

## 优化简化流程 减轻企业负担

——《关于无线电发射设备型号核准若干事项的公告》解读

工信部无线电管理局

9月29日,工业和信息化部发布了关于无线电发射设备型号核准若干事项的公告(以下简称《公告》)。为了更好地理解和执行《公告》,现就有关内容解读如下。

问:《公告》发布的背景是什么?

答:“不忘初心、牢记使命”主题教育活动中,工业和信息化部无线电管理局为切实解决企业在办理型号核准申请中遇到的困难和问题,回应企业期盼,通过实地调研走访和组织企业座谈会等形式,深入了解企业意见建议,并在充分考虑企业实际需求的基础上,进行认真研究论证。从深化“放管服”改革,优化营商环境,服务企业发展的角度出发,工业和信息化部无线电管理局决定对已获得型号核准证的产品允许变更的范围和变更流程进一步明确,并且免除了变更申请的型号核准测试,缩短变更申请的获证时间,满足企业关切。同时结合嵌入无线电发射模块的产品现状及发展趋势,全面梳理相关情况,对无线电发射设备模块管理的有关事项进行了细化,优化和简化了流程,以方便企业申请和办理,解决企业在无线电发射模块型号核准申请办理过程中的同系列产品合并申请以及如何界定产品范围等迫切需要解决的问题。

问:《公告》的主要内容有哪些?

答:《公告》主要内容有:一是进一步明确了无线电发射设备型号核准获证后的允许变更范围及申请程序;二是明确了“信息技术设备和家用电器设备”产品名录以及“同系列产品”的界定原则;三是明确了按照工信部无〔2014〕1号文件进行系列型号核准申请的适用模块类型。

问:获得型号核准证书的产品允许变更范围及申请程序有哪些变化?申请企业能够获得哪些实惠?

答:《公告》明确指出型号核准获证后共有六种情形允许变更,比以往执行的变更情形增加了“(三)委托生产企业

的质量体系发生变化”(四)元器件发生变化”和“(五)未实际投入生产和销售前,型号发生变化”三种情形,充分考虑了企业在生产和销售方面的实际情况,进一步满足了企业的需求。

此外,为方便企业的变更申请,对于《公告》中允许变更的六种情形,经审查,申请材料齐全,符合要求的,一律不再要求进行委托型号核准测试,进一步简化了流程,缩短了审批时限,更好地满足了企业的需求。需要注意的是,出于产品申请变更后,产品的射频性能可能发生变化的考虑,其中第(三)、第(四)和第(六)种情形,申请人除提交相关变更材料外,还需提交实验室自测报告或第三方检测报告。

问:“信息技术设备和家用电器设备”产品名录是如何确定的?

答:在充分考虑目前无线电技术在信息技术及家电领域应用的现状,及与相关产品准入许可或认证相衔接的基础上,明确了可按照工信部无〔2014〕1号文件实施的嵌入无线电发射模块的“信息技术设备和家用电器设备”产品名录,以方便企业按照系列型号申请型号核准。

问:按照工信部无〔2014〕1号文件进行系列型号核准申请的适用模块类型有哪些?

答:按照以往的实际需求和企业实际生产情况,可以按照工信部无〔2014〕1号文件合并申请型号核准证书的同系列产品仅指嵌入了无线局域网(含蓝牙)模块的“信息技术类设备和家用电器类设备”同系列产品。随着嵌入产品的无线电发射模块类型的增多,为满足物联网技术发展需要,方便企业对嵌入无线电发射模块的产品进行管理,《公告》将可按照工信部无〔2014〕1号文件合并申请型号核准证书的同系列产品扩展为嵌入了无线局域网(含蓝牙)、公众移动通信终端(含NB-IoT、eMTC)“限制性非独立操作使用的无线电发射模块”的“信息技术类设备和家用电器类设备”同系列产品,进一步减少了企业产品的型号核准数量,切实减轻了企业负担。

# 逐步形成安全产业规模 全面提升工业互联网安全保障能力

——《加强工业互联网安全工作的指导意见》解读



蒋国瑞

2019年8月28日,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》(简称《指导意见》),这是深入实施习近平总书记提出的工业互联网创新发展战略、落实党中央国务院工作部署的纲领性文件。《指导意见》明确了加强工业互联网安全指导思想和基本原则,制定了工业互联网安全发展的两阶段整体目标:到2020年年底,建立监督检查、信息共享和通报、应急处置等管理制度和企业安全主体责任制;制定设备、平台、数据等至少20项亟须的工业互联网安全标准和评估体系;初步建成国家工业互联网安全技术保障平台、基础资源库和安全测试验证环境;在汽车、电子信息、航空航天、能源等重点领域,形成至少20个创新实用的安全产品、解决方案的试点示范;培育若干具有核心竞争力的工业互联网安全企业;工业互联网安全保障体系初步形成。到2025年,制度机制健全完善,技术手段能力显著提升,安全产业形成规模,基本建立起较为完备可靠的工业互联网安全保障体系。《指导意见》围绕工业互联网安全保障体系,从管理、防护、数据保护、技术创新与产业发展等7个领域,布置了17项主要任务。

《指导意见》规划了我国工业互联网安全保障体系的整体布局,指出了工业互联网安全发展方向,明确了围绕设备、控制、网络、平台、数据安全等相关产品或产业升级和平台打造的主要任务。全面实施《指导意见》,将有效应对工业互联网发展面临的网络安全新风险、新挑战,全面提升工业互联网创新发展安全保障能力和服务水平,推动实体经济转型升级,促进制造强国、网络强国的建设。

### 实施加强工业互联网安全战略 增强生态系统竞争优势

目前,新工业革命与互联网创新发展正处于历史交汇期。发达国家抢抓新一轮工业革命机遇,加速布局工业互联网,构建数字驱动的工业新生态。美国先进制造战略的创新方向和基础建设主要是工业互联网,利用基础科学、人工智能、工业信息技术和互联网等领域的优势,构造全球性的工业互联网生态系统,通过大数据应用、云计算等软服务的加入,带动工业整体提升全流程全环节竞争力。德国工业4.0战略:利用其制造装备工业自动化、工业软件、人工智能等方面的领先地位,通过全工业体系的互联网协同,应用信息物理融合系统,一方面强化硬件制造优势,另一方面拓展软件服务能力。美国先进制造战略和德国工业4.0战略都是把工业互联网作为变革工业和确立竞争新优势的技术基础,注重将顶层设计与优势企业主导相结合,突出数据在整个架构中的核心作用,加强相关领域标准化进程。可见,发达国家高度重视抢占未来以工业互联网平台为核心的制造业生态发展主动权和话语权,各国参与工业互

联网发展的国际竞争日趋激烈。

《指导意见》的出台实施是非常及时的,它从战略高度指导企业和政府,在打造未来互联网等新一代信息技术与全球工业系统全方位深度融合集成所形成的新产业和新业态的同时,构建责任清晰、制度健全、技术先进的工业互联网安全保障体系,覆盖工业互联网规划、建设、运行等全生命周期,形成事前防范、事中监测、事后应急的能力,全面提升工业互联网创新发展安全保障能力和服务水平,在安全保护环境下抢占工业互联网生态系统的制高点和领先地位。

### 加强工业互联网安全建设 夯实相关产业发展基础

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》,指出通过系统构建网络、平台、安全三大功能体系,打造人、机、物全面互联的新型网络基础设施,形成智能化发展的新业态和应用模式。布置夯实网络基础、打造平台体系、加强产业支撑、促进融合应用、完善生态体系、提升安全防护能力、推动开放合作七大任务,并设立打造工业互联网基础设施升级改造、工业互联网平台建设及推广、标准研制及试验验证、关键技术产业化、工业互联网集成创新应用、区域创新示范建设、安全保障能力提升七大工程。力争到本世纪中叶,工业互联网网络基础设施全面支撑经济社会发展,工业互联网创新发展能力、技术产业体系以及融合应用等全面达到国际先进水平。2019年8月《指导意见》的出台实施是非常必要的,没有工业互联网安全,“互联网+先进制造”就没有保障,预期的战略目标就很难实现。

随着“互联网+先进制造业”深度融合,更多机器和设备实现互联,相关业务、平台、设备、用户的多样性不断丰富,传统的网络安全边界加速瓦解。工业互联网应用需要采集各类设备和机器的数据,实现多种数据的集中,也就意味着数据安全风险的增加。工业企业IT/OT技术进一步深度融合,也带来了一系列的工业互联网安全问题。特别是目前工业互联网面临着漏洞剧增、设备后门、组织威胁、工业网络病毒、攻击趋势五大主要安全风险的威胁。这些安全问题不仅影响着工业业务数据、设备功能、连续生产的安全,甚至影响到人身、环境和社区的安全,工业互联网安全面临着严峻的挑战。

《指导意见》的实施,从产业角度考虑,将进一步推动互联网、大数据、人工智能、网络安全和实体经济深度融合,防范并应对“互联网+先进制造业”产生的各种风险,解决工业互联网建设中的各种安全问题,夯实工业互联网创新发展安全保障能力和服务水平,升级优化传统产业,促进工业互联网安全相关的新产业、新业态和新模式的快速发展。

《指导意见》的部署,从战略角度考虑,将加快构建工业互联网安全保障体系,提升工业互联网安全保障能力,促进工业互联网高质量发展,推动现代化经济体系建设,护航制造强

国和网络强国战略实施。

### 落实《指导意见》主要任务 促进相关企业快速发展

《指导意见》是加强工业互联网安全建设与发展的纲领性文件,确立了总体目标与主要任务,为相关传统企业的转型升级和新兴企业的创新发展提出了明确的方向、目标和任务。

企业是加强工业互联网安全的主体,是落实《指导意见》的主力军,应当按照《指导意见》部署的任务,对口承担起适合于自身发展的项目,贵在“从我做起,马上行动”。

《指导意见》将给企业带来哪些机会呢?从企业视角解读如下:

1.推动工业互联网安全责任落实:落实企业主体责任,明确工业互联网安全责任部门和责任人,建立重点设备装置和系统平台联网前后的风险评估和安全审计等制度,建立安全事件报告和问责机制。

2.构建工业互联网安全管理体系:健全安全管理制度,建立分类分级管理机制,建立工业互联网安全标准体系。

3.提升工业互联网安全防护水平:夯实设备和控制安全,提升网络设施安全,强化平台和工业应用程序(APP)安全。

4.强化工业互联网数据安全保护能力:强化企业数据安全保护能力,建立工业互联网全产业链数据安全管理体系。

5.建设工业互联网安全技术手段:建设企业工业互联网安全技术保障平台,建立工业互联网安全基础资源库,建设工业互联网安全测试验证环境。

6.加强工业互联网安全公共服务能力:开展工业互联网安全评估认证,提升工业互联网安全服务水平。

7.推动工业互联网安全科技创新与产业发展:支持工业互联网安全科技创新,促进工业互联网安全产业发展。

工业互联网是连接工业系统产业链、价值链、信息链和创新链,支持工业智能化发展的关键基础设施,是新一代信息技术与制造业深度融合所形成的产业、业态和应用模式,是互联网从消费领域向生产领域,从虚拟经济向实体经济融合和拓展的核心载体。因此,加强工业互联网安全,涉及的企业除了传统的工业企业、互联网企业、通信企业和网络安全企业等企业以外,还包含工业互联网安全平台、服务、技术、管理、应用、标准和法律法规等相关的新企业。

《指导意见》的出台实施,将引领企业围绕总体目标和主要任务,凝聚共识,团结合作,协同推进,各司其责,形成合力,建立技术保障平台,制定安全标准和评估体系,建成安全测试验证环境,打造创新使用的安全产品和解决方案等,不断提升技术手段能力,逐步形成安全产业规模,逐步建成完备可靠的工业互联网安全保障体系。

(作者系北京工业大学经济与管理学院原副院长、中国电子信息产业发展研究院学术委员会信息安全分委会主任委员)

## 新兴数字基础设施建设助力 金砖国家参与第四次工业革命

赛迪智库世界工业研究所 李鑫

### 第四次工业革命 为金砖国家合作提供机遇

在迄今为止的每一场工业革命中受益的都是发达国家,有时甚至以牺牲发展中国家的利益为代价。第一次工业革命——蒸汽时代,英国;第二次工业革命——电气时代,德国和美国;第三次工业革命——信息技术、新材料、航空航天等,美国。第四次工业革命为金砖国家提供公平参与的机会。第四次工业革命是5G、人工智能、量子技术等新兴数字技术在各领域深度融合的多样化发展,不再由单一西方国家主导,某种程度上金砖国家与其他国家处于同一起跑线。相较于发达国家,金砖国家参与第四次工业革命的成本更低、负担更小。发达国家长期以来依赖自己的技术优势,希望依靠过去的技术保持在未来世界的领导地位,对既有成熟技术的颠覆与迭代阻力大,并形成了路径依赖。而金砖国家工业化程度参差不齐,没有形成路径依赖,对新技术接受程度高,在应用第四次工业革命技术方面甚至走在了发达国家的前面,具备“跨越式”“弯道超车”的优势。

### 新兴数字基础设施建设 是金砖国家合作的突破口

第四次工业革命技术的发展改变了基础设施的本质,传统的基础设施越来越多地将数字化融入其中,5G、遥感等新兴基础设施将成为未来经济的支柱。金砖国家参与第四次工业革命需要

完善的基础设施,尤其是适应5G、人工智能等新兴数字技术发展的基础设施。

一是新兴数字基础设施建设可以有效拉动国家经济增长,符合金砖国家的共同利益,阻力小。基础设施是经济支柱、增长的核心,是实现可持续发展目标的关键工具。通过基础设施建设可以有效增加金砖国家的就业、直接投资;同时,伴随基础设施建设的新兴技术的应用也可以提高金砖国家青年创新创业的热情。根据世界银行的数据,全球GDP中每多1%用于基础设施建设,全球GDP将增加2%,发展中国家GDP将增加7%。

二是全球新兴数字基础设施需求大、市场潜力巨大,未来大有可为。5G、人工智能等新兴技术方兴未艾,更需要新兴基础设施建设。到2024年,全球将有15亿人使用5G网络,东北亚将是核心地区。同时,全球数字基础设施建设投资需求旺盛,2016~2030年,亚洲基础设施建设投资需要26.166万亿美元(电力占56%、交通占32%、电信占9%),但是缺口巨大。仅亚洲发展中国家每年就需要1.7万亿美元投入基础设施建设,但该地区每年的投资不足9000亿美元。

三是发挥中国基建优势,引领未来全球新兴数字技术设施建设。基础设施建设合作可以充分发挥中国融资能力和建设速度等优势,这也是发达国家受限于国内体制所不能比拟的。另外,中国在某些新兴技术及新兴数字基础设施建设领域已经领先全球,可以在该领域的合作中处于主导地位。再者,技术的创新发展改变了基础设施建设的标准,包括项目的规划、交付和管理方式,通过在新数字基础设施建设领域的合作,为中国引领全球新兴数字技术基础设施建设奠定坚实基础。