佳效果。

3. 供应链管理

5G 工厂供应链涉及的实体和环节多样，直接套用传统网络安全技术会导致防护效果不佳，需从 5G 工厂供应链风险评估、供应链应急响应、供应商活动监控等方面，发展可统筹兼顾供应链全环节安全的技术体系。

（1）供应链风险评估：通过建设供应链系统实现 5G 工厂供应商可视化管理，为供应链上下游企业提供一站式的深度价值服务，实现工业供应链上下游数据互通、全链融合、综合提升平台运营效率与平台收益。利用多元统计分析、随机抽样等方法对供应链企业风险的范围、程度进行建模，挖掘各数据的潜在关系，评估各要素在供应链中间的地位和关系。通过建立动态模型可实现供应链企业风险动态监测，可对供应链风险进行有效管理。

（2）供应链应急响应：构建替代供应商、运输路线、资金来源的解决方案，建立供应链健康监测体系。在监测到供应链攻击后，按照攻击缓解、攻击根除、业务修复、事件跟踪的顺序，开展对应处置流程。

（3）供应商活动监控：充分收集供应链企业操作的数据，分析

并识别潜在的风险和漏洞，为企业采取积极措施来减轻风险和漏洞提供数据支撑，提升供应链的健壮性。强化采购业务的控制能力，减少进购产品不必要的检查。

六、产业发展及展望

5G 工厂会加速工业企业向更加智能的方向发展，推动工业企业数字化转型，并促进新型工业化。虽然 5G 工厂还存在很多网络安全方面的不足，但是庆幸的是这些问题得到了工业互联网企业、监管机构、网络安全设备商、电信运营商等相关单位的足够重视。5G 工厂网络安全将随着 5G 工厂的推进而快速发展，未来会呈现以下乐观而积极的趋势。

5G 工厂网络安全产业将迎来爆发式发展。未来几年，工业企业将开始建设 5G 工厂，随着 5G 工厂的市场规模不断扩大，网络安全的需求也会越来越大。5G 在工厂中的使用将带来新的网络安全挑战，旺盛的 5G 工厂建设需求又会促进网络安全技术的创新和研发，带动网络安全产业的发展，促进 5G 工厂网络安全产业的创新能力提升。当前大部分工业企业对 5G 工厂概念持积极拥抱的态度，但是在落地实施方面显得较为保守。5G 工厂引起的网络安全问题，正是工业企业的顾虑所在。需求将促进 5G 工厂网络安全产业在不久的将来取得爆发式发展。

政府部门将推动完善 5G 工厂网络安全监管体系。5G 工厂给工业企业带来数字化转型的同时，也将互联网安全问题带入到了工业网络领域。政府作为 5G 工厂建设的推动者和工业网络安全的监督者，将会兼顾 5G 工厂的建设推广和工厂网络安全防护，势必延续 5G+工业互联网、工业企业分类分级等政策，随着 5G 工厂建设的加速，将会越来越重视 5G 工厂网络安全监管。5G 在工厂中的使用，涉及 IT、OT

和 CT，传统的工业网络安全监管将无法适应新的 5G 工厂场景，政府将会推动 5G 工厂网络安全监管体系完善。

5G 工厂将促进 IT 与 OT 网络安全深度协调防御。5G 工厂使得 IT 与 OT 两个相对独立的网络实现融通，传统工厂 IT 网络的终端设备也会下沉至 OT 网络，原本相对明确的网络边界变得模糊。随着 5G 工厂的智慧化程度越来越高，IT、OT 中的各类应用系统之间的信息交互、数据共享等需求将会空前增加。5G 在融合 IT、OT 网络的同时，也会带入 5G 在互联网中防御能力，并融合工厂现有的 IT 与 OT 防御能力和策略，促进 IT 与 OT 网络安全深度协调防御。

电信运营商将携手安全设备商提供 5G 工厂网络安全定制服务。5G 网络的开放性，将加速推动工业互联网跨部门、跨行业、跨平台信息共享和联动，势必促进 OT 和 IT 网络融合。传统工业网络中的 OT 和 IT 网络安全设备由两类安全厂商提供，受限于资源及技术等多方面因素，暂未出现在两个领域同时做好的安全厂商。电信运营商有着丰富的 5G 网络运营经验和成熟的网络安全运营体系，可携手工业互联网企业、监管机构、OT 和 IT 网络安全设备商等，将 5G 工业互联网的安全能力打造成一种可定制的服务，根据工业企业的实际需求灵活定制，共同应对来自 5G 工厂带来的 OT 与 IT 网络融合安全挑战。

附录 1 缩略语表

缩略语	英文全称	中文全称
AGV	Automated Guided Vehicle	自动导向车
PLC	Programmable Logic Controller	可编程逻辑控制器
RTU	Remote Terminal Unit	远程终端单元
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
ERP	Enterprise Resource Planning	企业资源计划
CRM	Customer Relationship Management	客户关系管理
MES	Manufacturing Execution System	生产执行系统
PCD	Programmable Controller Device	可编程控制器设备
SCADA	Supervisory Control And Data Acquisition	数据采集与监视控制系统
SIS	Statistical information system	统计信息系统
DNN	Deep Neural Networks	深度神经网络
AI	Artificial intelligence	人工智能
FlexE	Flexible Ethernet	柔性以太网技术
VLAN	Virtual Local Area Network	虚拟局域网
CPF	Centralized Processing Function	无线集中管理平台
SMF	Session Management Function	会话管理功能
SRv6	Segment Routing IPv6	基于 IPv6 转发平面的段路由
iFIT	In-situ Flow Information Telemetry	随流检测
SLA	service-level agreement	服务及协议
OAM	Operation Administration and Maintenance	操作管理和维护
API	Application Programming Interface	应用程序编程接口
UEBA	User Entity Behavior Analytics	用户实体行为分析

DMZ	Demilitarized Zone	隔离区
COAP	Constrained Application Protocol	受限应用协议
MQTT	Message Queuing Telemetry Transport	消息队列遥测传输
Modbus	Modicon communication protocol	一种串行通信协议
OPC	Object Linking and Embedding (OLE) for Process Control	过程控制的对象链接与嵌入
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
PDU	Protocol Data Unit	协议数据单元
DN-AAA	Diameter Network Access Server to Authentication Authorization and Accounting	直径协议网络接入服务器到认证、授权和计费服务器
PKI	Public Key Infrastructure	公钥基础设施
DCS	Distributed Control System	分布式控制系统

附录 2 参考文献

[1] 中国信息通信研究院. 5G 全连接工厂建设白皮书（2022）

[2] 5G 确定性网络联盟. 5G 电力虚拟专网网络安全白皮书(2022)

[3] 安恒信息. 网络安全与数据保护白皮书（2022）

[4] 谛听网络安全团队. 工业控制网络安全态势白皮书（2022）

[5] 国家工业信息安全发展研究中心. 2022 年工业信息安全态势报告

[6] 张明岩, 方鹏飞, 窦静怡. 工业领域网络安全标准体系建设研究[J]. 工业信息安全, 2022, (05) : 74-80.

[7] 国家工业信息安全发展研究中心. 工业互联网数据安全白皮书（2020）

[8] 北京六方云信息技术有限公司. 工业互联网安全架构白皮书（2020）

[9] 工业互联网产业联盟. 工业互联网典型安全解决方案案例汇编 （2020）

[10] 新华三. 工业互联网技术白皮书（2022）

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院以做深大联接、做强大计算、做活大数据、做优大应用、做精大安全为己任，按照4+1+X 研发布局，开展面向 CUBE-Net 3.0 新一代网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国、智慧社会建设。联通研究院现有员工近 700 人，平均年龄 36 岁，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话： 010-87926100
邮编： 100176