中国移动 China Mobile | ZTE中兴

5G+工业互联网安全白皮书

参与编写单位：

中国移动通信集团有限公司

中兴通讯股份有限公司

中国信息通信研究院

北京邮电大学

三一重工股份有限公司

鞍钢集团自动化有限公司

江苏精研科技股份有限公司

哈尔滨电气集团有限公司

宝武集团韶关钢铁有限公司

编写组成员：

张滨、陆平、袁捷、俞承志、王继刚、张峰、李祥军、王庆、于乐、徐高峰、田慧蓉、郝晓龙、张静、张弘扬、滕志猛、邱勤、赵维铎、郝振武、江为强、程渤、赵帅、林兆骥、李珊、张瑜、魏立平、陈凯、常静、胡晶晶、许志成、王乙鸾、辛毅、杨志远、游世林、李溦

技术联系：

于乐 yule2020@139.com

徐高峰 xu.gaofeng1@zte.com.cn

前言

工业互联网是中国制造智能化、信息化的重要手段，将加速“中国制造”向“中国智造”转型，并推动实体经济高质量发展。党中央、国务院高度重视工业互联网发展，习近平总书记连续四年对推动工业互联网发展做出重要指示。在 2020 年 2 月 21 日，中央政治局会议再次强调，要推动工业互联网加快发展。

2020 年 3 月 4 日，中央政治局常委会作出加快新型基础设施建设进度的重要部署，5G 和工业互联网以其巨大的社会效益和经济效益被同时纳入“七大新基建”。5G 网络的高带宽、低时延、海量连接等特性与工业互联网的需求相吻合，必将成为工业数字化转型的关键基础设施。5G 与工业互联网的融合创新发展，将推动制造业从单点、局部的信息技术应用向数字化、网络化和智能化转变，其叠加倍增效应和巨大应用潜力将不断释放，同时也为 5G 开辟更为广阔的市场空间，从而有力支撑制造强国、网络强国建设。

随着 5G 网络的深度融入，工业网络边界也在不断的延伸，网络系统的硬件、软件及其系统中的数据更易遭受到破坏、更改、泄露，工业系统连续可靠运行、工业网络的持续服务面临越来越多的挑战。要让 5G 网络安全地赋能工业互联网，传统的安全解决方案不能满足所有的需求，必须要建立统一的 5G 工业互联网安全架构，基于工业互联网业务场景提供定制化的 5G 网络安全解决方案，加强工业互联网安全技术保障手段及数据安全防护技术手段建设，才能保障 5G+ 工业互联网行稳致远。

本白皮书针对智能制造、电网、矿山、港口等工业垂直行业在引入 5G 后的普适性安全需求，为 5G+ 工业互联网应用场景的安全防护提供参考。

本白皮书的目标读者包括但不限于工业企业、移动运营商、通信设备提供商、安全产品提供商、安全服务提供商、系统集成商，以及其他关心 5G+ 工业互联网安全相关的机构和个人。

目录

02

5G 与工业互联网融合发展概述

随着 5G 时代的到来，5G 将以其高带宽、低时延、海量连接等特性大幅提升工业互联网的信息化水平，逐步成为支撑工业生产的基础设施。5G 在可靠性和移动性的优势让其有望替代当前工业中广泛使用的有线和 WIFI 网络，5G 的大带宽、低时延，以及边缘计算特性更能推动智能制造中的工业视觉、AR、VR 及工业可穿戴应用快速发展；通过 5G 技术连接、收集并分析海量终端的数据，进而得到设备实时运行信息，最终可达到提质、增效、降成本的效果。

5G 技术应用从移动互联网向工业互联网应用领域扩展，将渗透到工业生产的各个领域，满足前所未有的工业连接和通信需求，主要包括如下三种典型的应用场景：

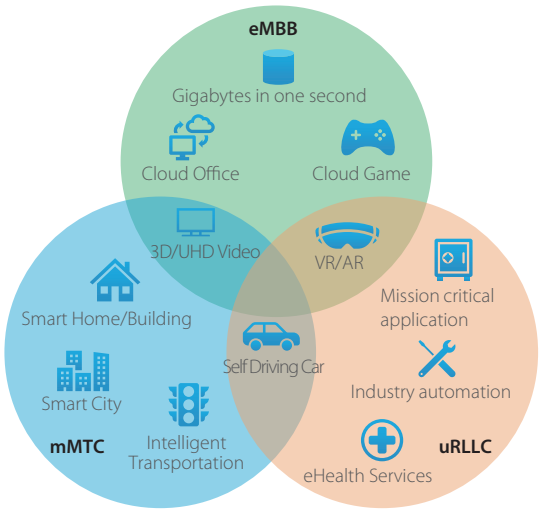

图 2-1 5G 行业应用场景

eMBB（增强型移动宽带）

在 5G 时代，AR/VR、高清视频、3D 等业务的流行将会驱动数据速率大幅提升，峰值速率超过 10Gbps，在工业环境下的具体应用包括 5G+ 机器视觉质检、5G+ 智能制造中的工业巡检无人机、5G+ 智能电网中的高空巡检机器人等。

uRLLC（超可靠低时延通信业务）

5G 网络 E2E 时延 <5ms、安全性和可靠性 >99.999%，能广泛满足工业生产领域的需求。例如 5G+ 港口中的远程操控桥吊作业、精准控制智能装卸，5G+ 矿山中的远程操控挖掘机、无人矿卡等。

mMTC（大规模机器通信业务）

5G 开启了万物互联的时代，其能提供低功耗、大连接（>1M 连接 /km^2）的网络服务，例如 5G+ 工业制造中的工业可穿戴、5G+ 智慧钢厂中的有害气体及温度检测等业务。

5G 网络高速率、超大连接、低时延的特点，将推动工业互联网快速发展和运用。5G 网络提供的灵活定制、弹性部署、多层次隔离等智能网络能力与工业生产中研发设计系统、生产控制系统及服务管理系统等相结合，可以全面推动 5G 工业互联网的研发设计、生产制造、管理服务等生产流程的深刻变革，实现制造业向智能化、服务化、高端化转型。

03

5G 与工业互联网
安全政策与标准

“5G网络的引入，打破了传统工业相对封闭可信的生产环境，病毒、木马、高级持续性攻击等安全风险对工业生产的威胁日益加剧，一旦受到网络攻击，将会造成巨大经济损失，并可能带来环境灾难和人员伤亡，危及公众安全和国家安全。”

2015 年 12 月 23 日乌克兰电力系统遭受攻击，黑客将 BlackEnergy 恶意软件植入乌克兰电力部门，造成电网故障并导致伊万诺 - 弗兰科夫斯克地区大约一半的家庭停电 6 小时。

针对工业互联网安全事故频发的现状，政府和标准组织从多个层面进行支撑保障，共同促进工业互联网安全生态建设。

2018 年 8 月 3 日晚，台积电营运总部和新竹科学园区的 12 英寸晶圆厂的电脑，遭到勒索病毒入侵，生产线全数停摆。几个小时之内，台积电在台湾北、中、南三处重要生产基地均未能幸免。各厂区直到 6 日才陆续全部恢复正常生产。这一事件直接影响台积电三季度 3% 的营业收入，公司的毛利润率下降一个百分点。

2018 年 8 月 4 日，攻击者使用恶意软件 TRITON 攻击中东某关键基础设施内的施耐德 Triconex 安全仪表系统（ SIS ），造成 SIS 系统失效，进而导致工业生产过程自动关闭。

2019 年 3 月 19 日挪威铝业公司 Norsk Hydro 遭到 LockerGoga 勒索软件攻击，致使主机死机，造成多个工厂关闭，部分工厂切换为手动运营模式，生产业务中断。

3.1 安全政策

为加强对工业互联网的安全管理，引导工业互联网安全有序的发展，各国政府相继出台多个法律法规和政府指导。

在国内，2017 年 6 月起正式实施的《中华人民共和国网络安全法》要求对包括工控系统在内的“可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”实行重点保护。2017 年 12 月发布的《关于深化“互联网 + 先进制造业”发展工业互联网的指导意见》以“强化安全保障”为指导思想、“安全可靠”为基本原则，提出“建立工业互联网安全保障体系、提升安全保障能力”的发展目标。2019 年 8 月工信部联合十部委下发《关于加强工业互联网安全工作的指导意见》，体系化推进工业互联网安全工作，全面提升工业互联网创新发展安全保障能力和服务水平。2019 年 12 月 1 日施行网络安全等级保护 2.0 标准，即《信息安全技术网络安全等级保护基本要求》，其中特别增加了对工业控制系统的安全要求。

国际上，2015 年 6 月美国国家标准与技术研究院发布《工业控制系统安全指南》，梳理工业控制系统典型威胁，提出安全防护技术框架。2019 年 5 月 ENISA(欧盟网络信息安全局) 发布《工业 4.0 网络安全：挑战与建议》报告，提供了可实施的安全措施，以加强欧盟工业 4.0 网络安全。2020 年 1 月欧盟出台《5G 网络安全欧盟工具箱》等一系列 5G 安全措施，应对 5G 网络安全问题。

2020 年 1 月美国出台《保障 5G 安全及其他法案》，提出“安全的下一代移动通信战略”。以解决 5G 和未来几代无线通信系统所面临的安全漏洞等问题。

3.2 安全标准

国内外相关标准组织针对 5G、工业互联网及应用等多个层面发布了标准规范。工业互联网产业联盟 2018 年相继发布《工业互联网安全防护总体要求》和《工业互联网平台安全防护要求》，规定了工业互联网应用场景下各组成对象不同安全等级的安全防护要求。针对 5G 网络安全，3GPP 发布了 TS33.501《Security Architecture and Procedures for 5G System》，中国通信标准化协会发布了 YD/T 3628-2019《5G 移动通信网 安全技术要求》。

2018 年 4 月 德国工业界牵头成立了 5G 产业自动化联盟 "(5G ACIA)，推动 5G 在工业生产领域的落地。在同年的德国汉诺威工业博览会上，发布了包含预测性维护网络、运动控制同步场景、绘图运动控制等工业互联六大场景的 TSN+OPCUA (OPC 统一架构) 测试床。

5G 与工业互联网融合发展，相关安全标准也在陆续出台和丰富，比如中国通信标准化协会发布的《工业通信网络 网络和系统安全 系统安全要求和安全等级》，3GPP 发布的 TS 22.104《Service requirements for cyber-physical control applications in vertical domains》。

这些安全标准的制定为 5G 与工业互联网的安全融合奠定了基础，对建立 5G 工业互联网一体化防护体系提供了标准依据。随着我国在新基建相关领域的持续发力，相信会有更多针对 5G 工业互联网场景的安全标准出台，为 5G+ 工业互联网应用的发展保驾护航。