工业互联网安全标准体系研究报告

（2020 版）

资助单位：深圳市市场监督管理局

编制单位：深圳市标准技术研究院

2020 年 09 月

————————本文受深圳标准领域专项资金资助————————

主要编写人员：

黎志文、胡龙珍、张旭杰、李媛红、欧阳莎、肖文康、易晓珊、闻葵花、罗宇民、成文清、陈雷、覃先德、祁泉、邱达赖、邓雪枝。

目　录

第一章 工业互联网安全概述

1.1 工业互联网的概念

当前，以数字化、网络化、智能化为本质特征的第四次工业革命正在兴起。工业互联网作为新一代信息技术与制造业深度融合的产物，通过对人、机、物的全面互联，构建起全要素、全产业链、全价值链全面连接的新型生产制造和服务体系，是数字化转型的实现途径，是实现新旧动能转换的关键力量。为抢抓新一轮科技革命和产业变革的重大历史机遇，世界主要国家和地区加强制造业数字化转型和工业互联网战略布局，全球领先企业积极行动，产业发展新格局正孕育形成。

近年来，我国工业互联网发展态势良好，有力提升了产业融合创新水平，有力加快了制造业数字化转型步伐，有力推动了实体经济高质量发展。工业互联网、5G、数据中心等数字基础设施日益成为新型基础设施的重要组成部分。这些高科技领域，既是基础设施，又是新兴产业，既有巨大的投资需求，又能撬动庞大的大消费市场，乘数效应、边际效应显著。推动工业互联网加快发展，统筹疫情防控和经济社会发展，是缓解经济下行压力、兼顾短期刺激有效需求和长期增加有效供给的优先选择。

自 2017 年《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》发布以来，工业和信息化部会同相关部门深入实施工业互联网创新发展战略，取得了积极进展。

一是工业互联网新型基础设施建设体系化推进。工业互联网网络覆盖范围规模扩张。基础电信企业积极构建面向工业企业的低时延、高可靠、广覆盖的高质量外网，延伸至全国 300 多个地市。“5G+工业互联网”探索推进，时间敏感网络、边缘计算、5G 工业模组等新产品在内网改造中探索应用。标识解析国家顶级节点功能不断增强，二级节点达 47 个，覆盖 19 省 20 个行业。平台连接能力持续增强。工业互联网平台超过一百个，跨行业、跨领域平台的引领作用显著。启动建设国家工业互联网大数据中心。

二是工业互联网与实体经济的融合持续深化。当前工业互联网已渗透应用到包括工程机械、钢铁、石化、采矿、能源、交通、医疗等在内的 30 余个国民经济重点行业。智能化生产、网络化协同、个性化定制、服务化延伸、数字化管理等新模式创新活跃，有力推动了转型升级，催生了新增长点。典型大企业通过集成方式，提高数据利用率，形成完整的生产系统和管理流程应用，智能化水平大幅提升。中小企业则通过工业互联网平台，以更低的价格、更灵活的方式补齐数字化能力短板。大中小企业、一二三产业融通发展的良好态势正在加速形成。

三是工业互联网产业新生态快速壮大。在国家政策引导下，27 个省（区、市）发布了地方工业互联网发展政策文件。各地加大投入力度，支持企业上云上平台和开展数字化改造，推动建立产业投资基金。北京、长三角、粤港澳大湾区已成为全国工业互联网发展高地，东北老工业基地和中西部地区则注重结合本地优势产业，积极探索各具特

色的发展路径。工业互联网产业联盟不断壮大，成员单位接近 1500 家，推进标准技术、测试验证、知识产权、产融对接等多方面合作。

四是工业互联网安全保障能力显著提升。构建了多部门协同、各负其责、企业主体、政府监管的安全管理体系，通过监督检查和威胁信息通报等举措，企业的安全责任意识进一步增强；建设国家、省、企业三级联动安全监测体系，服务 9 万多家工业企业、135 个工业互联网平台，协同处置多起安全事件，基本形成工业互联网安全监测预警处置能力。通过试点示范等，带动一批企业提升了安全技术攻关创新与应用能力。

今年是工业互联网创新发展三年行动收官之年，是全面建成小康社会，实现第一个百年奋斗目标的关键之年。2020 年 3 月 20 日，工信部印发《关于推动工业互联网加快发展的通知》，通知中要求各有关单位要加快拓展融合创新应用、加快健全安全保障体系；通知中各项举措的制定实施，既是立足当前巩固扩大工业互联网发展成效，培植壮大经济发展新动能的重要举措；更是面向未来为下一个五年发展奠定坚实基础的任务要求。

1.2 工业互联网安全的内涵

工业互联网包括网络、平台、安全三大体系，如下图 1 所示。其中，**网络体系是基础。**工业互联网将连接对象延伸到工业全系统、全产业链、全价值链，可实现人、物品、机器、车间、企业等全要素，以及设计、研发、生产、管理、服务等各环节的泛在深度互联。**平台**

体系是核心。工业互联网平台作为工业智能化发展的核心载体，实现海量异构数据汇聚与建模分析、工业制造能力标准化与服务化、工业经验知识软件化与模块化，以及各类创新应用开发与运行，支撑生产智能决策、业务模式创新、资源优化配置和产业生态培育。**安全体系是保障。**建设满足工业需求的安全技术体系和管理体系，增强设备、网络、控制、应用和数据的安全保障能力，识别和抵御安全威胁，化解各类安全风险，构建工业智能化发展的安全可信环境。

图 1 工业互联网体系框架

工业领域的安全一般分为 3 类：信息安全（Security）、功能安全（Functional Safety）和物理安全（Physical Safety）。传统工业控制系统安全最初多关注功能安全与物理安全，即防止工业安全相关系统或

设备的功能失效，当失效或故障发生时，保证工业设备或系统仍能保持安全条件或进入到安全状态。近年来，随着工业控制系统信息化程度的不断加深，针对工业控制系统的信息安全问题不断凸显，业界对信息安全的重视程度逐步提高。

与传统的工控系统安全和互联网安全相比，**工业互联网的安全挑战更为艰巨**：一方面，工业互联网安全打破了以往相对明晰的责任边界，其范围、复杂度、风险度产生的影响要大得多，其中工业互联网平台安全、数据安全、联网智能设备安全等问题越发突出；另一方面，工业互联网安全工作需要从制度建设、国家能力、产业支持等更全局的视野来统筹安排，目前很多企业还没有意识到安全部署的必要性与紧迫性，安全管理与风险防范控制工作亟待加强。

因此，工业互联网安全需要统筹考虑信息安全、功能安全与物理安全，聚焦信息安全，主要解决工业互联网面临的网络攻击等新型风险，并考虑其信息安全防护措施的部署可能对功能安全和物理安全带来的影响。由于物理安全相关防护措施较为通用，故在本报告中将不作重点考虑，主要对工业互联网的信息安全与功能安全进行研究。

1.3 工业互联网安全现状及发展趋势

1.3.1 工业互联网安全现状

当前，工业系统安全保障体系建设已较为完备，伴随新一代信息通信技术与工业经济的深度融合，工业互联网步入深耕落地阶段，工业互联网安全保障体系建设的重要性越发凸现。世界各主要发达国家

均高度重视工业互联网的发展，并将安全放在了突出位置，发布了一系列指导文件和规范指南，为工业互联网相关企业部署安全防护提供了可借鉴的模式，从一定程度上保障了工业互联网的健康有序发展，但随着工业互联网安全攻击日益呈现出的新型化、多样化、复杂化等特点，现有的工业互联网安全保障体系还不够完善，暴露出一些问题，总结如下：

（一）数据隐私和数据安全防护缺乏有效手段

工业互联网平台采集、存储和利用的数据资源存在数据体量大、种类多、关联性强、价值分布不均等特点，数据隐私与安全的主要关注点如下：

一是数据包含了敏感或个人隐私信息，因此数据在价值挖掘使用和发布的场景中可能会给个人、第三方和国家带来危害和损失，因此对隐私和重要数据的处理、使用、操作和发布、交流等生产流通环节都有安全与合规的要求；

二是数据需要多方的多维度融合才能创造价值，但往往每方都有自己数据的产权保护、个人数据和重要数据的合规责任，因此需要更安全的数据融合环境；

三是生产数据的每个环节需要相应的安全控制。工业互联网需要健康、稳定的发展，首要的是要解决企业对数据和隐私的担忧。

（二）OT 与 IT 融合较慢，人员的安全意识亟需提升

工业现场缺乏信息安全专家，对工业系统的信息安全关注度和重视度都不高，信息安全专家在面对生产优先的工业系统往往束手无策、

畏手畏脚。大部分工业互联网相关企业重发展轻安全，对网络安全风险认识不足。此外，很多智能工厂内部未部署安全控制器、安全开关、安全光幕、报警装置、防爆产品等，并缺乏针对性的工业生产安全意识培训和操作流程规范，使得人身安全难以得到保证。

（三）工业信息安全存在先天不足，安全防护能力难以快速提升

工控系统和设备在设计之处缺乏安全考虑，自身计算资源和存储空间有限，大部分不能支持复杂的安全防护策略，很难确保系统和设备的安全可靠。同时，当前专业工业信息安全企业和解决方案较少，工业企业风险发现、应急处置等网络安全防护能力普遍较弱。同时，工业生产迭代周期长、安全防护部署滞后、整体水平低、存量设备难以快速进行安全防护升级换代，整体安全防护能力提升时间长。

1.3.2 工业互联网安全风险分析

（一）工业互联网设备安全风险分析

工业互联网设备是指应用在工业互联网领域内具备灵敏准确的感知能力及行之有效的执行能力的智能化设备，例如智能终端、边缘网关、智能机器人等。当前，工业互联网智能设备行业应用正处于爆发性发展阶段，设备制造厂商往往只注重产品的可用性和易用性，受限于计算资源，很难实现细粒度的系统安全措施，导致设备自身存在众多安全缺陷。此外，真实制造环境中往往需要多种类型、多个厂商的工业互联网设备协同工作，在缺乏统一的安全技术规范来保证各系统交互安全情况下，大大的增加了攻击面，这将给工业互联网网络、

平台的安全性带来严峻的挑战。

风险点 1：工业互联网设备自身安全防护手段薄弱

设备直接暴露于互联网，或导致设备非法受控。由于工业互联网智能设备软件更新缓慢、厂商对漏洞不重视、用户对漏洞不了解导致当前市面上存在大量含有漏洞的设备直接暴露于互联网上。用户及厂商通常无法及时发现或修复漏洞，轻则导致正常功能被阻塞，影响设备功能安全，重则被攻击者利用来精心构建完整攻击链路，获取更高系统权限。

固件安全风险增加，或沦为不法攻击突破口。智能设备固件风险中，已知风险占绝大部分，与厂商在开发生命周期中忽略公开漏洞的排查和修复密切相关。已知风险信息的碎片化为漏洞排查增加了困难，但其公开属性却为攻击带来了便利。攻击者仅通过分析固件中存在的第三方库版本信息并查询相应版本漏洞库信息，就能获得潜在的固件安全风险。

开发人员安全意识薄弱，或加剧设备安全隐患。厂商在产品开发时通常直接调用第三方库，并且很少针对第三方库代码开展漏洞审查，是引发安全事件的主要原因。此外，开发阶段人员安全意识不足、使用弱口令、硬编码密钥、开启 SSH 服务和 FTP 服务等问题，都极易引发严重的安全事件。有大约 33.3%的厂商在产品出厂时完全不考虑安全因素。

风险点 2：工业互联网设备被用作跳板，向平台、网络发起攻击

智能设备数量的暴增为 DDoS 的成长提供温床。随着工业互联网

的发展，越来越多的智能设备暴露在互联网中，为承载 DDoS 功能的恶意样本进行扫描和传播提供了便利。同时由于各厂家良莠不齐的技术基础，导致各智能设备自身存在的系统与应用暴露出各种漏洞以被攻击者恶意利用。

多系统、跨平台为恶意代码感染提供便利。承载 DDoS 攻击的恶意代码家族，往往使用一套标准代码，以各种设备的弱口令、系统/应用漏洞的侵入为基础，在 MIPS、ARM、x86 等各种不同的平台环境编译器下进行编译，最终达到一个恶意代码家族跨多个平台、互相感染传播的目的，使传播更迅速。

海量设备为大流量攻击提供基础。智能设备数据庞大、安全性差、多数暴露外网，从僵尸网络搭建到数量达到一定规模，仅需数天时间便可完成。一旦目标被捕获，便成为了一个新的扫描源，如此反复便是一个成倍递增的扫描能力。目前，大流量攻击手段已经十分成熟，十万量级的僵尸网络便可以打出 TB 级的攻击流量。

智能设备安全接入措施不完善威胁平台安全。通常出于远程控制、数据分析、在线监测等业务需求，智能设备需要接入平台，与平台之间频繁进行数据交互。攻击者利用智能设备的安全缺陷获取智能设备的控制权限，将智能设备作为渗透进入平台的入口，进而窃取、伪造数据，危害平台安全。

（二）工业互联网网络安全风险分析

工业互联网的发展使得工厂内部网络呈现出 IP 化、无线化、组

网方式灵活化与全局化的特点，工厂外网呈现出信息网络与控制网络逐渐融合、企业专网与互联网逐渐融合以及产品服务日益互联网化的特点。这就造成传统互联网中的网络安全问题开始向工业互联网蔓延，具体表现为以下几个方面：工业互联协议由专有协议向以太网/IP 协议转变，导致攻击门槛极大降低；现有一些 10M / 100M 工业以太网交换机（通常是非管理型交换机）缺乏抵御日益严重的 DDoS 攻击的能力；工厂网络互联、生产、运营逐渐由静态转变为动态，安全策略面临严峻挑战等。此外，随着工业互联网的新技术的应用，如标识解析系统、5G 等，目前虽然还没有发现安全问题，但随着应用规模的不断扩大，安全风险也值得关注。

1、工业互联网标识解析系统安全风险

工业互联网标识解析体系是工业互联网网络体系重要组成部分，是支撑工业互联网互联互通的神经枢纽。目前，国家顶级节点已经在北京、上海、广州、重庆、武汉等五地上线运行，覆盖 25 个行业的 55 个二级服务节点完成部署上线，标识注册总量突破 38 亿，日均解析量超过 200 余万次，接入标识服务节点的企业超过 1700 家。整个系统涉及工业互联网终端、解析系统、网络、工控系统及各种通用协议和软硬件，呈开放式与互联网相连接，势必为工业互联网标识解析发展带来许多新的安全隐患，极易被攻击，一旦系统出现安全问题，将对标识解析体系和工业生产等造成重大影响。

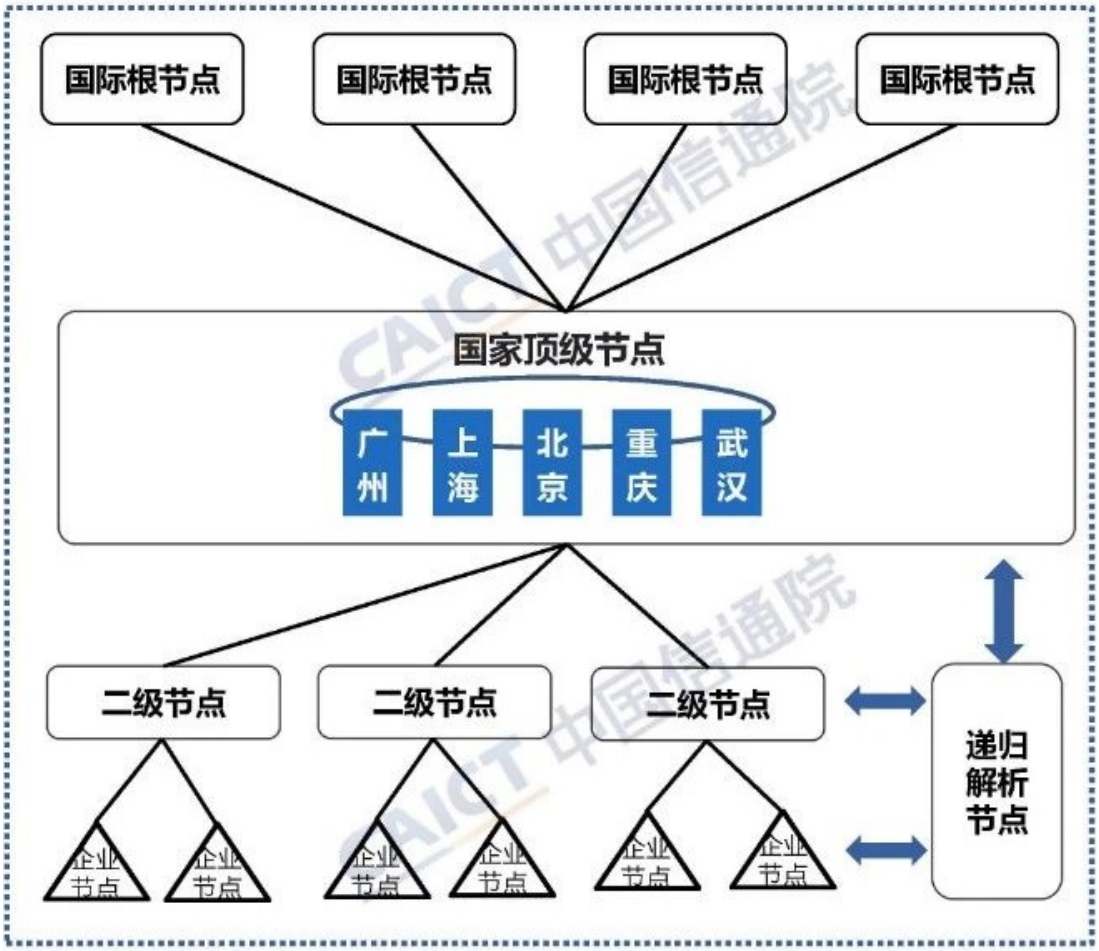

图 2 工业互联网标识解析体系

工业互联网标识解析系统的安全风险主要包括：架构安全风险（如节点可用性、节点协同风险、关键节点的关联性等）、数据安全风险（数据窃取、数据篡改、隐私泄露等）、运营安全风险（访问控制、业务连续性等）、以及身份安全风险（身份认证、越权访问等）。如下图 3 所示。

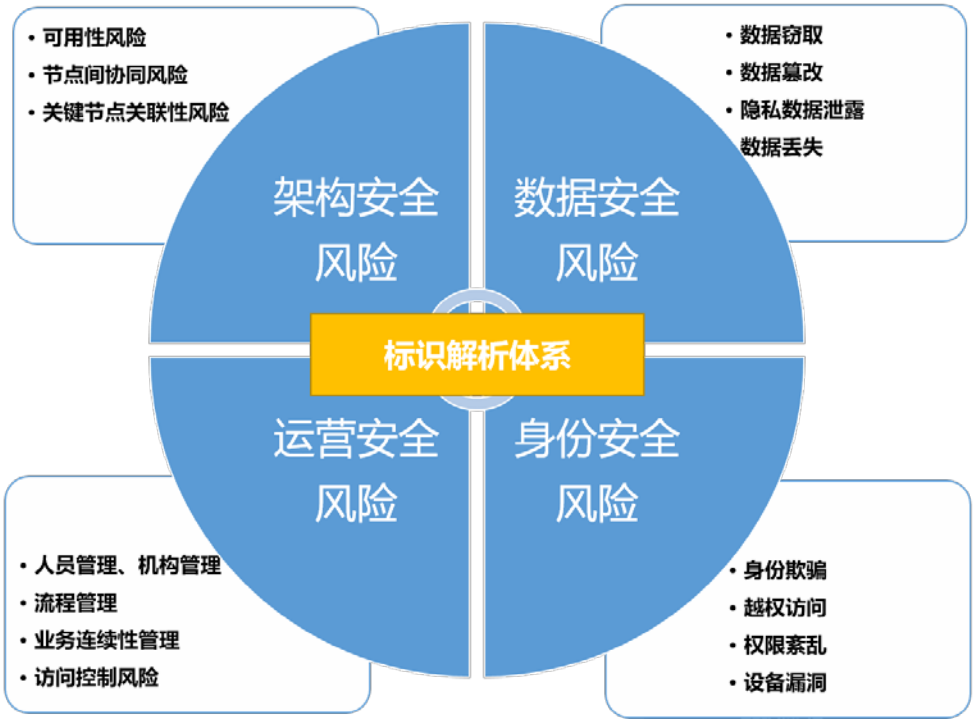

图 3 工业互联网标识解析体系安全风险

标识解析体系是工业互联网的关键信息基础设施，它解决的是把一串工业标识翻译成业务数据的问题。相较于 DNS 体系，标识解析体系更为复杂，因此存在的安全隐患和风险也更为突出：（1）标识解析体系的标准不统一，因此系统之间的联动和互操作就要复杂很多；（2）标识解析体系解析出的结果具有明显行业属性，不同行业的标识属性可能完全不同。正因为如此，标识解析体系需要考虑的安全风险更为广泛，而核心问题是要充分考虑标识解析结果的正确性，因此就要充分考虑标识解析体系中各节点的身份认证和访问控制问题，这也是标识解析体系能否安全可靠运转，有效支撑工业互联网、产业互联网健康发展的重要问题。关于身份认证和访问控制，一是要重点考虑标识解析体系的分级分层访问控制，二是要重点考虑采用不同标识解析体系的互操作认证。

2、5G 网络安全风险

5G 作为新一代移动通信技术，与传统网络相比，具有更高速率、更低功耗、更短时延和更大连接等特性。此外，5G 在大幅提升移动互联网业务能力的基础上，进一步拓展到物联网领域，服务对象从人与人通信拓展到人与物、物与物通信，开启万物互联的新时代。5G 主要面向的三大业务场景包括增强移动宽带（eMBB）、海量机器类通信（mMTC）和超可靠低时延通信（uRLLC）。

5G 网络是移动通信技术与人工智能、云计算、大数据等技术的高度融合以及系统架构的创新，涉及网络核心和管理架构以及通信协议的变革，而这些变革将使 5G 将带来更复杂的安全挑战。主要包括：

超大流量大大提升了基于流量检测、内容识别、加解密等技术的安全防护难度。5G 核心汇聚层达 200G/400G*N 的超大带宽以及传输低时延的要求，对网络安全态势感知、恶意流量攻击防御、恶意程序监控、不良信息监测等能力，以及对传输数据加解密能力，都提出高要求，提升了安全防护难度。

弱终端易成为受攻击对象。5G 万物互联，终端能力差异很大，弱终端由于资源、能力受限，难以采用全球用户身份模块（USIM）等强身份认证机制，终端自身安全防护能力也较弱，容易成为受攻击、受控对象。

超大连接易引发全网或局部规模攻击。5G 支持 100 万个连接/km，大量终端由于业务原因、网络抖动或受黑客控制，突发性大规模接入或重连，可能引发信令风暴或分布式拒绝服务（DDoS）攻击；海量

终端同时发起流量攻击，更可能超越、甚至击垮网络防御能力。

基础设施云化、IT 化进一步打破网络封闭状态。有别于传统网络，5G 全面引入 SDN/NFV、MEC、网络切片等技术，并采用全新的服务化架构，提出服务能力的开放，进一步打破网络封闭状态、安全边界模糊化，威胁传播更快、攻易防难，基础网络全面云化、IT 化对网络与信息安全保障带来新的挑战。

边缘云、D2D 通信模式的引入绕过现有中心化的监测体系。5G 引入的边缘云、D2D 通信，改变了原有的网络架构和通信模式，其中，边缘云分布式部署、计算能力、信息内容下沉，面临比中心化管理更严峻的内容安全风险；同时，边缘云业务流量本地卸载、D2D 通信流量不经核心网络，绕过了现有中心化的信息安全监测体系，难以对其进行有效监测和治理。

伪基站、身份泄漏问题得以解决，小基站安全性易受威胁。2G 时代的伪基站问题以及延续到 3G、4G 的用户识别码（IMSI）身份泄漏问题，在 5G 时代得以缓解，但是，为弥补宏基站高频覆盖问题，尤其是室内覆盖问题的各类小基站由于难以放置在专用的机房，物理安全较难得到保障，且需经公共网络回传，容易成为受攻击对象，并以此发起攻击，威胁网络与信息安全。

具体而言，5G 各层面的安全威胁主要包括终端侧、空口、gNB 基站、传输、MEC、核心网、虚拟网络平台、管理运营支撑系统（MBOSS）及其管理、能力开放等安全域的多种安全威胁，如下图 4 所示。

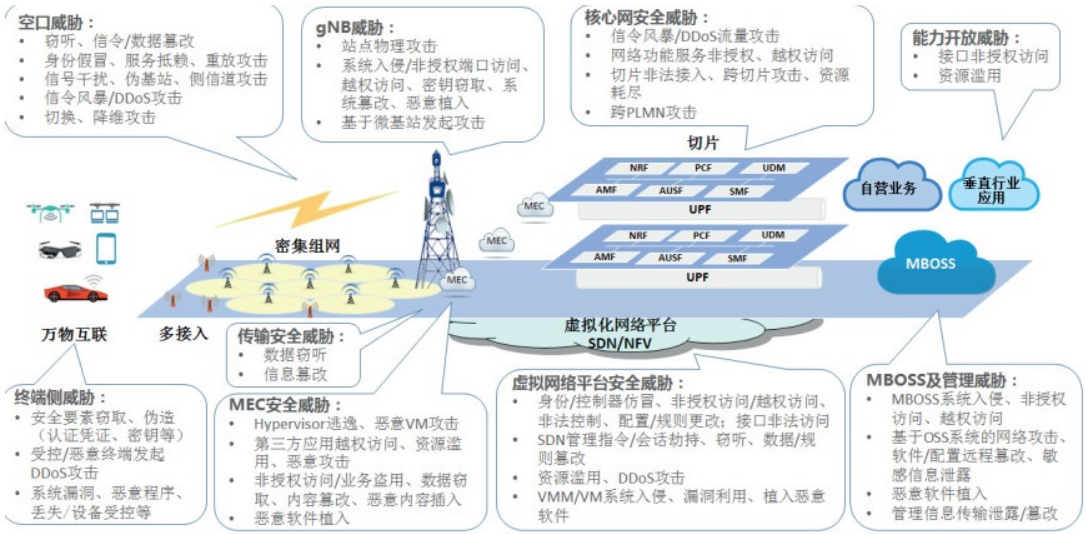

图 4 工业互联网-5G 网络安全风险与威胁

另外，5G 与信息技术及各行业的深度融合、数据量的爆炸式增长、海量终端连接等特点，也将大大增加安全监管的难度。

海量数据与舆情监测。5G 网络能力的大幅提升，将推动海量数据的生成和视频内容的发展，不良视频内容识别、海量数据的舆情分析等对安全监管带来挑战。

海量终端的溯源与取证。5G 支持海量终端连接，海量终端的身份管理和认证过程有别于传统终端，需要采用分布式认证、分级认证、基于（行业）用户认证或群组认证等新型认证方式，因此，海量终端的溯源、取证、上网日志留存等成为监管的难点。

（三）工业互联网控制安全风险分析

工业互联网使得生产控制由分层、封闭、局部逐步向扁平、开放、全局方向发展。其中在控制环境方面表现为信息技术（IT）与操作技术（OT）融合，控制网络由封闭走向开放；在控制布局方面表现为控

制范围从局部扩展至全局，并伴随着控制监测上移与实时控制下移。上述变化改变了传统生产控制过程封闭、可信的特点，造成安全事件危害范围扩大、危害程度加深、信息安全与功能安全问题交织等后果。

1、工业控制系统安全脆弱性

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》，工控系统分为生产管理层、过程监控层、现场控制层和现场设备层，涉及多种组件、应用和通信协议等，若一个环节保护不到位，就有可能导致整个工控系统被攻击而影响生产。脆弱性涉及管理层面和技术层面：

管理层面脆弱性包含：安全策略和制度不完善、安全职责不明确、安全意识薄弱、安全宣传与培训不完善、管理监督不到位、供应链管理机制欠缺、数据保护和备份管理不足、应急响应机制缺乏等；

技术层面脆弱性包含：安全架构设计不合理、操作系统陈旧、安全补丁不及时、访问控制不恰当、病毒或恶意程序防护不当、通信协议不安全、网络边界防护不足、系统配置不恰当、物理和环境保护薄弱、日志缺失或保留时间过短等。

2、工业控制系统安全威胁

威胁可能来自企业外部或内部，可能是恶意行为或非恶意行为，可能由人为因素或非人为因素（如自然灾害）导致。

就人为因素而言，来自外部的威胁主要是指攻击者利用工控系统的脆弱性，通过病毒（如震网病毒、勒索病毒）、钓鱼等方式发起攻击（比如高级持续性威胁 APT - Advanced Persistent Threat 攻击），渗

透进工控系统网络，进行非授权操作或者恶意破坏。攻击者可能包含恶意软件发布者、钓鱼或垃圾邮件发送者、僵尸网络操纵者、犯罪集团等。

来自内部的人为因素威胁主要是指心怀不满的内部员工或者工业间谍，利用工控系统管理或技术方面的缺陷，为恶意报复而删除企业核心数据，或为自身利益窃取企业核心机密售卖给竞争对手。此外，由于工控系统客观存在的脆弱性，人员在访问或操作工控系统时，也可能因为非恶意主观意愿，如误操作，对工控系统造成破坏和影响。

针对上述脆弱性和安全威胁，企业应从安全战略与合规、安全风险评估与管理、安全治理与架构、安全威胁与脆弱性管理、安全应急管理五个方面建立起安全防护体系，以降低安全风险，保护工业控制资产安全和正常生产秩序。

（四）工业互联网数据安全风险分析

大数据技术应用于工业互联网领域给企业带来巨大的效益，然而工业大数据对工业企业来说既是机遇也是挑战，在给企业带来巨大经济利益的同时，其本身所存在的安全问题也让企业面临着巨大的风险。一方面，由于工业控制系统的协议多采用明文形式、工业环境多采用通用操作系统且不及时更新、从业人员的网络安全意识不高，再加上工业数据的来源多样，具有不同的格式和标准，使其存在诸多可以被利用的漏洞。另一方面，在工业应用环境中，对数据安全有着更高的要求，任何信息安全事件的发生都有可能威胁工业生产运行安全、人

员生命安全甚至国家安全等。因而，研究工业大数据安全管理，加强对工业企业的安全保护变得尤为重要。

工业大数据安全是跨多工业领域与学科的综合性问题，需要结合法律法规、行业特点、工业技术等多维度进行研究。考虑到工业大数据平台所承载的工业数据的巨大价值，因此这里将整个工业大数据安全技术体系分为工业大数据接入安全、工业大数据平台安全、工业大数据应用安全三个层次。

（1）工业大数据接入安全

工业大数据接入安全必须保障工业边缘设备实时数据采集、工业远程状态监控、工业企业系统数据抽取等从外部系统获取工业数据，并进行清洗、转换、传输以进入工业大数据平台的完整数据传输链的安全。

数据采集端支持采集模块的注册及安全认证机制，保障数据采集应用的合规性，采集数据的准确性；边缘计算模块支持统一模块管理下发及签名校验机制，保障数据预处理应用的合法性和可靠性；数据传输通路支持通道加密，保障传输过程中的机密性和完整性。

（2）工业大数据平台安全

工业大数据平台安全是对工业数据资源的存储、访问、运算等功能的安全保障，包括数据的存储安全、计算安全、平台管理安全以及基础设施安全。

平台存储安全支持数据多备份设置与恢复机制，并采用数据访问控制机制来防止数据的越权访问；计算安全支持计算发起方的身份认

证和访问控制机制，确保只有合法的用户或应用程序才能发起数据处理请求；平台管理安全包括平台组件的安全配置、资源安全调度、补丁管理、安全审计等，确保整个平台组件及运行状态安全可控，同时还应强化平台的数据隔离和访问公职机制，实现数据“可用不可见”；平台软硬件基础设施安全包括基础网络安全、虚拟化安全等，从而保障整个大数据平台的安全运行。

（3）工业大数据应用安全技术

工业大数据应用会对存储于工业大数据平台的海量数据进行查询、分析、计算、导出等操作，因此在工业大数据平台提供数据服务的同时，其安全风险也随之被暴露，攻击者可利用各类已知或未知漏洞发起攻击，达到破坏系统或者获取数据信息的目的，因此需要对数据应用安全进行严格管控。

工业大数据应用安全应从几方面考虑：支持应用访问签名机制，确保只有授权的应用才能提交数据访问请求；支持应用数据按需访问，避免数据访问范围的扩大化；支持应用行为实时监控，实时拦截应用中包含的攻击行为，包括数据访问范围、频率、SQL 语句合法性等；建立完整的应用流程管理机制，包括应用的提交、执行、状态监控、结果审计等，确保每个应用的审批、控制于追责有效结合，避免高权限人员的恶意操纵或误操作行为；构建完备的应用测试环境及测试规范，确保只有符合安全策略的应用可以审批执行。

（五）工业互联网平台安全风险分析

平台是工业互联网发展的关键，工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量 数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台，包括边缘、平台（工业 PaaS）、应用三大核心层级。工业互联网平台连接业务复杂，连接设备种类繁多，数据格式多样，在推进智能化、柔性化、协同化生产的同时，安全边界也越发模糊，受攻击面不断扩大，工业互联网平台各层均存在安全风险。

图 5 工业互联网平台功能架构图

如上图 5 所示，从工业互联网平台功能架构来看，可将工业互联网平台安全风险分为边缘层安全风险、工业 IaaS 安全风险、工业 PaaS 安全风险、工业 SaaS 安全风险与平台数据安全风险等五个方面。

边缘层安全风险：边缘层安全是指工业互联网平台与工业企业接

入过程中数据采集、协议转换、边缘计算的安全。由于智能传感器、边缘网关等边缘终端设备计算资源有限，安全防护能力薄弱，工业互联网平台在数据采集、转换、传输的过程中，数据被侦听、拦截、篡改、丢失的安全风险更高，攻击者可利用边缘终端设备漏洞对平台实施入侵或发起大规模网络攻击。

工业 IaaS 安全风险：工业 IaaS 安全是指工业互联网平台云基础设施的安全，包括主机设备物理安全、虚拟化系统安全、虚拟化网络安全、虚拟化管理安全、工业数据存储安全等。工业 IaaS 是虚拟化、资源池化的信息基础设施，面临着虚拟机逃逸、跨虚拟机侧信道攻击、镜像篡改等新型攻击方式的威胁。另外，多数平台企业使用第三方云基础设施服务商提供的 IaaS 服务，存在数据安全责任边界不清晰等安全问题。

工业 PaaS 安全风险：工业 PaaS 为用户提供了包括工业应用开发工具、工业微服务组件、工业大数据分析平台、数据库、操作系统、开发环境等在内的软件栈，允许用户通过网络来进行应用的远程开发、配置、部署，并最终在服务商提供的数据中心内运行。工业 PaaS 所面临的安全威胁主要有非法窃取或访问软硬件资源、拒绝服务攻击、恶意软件植入等。通用 PaaS 平台感染病毒、木马，可造成平台瘫痪、服务中断、数据丢失等严重后果。工业应用开发工具、微服务组件存在漏洞，将影响工业 APP 的正常开发和使用。工业大数据分析平台汇聚海量工业企业的工艺参数、产能数据等高价值数据，被黑客入侵可能导致敏感信息泄露，威胁平台数据安全。可以借助于数据加密、

防火墙、访问控制机制、强制执行最小权限规则、反病毒软件和入侵检测工具等技术和管理手段进行安全性增强。

工业 SaaS 安全风险：工业 SaaS 安全是指工业互联网平台应用层的应用服务安全。其中，工业 APP 涉及专业工业知识、特定工业场景，集成封装多个低耦合的工业微服务组件，功能复杂、安全设计规范缺乏，可能存在安全漏洞和缺陷，面临的工业 APP 漏洞、API 通信安全、用户管控、开发者恶意代码植入等应用安全问题更为突出。

平台数据安全风险：平台数据安全涉及接入平台、平台运行、平台退出三个阶段中的数据安全。其中，在接入平台阶段，包括上述边缘层接入以及工业 APP 接入到平台过程中数据面临的侦听、拦截、篡改、丢失、窃取等安全风险；在平台运行阶段，主要面临数据存储安全风险；在平台退出阶段，涉及用户迁移平台或完全退出平台时数据泄露与备份的安全风险。

（六）工业 APP 的安全风险分析

工业互联网 APP（简称工业 APP）是基于工业互联网，承载工业知识和经验，满足特定需求的工业应用软件，是工业技术软件化的重要成果。在 2018 年工业和信息化部网络安全管理局组织开展的工业互联网安全检查评估工作中发现，国内某平台的工业 APP 存在大量反编译、Webview 明文存储密码、Janus 签名机制漏洞等。攻击者可利用漏洞窃取客户端数据，包括手机号、密码，以及设备运行状态、设备工作时间、重大敏感工程位置等敏感信息。当连接设备出现故障

报警时，攻击者还可通过截获、篡改设备故障信息，使用户在工业 APP 客户端上无法接收设备报警信息，导致大型机械设备出现持续异常故障， 进而造成重大工程事故。

总体来说，工业 APP 面临安全风险包括以下几个方面：

传统开发环境与运行环境风险。由于运行环境和应用组件可能由于在内存结构、数据处理、环境配置及系统函数等各面方设计原因会导致内存溢出、敏感信息管理及封装和隐藏缺陷等问题，包括会出现其反序列化漏洞等。直接导致上层应用程序调用时出现下面的输入验证、隐藏域、漏缓冲区溢出、跨站请求伪造等问题甚至会造成软件的运行异常、数据丢失等严重问题。

安全机制不健全。即工业 APP 目前还处于起步阶段，很多场景下没有考虑安全措施，自身缺乏在身份认证、访问控制、数据存储加密、通信加密、安全校验和权限管理等方面的安全设计，

PaaS 层没有足够标准安全 API（Security API）。大量工业互联网平台目前也探索阶段，在安全上尚没有安全机制，没有足够的安全 API 供 SaaS 层调用。

API 误用（API Abuse)。API 是调用者与被调用者之间的一个约定，大多数的 API 误用是由于调用者没有理解约定的目的所造成的。当使用 API 不当时，也会引发安全问题。

时间和状态。分布式计算与时间和状态有关。线程和进程之间的交互及执行任务的时间顺序往往由共享的状态决定，如信号量、变量、文件系统等。与分布式计算相关的缺陷包括竞态条件、阻塞误用等。

代码质量问题。低劣的代码质量会导致不可预测的行为。对于攻击者而言，低劣的代码使他们可以以意想不到的方式威胁系统。常见的该类别缺陷包括死代码、空指针解引用、资源泄漏等。

软件反编译风险。工业 APP 软件缺乏足够的代码混淆、花指令、跳转等方式增加工业 APP 源代码的不可读性，很可能被反编译后获取主要重要信息、或者被篡改重要数据。

1.3.3 工业互联网安全发展趋势

总结起来，工业互联网安全发展的总体趋势是：传统的安全防御技术已无法抗衡新的安全威胁，防护理念将从被动防护转向主动防御。其几大发展趋势总结如下：

（一）融合安全技术成为 OT 与 IT 融合趋势下的必然选择

工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

工业控制系统面临着安全事件危害范围扩大、危害程度加深、信息安全与功能安全问题交织等安全风险；控制环境方面表现为信息技术（IT）与操作技术（OT）融合，控制网络由封闭走向开放；控制布局方面表现为控制范围从局部扩展至全局，并伴随着控制监测上移与实时控制下移。

工业互联网安全所采用的技术必然要 IT 安全、OT 安全以及 IT 与 OT 安全以及 IT 与 OT 融合安全技术如工业 VPN、工业 NAT、工

业入侵检测、工控网络接入控制、无需依赖外部特征库的 AI 智能分析与检测等才能够满足工业互联网安全建设目标，从而使得工业系统既防护 OT 内部威胁，也防护 IT 威胁。

（二）工业互联网未知威胁防范成为难点

新基建筑牢基础并加速工业数字化转型，强化工业互联网建设，催生 5G/IoT 等新场景机会。数字化转型时代，经济利益驱动网络攻击不断升级，关键基础设施和工业互联网保护面临更大挑战。

首先，超大规模泄露已趋于常态化。据报道“每月上亿条信息泄露，涉及政府数据、医疗信息、账户凭证、企业用户信息等敏感数据，平均数据泄露成本高达 392 万美元”。

其次，勒索软件手段升级、加大赌注。勒索软件转向有针对性威胁，80%的攻击针对企业，其中 68%的要钱，并演进为两阶段攻击。攻击目标从盲目感染到针对财务/ERP 等高价值资产，手段从钓鱼方式投递到利用 APT 高危漏洞，套现方式变为先在互联网部分公开窃取数据催缴赎金，获取赎金后，继续贩卖窃取的信息。

最后，关键基础设施面临更大的安全风险。90%的受访企业在过去两年遭遇过网络攻击，其中一半的网络攻击造成关键基础设施的“停转”。

在实现态势感知的过程中，对采集的大量安全数据如何进行分析，发现潜在风险一直是个难点，尤其是面对工业互联网平台复杂的架构。面对这一难题，应当引入目前在已经逐渐成熟的机器学习技术，通过 AI 的助力去认知网络、学习现状、总结风险，从而将主动防御这一目

标落实，实现更高的安全防护水平。

（三）云平台成为安全防护的重点

未来制造系统将呈现扁平化特征，传统以 ISA-95 为代表的“金字塔”体系结构被逐渐打破，ERP、MES、PLM 等处于不同层次的管理功能基于平台实现集成融合应用，工业互联网平台将成为未来制造系统的中枢与核心环节。借助平台提供的数据流畅传递和业务高效协同能力，能够第一时间将生产现场数据反馈到管理系统进行精准决策，也能够及时将管理决策指令传递到生产现场进行执行，通过高效、直接的扁平化管理实现制造效率的全面提升。

平台作为工业互联网的核心，汇聚了各类工业资源，因而在未来的防护中，对于平台的安全防护将倍受重视。平台使用者与提供商之间的安全认证、设备和行为的识别、敏感数据的共享等安全技术将成为刚需。

当前工业互联网平台主要采用云计算和大数据技术搭建而成，针对云平台的保护显得尤为重要。企业工业互联网云平台有如下安全风险或难题需要解决：

（1）云内更多东西访问，边界防护失效；缺乏威胁隔离机制，网络威胁一旦进入云平台内部，可以肆意横向蔓延；

（2）流量流向不可视：用户无法直观感受到虚机之间数据流量大小、流向变化；

（3）威胁态势无感知，虚拟层漏洞不易修复：云内主机成倍增加，横向访问占据 80%以上，安全态势难以全局掌控；

（4）安全策略调整不灵活：云内 IP 地址动态分配、虚拟位置不确定、IP 地址动态分配、VLAN 隔离方式太复杂，业务区域边界不确定；

（5）关键数据被窃取：相较于外部攻击，恶意的内部人员造成的危害风险更大，而缺乏相关审计措施。

（四）内生安全防御和补偿式安全防御将长期并存

内生安全防御通常在设备层面通过对设备芯片与操作系统进行安全加固，并对设备配置进行优化的方式实现应用程序脆弱性分析。可通过引入漏洞挖掘技术，对工业互联网应用及控制系统采取静态挖掘、动态挖掘，实现对自身隐患的常态化排查；各类通信协议安全保障机制可在新版本协议中加入数据加密、身份验证、访问控制等机制提升其安全性。

但另一方面，工业现场还存在大量的不安全控制协议、不安全的工业设备、不可靠的工控网络、不安全的工业软件等，而更新这些系统又显得不现实，而且周期特别长，同时完全采用内生安全防御方式，在某些情况下并非经济高效，所以采用类似网关的补充式安全防御也非常必要。

（五）工业互联网安全防护自动化与智能化将不断发展

未来对于工业互联网安全防护的思维模式将从传统的事件响应式向持续智能响应式转变，旨在构建全面的**预测、基础防护、响应和恢复能力**，抵御不断演变的高级威胁。工业互联网安全架构的重心也将从被动防护向持续普遍性的监测响应及自动化、智能化的安全防护

转移。

（六）对大数据的保护将成为防护热点

工业大数据的不断发展，对数据分类分级保护、审计和流动追溯、大数据分析价值保护、用户隐私保护等提出了更高的要求。未来对于数据的分类分级保护以及审计和流动追溯将成为防护热点。

首先是应用数据领域的安全解决方案。包括对已经有权限访问敏感数据的人员或主机发起的数据滥用、数据窃取份风险，能针对泄露事件快速溯源定位到可疑对象，从而建立起威慑能力；以及对应用系统上流动的敏感数据类型、数量、数据载体、暴露面、数据六项等多个对象进行识别并监控其状态变化、分析变化影响，帮助数据安全管理人员进行业务层的流动态势和风险评估。

其次是大数据平台安全方案。即针对大数据平台（Hadoop 以及相关组件）的 4A（账号、认证、授权、审计）+数据运维和分析的安全管理。最后是数据地图。主要围绕隐私合规要求，梳理和识别隐私数据做分类分级、隐私数据的数据流（采集点、存储地域、使用系统和用途、外流去向）、分析隐私数据的授权信息，并按数据主体汇集数据，以提供数据主体权利的支持。

（七）工业互联网安全态势监测与感知将成为重要技术手段

工业互联网安全态势感知对影响工控网络安全的诸多要素进行获取、理解、评估以及预测未来的发展趋势，成为下一代安全技术的焦点。网络安全态势感知是对网络安全性定量分析的一种手段，是对网络安全性的精细度量。

借助人工智能、大数据分析以及边缘计算等技术，基于协议深度解析及事件关联分析机制，分析工业互联网当前运行状态并预判未来安全趋势，实现对工业互联网安全的全局掌控，并在出现安全威胁时通过网络中各类设备的协同联动机制及时进行抑制，阻止安全威胁的继续蔓延。

工业互联网安全态势监测与感知建设对提升工业互联网安全防护能力至关重要。从政府监管层面来说，应做好顶层设计，结合国家工业互联网产业需求，统筹设计国家工业互联网安全监测技术平台功能和架构。加强构建“国家级-省级-企业级”专业化安全监测和预警通报技术手段，实现工控网络相关企业安全态势可感、可知、可监管。

第二章 工业互联网安全政策及防护框架

2.1 国外工业互联网安全相关政策进展

2.1.1 美国工业互联网安全

美国把工业互联网作为“国家先进制造战略计划”的重要方向，发挥自身强大的信息技术优势，依托工业互联网联盟（IIC）以及通用、思科、IBM 等龙头企业，抓紧战略布局和生态打造，推动工业互联网在制造、能源、交通等多领域应用。目前，IIC 已汇聚 33 个国家近 300 家成员单位，通过架构顶层设计、标准化需求研究、技术标准验证等工作，试图打造全球工业互联网发展枢纽。美国产业界对工业互联网安全高度重视，IIC 下设安全任务组，主要负责安全相关的研究工作，推动业界形成共识，推进安全实践。

2016 年 9 月 19 日，美国工业互联网联盟（IIC）正式发布《工业互联网安全框架（IISF）》1.0 版本，从功能视角出发，以安全模型和策略作为总体指导，部署通信、端点、数据、配置管理、监测分析等方面的安全措施。同时，明确定义了构建工业互联网可信体系的五大关键要素，即：Security（信息安全）、Safety（功能安全）、Reliability（可靠性）、Resilience（弹性）和 Privacy（隐私安全）。如图 13 所示，拟通过该框架的发布为工业互联网安全全面深入研究与实施提供理论指导。总的来看，美国 IISF 聚焦于 IT 安全，侧重于安全实施，明确了具体的安全措施，具有很好的借鉴意义。

图 6 美国工业互联网安全可信体系

2018 年 3 月 12 日，美国 IIC 发布《端点安全最佳实践》白皮书，明确定义了端点安全所需的 3 个级别，即基本级、增强级和关键级，细化了每个安全级别应部署的安全防护措施。其中，基本级提供了针对使用基础资源简单违规的防护策略；增强级提供了针对使用中等资源复杂手段攻击的防护策略；关键级进一步加强，提供了针对使用扩展资源的复杂手段来攻击的防护策略。端点安全最佳实践构建了端点可信体系，为端点安全防护提供了可借鉴的参考模式，可更好地指导企业部署端点安全实施。

2018 年 4 月 12 日，美国 IIC 发布《安全成熟度模型：描述和预期效果》（SMM）白皮书，在充分考虑实施过程中的可适用性、不断变化的威胁环境，以及在未来可扩展性的基础上，建立成熟度概念模型。通过构建 SMM，明确当前成熟度级别、目标成熟度级别以及从当前状态到目标状态的机制和过程。同时，SMM 分层次定义了维度、域和实践，可清晰地从整体的各个维度到个体实践获知成熟度和差距分析，从而可更好地为企业进行工业互联网安全评估提供理论指导。

2019 年 2 月 25 日，美国 IIC 发布《安全成熟度模型：从业者指南》白皮书，从维度、域、实践层面详细描述了为达到安全性必须采取的措施。此外，还包含 3 个案例研究，指导利益相关者如何在实践中应用 SMM。

2019 年 7 月 22 日，美国 IIC 发布《数据保护最佳实践白皮书》，专门就工业互联网数据安全提出了产业最佳实践，反映了产业界对数据安全的高度关注，逐步推动数据安全实施，并以数据安全策略推动建立完备的安全体系。

2019 年 7 月 29 日，美国 IIC 发布《在实践中管理和评估 IIoT 可信度》白皮书，作为工业物联网可信度的入门指南，由 IT 与 OT 融合驱动，详细介绍了可信度的定义、示例和管理 IIoT 系统可信度的最佳实践方法。

美国 IIC 高度重视汽车安全，以汽车行业为切入点，在安全组下设了汽车安全任务组，创建了汽车安全演示环境，该演示环境提供了开放的汽车功能安全和信息安全架构验证平台，可模拟仿真由信息安全导致的功能安全问题。美国 IIC 强调成果的实践性，将围绕汽车全产业链不断开展针对汽车安全技术和产品的全面深入调研，聚焦自动驾驶安全和 V2X 通信安全，并协同推进《汽车可信白皮书》的撰写。

此外，美国 IIC 安全组还广泛开展与我国工业互联网产业联盟（IIC）、德国工业 4.0、美国电气制造商协会、日本工业价值链促进会等的交流合作，分享各自的工作推进情况，就共同关注的 IoT 环境下的网络连接安全、设备安全、风险挑战、安全用例的适用性，以及风

险评估等问题进行积极讨论，探讨未来联合召开安全论坛、联合发布报告等合作的可能性。在标准方面，美国 IIC 已与 ISO 等 20 多个国际标准化组织、开源组织和区域标准研制部门建立了协作关系，推动研究成果向标准的高效转化。

2.1.2 德国工业 4.0 安全

德国电工电子与信息技术标准化委员会（DKE）于 2015 年 4 月发布了工业 4.0 参考架构模型（RAMI4.0），工业 4.0 的概念旨在以 RAMI4.0 模型为形式，制定数字化描述规则，用来描述贯彻整个全生命周期的技术对象和价值链变化。安全作为重要组成部分贯穿于整个架构，并指出需从全生命周期统筹考虑所有资产的安全风险，并对资产所有者提供实时保护措施。

德国发布《工业 4.0 实施战略》，明确了工业 4.0 的关键技术演进方向、标准化路径及相关安全问题，提出重视与现有安全标准的结合，强调在实施安全标准的过程中继续完善与创新标准，从而提高工业 4.0 的整体安全性。

2019 年 2 月 5 日，德国联邦经济和能源部长在柏林发布《国家工业战略 2030：对于德国和欧洲产业政策的战略指导方针》的计划草案（以下简称《德国工业战略 2030》）。该战略旨在与工业利益相关者一道，努力确保或重夺所有相关领域在德国国内、欧洲乃至全球的经济技术实力、竞争力和工业领先地位。《德国工业战略 2030》基于可靠的、经过检验的社会市场经济原则，制定了相应标准以证明或否定

（通常如此）特殊情况下国家行为的必要性。这有助于有效地限制国家干预，但如果有更高层面的经济考虑需要国家干预，则可以赋予其合法性。

其他方面的政策和举措还包括：设立德国工业 4.0 在线图书馆，在安全方面，经过不断的实践，出版了包括《工业 4.0 中的 IT 安全》《安全身份标识》《跨企业安全通信》《工业 4.0 安全指南》在内的一系列刊物。

德国工业 4.0 平台十分重视数据安全保护，积极推动与我国在工业互联网数据方面的交流合作，并在数据保护方面达成共识。

2.1.3 其他国家工业互联网安全政策

欧盟方面，2017 年 11 月 20 日，欧盟网络空间安全局发布的《欧盟关键信息基础设施环境中的物联网安全基线指南》，对物联网安全现状及安全基线建议进行了全面总结，以期进一步促进欧洲物联网产业的健康快速发展。其主要内容包括：物联网的体系架构、威胁和风险分析、安全方法和实践、差距分析以及改进物联网安全的高层建议。2018 年 5 月 25 日正式生效的《通用数据保护条例》对企业的数据保护义务提出了全新的监管要求，严格规定了企业对客户数据的搜集、存储使用的规范和准则。

日本方面，加强终端设备安全保护。日本针对网络安全的法律法规制定相对美国起步较晚，总务省于 2017 年 10 月出台了《物联网安全综合对策》，对物联网安全对策进行部署。此外，为了减少黑客利

用联网设备攻击东京奥运会基础设施的可能性，2019 年 1 月，日本通过一项法律修正案，允许政府人员使用默认密码和密码词典来尝试登陆日本消费者的联网设备，将政府人员尝试登录私人联网设备的行为合法化。2019 年 4 月，日本经济产业省商务信息政策局正式公开了《网络/物理安全对策框架》及其配套的一系列行动计划，鼓励日本积极与其他国家和国际组织展开合作，共同制定关键信息基础设施保护国际规范。

韩国方面，2019 年 9 月，韩国政府制定《国家网络安全基本规划》，政府将通过改善国家信息通信网和主要信息通信设施的安全环境增强网络修复和存活能力，开发和推广安全便利的新一代安全基础设施，提高核心基建设施的安全性。

新加坡方面，2019 年 1 月，新加坡信息通信媒体发展局发布《物联网网络安全指南》，提出了物联网网络安全的基础概念、检查表和基线建议，重点关注物联网系统采集、开发、运营和维护各个环节的安全，基于对案例的研究提供了有关物联网安全实施的更多细节。2019 年 10 月，新加坡和英国签署名为《安全设计：英国和新加坡就物联网进行合作的联合声明》的协议，以加强两国在联网设备安全方面的合作伙伴关系。

2.2 我国工业互联网安全相关政策进展

党中央、国务院高度重视工业互联网安全。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。

2017 年 11 月 27 日，国务院发布《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，将安全保障与网络、平台建设共列，成为重要的三大体系之一。

2018 年 6 月 7 日，工信部印发了《工业互联网发展行动计划》（2018—2020 年）。明确并细化了安全相关未来 3 年工业互联网安全行动的总体目标、行动内容。

2018 年 9 月，在长三角峰会上发布了《工业互联网安全框架》，在国内首次提出了工业互联网安全框架，旨在指导工业互联网相关企业开展安全防护体系建设，提升安全防护能力。

2018 年年底，中国信通院支撑工信部研究制定了工业互联网安全标准体系框架，框架包括总体性标准、基础共性标准、安全防护标准、安全管理与服务标准、垂直领域应用标准 5 大类标准。

2019 年 1 月 25 日，工信部、国标委两部委联合印发了《工业互联网综合标准化体系建设指南》，明确了网络、平台、安全、应用相关建设内容。其中安全标准包括“设备安全”“控制系统安全”“网络安全”“数据安全”“平台安全”“应用程序安全”“安全管理”。

2019 年 7 月 26 日，工信部、教育部等十部委联合发布了《加强工业互联网安全工作的指导意见》，提出了 7 大任务和 17 项重点工作，并提出 4 项重点保障举措，为开展工业互联网安全工作提供切实可行的指引。

2019 年 10 月 22 日，工信部印发《关于加快培育共享制造新模式 新业态 促进制造业高质量发展的指导意见》，提出强化安全保障

体系。围绕应用程序、平台、数据、网络、控制和设备安全，统筹推进安全技术研发和手段建设，建立健全数据分级分类保护制度，强化共享制造企业的公共网络安全意识，打造共享制造安全保障体系。

2020 年 3 月 20 日，工信部印发《关于推动工业互联网加快发展的通知》，通知中要求各有关单位要加快拓展融合创新应用、加快健全安全保障体系、加快壮大创新发展动能、加快完善产业生态布局、加大政策支持力度。

我国工业互联网联盟（AII）专门设有安全组，自成立以来，在标准研制、实验验证、产业推广、国际合作方面已取得多项成果。AII 还发布了一系列工业互联网安全产业报告，如《工业云安全防护参考方案》《中国工业互联网典型安全解决方案汇编》《工业互联网安全威胁态势报告》（年度报告）、《工业互联网安全框架》等。此外，为规范工业互联网安全评估评测工作，构建工业互联网安全评估评测体系，培育工业互联网评估评测人才队伍和安全人才队伍，开展了工业互联网安全评估师能力认定工作和安全工程师能力认定工作。

2.3 深圳市工业互联网安全相关政策及举措

为落实中央和广东省关于发展工业互联网的决策部署，深圳市精准施策、多措并举，发力新基建、培育新动能，以加快推动工业互联网建设为契机，突破工业发展瓶颈，深入践行高质量发展战略，全面实现工业转型升级，为粤港澳大湾区和深圳先行示范区建设注入强劲动力。

深圳市作为制造业大市和新一代信息技术产业重镇，近年来一直着眼长远、谋篇布局，稳步推进工业互联网的政策体系完善、产业生态培育和应用模式建设。

在政策引领上，2018 年 6 月 14 日，深圳市人民政府办公厅印发《深圳市关于加快工业互联网发展的若干措施》和《深圳市工业互联网发展行动计划（2018—2020 年）》，提出到 2020 年，将深圳市建成创新驱动、应用引领、生态活跃的全国工业互联网领先地区。在今年的市政府工作报告中，也专门提出要建设一批工业互联网平台和智能工厂，推进制造业数字化、网络化、智能化升级改造。

在生态培育上，深圳市一方面建立了“深圳市工业互联网专家委员会”，着力为工业互联网发展提供智力支撑。另一方面积极推动华为、腾讯、富士康等龙头企业联合成立“深圳市工业互联网联盟”，合力促进行业资源对接和应用推广。与此同时还开展“工业互联网大会”、“工业互联网巡回大讲堂”等活动，大力推广企业数字化转型的经验做法。这一套“组合拳”打造出了良好的工业互联网发展生态，形成了以专家智库为支撑、以产业联盟为载体、以产业集群为依托的“体系作战”的强大优势。

在应用模式上，深圳市不断推进工业互联网创新探索，新模式、新业态不断涌现，呈现出融合应用逐渐丰富，应用生态日趋成熟的良好发展态势。速加网、衣全球等一批“网络工厂”，创新了“总部（深圳）+工厂（珠三角）”进行跨地域生产制造的新模式、新业态。速加网为传统的机械零部件制造业构建加工协同智造网络，智能匹配供需

信息、提供免费 SaaS 系统实现透明化生产。衣全球打通了渠道销售、数据运营、货品供应、库存管控，有效通过后端快反生产支撑前端直播。

分区谋划，因地制宜促发展。在深圳市委、市政府全面推动下，宝安、龙岗、龙华等工业大区积极推进区域试点示范，加强工业互联网发展政策规划，加快推进工业互联网产业示范基地建设，形成各有特色的工业互联网发展格局。

宝安区通过工业互联网为产业赋能，打造了产业链协同、产融协同、区域协同的融通发展格局。近期获批的深圳宝安区国家新型工业化产业示范基地（工业互联网）是全国 4 个工业互联网示范基地之一，拥有 5G 与新型工业网络、智能装备与智能终端、人工智能、半导体与柔性电子等先进产业集群，围绕工业互联网的新产业体系业已形成。

龙岗区通过区政府采购龙头企业协助开展工业企业数字化转型服务项目，实施“龙岗区智能制造标杆企业计划”和“龙岗区中小企业上云计划”。力争在 5 年内构建政府、工业云服务商和工业企业之间的沟通桥梁，加快“政、产、学、研、用”的深度融合，推进区工业企业积极投入数字化转型，带动龙岗区整体制造业产业集群转型升级、提升工业互联网能力，带动制造业创新发展。

龙华区借力产业优势，深化“互联网+先进制造业”。作为全省首批“工业互联网产业示范基地”，龙华区凭借自身产业优势，加强基础设施建设和多层次平台建设、创新应用提升、大力发展 5G+工业互联网应用，已经驶入了工业互联网发展快车道。下一步将全力实施基

础网络升级改造、实平台梯度培育、创新应用示范、生态环境四大工程，着力构建完整的工业互联网生态体系。

改革开放 40 年，求新、求变已经成为深圳这座城市的绚丽底色。勇立工业互联网建设的潮头，发力“新基建”、创造新模式、形成新优势、推动新突破、开拓新空间，正汇聚起不竭新动能，推动深圳继续破浪前进、先行示范。

2.4 国内外工业互联网安全防护框架

2.4.1 国外工业互联网安全防护框架

（一）美国工业互联网安全框架（IISF）

2016 年 9 月 19 日，美国工业互联网联盟（IIC）历经两年时间正式发布工业《工业互联网安全框架（IISF）》（V1.0），拟通过该框架的发布为工业互联网安全研究与实施部署提供指导。

IISF 的实现主要从功能视角出发，定义了 3 个层次的 6 个安全功能，如下图 7 所示。顶层包括 4 个核心安全功能，分别为端点保护、通信和连接保护、安全监控与分析、安全配置管理。端点保护：实现设备在边缘侧和云侧的防御能力，主要关注点包括物理安全功能、网络安全技术和身份鉴权。通信和连接保护：利用端点的身份标识与授权能力实现链路层面的认证和授权，主要关注点包括信息流的完整性和保密性。为了与端点和通信保护实现协同，在整个运行周期，安全监控和分析、安全配置和管理必须在系统层面相应启动。

在 4 个核心安全功能之下是一个通用的数据保护层，对这 4 个功能中产生的数据提供保护；最下层是覆盖整个工业互联网的安全模型和策略层，它将上述 5 个功能紧密结合起来，实现端到端的安全防护。

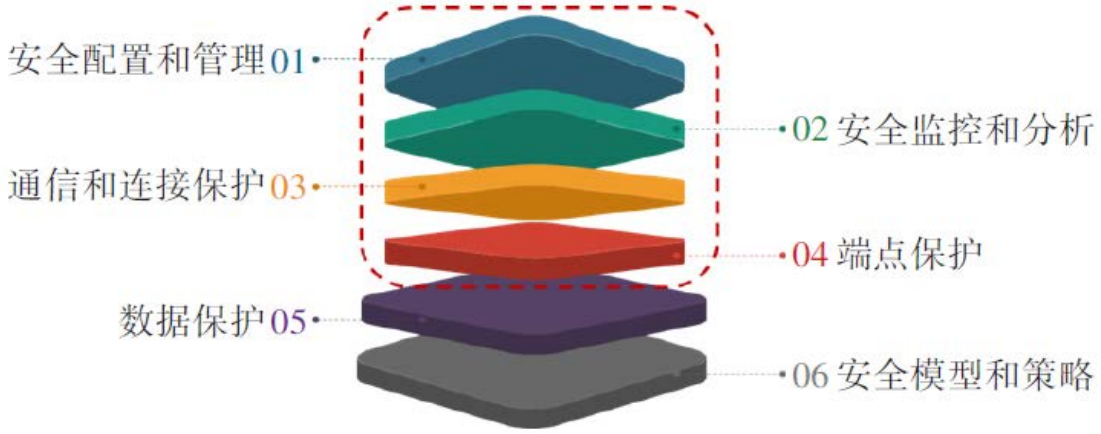

图 7 美国工业互联网安全实施框架

总得来看，美国 IISF 聚焦于 IT 安全，侧重于安全实施，明确了具体的安全措施，对于工业互联网安全框架的设计具有很好的借鉴意义。

（二）德国工业 4.0 安全框架（RAMI 4.0）

德国工业 4.0 注重安全实施，由网络安全组牵头出版了《工业 4.0 安全指南》、《跨企业安全通信》、《安全身份标识》等一系列指导性文件，指导企业加强安全防护。德国虽然从多个角度对安全提出了要求，但是并未形成成熟的安全体系框架。但安全作为新的商业模式的推动者，在工业 4.0 参考架构（RAMI 4.0）中起到了承载和连接所有结构元素的骨架作用。

在工业 4.0 参考架构（RAMI4.0）中，定义了一个涵盖 CPS 功能

视角、全生命周期价值链视角和全层级工业系统视角三个视角构建了如图 8 所示的工业 4.0 参考架构（RAMI4.0）。从 CPS 功能视角看，安全应用于所有不同层次，因此安全风险必须做整体考虑；从全生命周期价值链视角看，对象的所有者必须考虑全生命周期的安全性；从全层级工业系统视角看，需要对所有资产进行安全风险分析，并对资产所有者提供实时保护措施。

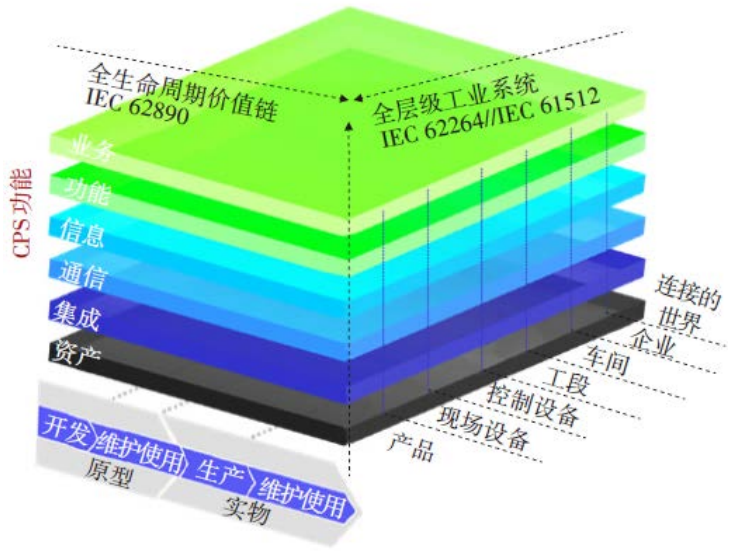

图 8 德国工业 4.0 参考架构

安全性是工业 4.0 组件设计的基石，它可以确保生产设施和产品本身不对人和环境产生威胁，并且保证数据和信息不被滥用。随着工业 4.0 以全新方式整合资源、技术、应用和模式，对整个系统的信息安全防护提出了新的挑战，并呈现出安全架构复杂化，安全防御多维化，安全等级扁平化等特点。

德国 RAMI 4.0 采用了分层的基本安全管理思路，侧重于防护对象的管理。在工业互联网安全框架的设计过程中可借鉴这一思路，并且从实施的角度将管理与技术相结合，更好地指导工业互联网企业部

署安全实施。

（三）日本工业价值链参考架构（IVRA）

日本工业价值链促进会（Industrial Value Chain Initiative，IVI）是一个由制造业企业、设备厂商、系统集成企业等发起的组织，旨在推动“智能工厂”的实现。2016 年 12 月 8 日，IVI 基于日本制造业的现有基础，推出了智能工厂的基本架构《工业价值链参考架构（Industrial Value Chain Reference Architecture ，IVRA）》。

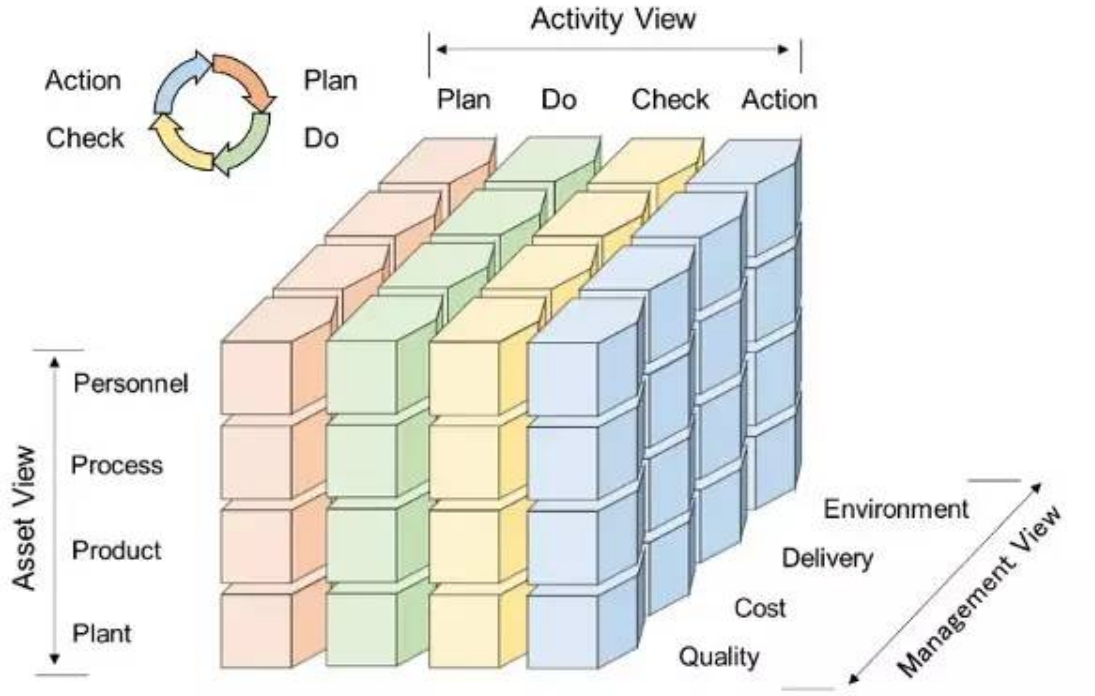

图 9 日本工业价值链参考架构 IVRA

从制造业一直追求的质量、成本和效率（产出）传统要素加上环保要求的管理角度出发，结合生产环境的资产（人、流程、产品和工厂）角度和作业流程（计划、执行、查验和反应）角度，细分出智能制造单元，对信息化在生产过程的优化，作了细致的分析，进而提出

了智能制造的总体功能模块架构，在不同的（设备、车间、部门和企业）层次上，分析知识/工程流程（相当于产品链）和供给流程（相当于价值链）的各个环节的具体功能构成，颇具有独到之处。

IVRA 也是一个 3 维模式。3 维模式的每一个块被称为“智能制造单元（SMU）”，将制造现场作为 1 个单元，通过 3 个轴进行判断。纵向作为“资源轴”，分为员工层、流程层、产品层和设备层。横向作为“执行轴”，分为 Plan、Do、Check 和 Action（PDCA 循环）。内向作为“管理轴”，质量（Q）、成本（C）、交货期（D）、环境（E）（QCDE 活动）。

IVRA 还将智能制造单元（SMU）之间的联系定义为“轻便载入单元（PLU）”，具体而言，分为价值、物料、信息和数据等 4 个部分。用便携装载单元（Portable Loading Unit，PLU），在保证安全和可追溯的条件下，实现了不同 SMU 之间资产的转移，模拟了制造活动中物料、数据等有价资产的转化过程，从而真实地反映了企业内和企业间的价值转换情况，充分体现了价值链的思想。

与 RAMI 4.0 相比，IVRA 的一大特征是通过 SMU 等形式，纳入了包括具体的员工共操作等在内的“现场感”特征。日本制造业以丰田生产方式为代表，一般都是通过人力最大化，来提升现场生产能力，实现效益增长。IVI 向全世界发布的智能工厂新参考架构嵌入了“日本制造业”的特有价值导向，期望成为世界智能工厂的另一个标准。

（四） 相关框架共性分析

通过对以上相关安全框架的分析，可以总结出以下三方面的共性特征：

一是分类别部署安全防护措施。上述三个安全框架都体现出分类别部署安全防护措施的思想。美国 IISA、德国工业 4.0 架构和日本 IVRA 是根据资产类型的不同分别阐述其安全防护措施。工业互联网安全框架在设计时应根据防护对象的不同部署针对性的安全防护措施，以便能更好地发挥安全防护措施的防护效果。

二是构建动态安全模型成为主流。美国 IISA 及德国工业 4.0 架构中均强调对安全风险进行持续的监测与响应，充分说明相对安全观已成为目前安全界的共识。日本 IVRA 则强调通过动态循环实现生产现场、组织架构、工作流程等方面的改进，通过一系列的循环往复、迭代升级最终实现工业互联网和智能制造。

三是技术手段与管理手段相结合。美国 IISF、德国工业 4.0 架构及日本 IVRA 在设计过程中均强调了技术手段与管理手段相结合的重要性。日本 IVRA 还高度重视人员管理和知识管理在工业互联网中的作用。IVRA 将其基本智能制造单元 SMU 定义为必须是有人管理、能根据需要调整内部结构、具有自主决策能力的机构。同时，SMU 的资产包括人员、工程、产品和工艺（知识）；而且，在生产现场的工作人员以及生产工艺、方法、专有技术等知识，都是十分宝贵的资产。

2.4.2 我国的工业互联网安全防护框架

我国的工业互联网安全框架是由中国信息通信研究院下设的工业互联网产业联盟提出的，也是从防护对象、防护措施和防护管理三个视角构建，如下图 10 所示。针对不同的防护对象部署相应的安全防护措施，根据实时监测结果发现网络中存在的或即将发生的安全问题并及时做出响应。同时加强防护管理，明确基于安全目标的可持续改进的管理方针，从而保障工业互联网的安全。

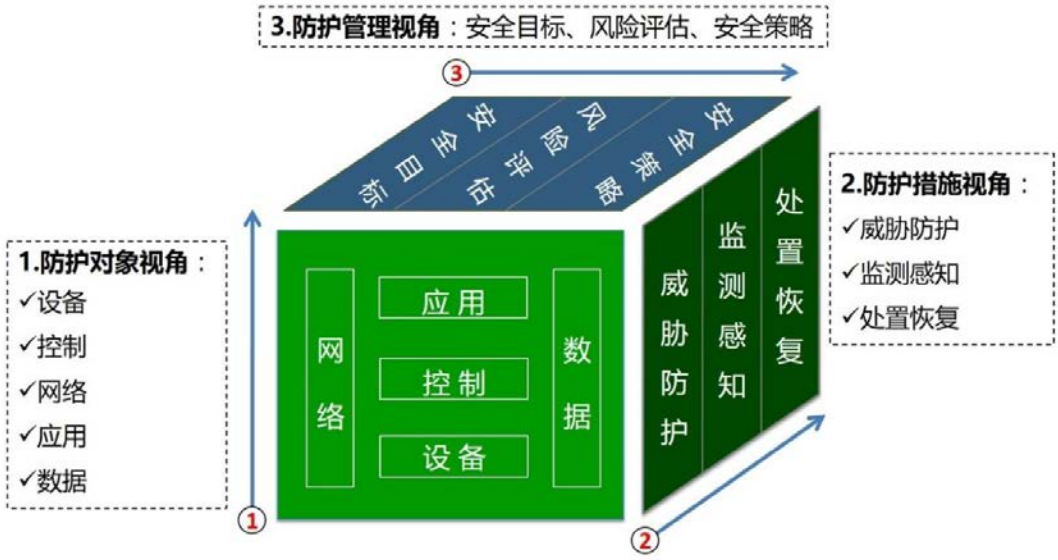

图 10 工业互联网安全框架

其中，防护对象视角涵盖设备、控制、网络、应用和数据五大安全重点；防护措施视角包括威胁防护、监测感知和处置恢复三大环节，威胁防护环节针对五大防护对象部署主被动安全防护措施，监测感知和处置恢复环节通过信息共享、监测预警、应急响应等一系列安全措施、机制的部署增强动态安全防护能力；防护管理视角根据工业互联网安全目标对其面临的安全风险进行安全评估，并选择适当的安全策略作 为指导、实现防护措施的有效部署。

工业互联网安全框架的三个防护视角之间相对独立，但彼此之间又相互关联。从防护对象视角来看，安全框架中的每个防护对象，都需要采用一系列合理的防护措施并依据完备的防护管理流程对其进行安全防护；从防护措施视角来看，每一类防护措施都有其适用的防护对象，并在具体防护管理流程指导下发挥作用；从防护管理视角来看，防护管理流程的实现离不开对防护对象的界定，并需要各类防护措施的有机结合使其能够顺利运转。工业互联网安全框架的三个防护视角相辅相成、互为补充，形成一个完整、动态、持续的防护体系。

（一）防护对象视角

防护对象视角主要包括设备、控制、网络、应用、数据五大防护对象，如图 11 所示。具体内容包括：

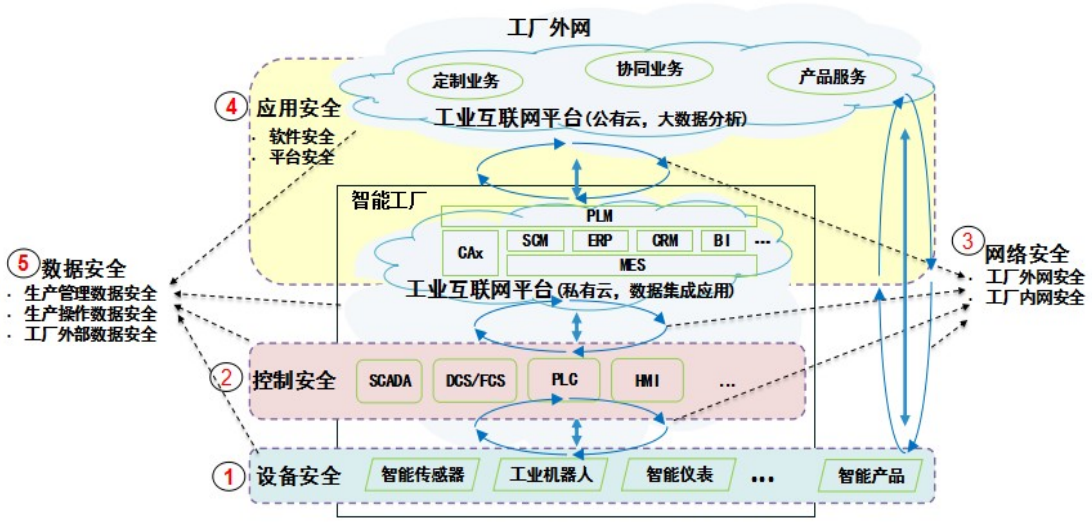

图 10 防护对象视角

✧ 设备安全

设备安全包括工厂内单点智能器件、成套智能终端、边缘网关、智能机器人等智能设备和智能产品的安全，具体涉及操作系统/应用

软件安全与硬件安全两方面。

操作系统/应用软件安全：首先，工业互联网设备供应商需要采取措施对设备固件进行安全增强，阻止恶意代码传播与运行；工业互联网设备供应商可从操作系统内核、协议栈等方面进行安全增强，并力争实现对于设备固件的自主可控；其次，设备操作系统与应用软件中出现的漏洞对于设备来说是最直接也是最致命的威胁。设备供应商应对工业现场中常 见的设备与装置进行漏洞扫描与挖掘，发现操作系统与应用 软件中存在的安全漏洞，并及时对其进行修复；最后是补丁的升级管理。工业互联网企业应密切关注重大工业互联网现场设备的安全漏洞及补丁发布，及时采取补丁升级措施，并在补丁安装前对补丁进行严格的安全评估和测试验证。

硬件安全：对于接入工业互联网的现场设备，应支持基于硬件特征的唯一标识符，为包括工业互联网平台在内的上层应用提供基于硬件标识的身份鉴别与访问控制能力，确保只有合法的设备能够接入工业互联网并根据既定的访问控制规则向其他设备或上层应用发送或读取数据。此外，应支持将硬件级部件（安全芯片或安全固件）作为系统信任根，为现场设备的安全启动以及数据传输机密性和完整性保护提供支持。除此之外，工业互联网企业应在工业现场网络重要控制系统（如机组主控 DCS 系统）的工程师站、操作员站和历史站部署运维管控系统，实现对外部存储器（如 U 盘）、键盘和鼠标等使用 USB 接口的硬件设备的识别，对外部存储器的使用进行严格控制。同时，注意部署的运维管控系统不能影响生产控制区各系统的正常运行。

✧ 控制安全

控制安全包括控制协议安全、控制软件安全以及控制功能安全。

控制协议安全：包括身份认证、访问控制、传输加密、健壮性测试等。为了确保控制系统执行的控制命令来自合法用户，必须对使用系统的用户进行身份认证，未经认证的用户所发出的控制命令不被执行。不同的操作类型需要不同权限的认证用户来操作，如果没有基于角色的访问机制，没有对用户权限进行划分，会导致任意用户可以执行任意功能。在控制协议设计时，应根据具体情况，采用适当的加密措施，保证通信双方的信息不被第三方非法获取。控制协议在应用到工业现场之前应通过健壮性测试工具的测试。

控制软件安全：包括软件防篡改、认证授权、恶意软件防护、补丁升级更新、漏洞修复加固、协议过滤和安全监测审计。软件防篡 改是保障控制软件安全的重要环节；控制软件的应用要根据使用对象的不同设置不同的权限，以最小的权限完成各自的任务；对于控制软件应采取恶意代码检测、预防和恢复的控制措施；控制软件的变更和升级需要在测试系统中经过仔细的测试，并制定详细的回退计划；控制软件的供应商应及时对控制软件中出现的漏洞进行修复或提供其他替代解决方案；最后，通过对工业互联网中的控制软件进行安全监测审计可及时发现网络安全事件，避免发生安全事故，并可以为安全 事故的调查提供详实的数据支持。

控制功能安全：要考虑功能安全和信息安全的协调能力，使得信息安全不影响功能安全，功能安全在信息安全的防护下更好地执行

安全功能。现阶段功能安全具体措施主要包括：确定可能的危险源、危险状况和伤害事件；结合典型生产工艺、加工制造过程、质量管控等方面的特征，分析安全影响；考虑自动化、一体化、信息化可能导致的安全失控 状态，确定需要采用的监测、预警或报警机制、故障诊断与 恢复机制、数据收集与记录机制等；明确操作人员在对智能化系统执行操作过程中可能产生的合理可预见的误用以及智能化系统对于人员恶意攻击操作的防护能力；智能化装备和智能化系统对于外界实物、电、磁场、辐射、火灾、地震等情况的抵抗或切断能力，以及在发生异常扰动或中断时的检测和处理能力。

✧ 网络安全

工业互联网网络安全防护应面向工厂内部网络、外部网络及标识解析系统等方面，具体包括网络结构优化、边界安全防护、接入认证、通信内容防护、通信设备防护、安全监测审计等多种防护措施，构筑全面高效的网络安全防护体系。

网络优化设计：在网络规划阶段，需设计合理的网络结构。网络边界安全：根据工业互联网中网络设备和业务系统的重要程度将整个网络划分成不同的安全域，形成纵深防御体系。网络接入认证：网络应对接入的设备与标识解析节点进行身份认证，保证合法接入和合法连接；接入网络的设备与标识解析节点应该具有唯一性标识。通信和传输保护：指采用相关技术手段来保证通信过程中的机密性、完整性和有效性，防止数据在网络传输过程中被窃取或篡改，并保证合法用户对信息和资源的有效使用。网络设备安全防护：网络设备与标识解

析节点需要采取一系列安全防护措施，主要包括：①对登录网络设备与标识解析节点进行运维的用户进行身份鉴别，并确保身份鉴别信息不易被破解与冒用；②对远程登录网络设备与标识解析节点的源地址进行限制；③对网络设备与标识解析节点的登录过程采取完备的登录失败处理措施；④启用安全的登录方式（如 SSH 或 HTTPS 等）。网络安全监测指通过漏洞扫描工具等方式探测网络设备与标识解析节点的漏洞情况，并及时提供预警信息。

✧ 应用安全

应用安全包括工业互联网平台安全与工业应用程序安全两大类，其范围覆盖智能化生产、网络化协同、个性化定制、服务化延伸等方面。目前工业互联网平台面临的安全风险主要包括数据泄露、篡改、丢失、权限控制异常、系统漏洞利用、账户劫持、设备接入安全等。对工业应用程序而言，最大的风险来自安全漏洞，包括开发过程中编码不符合 安全规范而导致的软件本身的漏洞以及由于使用不安全的第三方库而出现的漏洞等。

相应地，工业互联网应用安全也应从工业互联网平台安全与工业应用程序安全两方面进行防护。对于工业互联网平台，可采取的安全措施包括安全审计、认证授权、DDoS 攻击防护等。对于工业应用程序，建议采用全生命周期的安全防护，在应用程序的开发过程中进行代码审计并对开发人员进行培训，以减少漏洞的引入；对运行中的应用程序定期进行漏洞排查，对应用程序的内部流程进行审核和测试，并对公开漏洞和后门并加以修补；对应用程序的行为进行实时监测，

以发现可疑行为并进行阻止，从而降低未公开漏洞带来的危害。

✧ 数据安全

数据安全包括涉及采集、传输、存储、处理等各个环节的数据以及用户信息的安全。对于工业互联网的数据安全防护，应采取明示用途、数据加密、访问控制、业务隔离、接入认证、数据脱敏等多种防护措施，覆盖包括数据收集、传输、存储、处理等在内的全生命周期的各个环节。

数据收集：工业互联网平台应遵循合法、正当、必要的原则收集与使用数据及用户信息，公开数据收集和使用的规则，向用户明示收集使用数据的目的、方式和范围，经过用户的明确授权同意并签署相关协议后才能收集相关数据。

数据传输：为防止数据在传输过程中被窃听而泄露，工业互联网服务提供商应根据不同的数据类型以及业务部署情况，采用有效手段确保数据传输安全。例如通过 SSL 保证网络传输数据信息的机密性、完整性与可用性，实现对工业现场设备与工业互联网平台之间、工业互联网平台中虚拟机之间、虚拟机与存储资源之间以及主机与网络设备之间的数据安全传输。

数据存储：一是访问控制，数据访问控制需要保证不同安全域之间的数据不可直接访问，避免存储节点的非授权接入，同时避免对虚拟化环境数据的非授权访问。二是存储加密，工业互联网平台运营商可根据数据敏感度采用分等级的加密存储措施（如不加密、部分加密、完全加密等）。三是备份和恢复，工业互联网服务提供商应当根据用

户业务需求、与用户签订的服务协议制定必要的数据备份策略，定期对数据进行备份。当发生数据丢失事故时能及时恢复一定时间前备份的数据，从而降低用户的损失。

数据处理：数据处理过程中，工业互联网服务提供商要严格按照法律法规以及在与用户约定的范围内处理相关数据，不得擅自扩大数据使用范围，使用中要采取必要的措施防止用户数据泄露。另外，在资源重新分配给新的租户之前，必须对存储空间中的数据进行彻底擦除，防止被非法恶意恢复。当工业互联网平台中存储的工业互联网数据与用户个人信息需要从平台中输出或与第三方应用进行共享时，应当 在输出或共享前对这些数据进行脱敏处理。

（二）防护措施视角

为帮助相关企业应对工业互联网所面临的各种挑战，防护措施视角从生命周期、防御递进角度明确安全措施，实现动态、高效的防御和响应。防护措施视角主要包括威胁防护、监测感知和处置恢复三大环节，如图 11 所示。

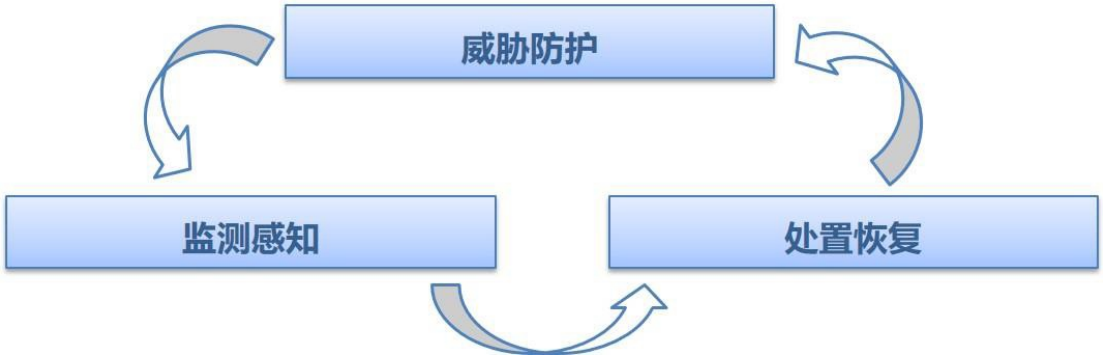

图 11 防护措施视角

1、威胁防护：针对五大防护对象，部署主被动防护措施，阻止外部入侵，构建安全运行环境，消减潜在安全风险。

2、监测感知：部署相应的监测措施，主动发现来自系统内外部的安全风险，具体措施包括数据采集、收集汇聚、特征提取、关联分析、状态感知等。

3、处置恢复：建立响应恢复机制，及时应对安全威胁，并及时优化防护措施，形成闭环防御。处置恢复机制是确保落实工业互联网信息安全管理，支撑工业互联网系统与服务持续运行的保障。通过处置恢复机制，在风险发生时灾备恢复组织能根据预案及时采取措施进行应对，及时恢复现场设备、工业控制系统、网络、工业互联网平台、工业应用程序等的正常运行，防止重要数据丢失，并通过数据收集与分析机制，及时更新优化防护措施，形成持续改进的防御闭环。处置恢复机制主要包括响应决策、备份恢复、分析评估等。

（三）防护管理视角

防护管理视角的设立，旨在指导企业构建持续改进的安全防护管

理方针，在明确防护对象及其所需要达到的安全目标后，对于其可能面临的安全风险进行评估，找出当前与安全目标之间存在的差距，制定相应的安全防护策略，提升安全防护能力，并在此过程中不断对管理流程进行改进。防护措施视角的内容如图 12 所示。

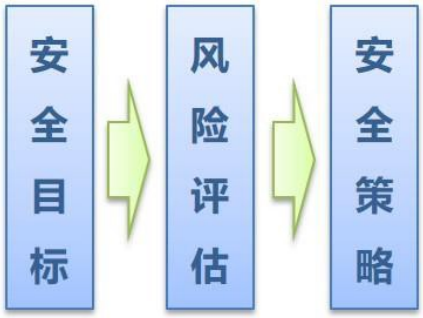

图 12 防护管理视角

✧ 安全目标

为确保工业互联网的正常运转和安全可信，应对工业互联网设定合理的安全目标，并根据相应的安全目标进行风险评估和安全策略的选择实施。工业互联网安全目标并非是单一的，需要结合工业互联网不同的安全需求进行明确。工业互联网安全包括保密性、完整性、可用性、可靠性、弹性和隐私安全六大目标，这些目标相互补充，共同构成了保障工业互联网安全的关键特性。

保密性：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。

可用性：确保授权用户或实体对信息及资源的正常使用不会被异

常拒绝，允许其可靠而及时地访问信息及资源。

可靠性：确保工业互联网系统在其寿命区间内以及在正常运行条件下能够正确执行指定功能。

弹性：确保工业互联网系统在受到攻击或破坏后恢复正常功能。

隐私安全：确保工业互联网系统内用户的隐私安全。

✧ 风险评估

风险评估为管控风险，必须定期对工业互联网系统的各安全要素进行风险评估。对应工业互联网整体安全目标，分析整个工业互联网系统的资产、脆弱性和威胁，评估安全隐患导致安全事件的可能性及影响，结合资产价值，明确风险的处置措施，包括预防、转移、接受、补偿、分散等，确保在工业互联网数据私密性、数据传输安全性、设备接入安全性、平台访问控制安全性、平台攻击防范安全性等方面提供可信服务，并最终形成风险评估报告。

✧ 安全策略

工业互联网安全防护的总体策略，是要构建一个能覆盖安全业务全生命周期的，以安全事件为核心，实现对安全事件的“预警、检测、响应”动态防御体系。能够在攻击发生前进行有效的预警和防护，在攻击中进行有效的攻击检测，在攻击后能快速定位故障，进行有效响应，避免实质损失的发生。

安全策略中描述了工业互联网总体的安全考虑，并定义了保证工业互联网日常正常运行的指导方针及安全模型。通过结合安全目标以

及风险评估结果，明确当前工业互联网各方面的安全策略，包括对设备、控制、网络、应用、数据等防护对象应采取的防护措施，以及监测响应及处置恢复措施等。同时，为打造持续安全的工业互联网，面对不断出现的新的威胁，需不断完善安全策略。

第三章 工业互联网安全标准现状及需求

3.1 国内外工业互联网安全标准化组织

3.1.1 国外安全领域相关标准化组织

（一）ISO/IEC JTC1

国际标准化组织（ISO）和国际电工委员会（IEC）联合成立的信息技术委员会 JTC1 是非常活跃的信息技术领域国际标准化组织。JTC1 技术委员会下设的 SC 27 组专门负责安全技术标准研究，已经发布了 181 项国际标准，在研标准项目 74 项。JTC1 SC27 组共设置了 5 个工作组，分别从事信息安全管理体系（WG1）、密码学与安全机制（WG2）、安全评价测试与规范（WG3）、安全控制与服务（WG4）、身份管理与隐私保护（WG5）等信息安全技术的一般方法和标准化研究工作。

WG1 主要负责信息安全管理体系（ISMS）国际标准的制定和修订工作，其核心是 ISO/IEC 27000 系列标准。ISO/IEC 27000 系列标准族由以下系列标准构成：

表 1 ISO/IEC 27000 系列标准

序号	组织名称	标准研究内容
1	ISO/IEC 27000	概述及词汇
2	ISO/IEC 27001	要求
3	ISO/IEC 27002	信息安全管理实施准则
4	ISO/IEC 27003	信息安全管理体系实施指南

5	ISO/IEC 27004	信息安全管理度量办法
6	ISO/IEC 27005	信息安全风险管理
7	ISO/IEC 27006	对提供信息安全管理体系审核及认证机构的要求
8	ISO/IEC 27007	信息安全管理体系审核指南
9	TR 27008	审核员对 ISMS 控制的指南
10	ISO/IEC 27010	信息安全管理行业间交流指南
11	ISO/IEC 27013	ISO/IEC 20000-1 与 ISO/IEC 27000 集成实施指南
12	ISO/IEC 27014	信息安全治理框架
13	TR 27016	信息安全管理—组织的经济作用

当前，WG1 正与 WG4、WG5 联合开展应对物联网安全和隐私、云计算、大数据的标准化工作，目标是制定指南以及提供解决方案。我国承担了 ISO/IEC 27007（信息安全管理体系审核指南）的项目联合编辑工作。我国的信息安全标准化部门、管理体系认证认可管理部门、ISMS 认证机构、实施 27001 的组织等应密切关注 ISO/IEC 27000 系列标准族发展动向，提前做好准备，积极应对国际标准相应变化。

WG4 负责信息安全控制与服务方面的标准研制和维护。WG4 负责制定的标准中直接与大数据相关的标准有正在编制中的 ISO/IEC 20547-4《信息技术 大数据参考架构 第 4 部分：安全与隐私保护》；涉及大数据运行平台计算安全的标准有正在编制中的 ISO/IEC 19086-4《云计算 服务水平协议（SLA）框架 第 4 部分：安全与隐私保护》；涉及数据存储安全的标准有 ISO/IEC 27040-2015《信息技术 安全技术 存储安全》；涉及信息安全事件管理及调查取证的标准有 ISO/IEC 27035《信息技术 安全技术 信息安全事件管理》（包括三个部分）、ISO/IEC 27037-2012《信息技术 安全技术 数字证据的识别、收集、获得和保全指南》、ISO/IEC 27038-2014《信息技术 安全技术 数字脱

敏规范》、ISO/IEC 270341-2015《信息技术 安全技术 确保事件调查方法适宜性和充足性的指南》、ISO/IEC 27042-2015《信息技术 安全技术 数字证据分析和解释指南》、ISO/IEC 27043-2015《信息技术 安全技术 事件调查原则和过程》和 ISO/IEC 27050《信息技术 安全技术 电子发现》（包括四个部分）。

WG5 负责身份管理和隐私保护方面的标准研制和维护。WG5 负责制定的标准中涉及个人隐私保护方面的标准有 ISO/IEC 29100-2011《信息技术 安全技术 隐私保护框架》、ISO/IEC 29101-2013《信息技术 安全技术 隐私保护体系结构框架》、ISO/IEC 29134《信息技术 安全技术 隐私影响评估指南》、ISO/IEC 29151《信息技术 安全技术 可识别个人信息（PII）保护实践指南》、ISO/IEC 29184《信息技术 安全技术 在线隐私通知和准许指南》、ISO/IEC 29190-2015《信息技术 安全技术 隐私保护能力评估模型》、ISO/IEC 29191-2012《信息技术 安全技术 部分匿名、部分不可链接鉴别要求》、ISO/IEC 27018-2014《信息技术 安全技术可识别个人信息（PII）处理者在公有云中保护 PII 的实践指南》、ISO/IEC 27550《信息技术 安全技术 隐私保护工程》和 ISO/IEC 27551《信息技术 安全技术 对 ISO/IEC 27001 在隐私保护管理方面的增强要求》。

（二）IEC

国际电工委员会（IEC）中与安全相关的标准主要集中在工业控制安全领域和电力系统信息安全领域。工业控制安全领域的标准主要

是 IEC 62443《工业过程测量、控制和自动化网络与系统信息安全》系列标准，该系列标准广泛涵盖了制造和控制系统电子安全的概念，涵盖了不同行业的不同类型的系统、设施和工厂。电力系统信息安全领域，IEC 近年来发展迅速，仅在 2016 至 2019 年间发布的电力系统信息安全相关标准就有 10 个。

工业控制安全领域：IEC 62443《工业过程测量、控制和自动化网络与系统信息安全》系列标准是 IEC TC 65 WG10 为实现工业控制系统的安全保护而制定的标准，旨在提出一整套建立工业自动化系统的安全保障措施，涉及安全规程的建立和运行，以及对工业自动化控制系统的安全技术要求，明确可采用的安全技术及应用方法。

IEC 62443 系列标准是在国际上被广泛采纳和认可的工控系统标准。各国、各行业制定工控相关标准政策都会参考和吸收该标准提供的概念、方法、模型。IEC 62443 标准中的工控系统是指 IACS (industrial automation and control system)。IEC 62443 标准是一个系列，分为四个部分，12 个文档，四部分的介绍如下：

第一部分描述了信息安全的通用方面，如术语、概念、模型、缩略语、符合性度量；

第二部分主要针对用户的信息安全程序。主要包括整改信息安全系统的管理、人员和程序设计方面，是用户建立其信息安全程序是需要考虑的；

第三部分主要针对系统集成商保护系统所需的技术性信息安全要求。它主要是系统集成商在把系统组装到一起是需要处理的内容。

包括网络安全技术、设计方法、评估方法、安全要求和信息安全保障等级的定义和要求；

第四部分：讨论 IACS 的安全开发生命周期和安全组件开发的要求。例如，IEC 62443-2-4“IACS 服务提供商的安全计划要求”标准化了集成和维护活动的安全功能，允许资产所有者选择最适合其站点的功能。IEC 62443-2-4、IEC 62443-3-1 和 IEC 62443-3-3 定义了基于攻击者强度的安全级别区分，这对于系统设计很有价值。

IEC62443 标准通过四个部分，对资产所有者、系统集成商、组件供应商进行了相关信息安全的要求。

电力系统信息安全领域：IEC 62351《电力系统管理及关联的信息交换—数据和通信安全性》是 IEC TC 57 WG15 为保障电力系统安全运行，针对有关电力通信协议而制定的数据和通信安全标准，是当前 IEC 60870-5、IEC 61850 等常用电力系统通信协议和规约的安全增强标准。

2020 年 3 月 27 日，IEC 发布了 IEC 63056:2020《电力储能系统—使用二次锂电池和蓄电池的安全要求》，标准中规定了最高直流电压为 1500 V 的电力储能用二次锂电池和电池组的安全要求和测试，涵盖了各种电储能系统的电池，其产品应用示例包括：电信系统、中央应急照明和报警系统、固定启动系统、光伏系统和家用（住宅）储能系统（HESS）等。

2018 年 11 月，IEC 发布了 IEC 62351-4《电力系统管理及信息交换：数据和通信安全性第 4 部分：MMS 及其衍生物的概要》，为基于

制造消息规范的应用程序握手期间的身份验证明确了传输层和应用层的安全要求。

2016 年 8 月，IEC 发布 IEC 62351-13《电力系统数据和通信安全-规范中涉及的安全主题指南》

IEC62368-1 标准：IEC62368-1 是一个全新的关于产品安全的国际标准，其内容要求涵盖信息技术设备、音视频设备、通信设备，在未来几年将取代现行的 IEC 60950-1 和 IEC 60065 标准。相比现行的标准，IEC62368-1 引入了全新的安全防护理念-“防止潜在危险源的安全工程学”，使得标准能够跳出产品形态结构和过往经验的限制，从产品无论如何变化都离不开能量源这一关键所在着手，对产品使用的危险能量源进行应对和防护，从而实现对产品安全性的有效管控和提升。

（三）ITU-T

国际电信联盟（ITU）是世界各国政府的电信主管部门之间协调电信事务方面的一个国际组织，由电信标准部门（ITU-T）、无线电通信部门（ITU-R）和电信发展部门（ITU-D）3 个机构组成。ITU-T SG17（安全研究组）工作组目前正致力于研究网络安全、安全管理、安全架构和框架，打击垃圾邮件、身份管理、保护个人身份信息，以及物联网、智能电网、智能手机、软件自定义网络（SDN）、Web 服务、大数据分析、社交网络、云计算、移动金融系统、IPTV 和远程生物识别的应用和服务等的安全性。规定安全通信服务研究领域包括：家

庭网络安全、移动安全、基于应用层安全协议以及网页服务安全。如基于证书的家庭网络安全研究，移动通信认证架构研究，移动通信增值服务安全研究以及反垃圾信息研究等。网络安全仍然是第 17 研究组议程的重点。此外，第 17 研究组正在协调安全标准化工作，包括打击假冒和移动设备盗窃，IMT-2020，基于云的事件数据技术，电子卫生，开放身份信任框架，射频识别（RFID）和儿童在线保护。

在物联网安全方面，主要的物联网安全标准包括 X.1171 标签识别应用的威胁和需求分析，针对泛在传感网络安全的 X.usnsec 系列标准等。如 ITU-T X.805 建议书使电信网络运营商和企业能够从安全角度提供端到端架构的描述，允许运营商精确定位网络中的所有易受攻击点并对其进行缓解；ITU-T X.1254 建议书为实体认证保证框架，该框架定义了四个级别的实体认证保证以及四个级别中每个级别的标准和威胁。该建议书可以跨各方安全地交换数据，并减少欺诈，身份盗用和黑客破坏组织的能力。值得一提的是，2017 年，ITU-T 启动了区块链安全问题研究。

为了更好地推进物联网标准化工作，加快标准化进程，国际电信联盟-电信部门（ITU-T）管理层在 2015 年 6 月的会议上决定将原来分散在 ITU-T 不同研究组的物联网、智慧城市的标准化工作合并，成立新的物联网标准化研究组 SG20，推进物联网与智慧城市相关标准化工作。

2017 年 3 月，SG20 研究组正式更名为“物联网和智慧城市研究组”，设置两个工作组（Working Party，简称 WP）和 7 个课题（Question,

简称 Q），WP1 下设 4 个课题（Q1 网络和基础设施、Q2 需求和能力、Q3 体系和协议、Q4 业务和应用）。WP2 下设 3 个课题（Q5 术语和新技术、Q6 安全和标识、Q7 智慧城市评估）。但是其涉及安全、认证等的部分标准化工作仍然分散在 SG17 研究组。

在大数据安全方面，ITU-T 在 2013 年 11 月发布了《大数据：今天巨大，明天平常》报告，并在其下属相关研究组开展了多项大数据和大数据安全相关的标准化工作。ITU-T SG13（聚焦于 IMT-2020、云计算和可信网络基础设施的未来网络研究组）负责制定的大数据相关标准包括：已发布的 ITU Y.3600《大数据 基于云计算的要求和能力》，以及在编制中的《大数据 元数据框架和概念模型》、《大数据 数据集成概述和功能要求》、《大数据 数据溯源要求》、《大数据交换框架和要求》、《数据存储联合的要求和能力》、《大数据即服务的功能架构》、《大数据 数据保全概述和要求》、《大数据驱动联网要求》、《基于 DPI 的大数据驱动联网框架》和《应用于网络大数据语境下的深度包检测机制》等。

ITU-T SG17（安全研究组）负责制定的大数据安全相关标准包括编制中的《移动互联网服务中的大数据分析安全要求和框架》、《大数据即服务的安全指南》，《电子商务业务数据生命周期管理安全参考架构》等。

（四）NIST

美国国家标准技术研究院（NIST）致力于美国工业信息安全标准

的建设，在工业信息安全标准方面不断加强投入。在工控安全方面，发布了一系列工控安全的指南和规范性文件，包括 NIST SP 800-82《工业控制系统信息安全指南》、NIST IR 7176《系统保护轮廓—工业控制系统》《中等健壮环境下的 SCADA 系统现场设备保护概况》等。在电力、石油、天然气、核电等领域，美国也发布了一系列典型行业的工控安全标准，例如 API 1164《管道 SCADA 安全》、NIST IR 7628《智能电网信息安全指南》。下面对具有广泛指导意义的两大指南：NIST SP 800-82《工业控制系统信息安全指南》和 NIST IR 7628《智能电网信息安全指南》做介绍。

NIST SP 800-82《工业控制系统（ICS）安全指南》于 2010 年 10 月发布，是 NIST 依据 2002 年《联邦信息安全管理法》、2003 年国土安全总统令 HSPD-7 等编制而成。该指南概述了 ICS 和典型的系统拓扑结构，指出了对于这些系统的典型威胁和脆弱点所在，为消减相关风险提供了建议性的安全对策。同时，根据 ICS 的潜在风险和影响水平的不同，指出了保障的不同方法和技术手段。该指南适用于电力、水利、石化、交通、化工、制药等行业的 ICS 系统。

NIST SP 800-82 给出了 ICS 安全保护的建议和指导，但是在实际应用中，应以其为指导，对系统执行基于风险的评估，在满足原有控制措施目标的前提下对建议进行裁剪和补充，给出满足特定安全需求、业务需求和运行需求的安全解决方案并实施。

NIST IR 7628 是 NIST 发布的《智能电网信息安全指南》，指南分析了智能电网的逻辑结构和信息安全需求，并提出了智能电网信息安

全防护的策略和架构，目的在于协助电网领域相关者去识别风险、落实网络安全要求，电网相关者可以包括设备制造商、电网运营商、集成服务商、监管部门、学术机构、标准组织机构等。

作为国家层面智能电网信息安全防护战略规划与指南，NIST IR 7628 提供了用于指导智能电网风险管理的相关内容，在网络安全风险管理框架和策略的基础上，进行了智能电网私有性影响评估和逻辑界面分析，提出了先进测量基础设施的安全需求。NIST IR 7628 提出了一个普适性的框架，电力企业可以根据此框架制定基于自身特征、风险与脆弱性的信息安全战略规划，相关的电力设备厂商和管理部门也可将 NIST IR 7628 中的安全措施作为工作指南的基本素材。

3.1.2 国内安全领域相关标准化组织

（一）TC 260

全国信息安全标准化技术委员会（TC 260）是国家标准化管理委员会的直属标准委员会，成立于 2002 年，秘书处单位是中国电子技术标准化研究院。TC 260 是在信息安全领域内，专业从事信息安全标准化工作的技术工作组织。负责全国信息安全技术、安全机制、安全服务、安全管理、安全评估等领域标准化工作，并负责统一协调申报信息安全国家标准年度计划项目，组织国家标准的送审、报批工作。截止目前，TC 260 共组织 420 项信息安全国家标准制修订项目，其中正式发布国家标准 313 项。

加强标准体系建设，TC 260 专门成立了 WG1-信息安全标准体系

与协调工作组，负责研究信息安全标准体系，跟踪国际信息安全标准发展动态，分析国内信息安全标准的应用需求，其制定的信息安全标准体系框架如下图 13 所示。可以看出，TC 260 的标准体系框架混合了标准属性和标准研究内容两种分类方式，将信息安全标准分为基础标准、技术与机制、管理标准、测评标准、密码技术、保密技术。TC 260 内部的工作组基本参照标准体系框架的分类方法进行划分，近两年根据技术发展趋势，专门成立了 SWG-BDS 大数据安全标准特别工作组，负责大数据、云计算、智慧城市相关的安全标准化研制工作。

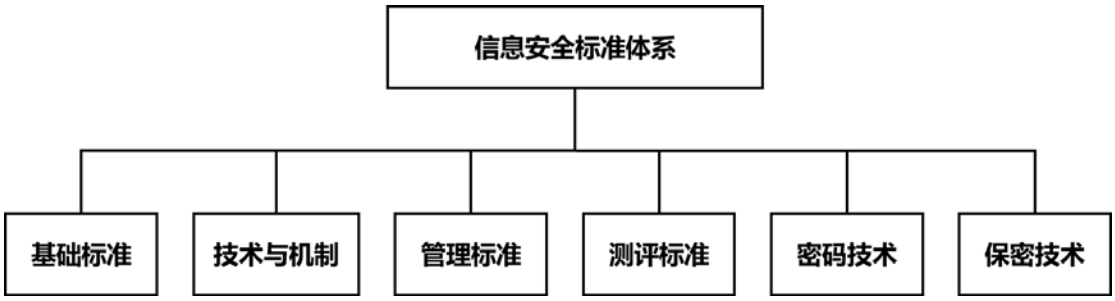

图 13　TC 260 信息安全标准体系框架

WG1-信息安全标准体系与协调工作组研究的项目包括：《信息安全技术 物联网安全体系架构》、《车载信息服务系统信息安全标准化研究》、《信息安全技术 智慧城市公共支撑与服务平台安全要求》、《信息安全标准体系研究》、《信息安全技术 智慧城市公共支撑与服务平台安全要求》。

WG3-密码技术工作组负责密码算法、密码模块，密钥管理标准的研究与制定。已发布密码技术相关国家标准 37 项，在研标准 10 项。WG4-鉴别与授权工作组负责国内外 PKI/PMI 标准的分析、研究和制定，目前已发布国家标准 62 项，今年 3 月份新发布了 5 项密码技术方面的国家标准，在研标准 15 项。WG5-信息安全评估工作组负责调

研国内外测评标准现状与发展趋势；研究提出测评标准项目和制定计划。目前已发布国家标准 111 项，今年发布 7 项，在研标准 32 项。WG6-通信安全标准工作组负责调研通信安全标准现状与发展趋势，研究提出通信安全标准体系，制定和修订通信安全标准。目前已发布国家标准 21 项，今年新发布 1 项，在研标准 9 项。WG7-信息安全管理工作组负责信息安全管理标准体系的研究和信息安全管理标准的制定工作。目前已发布国家标准 65 项，今年新发布 6 项，在研标准 27 项。SWG-BDS 大数据安全标准特别工作组负责大数据和云计算相关的安全标准化研制工作。具体职责包括调研急需标准化需求，研究提出标准研制路线图，明确年度标准研制方向，及时组织开展关键标准研制工作。目前已发布国家标准 17 项，今年新发布 2 项，在研标准 12 项。

（二）TC 124

全国工业过程测量控制和自动化标准化技术委员会（TC 124）是专业负责全国工业过程测量和控制（即工业自动化仪表）等专业领域的标准化工作。国际对口国际电工委员会 IEC/TC65“工业过程测量、控制和自动化”和国际标准化组织 ISO/TC30“封闭管道中流体流量的测量”。主要工作包括：制定工业过程测量和控制用通信网络协议标准，各类仪器仪表、执行机构、控制设备标准和安全标准。

TC 124 目前下设 10 个分委会，其中 SC 10 系统及功能安全分技术委员会与 2010 年 1 月成立，主要负责工作条件（如 EMC）、系统

评估方法、功能安全、安全仪表系统等方面的标准化工作。目前已发布的系统及功能安全方面的国家标准包括：GB/T 38129-2019《智能工厂 安全控制要求》、GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》系列标准、GB/T 35673-2017《工业通信网络 网络和系统安全 系统安全要求和安全等级》、GB/T 33007-2016《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》、GB/T 33008《工业自动化和控制系统网络安全 集散控制系统（DCS）》系列标准、GB/T 30976.1-2014《工业控制系统信息安全》系列标准、GB/T 26333-2010《工业控制网络安全风险评估规范》等。

目前正在制定的国家标准包括：20184669-T-604《数字化车间功能安全要求》、20184671-T-604《数字化车间信息安全要求》、20190632-T-604《功能安全应用指南》系列标准、20184400-T-604《过程工业安全监测系统有效性评估规范》等标准。TC 124/SC 10 近些年来在智能制造、工业网络安全等领域的工作取得了突出成绩，有力促进了产品质量提升和先进技术的广泛应用，为工业自动化行业的平稳健康发展发挥了重要的推动作用。

（三）TC 485

全国通信标准化技术委员会（TC 485）于 2009 年 5 月 15 日由国家标准化管理委员会正式批准成立，主要负责通信网络、系统和设备的性能要求、通信基本协议和相关测试方法等领域的国家标准制修订工作。TC 485 由国家标准化管理委员会主管，工业和信息化部作为

业务指导单位，中国通信标准化协会（CCSA）作为秘书处承担单位。全国通信标准化技术委员会的运作与中国通信标准化协会的运作机制相统一，协会各组成机构均作为全国通信标准化技术委员会的组成机构；在全国通信标准化技术委员会内开展国家标准制修订工作，需遵循中国通信标准化协会相关工作程序和管理办法的规定。

TC 485 目前正在制修订的通信和网络安全的国家标准包括：20132190-T-339《基于云计算的电子政务公共平台安全规范 第 3 部分：服务安全》、20132192-T-339《基于云计算的电子政务公共平台安全规范 第 4 部分：应用安全》、20190764-T-339《网络关键设备安全技术要求 交换机设备》等标准。《基于云计算的电子政务公共平台安全规范》预计分为 4 个部分：总体要求、信息资源安全、服务安全和应用安全。其中，应用安全标准则规定了基于云计算的电子政务公共平台的应用安全实施、应用安全运维、应用安全管理、应用安全测试等要求，适用于基于云计算的电子政务公共平台上所提供的应用的安全建设、实施和管理过程。电子政务公共平台服务提供机构应充分考虑云计算技术应用带来的应用安全风险，针对可能出现的数据丢失与泄露、共享技术漏洞、不安全的应用程序接口等问题，设计相应的应用安全保护措施。

（四）TC 82

全国电力系统管理及其信息交换标准化技术委员会（TC 82）于 2010 年 12 月成立，秘书处设在国网电力科学研究院。下设有变电站

工作组、通信安全工作组、配电网工作组等 7 个工作组。其中的通信安全工作组主要负责 IEC 62351 等电力系统的数据和通信安全方面的标准，与 IEC TC 57 的 WG15 对口。近些年来发布的一系列的电力安全领域的国家标准包括：GB/T 38318-2019《电力监控系统网络安全评估指、GB/T 36572-2018《电力监控系统网络安全防护导则》、GB/Z 25320《电力系统管理及其信息交换 数据和通信安全》系列标准。

电力监控系统是指用于监视和控制电力生产及其供应过程的、基于计算机及网络技术的业务系统及智能设备、以及作为基础支撑的通信和数据网络等，其可靠运行是确保电力生产安全的基础。面临的网络安全威胁包括黑客入侵、旁路控制、完整性破坏、越权操作、拦截篡改、信息泄露、网络欺骗、身份伪装、拒绝服务攻击等，需要有一套行之有效的安全防护措施和指导体系以保证电力系统正常运行。GB/T 36572-2018《电力监控系统网络安全防护导则》规定了电力监控系统网络安全防护的基本原则、体系架构、防护技术、应急备用措施和安全管理要求。标准适用于发电、配电、用电、电网调度等电力生产各环节的电力监控系统安全防护，覆盖其规划设计、研究开发、施工建设额、安装调试、系统改造、运行管理、退役报废等各阶段。

GB/Z 25320 系列标准等同采用 IEC 62351 系列标准，包括以下 8 个部分：通信网络和系统安全—安全问题介绍、术语、通信网络和系统安全—包含 TCP/IP 的协议集、包含 MMS 的协议集、IEC 60870 及其衍生标准的安全、IEC 61850 的安全、网络和系统管理的数据对象模型、电力系统管理的基于角色访问控制。GB/Z 25320 系列标准通过

在相关的通信协议以及在信息基础设施管理中增加特定的安全措施，已提高和增强电力系统的数据及通信的安全。

（五）CCSA

中国通信标准化协会（CCSA）是专业负责信息通信领域国家标准、行业标准以及团体标准的制修订工作，承担国家标准化管理委员会、工业和信息化部信息通信领域标准归口管理工作的组织，“全国通信标准化技术委员会”（TC485）和“全国通信服务标准化技术委员会”（TC543）秘书处也都设在该协会。

近年来，协会加强了研究组织架构的建设，积极拓展标准研究领域。2019 年：为支撑 5G 商用部署，成立了“5G 网络端到端切片特设项目组”；为加快推进通信行业数据安全标准研制，支撑工信部行业数据安全监管，成立了 TC 8“数据安全特设项目组”。为加强我国网络空间安全技术、试验、风险评估等工作，成立了 TC 614“网络 5.0 安全标准推进委员会”，开展网络靶场相关的标准化工作。

工业互联网安全领域方面的标准化制定工作，是由 CCSA 成立的工业互联网特设组（TS8）下设的安全组（WG5）负责，目前还没有直接以工业互联网安全命名的国家标准发布，但有一系列工业互联网安全标准正在制定当中，如下表 2 所示：

表 2 CCSA 制定的工业互联网安全标准明细表

序号	标准名称	所处状态	类型
1	工业互联网安全防护总体要求	正在审查	行业标准
2	工业互联网安全接入技术要求	正在审查	行业标准

3	工业互联网平台安全防护要求	正在审查	行业标准
4	工业互联网数据安全保护要求	正在审查	行业标准
5	工业互联网安全能力成熟度评估规范	正在征求意见	行业标准
6	工业互联网平台安全防护检测要求	正在征求意见	行业标准
7	工业互联网平台安全风险评估规范	正在征求意见	行业标准
8	工业互联网安全服务能力认定准则	正在征求意见	行业标准
9	工业互联网安全监测与管理系统建设要求	正在征求意见	行业标准

（六）AII

工业互联网产业联盟（AII）立足于搭建工业互联网的合作与促进平台，聚集工业界和信息通信界的中坚力量及相关机构，服务企业，支撑政府决策，推进工业互联网发展，为实施《中国制造 2025》和推动“互联网+”发展提供必要支撑。是在自愿、平等、互利、合作的基础上，由国内外工业互联网产业相关的企、事业单位、社团组织、高等院校、科研院所等自愿结成的跨行业、开放性、非营利性的社会组织。秘书处设在中国信息通信研究院，业务接受工业和信息化部指导。

联盟下设的安全组专业负责研究工业互联网安全问题，具体工作范畴包括：调研、论证工业互联网信息安全问题，提炼相关行业安全需求；建立工业互联网信息安全标准、规范和测评体系；提出工业互联网安全解决方案，在行业进行试点等。2020 年安全组的六大工作目标和成果分别是：一是研究制定工业互联网安全相关指导性文件。出台《工业互联网企业网络安全分类分级管理指南》，开展工业互联网

企业分类分级试点。二是完善工业互联网相关企业安全信息通报处置机制。定期发布工业互联网安全态势报告。三是开展工业互联网典型平台、工业企业、工业 APP 安全检查和检测。对不少于 20 家典型平台、工业企业开展检查检测，对不少于 100 个工业 APP 开展检测分析，增强 APP 安全性。四是建设完善工业互联网三级安全监测体系。扩大国家态势感知平台监测范围，建设完善省级态势感知平台，逐步实现全国地域覆盖，监测对象扩大到 150 个重点平台、10 万家以上工业互联网企业。五是加强工业互联网安全威胁通报和处置技术支撑。支持建设企业级安全监测平台，并向工业和信息化部网络安全相关平台提供安全威胁数据。六是加快“新一代工业互联网系统安全技术”关键核心技术集成攻关大平台建设。提出新一代工业互联网系统全生命周期内生安全体系架构。研制工业互联网系统多维感知与安全联动系统、安全监视与安全增强设备、内生安全边缘控制装备与监控平台等系统装备。初步建成工业互联网系统安全先进试验场。目前各项工作正在有序进行当中。

3.2 我国工业互联网安全标准现状及需求分析

3.2.1 标准现状分析

我国正在加速开展工业互联网安全标准研制，发布有《工业互联网安全防护总体要求》、《工业互联网平台安全防护要求》等重点标准规范 2 项，同步立项《工业互联网安全接入技术要求》、《工业互联网数据安全保护要求》、《工业互联网安全能力成熟度评估规范》、《工业互联网平台安全防护检测要求》、《工业互联网平台安全风险评估规范》、《工业互联网安全服务能力认定准则》、《工业互联网安全监测与管理系统建设要求》、《工业 APP 安全防护要求》、《工业 APP 安全检测要求》、《工业互联网企业侧安全监测与协同管理系统技术要求》、《工业互联网企业侧安全监测与协同管理系统接口规范》、《工业互联网安全防护检测要求》、《工业互联网安全风险评估规范》、《工业互联网设备安全防护要求》、《工业互联网标识解析系统安全保护要求》等相关国家标准、行业标准和工业互联网产业联盟标准共 17 项。

（一）工业控制系统安全标准

2019 年 8 月，TC 260 新发布了一系列工业控制系统安全相关标准，包括 GB/T 37933-2019《信息安全技术 工业控制系统专用防火墙技术要求》、GB/T 37941-2019《信息安全技术 工业控制系统网络审计产品安全要求》、GB/T 37954-2019《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》、GB/T 37962-2019《信息安全技

术 工业控制系统产品信息安全通用评估准则》和 GB/T 37980-2019《信息安全技术 工业控制系统安全检查指南》。

《信息安全技术 工业控制系统专用防火墙技术要求》标准规定了工业控制系统专用防火墙的安全功能要求、自身安全要求、性能要求和安全保障要求。其与通用防火墙的主要差异体现在：一是通用防火墙除了需具备基本的五元组过滤外，还需要具备一定的应用层过滤防护能力；二是工业控制系统专用防火墙需要比通用防火墙具有更高的环境适应能力；三是工业控制系统专用防火墙比通用防火墙具有更高的实时性、可靠性和稳定性等要求。

《信息安全技术 工业控制系统网络审计产品安全要求》标准适用于工业控制系统网络审计产品的设计、生产和测试。与通用安全审计产品的差异性体现在：一是通用安全审计产品主要针对应用于互联网的通用协议进行分析和记录；二是用于工业控制环境的安全审计产品可能有部分组件部署在工业现场环境，因此比通用安全审计产品需要具有更高的环境适应能力；三是工业控制环境中，通常流量相对较小，流量类型相对固定，对可靠性要求更高。

《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》标准适用于工业控制系统漏洞检测产品的设计、开发和测评。工业控制系统漏洞检测产品可以用于离线环境、工业控制系统试运行期间或工业系统维修期间，能够对工业控制系统中的工业控制设备、通信设备、安全保护设备以及工业控制软件等进行自动检测，发现存在的漏洞。

《信息安全技术 工业控制系统产品信息安全通用评估准则》标准定义了工业控制系统产品信息安全评估的通用安全功能组件和安全保障组件集合，规定了工业控制系统产品的安全要求和评估准则。该标准适用于工业控制系统产品安全保障能力的评估、产品安全功能的设计、开发和测试。

《信息安全技术 工业控制系统安全检查指南》标准规定了工业控制系统信息安全检查的范围、方式、流程、方法和内容。标准适用于开展工业控制系统的信息安全监督检查、委托检查工作，同时也适用于各企业在本集团（系统）范围内开展相关系统的信息安全自查。标准的发布和实施能有效指导我国国家关键基础设施中相关工业控制系统行业用户开展工业控制系统信息安全自评工作，并为国家对重点行业工业控制系统信息安全检查等工作提供支撑，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。

（二）等保 2.0 系列标准

2019 年 5 月，网络安全等级保护制度 2.0 标准 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》、GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》、GB/T 25070-2019《信息安全技术网络安全等级保护安全设计技术要求》国家标准正式发布，2019 年 12 月 1 日实施。等保 2.0 扩展了网络安全保护的范围，提高了对关键信息基础设施进行等级保护的要求，并且针对不同保护对象的安全目标、技术特点、应用场景的差异，采用了安全通用要求与安

全扩展要求结合的方式，以更好地满足安全保护共性化与个性化要求，提升了等级保护的普适性与可操作性。同时，对工业控制系统提出了安全扩展要求，以适用工业控制的特有技术和应用场景特点。安全拓展要求主要针对物理环境安全、网络和通信安全、设备和计算安全、安全建设管理和安全运维管理提出了具体的标准。

2017 年，《中华人民共和国网络安全法》的正式实施，标志着等级保护 2.0 的正式启动。网络安全法明确“国家实行网络安全等级保护制度。”（第 21 条）、“国家对一旦遭到破坏、丧失功能或者数据泄露，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，在网络安全等级保护制度的基础上，实行重点保护。”（第 31 条）。上述要求为网络安全等级保护赋予了新的含义，重新调整和修订等级保护 1.0 标准体系，配合网络安全法的实施和落地，指导用户按照网络安全等级保护制度的新要求，履行网络安全保护义务的意义重大。

✧ 等级保护 2.0 标准体系

随着信息技术的发展，等级保护对象已经从狭义的信息系统，扩展到网络基础设施、云计算平台/系统、大数据平台/系统、物联网、工业控制系统、采用移动互联技术的系统等，基于新技术和新手段提出新的分等级的技术防护机制和完善的管理手段是等级保护 2.0 标准必须考虑的内容。关键信息基础设施在网络安全等级保护制度的基础上，实行重点保护，基于等级保护提出的分等级的防护机制和管理手段提出关键信息基础设施的加强保护措施，确保等级保护标准和关键信息基础设施保护标准的顺利衔接也是等级保护 2.0 标准体系需要考

虑的内容。等级保护 2.0 标准体系主要标准如下：

- 网络安全等级保护条例（总要求/上位文件）
- 计算机信息系统安全保护等级划分准则（GB 17859-1999）（上位标准）
- 网络安全等级保护实施指南（GB/T 25058-2020）
- 网络安全等级保护定级指南（GB/T 22240-2020）
- 网络安全等级保护基本要求（GB/T 22239-2019）
- 网络安全等级保护设计技术要求（GB/T 25070-2019）
- 网络安全等级保护测评要求（GB/T 28448-2019）
- 网络安全等级保护测评过程指南（GB/T 28449-2018）

✧ 主要标准的框架结构

《GB/T 22239-2019》、《GB/T 25070-2019》和《GB/T28448-2019》三个标准采取了统一的框架结构，如下图 14 所示。

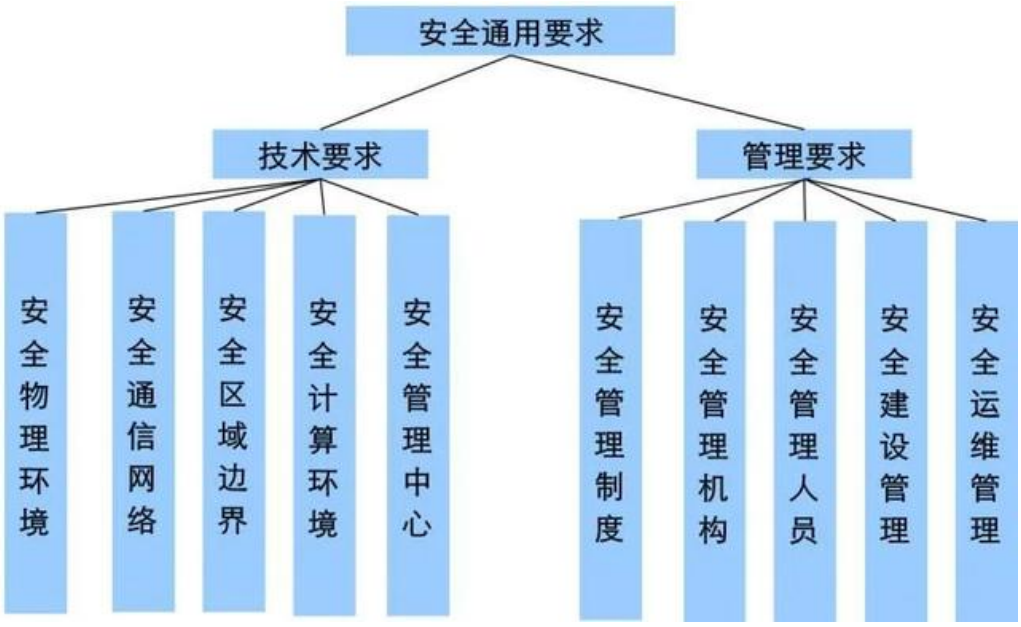

图 14　安全通用要求框架结构

安全通用要求细分为技术要求和管理要求。其中技术要求包括

“安全物理环境”、“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”；管理要求包括“安全管理制度”、“安全管理机构”、“安全管理人员”、“安全建设管理”和“安全运维管理”。

✧ 主要标准的内容

安全通用要求

安全通用要求针对共性化保护需求提出，无论等级保护对象以何种形式出现，需要根据安全保护等级实现相应级别的安全通用要求。安全扩展要求针对个性化保护需求提出，等级保护对象需要根据安全保护等级、使用的特定技术或特定的应用场景实现安全扩展要求。等级保护对象的安全保护需要同时落实安全通用要求和安全扩展要求提出的措施。

安全扩展要求

安全扩展要求是采用特定技术或特定应用场景下的等级保护对象需要增加实现的安全要求。包括以下四方面：

1、云计算安全扩展要求是针对云计算平台提出的安全通用要求之外额外需要实现的安全要求。主要内容包括“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云计算环境管理”和“云服务商选择”等。

2、移动互联安全扩展要求是针对移动终端、移动应用和无线网络提出的安全要求，与安全通用要求一起构成针对采用移动互联技术的等级保护对象的完整安全要求。主要内容包括“无线接入点的物理

位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等。

3、物联网安全扩展要求是针对感知层提出的特殊安全要求，与安全通用要求一起构成针对物联网的完整安全要求。主要内容包括“感知节点的物理防护”、“感知节点设备安全”、“网关节点设备安全”、“感知节点的管理”和“数据融合处理”等。

4、工业控制系统安全扩展要求主要是针对现场控制层和现场设备层提出的特殊安全要求，它们与安全通用要求一起构成针对工业控制系统的完整安全要求。主要内容包括“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”和“控制设备安全”等。

（三）密码应用标准

密码技术是网络安全的核心技术和基础支撑，密码技术、管理和应用标准化是大规模商用的必由之路。2017 年 11 月，密码行业标准化技术委员会（密标委）发布了 2018 版《密码标准应用指南》，用以指导国内各行业正确使用密码算法、技术和产品。国内商用密码生产商、技术服务商、密码应用单位（特别是金融机构、政府机构等）应遵循该指南和具体相关的密码标准，从产品研发、技术应用、保密管理等角度，落实好国产密码的自主可控政策。

✧ 密码标准框架

《密码标准应用指南》将密码标准体系框架划分为：密码基础类

标准、基础设施类标准、密码设备类标准、密码服务类标准、密码检测类标准、密码管理类标准、密码应用类标准，如下图 15 所示。

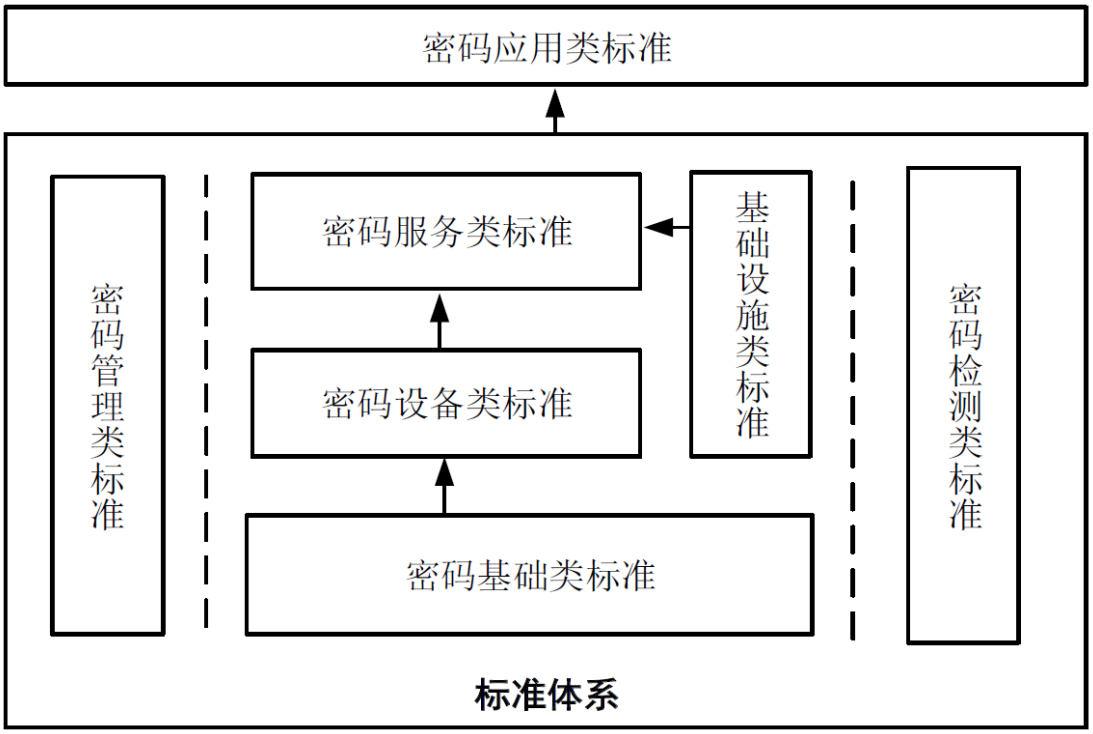

图 15　密码标准体系框架

其中，（1）密码基础类标准主要规定了通用密码技术和算法的要求；（2）基础设施类标准主要规定了认证体系等密码基础设施的要求；（3）密码设备类标准主要规定了接口、规格和安全要求；（4）密码服务类标准规定了密码报文、调用接口等方面的要求；（5）密码检测类标准针对基础类标准、设备类标准、服务类标准等对定了相应的检测要求；（6）密码管理类标准规定了设备管理、密钥管理、设备监察等方面的要求；（7）密码应用类标准规定了使用密码技术实现密码应用的要求（如动态口令、电子签章等、IC 卡应用等）。

✧　密码应用类标准

密码应用类标准包括：GB/T 38556-2020《信息安全技术 动态口

令密码应用技术规范》、GB/T 38541-2020《信息安全技术 电子文件密码应用指南》、GB/T 33560-2017《信息安全技术 密码应用标识规范》、GB/T 37033《信息安全技术 射频识别系统密码应用技术要求》系列标准。

在国家大力提倡网络安全自主可控的形势下，各行各业（特别是金融、政府、电信、电子商务、军队等）对国产密码产品和技术的应用需求越来越迫切，同时，随着网络安全等级保护 2.0 时代的到来，也对重要信息系统的密码产品和技术应用提出了更高要求。我们相信，以国家安全和自主可控为出发点，更好地贯彻《密码标准应用指南》，大力发展国产密码产品和技术应用，定会为我国的网络安全事业做出更大贡献。

（四）数据共享安全标准

随着大数据技术和应用的快速发展，促进跨部门、跨行业数据共享的需求已经非常迫切。但是，安全问题是影响数据共享发展的关键问题，世界各国对数据共享的安全越来越关注，包括美国、欧盟和中国在内的很多国家都在制定数据安全相关的法律法规来推动数据共享的合法利用和安全保护。

在推动数据开放共享方面，国家首先启动政务信息资源的开放和共享工作，通过政务信息资源的开放共享，引导企业、社会组织等主动采集并开放数据，实现政府和社会互动的大数据采集形成、合作开发和综合利用机制，取得了一定的成果。2020 年发布了 GB/T 38664

《信息技术 大数据 政务数据开放共享》系列标准，包括总则、基本要求、开放程度评价 3 个部分。其他比较重要的标准还包括 GB/T 34080《基于云计算的电子政务公共平台安全规范》系列标准和 GB/Z 24294《信息安全技术 基于互联网电子政务信息安全实施指南》系列标准。

✧ **数据共享安全保密风险分析**

政务大数据环境下数据共享除了面临传统数据的安全保密风险，由于其独特的特征，政务大数据环境下数据共享引入一些新的安全保密风险。

一是共享交换平台安全风险。共享交换平台作为数据汇聚的中心，成为极有价值的攻击目标。电子政务信息共享交换平台汇聚了海量共享交换数据，成为极有价值的攻击目标，即备受 APT 组织关注的重要目标。共享交换平台采用分布式部署，分布式环境下，涉及的软件和硬件较多，任何一点遭受故障或攻击，都可能导致整体安全出现问题。攻击者也可以从防护能力最弱的节点着手进行突破，通过破坏计算节点、篡改传输数据和渗透攻击，最终达到破坏或控制整个分布式系统的目的。

二是数据安全风险。政务大数据环境下的数据交换作为一种新应用场景，具有非涉密数据大量汇聚后可能涉密、多主体参与、数据持续流动等业务特点，由此引发了很多新的安全保密风险。数据持续流动导致责任划分不清、权限难以控制、问题难以追责等。数据整合共享过程中、有多个主体在参与——数据提供方、数据共享交换服务方

和数据使用方，而数据又在不同主体之间流动，这就导致主体的保密责任不清晰，数据失泄密难以追查。数据流动过程中容易失控。数据流动过程中，多个数据使用方权限控制的安全性不足，导致非授权用户的越权访问。

三是用户与管理终端安全风险。用户或管理终端可能成为攻击整合共享交换平台的跳板。用户或管理终端的防护不足将使得共享交换平台整体的安全防护薄弱点增多，增大被攻击的风险。目前，各政务部门的平台安全防护能力建设不一，有些部门根据等级保护要求对自身终端进行了安全防护，而有些部门并没有采用有足够安全强度的防护。达不到安全防护强度的用户或管理终端极有可能成为攻击整合共享交换平台的跳板。

因此，政务信息共享交换安全保密防护体系应遵循政务信息资源安全共享系列标准，包括技术标准、管理指南、政务信息资源分类分级指南等，同时，通过深入研究政务信息数据整合汇聚后定密规则、策略等的关键问题，制定并完善政务信息整合共享安全保密管理指南规范。

数据共享作为政务大数据的一个非常重要的业务应用，强烈建议政府和企业关注数据共享安全保密问题，以共享交换业务作为驱动，以防止敏感数据泄露为目的，深挖数据安全保密需求，加强数据共享安全保密顶层规划和设计，发展安全保密防护关键技术研究，从根本上提升数据共享安全保密防护水平。

3.2.2 标准需求分析

随着《关于深化“互联网+先进制造业”发展工业互联网的指导意见》、《加强工业互联网安全工作的指导意见》等政策文件的发布和实施，工业互联网安全体系架构进一步明确，但工业互联网安全标准化工作还在起步阶段。从《工业互联网综合标准化体系建设指南》的内容来看，《工业通信网络和系统安全术语、概述和模型》《工业互联网网络安全总体要求》《工业互联网安全 接入技术要求》等网络安全标准，《工业互联网数据安全保护要求》等数据安全标准，《工业互联网平台安全防护要求》《工业互联网 安全体系框架》《工业互联网平台 质量管理要求》等平台安全标准正在加紧制定中，但目前还难以满足工业互联网发展的安全需求。

另外一方面，工业互联网安全体系框架类的标准亟待填补。目前，尚未有正式发布的工业互联网安全体系框架类标准。随着工业互联网的快速发展，工业互联网安全体系概念的范围逐渐扩展，各类工业互联网安全标准逐步推进。同时，工业领域新技术新应用的标准也在加紧研制中，但相关标准间缺乏严格的逻辑关联，亟需开展工业互联网安全体系框架类标准制定，为工业互联网安全标准的研制提供思路和方向。

目前除 TC260、TC124、CCSA 开展工业互联网安全标准研制外，其它标准化组织也在推进相应安全标准，应通过标准化组织间的沟通机制，体系化推进标准建设。同时，工业互联网领域安全标准还需要引用或参照已有的可适用于工业互联网领域的安全标准，以及 5G、

大数据、区块链及人工智能等新技术应用领域安全标准，达到工业互联网安全生态的协同发展。

第四章 工业互联网安全标准体系建设

4.1 工业互联网安全与其他领域安全的总体关联

工业互联网是在传统的工业制造、通信与互联网领域发展起来的，物联网、大数据、云计算、人工智能、区块链等新兴技术的发展能够从智能制造、通信传输、计算、数据存储等方面快速推动工业互联网相关技术的发展。工业互联网安全也与这些技术在工业领域的安全有着密切的关系，具体关联图如下图 16 所示。需要说明的是，图 16 仅是对工业互联网安全和其他领域（如工业控制系统、物联网、大数据、云计算等方面）安全的概念和边界进行区分，仅是对各概念的交叉和包含关系进行直观展示，而非严格的集合图。

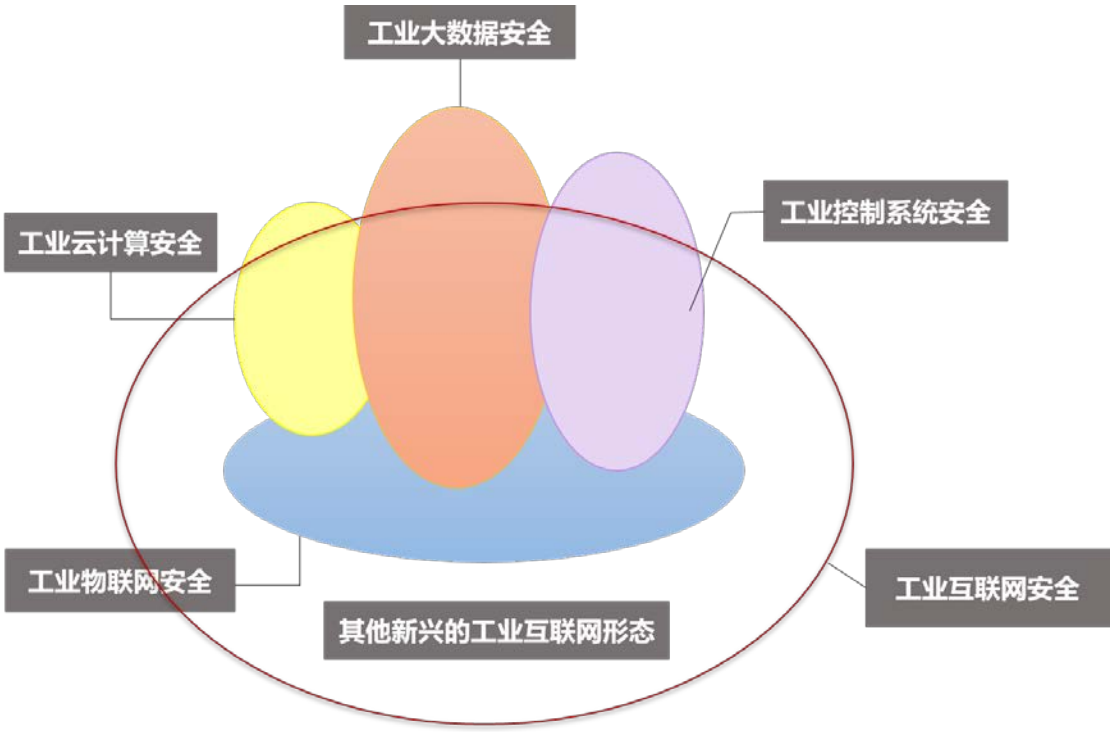

图 16　工业互联网安全与其他领域安全的关系图

具体来说，工业互联网安全覆盖工业控制系统安全、工业物联网

安全、工业大数据安全、工业云安全及其他新兴的工业互联网形态。工业控制系统是一个通用术语，它的安全包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统（如可编程逻辑控制器（PLC））的安全；工业物联网指的是物联网在工业中的应用，工业互联网安全涵盖了工业物联网安全，但进一步延伸到企业的信息系统、业务流程和人员等的安全；工业云平台指的是工业领域的云平台，包括了 IAAS（基础设施服务化）、PAAS（平台服务化）、SAAS（软件服务化）三个层面，工业互联网平台是工业云平台的扩展与延伸；不仅能够支持工业云平台的所有功能，而且要支撑工业物联网应用，实现 IT 与 OT 融合。工业云平台汇聚了海量的、异构的、结构化、半结构化和非结构化的数据，这些数据就是工业大数据，通过大数据驱动，可实现对工业中的产品、制造工艺和设备进行监控、控制和优化等功能。另外，工业互联网的安全还包括其他新兴的工业互联网形态如工业属性带来的保护场景的多样性的安全挑战等。因此，传统的网络安全保障体系已难以做到全面有效防护，亟需建立针对性强、特色鲜明的工业互联网安全保障体系和工业互联网安全标准体系。

但与此同时，其他领域已有的安全标准体系框架可以为我们制定和构建工业互联网安全标准体系框架提供参考，我们在构建工业互联网安全标准体系时需充分借鉴和吸收其他领域已有的安全标准体系。下面分别对工业控制系统安全标准体系、物联网安全标准体系、工业大数据安全标准体系、云计算安全标准体系和工业互联网标准体系进行详细阐述。

4.1.1 工业控制系统安全标准体系框架

工业控制系统安全标准是工业控制系统安全保障体系的重要组成部分，对于各行业企事业单位开展工业控制系统安全防护工作具有促进、规范和指导等多重意义。由于我国工业控制系统安全防护建设整体起步较晚，工业控制系统安全标准亦有明显的滞后。随着近年来以 TC 260 为主导的标准化组织加快了工业控制系统安全标准制定的进程,我国工业控制系统安全标准体系逐渐步入了“快车道”，大量工业控制系统安全标准相继研制，TC 260 提出的工控安全标准体系框架如下图 17 所示。

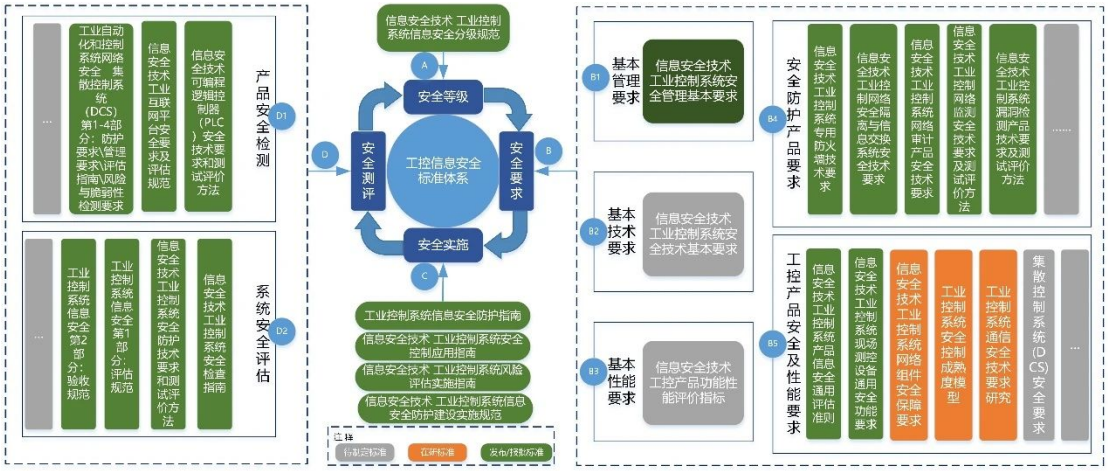

图 17 工业控制系统安全标准体系框架

工业控制系统安全标准体系包括安全等级、安全要求、安全实施和安全测评四类标准。四类标准作为开展工业控制系统信息安全工作的四个阶段，依次形成循环，切实提高工业控制系统的信息安全保障能力。同时，在每类标准的基础上，可按照标准所涉及的主要内容进行细分。

（1）安全等级类标准

TC 260 于 2018 年 6 月发布了 GB/T 36324-2018《信息安全技术 工业控制系统信息安全分级规范》（以下简称《分级规范》）标准，标准规定了基于风险评估的工业控制系统信息安全等级划分规则和定级方法，提出了等级划分模型和定级要素，包括工业控制系统资产重要程度、存在的潜在风险影响程度和需抵御的信息安全威胁程度，并明确了各个等级工业控制系统所具备的潜在风险影响、信息安全威胁、信息安全能力和信息安全管理方面的特征。

（2）安全要求类标准

针对工业控制系统信息安全实际情况，分别从基本管理要求、基本技术要求和基本运维要求三个方面对工业控制系统的信息安全提出安全要求。同时，在上述三类基本要求基础上，也针对具体产品和技术提出安全防护要求，如工业控制系统终端安全要求、漏洞检测技术要求、网络监测安全技术要求和测试评价方法、网络审计产品安全技术要求等。

2019 年 8 月，GB/T 37933-2019《信息安全技术 工业控制系统专用防火墙技术要求》正式发布，标准为工控防火墙制造商提供了详细的功能要求、开发要求和性能指标，同时为第三方产品检测单位、用户企业提供了对工控防火墙产品的功能、性能评价指标，对于国内工控防火墙产品市场能够起到良好的规范效应。

（3）安全实施类标准

安全实施类标准主要为工业控制系统信息安全实施提出安全指导。目前，安全实施类的指南和标准包括《工业控制系统信息安全防护指南》、GB/T 32919-2016《信息安全技术 工业控制系统安全控制应用指南》、GB/T 36466-2018《信息安全技术 工业控制系统风险评估实施指南》和 20173583-T-469《信息安全技术 工业控制系统信息安全防护建设实施规范》，上述几项标准的介绍已在本报告的 3.2.1 章节标准现状分析中进行阐述。

（4）安全测评类标准

制定工业控制系统相关产品测评以及安全能力评估等第三方测评与服务类标准，确保信息安全控制措施的科学性和有效性，根据风险评估和测评结果及时调整信息安全策略，助力工业企业提升信息安全防护能力。产品安全检测方面：目前在制定的标准包括《信息安全技术 可编程逻辑控制器（PLC）安全技术要去和测试评价方法》（征求意见稿）、《信息安全技术 工业互联网平台安全要求及评估规范》（征求意见稿）等；系统安全评估方面：目前已发布的标准包括 GB/T 37980-2019《信息安全技术 工业控制系统安全检查指南》、GB/T 30976.1-2014《工业控制系统信息安全第 1 部分：评估规范》、GB/T 30976.2-2014《工业控制系统信息安全第 2 部分：验收规范》等。

4.1.2 物联网安全标准体系框架

TC 260 的通信安全标准工作组于 2019 年 10 月份发布了《物联网安全标准化白皮书》，白皮书中提出了物联网安全标准体系框架，如下图 18 所示。

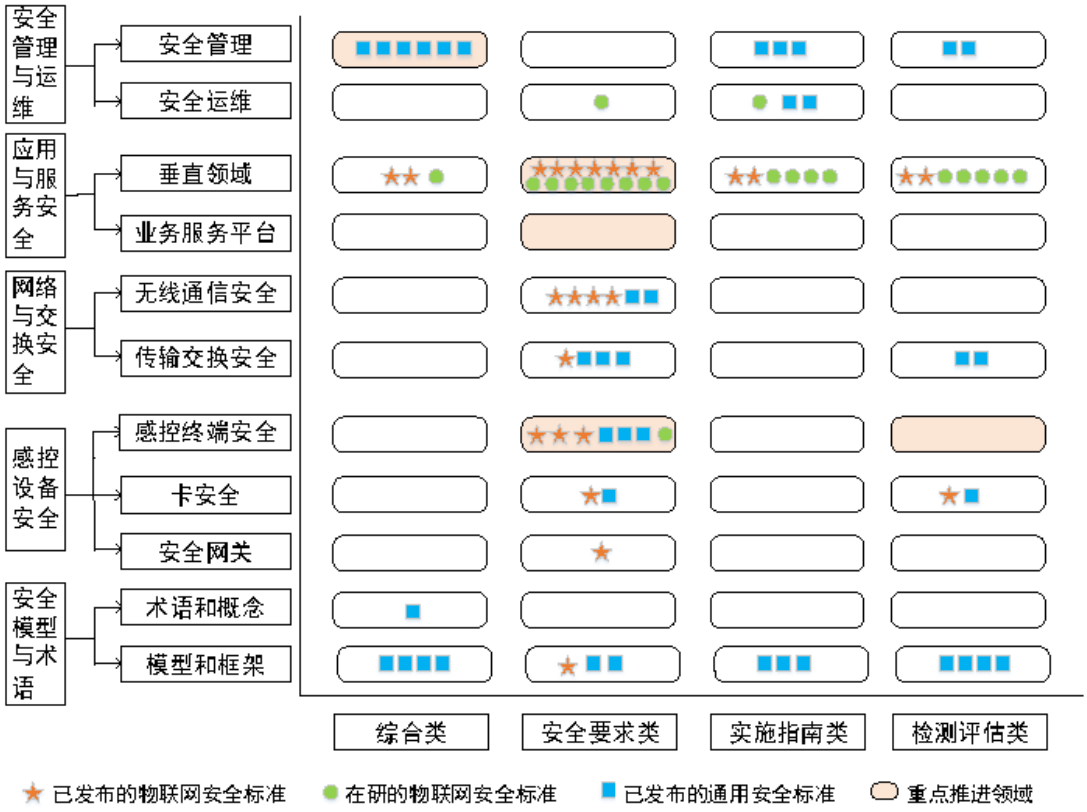

图 18 物联网安全标准体系框架

物联网安全标准体系包括安全模型与术语类标准、感控设备安全类标准、网络与交换安全标准、应用与服务类标准、安全管理与运维类标准。

（1）安全模型与术语类标准

安全模型与术语类标准包括术语和概念、模型和框架两个子类。

术语和概念：物联网安全技术术语相关标准是在物联网安全方面进行技术交流的基础语言。规范术语定义和术语之间的关系，有助于准确理解和表达技术内容，方便技术交流和研究。物联网安全技术术语相关标准需要包含已发布的国家标准、国际标准和国外先进标准中规范的大数据安全相关术语及其定义，例如 ISO/IEC JTC1/SC27、ITU 等制定的已发布国际标准的术语和定义，以及 SAC TC260 制定的已发布国家标准的术语和定义，应适用于任何从事或关注物联网安全的组织和个人。

模型和框架：物联网的概念模型是理解和进一步研究物联网的基础，客观的物联网概念模型将引导有实用价值的物联网理论研究和技术开发。物联网安全参考架构相关标准是对物联网安全内在的要求、设计结构和运行建立的一个开放的物联网安全技术模型，规范物联网安全体系架构有助于准确理解物联网安全保障体系的结构层次、功能要素及其关系，是物联网安全其他标准制定参考的基础。

（2）感控设备安全类标准

感知设备安全类标准包括感控终端安全、智能物联卡安全以及安全网关三个子类。

感控终端安全：感控终端具备感知和/或控制功能。具备感知功能的设备通常以上行数据为主，其采集的数据量和实时性要求不同，其安全标准可以分别制定。可以将感知设备安全标准划分成以下几类：①上行数据量较小且实时性要求不高场景的感知设备安全标准，如：

RFID 系统；②上行数据量较大且实时性要求较高场景的感知设备安全标准，如：车载传感系统；③上行数据量大，但是实时性要求不高场景的感知设备安全标准，如：音视频采集系统。

智能物联卡安全：智能物联网卡的主要任务是提供设备接入移动通信网络的设备身份标识，这类安全标准应侧重于卡内信息的不可篡改、完整性和可用性，而且由于卡内计算存储能力受限，其安全机制应尽量轻量化，减少安全负担。

安全网关：安全网关是感知层能力的“重机枪”，起到承上启下作用，大量数据由此转发，包括上行数据和下行数据。安全网关能力一般包括：设备安全接入能力、数据安全转发能力、安全存储能力、安全协议转换能力、敏感数据过滤能力以及自身安全，其安全标准可以按照其安全能力进行分级。

（3）网络与交换安全类标准

网络与交换安全标准包括无线通信安全、网络设备安全以及传输交换安全三个子类。

无线通信安全：物联网的快速发展对无线通信技术提出了更高的要求，物联网中的无线通信标准应覆盖到感知终端接入鉴权、空中接口协议、通讯接口、通讯协议及参数、通信数据安全、通信密钥管理、双向认证，日志审计等方面的要求。

网络设备安全：物联网网络采用多种异构网络，通信传输模型相比互联网更为复杂，算法破解、协议破解、中间人攻击等诸多方式以

及 Key、协议、核心算法、证书等暴力破解情况时有发生，因此物联网网络传输交换相关的标准应考虑到通讯协议安全、传输数据安全（数据发送和接收时对数据的处理，包括对数据的加密和解密能力，完整性校验和验证能力，对通信方的身份鉴别能力的要求）、防重放攻击、密钥管理等需求。

（4）应用与服务安全类标准

应用与服务安全类标准包括通用应用服务和垂直领域两个子类。

业务服务平台安全：本类标准主要为物联网生态系统中业务运营使用的通用业务服务平台提出规范要求，包括但不限于数据安全防护、身份认证、访问控制等，引导相关安全技术、产品、及产业的健康发展。

垂直领域安全：针对智慧城市、工业互联网、家庭物联网、车联网、智能安防、智慧医疗、公共服务等不同的应用领域，围绕领域物联网应用的特点，针对不同领域的安全风险及需求，针对性地建立相关安全标准，指导各领域物联网的安全建设和运营，支撑各领域物联网的健康、快速发展。

（5）安全管理与运维类标准

安全管控与运维标准包括安全管理、安全运维两个子类。

安全管理：包括对物联网网络、传输、业务应用、服务、设备、卡等的安全管理，涉及对安全事件的应急响应管理及安全漏洞管理等

标准。

安全运维：物联网安全运维涉及物联网平台系统安全规划设计、安全开发建设、安全生产、安全退网等各个方面，有必要通过标准定义各阶段的任务目标、安全运营要求和安全防护方法，以有效组织各相关方安全合规生产，包括判断异常行为、发现安全隐患并及时控制处理等。

4.1.3 工业大数据安全标准体系

大数据技术应用于工业领域给企业带来巨大的效益，然而工业大数据对工业企业来说既是机遇也是挑战，在给企业带来巨大经济利益的同时，其本身所存在的安全问题也让企业面临着巨大的风险。一方面，由于工业控制系统的协议多采用明文形式、工业环境多采用通用操作系统且不及时更新、从业人员的网络安全意识不高，再加上工业数据的来源多样，具有不同的格式和标准，使其存在诸多可以被利用的漏洞。另一方面，在工业应用环境中，对数据安全有着更高的要求，任何信息安全事件的发生都有可能威胁工业生产运行安全、人员生命安全甚至国家安全等。因而，研究工业大数据安全管理，加强对工业企业的安全保护变得尤为重要。工业大数据安全标准体系框架图如下图 19 所示。

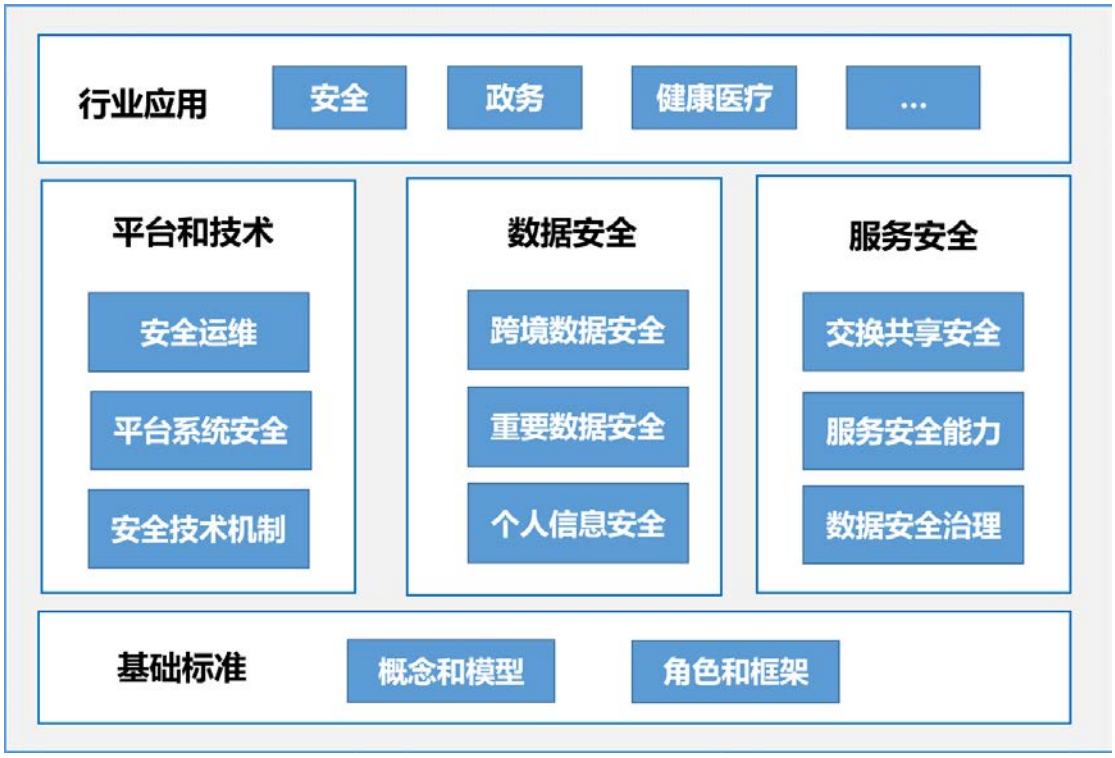

图 19 工业大数据安全标准体系框架

工业大数据安全标准中核心是数据安全，围绕数据安全，需要技术、系统、平台方面的安全标准以及业务、服务、管理方面的安全标准支撑，分别纳入了平台和技术类标准以及服务安全类标准。

（1）基础类标准

工业大数据基础类安全标准为整个大数据安全标准体系提供包括概念、角色、模型、框架等基础标准，明确大数据生态中各类安全角色及相关的安全活动或功能定义，为其它类别标准的制定奠定基础。

（2）平台和技术类标准

平台和技术类标准主要针对大数据服务所依托的基础平台、业务应用平台及其安全防护技术、平台安全运行维护技术展开，具体包括安全技术与机制、系统平台安全和安全运维三部分。

安全技术与机制标准：主要涉及大数据安全相关的技术、机制方面的标准，包括分布式安全计算、安全存储、数据溯源、密钥服务、细粒度审计等技术和机制。

平台系统安全标准：主要涉及大数据平台系统建设和交付相关的安全标准，为大数据安全运行提供基础保障。主要包括基础设施、网络系统、数据采集、数据存储、数据处理等多层次的安全技术防护。

安全运维标准：主要涉及大数据安全运行相关的安全标准，针对大数据运行过程中可能发生的各种事件和风险做好事前、事中、事后的安全保障。包括大数据系统运行维护过程中的风险管理、系统测评等技术标准等。

（3）数据安全类标准

数据安全类标准主要包括个人信息、重要数据、数据跨境安全等安全管理与技术标准，覆盖数据生命周期的数据安全，包括分类分级、去标识化、数据跨境、风险评估等内容。

个人信息安全标准：主要涉及针对个人信息处理活动应遵循的原则和安全要求、个人信息安全影响评估等标准内容，用以健全个人信息安全标准体系，指导组织内部建立个人信息保护策略，指导产品、服务、内部信息系统的设计、开发和实现，并指导个人信息保护实践，为《网络安全法》的实践落地提供技术支撑，切实保护个人信息。

重要数据安全标准：主要围绕重要数据的生命周期，从重要数据治理、管理、技术、基础保障、安全评价等全方位、细粒度的制定对

应的重要数据安全标准，用以指导重要数据的管理和保护，并为《网络安全法》的实践落地提供技术支撑。

跨境数据安全标准：标准旨在规范指导跨境数据处理。包括为国家开展数据出境安全评估提供技术标准支撑，为企业开展数据出境安全风险自评估提供规范指南。通过制定相关标准，使企业可以按照规定的安全评估流程、评估要点、评估方法等内容，合理有效地开展数据出境安全评估，同时为行业主管或监管部门对本行业（领域）数据出境安全评估指导、监督等工作提供依据。

（4）服务安全类标准

服务安全类标准主要是针对开展大数据服务过程中的活动、角色与职责、系统和应用服务等要素提出相应的服务安全类标准；针对数据交易、开放共享等应用场景，提出交易服务安全类标准，包括大数据交易服务安全要求、实施指南及评估方法等。

（5）行业应用安全类标准

行业应用安全类标准主要是针对重要行业和领域大数据应用，对涉及国家安全、国际民生、公共利益的大数据应用的安全防护，形成面向重要行业和领域的大数据安全指南，指导相关的大数据安全规划、建设和运营工作。

4.1.4 云计算安全标准体系

云计算安全涉及服务可用性、数据机密性和完整性、隐私保护、物理安全、恶意攻击防范等诸多方面，是影响云计算发展的关键因素之一。云安全不是单纯的技术问题，只有通过技术、服务和管理的互相配合，形成共同遵循的安全规范，才能营造保障云计算健康发展的可信环境。依据我国云计算生态系统中技术和产品、服务和应用等关键环节，以及贯穿于整个生态系统的云安全，结合国内外云计算发展趋势，构建云计算综合标准化体系框架云计算综合标准化体系框架如下图 20 所示。

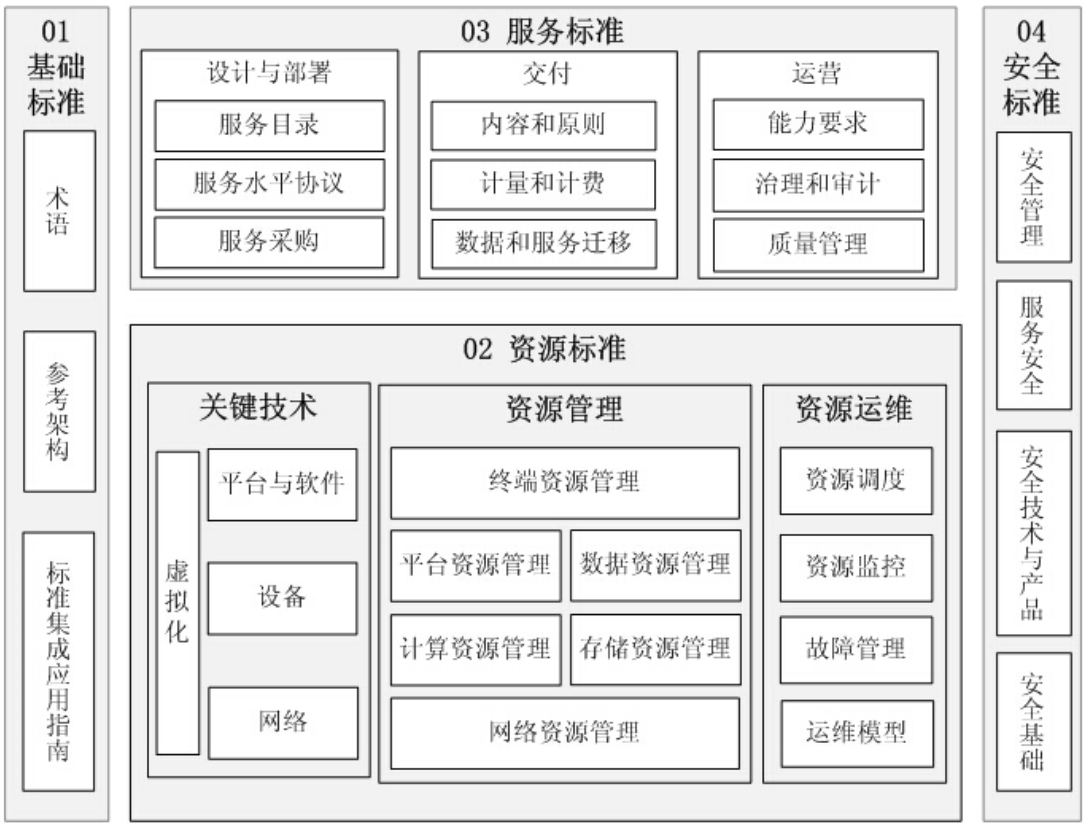

图 20 云计算综合标准化体系框架

云计算综合标准化体系包括“云基础”、“云资源”、“云服务”和

“云安全”4 个部分，云基础标准用于统一云计算及相关概念，为其他各部分标准的制定提供支撑。主要包括云计算术语、参考架构、指南；云资源标准用于规范和引导建设云计算系统的关键软硬件产品研发，以及计算、存储等云计算资源的管理和使用，实现云计算的快速弹性和可扩展性。主要包括关键技术、资源管理和资源运维等；云服务标准用于规范云服务设计、部署、交付、运营和采购，以及云平台间的数据迁移。主要包括服务采购、服务质量、服务计量和计费、服务能力评价等；云安全标准用于指导实现云计算环境下的网络安全、系统安全、服务安全和信息安全，主要包括云计算环境下的安全管理、服务安全、安全技术和产品、安全基础等方面的标准。下面就云安全类的标准进行说明：

（1）安全基础类标准

安全基础类标准主要包括云安全术语、云安全指南、模型与框架三类。其中，云安全术语标准主要统一云计算相关的基本术语、定义和概念，用于指导云计算平台安全方面的设计、开发、应用、维护、监管以及云服务安全等；云安全指南标准主要制定合规性、身份管理、虚拟化、数据和隐私保护、可用性、事件响应等方面的云安全标准，为保障云安全提供指导；模型与框架标准主要制定云计算安全参考模型和框架标准，规定云安全中的各类角色、活动，为云服务的开发和使用提供安全参考框架。

（2）安全技术与产品类标准

安全技术与产品类标准包括软件安全、设备安全、技术和产品安全测评三类。其中，软件安全标准主要制定接口安全、虚拟机安全、身份管理、密钥管理、云存储安全等方面的软件安全标准，为软件设计、开发提供支持；设备安全标准主要制定虚拟防火墙、入侵检测系统、虚拟网关、服务器、终端等设备的安全标准，为设备的设计、开发和交付提供支持；技术和产品安全测评标准主要制定软件产品、系统和设备测试方法的标准，为开展技术和产品安全测评提供指导。

（3）服务安全类标准

服务安全类标准包括业务安全、运营安全和服务安全测评三大类。其中，业务安全标准主要制定云计算数据中心、移动云、健康云、政务云等业务应用的安全标准，为行业云的建设和应用提供支持；运营安全标准主要制定云服务运营安全方面的标准，规范云服务运营安全目标、安全过程、安全风险管理等；服务安全测评标准主要制定云服务安全测评方面的标准，规范云服务安全测试和评价。

（4）安全管理类标准

安全管理类标准包括管理基础、管理支撑技术、安全监管三类。其中，管理基础标准主要制定数据保护、供应链保护、通信安全和个人信息保护等方面的安全管理标准，提出数据保护、供应链保护、通信安全以及个人信息采集、存储和使用等特定的安全控制措施和实施

指南；管理支撑技术标准主要制定云安全配置基线、安全审计流程等方面的标准，规范云平台中的安全配置基线，安全审计流程、安全责任认定、隐私保护以及风险评估等架构和要求；安全监管标准主要制定政府部门对云服务进行安全监管方面的标准，规范云服务提供商应满足的安全要求，云计算平台应具备的安全功能和应采取的安全措施，以及对云服务提供商进行测评的第三方测评机构的认可要求。

4.1.5 工业互联网标准体系框架

《工业互联网综合标准化体系建设指南》指导文件从工业互联网产业发展实际出发，运用综合标准化的理念和方式，着力构建了一套重点突出、协调配套、科学开放、融合创新的工业互联网标准体系，涵盖了工业互联网关键技术、产品、管理和应用需求等各个方面。工业互联网标准体系框架如下图 21 所示，包括基础共性、总体、应用三大类标准，下一步需加快基础共性、总体性、安全、应用等重点领域标准的制定和实施，促进工业互联网产业持续快速健康发展。

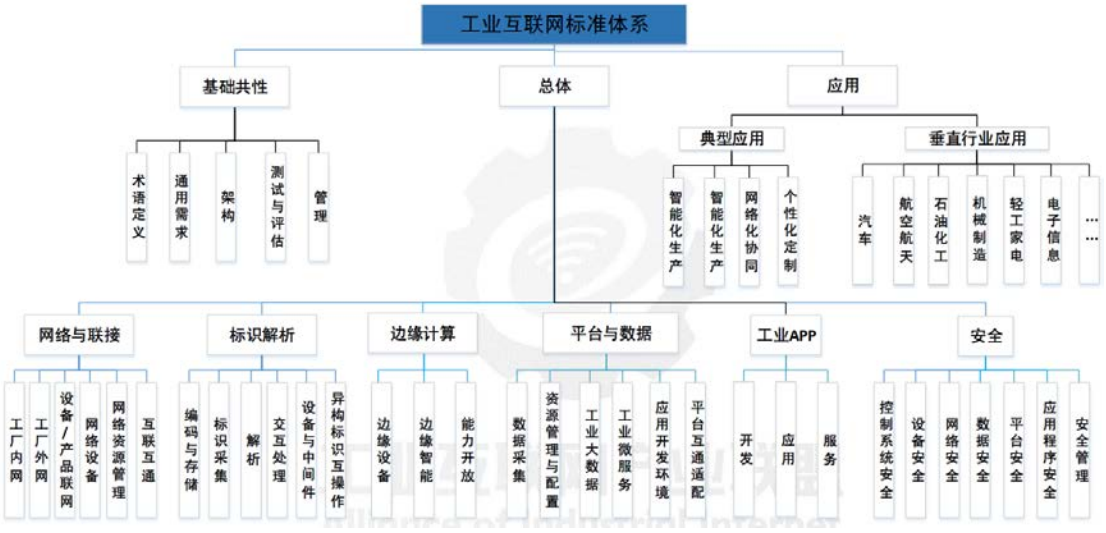

图 21 工业互联网标准体系框架

基础共性标准主要规范工业互联网的通用性、指导性标准，包括术语定义、通用需求、架构、测试与评估、管理等标准。

总体标准包括网络与联接标准、标识解析标准、边缘计算标准、平台与数据标准、工业 APP 标准和安全标准。其中，安全标准主要包括设备安全、控制系统安全、网络安全、数据安全、平台安全、应用程序安全、安全管理等标准。

应用标准包括典型应用标准和垂直行业应用标准等。典型应用标准：包括智能化生产标准、个性化定制标准、网络化协同标准、服务化转型标准。垂直行业应用标准是指依据基础共性标准、总体标准和典型应用标准，面向汽车、航空航天、石油化工、机械制造、轻工家电、电子信息等重点行业领域的工业互联网应用，开发行业应用导则、特定技术标准和管理规范，优先在重点行业领域实现突破，同时兼顾传统制造业转型升级的需求，逐步覆盖制造业全应用领域。

4.2 工业互联网安全标准体系构建及推进

4.2.1 工业互联网安全标准体系框架

项目组根据《加强工业互联网安全工作的指导意见》、《《关于推动工业互联网加快发展的通知》等文件精神，以及《工业互联网综合标准化体系建设指南》和网络安全等级保护 2.0 安全框架的具体要求，并在充分认识和理解上述各大领域已有的安全标准体系框架的基础上，按照多维考虑、纵向分层、横向分类的总体思想，构建了工业互联网安全标准体系框架，如下图 22 所示。

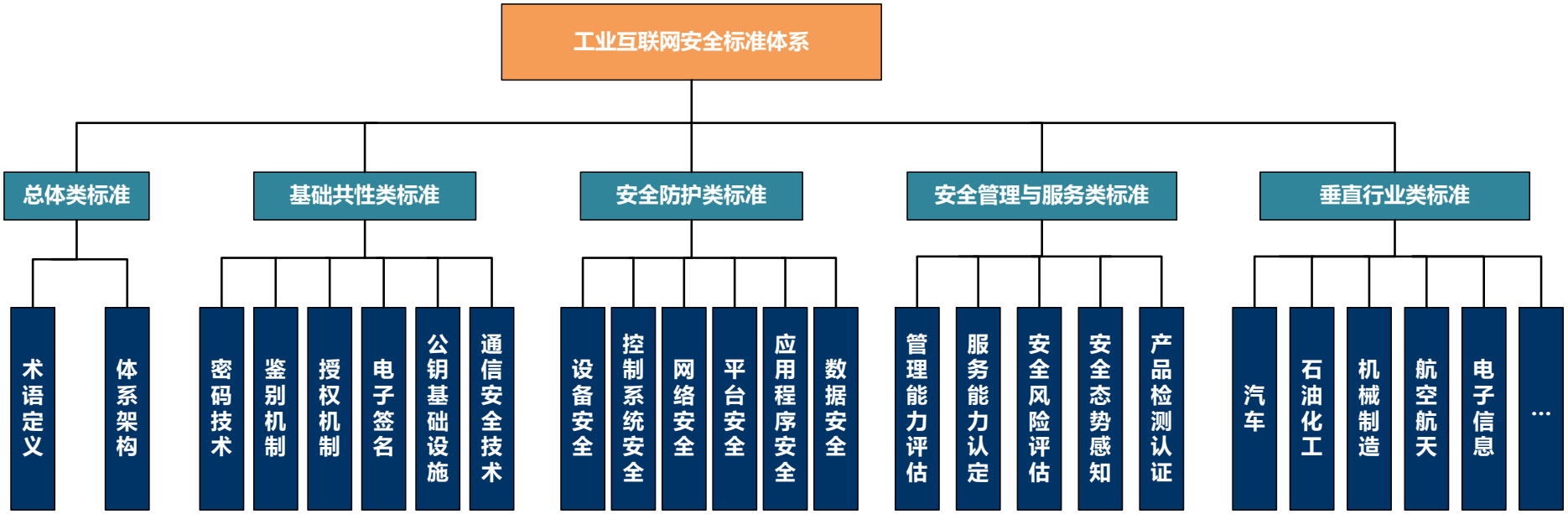

图 22 工业互联网安全标准体系框架

4.2.2 工业互联网安全标准体系框架梳理

工业互联网安全标准体系框架从以下五个维度分类提出工业互联网安全标准，它们分别是：总体类标准、基础共性类标准、安全防护类标准、安全管理与服务类标准和垂直行业类标准。

（一）总体类标准

总体类标准为整个工业互联网安全标准体系提供总体基础性标准，包括术语定义和安全架构两个子类。

术语标准是在工业互联网安全方面进行技术交流的基础语言，规范术语定义和术语之间的关系，有助于准确理解和表达技术内容，方便技术交流和研究。

工业互联网安全架构标准是对工业互联网安全内在的要求、设计结构和运行建立的一个开放的工业互联网安全技术模型，规范工业互联网安全体系架构有助于准确理解工业互联网安全保障体系的结构层次、功能要素及其关系，是工业互联网安全其他标准制定参考的基础。工业互联网安全参考架构需通过借鉴国际上现有的科研成果，针对工业互联网安全的需求，给出工业互联网安全参考模型，并作为工业互联网安全参考模型的重要补充，给出工业互联网安全参考架构的结构层次和功能要素，以及各结构层次和功能要素之间的关系，应适用于任何从事或关注工业互联网系统安全的组织和个人。

（二）基础共性类标准

基础共性类标准包括密码技术、鉴别机制、授权机制、电子签名、公钥基础设施、通信安全技术等通用性技术类标准。

密码技术标准包括密码算法、密码模块，密钥管理、密码设备应用接口、可信计算密码支撑平台功能与接口规范等标准；鉴别机制标准包括实体鉴别、消息鉴别等不同类别的鉴别方式的界定、鉴别保障框架等标准的制定和研究；授权机制标准包括访问控制、安全断言标记语言、地理空间可扩展控制、授权应用程序判定接口规范等标准；电子签名技术和产品的应用，使得电子签章变得更为高效、安全、且低成本，更为核心的是使得签署文件不可篡改、不可抵赖和不可丢失，虽然我国于 2004 年就已经提出了《电子签名法》但是缺乏与之相关的配套标准，亟需制定与企业需求相适应的电子签名相关标准；公钥基础设施安全标准包括公钥基础设施安全技术要求、在线证书的管理、PKI 组件的最小互操作、时间戳规范等一系列标准；通信安全类标准包括数据和通信系统相关的安全术语和定义、端到端的通信系统安全架构、通信安全技术要求、通信安全协议等标准的制定和研发。

（三）安全防护类标准

安全防护类标准主要包括设备安全、控制系统安全、网络安全、数据安全、平台安全、应用程序安全标准。

设备安全标准：

主要规范工业互联网中各类终端设备在设计、研发、生产制造以

及运行过程中的安全防护、检测及其它技术要求，包括数据采集类设备、智能装备类设备（如可编程逻辑控制器（PLC）、智能电子设备（IED）等）等。对于每一类终端设备，均包括但不限于设计规范、防护要求（或基线配置要求）、检测要求等标准。

控制系统安全标准：

主要规范工业互联网中各类控制系统中的控制软件与控制协议的安全防护、检测及其它技术要求，包括数据采集与监视控制系统（SCADA）、集散控制系统（DCS）、现场总线控制系统（FCS）等安全标准。

网络安全标准：

主要规范承载工业智能生产和应用的通信网络与标识解析系统的安全防护、检测及其它技术要求，以及相关网络安全产品的技术要求。

数据安全标准：

主要规范工业互联网数据相关的安全防护、检测及其它技术要求，包括工业大数据、用户个人信息等数据安全技术要求、数据安全管理规范等标准。

平台安全标准：

主要规范工业互联网平台的安全防护、检测、病毒防护及其它技术要求，包括边缘计算能力、工业云基础设施（包括服务器、数据库、虚拟化资源等）、平台应用开发环境、微服务组件等安全标准。

应用程序安全标准：

主要规范用于支撑工业互联网智能化生产、网络化协同、个性化定制、服务化延伸等服务的应用程序的安全防护与检测要求，包括支撑各种应用的软件、APP、Web 系统等。

（四）安全管理与服务类标准

安全管理与服务类标准主要包括管理能力评估、服务能力认证、安全风险评估、安全态势感知、产品检测认证标准。

安全管理能力评估标准包括工控场所安全管理要求、集成商安全管理要求、用户企业安全管理要求、产品全生命周期的安全管理要求等规范；服务能力认证包括服务质量评估、服务能力评估、工业互联网服务安全评估的基本程序及要求等；安全风险标准主要规范工业领域系统、设备、产品等的安全检查、安全风险评估要素，提供安全检查和风险评估的指标、评估方法和评估模型等；安全态势感知标准主要规范工业控制系统、工业现场等的安全态势感知、监测预警服务的安全要求。包括态势感知及监测预警系统建设规范、态势感知及监测预警技术规范、态势感知及监测预警体系建设等标准；安全检测认证标准主要为工业控制系统、工业互联网平台、工业大数据等的安全检测认证提供标准参考。

（五）垂直行业类标准

在总体类标准、基础共性类标准、安全防护类标准、安全管理与服务类标准的基础上，面向汽车、石油、化工、机械制造、航空航天

等重点行业领域，结合行业特色和需求，研制更具针对性、对行业更有指导作用的工业互联网安全国家标准/行业标准。

通过梳理工业互联网安全标准体系框架，可以明确现有标准的定位，并根据工业互联网产业发展现状和重点关注的问题确定近期标准工作重点。避免标准研制不协调的情况发生，更好的推动工业互联网的应用和产业发展，制定符合中国国情和工业互联网产业特点的安全标准，促进工业互联网安全标准研制有序开展。

4.2.3 工业互联网安全重点标准化方向

未来，工业互联网安全标准化工作应坚持“统筹规划、重点突出、急用先行”的原则，加快急需工业互联网安全标准研制和标准体系建设，加强标准落地应用。工业互联网安全领域重点标准化方向如下表 3 所示。

表 3 工业互联网安全重点标准化方向

标准类别		标准名称	标准内容
总体类	安全架构	工业互联网安全体系框架	基于工业互联网的架构、安全防护需求等，从设备和控制安全、平台安全、数据安全、网络和 应用安全等维度，研究提出工业互联网安全体系框架。
安全防护类	设备和控制安全	工业互联网设备安全接入要求	针对工业控制设备、智能终端等工业互联网设备接入工业互联网平台时存在的安全问题及接入需求，从设备接入前安全评估、接入过程安全控制、接入后安全检测等方面，提出工业互联网设备

			安全接入要求。
	工业互联网网络安全（标识解析）	工业互联网安全-标识解析与交互处理安全要求	根据工业互联网标识解析面临的安全问题，提出标识解析过程以及标识在各解析节点间的交互安全要求。
	工业互联网平台安全	工业互联网平台服务安全要求	针对工业互联网平台提供的服务，提出工业互联网平台服务安全要求，包括平台开发服务安全、工业 APP 服务安全等。
	工业互联网数据安全	工业互联网数据分类分级与安全防护指南	从落实主体安全责任的角度，对工业互联网数据提出分类方法，从数据遭破坏产生的后果影响程度提出数据分级方法，从安全管理和技术的角度，对工业互联网数据提出不同级别的安全防护要求。
		工业互联数据交换共享安全	针对工业互联网数据交换与共享中的互信互任、权限控制、责任界定、安全共享等方面，提出工业互联网数据安全交换共享模型和要求。
安全管理与服务类	安全态势感知	工业互联网安全态势感知平台技术要求	在安全管理与服务过程中有效组织各相关方、及时判断异常行为，在工业互联网安全态势感知、事件应急响应等方面加快安全标准研制，推动工业互联网安全生态的有效协同。
	安全测试与评估	工业互联网安全测试与评估指南	面向工业互联网平台、工业数据等，提出安全测试和评估的内容、方法和工作流程。

第五章 工业互联网安全标准化工作建议

当前，我国工业互联网安全标准化工作取得阶段性进展，标准化工作顶层制度和体系机制日益健全完善，关键基础标准及重点领域标准取得明显进展，为工业互联网驶入健康发展快车道提供了有效支撑。下一步应着眼于工业互联网未来发展可能面临的网络安全新形势和新需求，从规范行业安全管理、完善安全技术标准、构建新型有效的安全防护体系、探索和研究新技术新应用等多个维度着手，联合政府和行业力量，共同打造工业互联网安全生态，积极推动工业互联网安全健康发展。

5.1 工业互联网安全标准化工作存在的问题

2019 年 7 月，工业互联网安全标准体系的建设性指导文件《加强工业互联网安全工作的指导意见》正式印发，从国家层面上确立了工业互联网安全标准体系的建设思路、建设目标及内容，为各行业和企业开展工业互联网安全工作提供了切实可行的指引。

各方在积极推进安全标准化工作时，也逐渐暴露出当前工作中存在的一些问题，如“各标准化机构和组织合作交流较少、概念统一性差、标准培训力度不够、企业对安全标准化规范理解不足、标准落地应用困难”等，具体说明如下：

（一）不同标准化组织之间缺乏有效的合作和交流

目前我国的标准化工作机制，名义上是国家标准化管理委员会统

一管理全国标准化工作，但实际上不同程度地存在各部门、各行业各自为政现象。各个产业的标准化专业技术组织与科研机构分散在各个政府部门和行业中，导致了在实际的运作过程中不同部门之间缺乏有效的协调和沟通。具体到安全标准化领域：目前，TC 260、TC 82、TC 124、TC 196 等国家标准化技术委员会在积极推进信息安全领域、电力安全领域、工业控制和自动化领域、通信安全领域等与工业互联网安全相关的标准研制工作，但是各标准化技术委员会、标准工作组之间合作交流较少，一定程度上存在标准交叉、重复的现象。

（二）工业互联网安全体系框架未形成，其概念统一化不足

由于我国工业互联网安全标准体系还未形成统一的安全体系框架，导致我国工业互联网安全相关标准汇总的概念统一化不足，出现基本概念和术语界定存在不一致的情况。此外，在工业信息安全领域，部分引入的国外标准中，其术语定义更多是根据字面意思直接翻译外文，与我国相关概念的实际内涵有偏差，导致实际应用困难。

（三）工业互联网安全相关知识普及程度不够，企业缺乏安全意识

在调研过程中发现，有些企业对于“工业互联网”、“标识解析”、“新基建”等词语的概念和理解不清晰，部分企业对开展安全标准化工作的重要性和必要性认识不足，未能理解开展安全标准化工作的意义，仅把取得安全标准化达标证书作为企业生存的唯一目的，而忽视了从根本上提高企业整体安全管理水平，缺乏主动开展标准化达标创

建的积极性。

（四）安全标准培训力度不够、落地应用困难

CCSA、工业互联网产业联盟近些年来在积极推进工业互联网领域各标准的制定，安全方面发布有《工业互联网 安全总体要求》和《工业互联网平台 安全防护要求》等行业标准和联盟标准，但其标准标准宣贯培训力度不足，导致企业在安全标准应用中存在理解偏差等问题。另外一方面，工业互联网安全是与各行业的具体场景息息相关的，不同行业中的安全需求差异较大。其通用性国家标准很难满足各行业的实际需求，导致在实际应用中标准落地的指导性意义不强。

5.2 工业互联网安全标准化工作建议

工业互联网安全标准化工作是构建工业互联网安全保障体系的技术保障，新时代下的工业互联网安全标准化工作必须坚持紧紧围绕我国安全建设主线，谋划部署推进，未来工业互联网安全标准的研制也将对“产学研用”产生更大的推动作用。

5.2.1 政府层面的安全标准化工作建议

（一）构建工业互联网安全责任体系和制度环境

一是深入贯彻落实《网络安全法》，明确安全监管部门、各行业主管部门、行业企业、工业互联网平台提供商等不同主体的法律责任和义务，构建权责分明的工业互联网安全责任体系；二是研究建立工

业互联网安全防护工作体系，与现有通信网络安全防护管理体系、工业控制系统安全防护体系做好衔接，统筹协调不同行业主管部门联合开展针对工业互联网的安全检查和风险评估，督促指导各责任主体落实安全防护要求；三是制定出台工业互联网安全指导性文件，指导企业开展工业互联网安全防护工作；四是完善工业互联网安全信息共享和突发事件应急处置机制，建设针对工业互联网的木马病毒样本库、漏洞库等。

（二）强化工业互联网产业整体布局

一是重点突破工业互联网核心技术瓶颈，支持国内相关厂商与科研院所强强联合，研发应用广泛、但严重依赖国外的工业软硬件产品，如大型 PLC 设备、高端 SCADA 系统等；二是加强工业互联网核心环节如工业互联网平台的自主研发与部署，带动相关产业形成工业互联网自主发展的产业生态链；三是着力推动国产工业互联网软硬件产品和平台的市场应用，鼓励和支持能源、电力、制造、交通等重点行业采用国产技术和产品，以推动国产化应用促进工业互联网产业发展。

（三）建立工业互联网安全标准和评估认证体系

一是基于本报告中的工业互联网安全标准体系，明确标识解析系统、工业互联网平台、工业大数据、工业控制系统等安全防护要求，推动安全标准在各行业的应用，指导工业企业开展安全保障体系建设；二是推动构建工业互联网安全认证体系，依托工业互联网产业联盟和

深圳市工业互联网联盟，倡导企业开展安全能力评估和认证，加强宣传推广形成行业标杆，引领工业互联网全行业安全防护能力不断提升。

（四）推动工业互联网安全技术研发和应用示范

一是推动适用于工业互联网的工业防火墙、入侵检测、安全审计等一系列安全技术和产品研发，发展具有行业针对性的安全解决方案，切实推动工业互联网安全技术创新的应用化和产业化；二是选取能源、电力、制造、交通等典型行业，组织开展工控安全防护、安全监测预警、工业互联网平台和大数据防护等重点方向的试点示范，形成一批工业互联网安全防护的典型方案与最佳实践，依托工业互联网产业联盟强化产业互动，发挥试点示范的带动促进作用，引导企业加强安全保障能力建设。

5.2.2 标准化组织及单位的安全标准化工作建议

（一）充分发挥各标准化组织的作用，加强沟通与合作

在进行工业互联网安全标准研制时，标准承研单位应积极与相关标准化技术委员会进行沟通确认，充分考虑标准的衔接性和适用性，避免出现标准重复、冲突等现象。同时，应注重提升标准的整体推进水平；目前，工业控制系统安全和电力系统安全标准制定成效明显，但网络安全、平台安全、数据安全，特别是设备安全、应用安全制定滞后，应切实考虑现实需求，在重点抓好关键基础和急用标准制定的同时，加快推进短板标准制定进度，整体性发挥标准基础性、战略性、

引领性作用。

（二）加强工业互联网安全框架研究，不断完善安全标准体系

随着工业互联网在各行业各领域加速深入落地实施，工业互联网安全重要性日益突显，标准需求加速增长，安全标准要求逐步提高。但相关标准间缺乏严格的逻辑关联，急需开展工业互联网安全体系框架类标准制定，为工业互联网安全标准的研制提供思路和方向。同时，结合国内外工业互联网安全发展新趋势，适时完善工业互联网安全标准体系及建设性指导文件，以更加有效地指导工业互联网安全标准制定工作。

（三）强化企业参与制定力度，定期开展标准化专题培训

在科研院所、检测认证机构、高等院校等单位主导标准制定的现实格局下，要下力气提升相关企业参与的积极性，充分发挥企业作为标准的重要实践和落实主体的优势，切实提升标准在实践中的指导规范作用。因此，应加强面向工业互联网应用企业开展安全相关领域的知识普及工作，通过举办工业互联网讲座、论坛、媒体宣传等手段，提高全社会对工业互联网的认识，以适应工业互联网的发展。同时，充分发挥地方标准化组织、协会、联盟和专业机构等的作用，通过多种渠道宣传工业互联网安全标准化应用案例和突出成绩，并有针对性的开展面向企业特别是中小型企业的安全标准化专题培训。

（四）大力推动标准的实施应用和推广工作

一是加强标准宣贯培训。坚持标准研制和宣贯并重，着重利用网络媒体、专业的互联网平台、社交平台等多种渠道，加大对标准的解读和宣传力度；二是积极组织开展标准试验验证。建设一批新技术标准符合性试验验证系统，开发和推广仿真和测试工具，测试验证标准符合网络安全管理、产业发展、用户使用等方面的实践要去，确保标准管用、好用。三是组织开展电子信息制造业、机械装备制造业、高技术制造业以及服装制造业等重点领域安全标准的试点示范。组织遴选工业互联网标准典型案例，推广一些实施效果好、示范效应强的标准。

5.2.2 企业层面的安全标准化工作建议

（一）落实政策法规，建立健全工业互联网安全管理制度

企业可依据《网络安全法》、《关于印发加强工业互联网安全工作的指导意见的通知》、《工业控制系统信息安全防护指南》、《工业互联网企业网络安全分类分级指南》、《工业数据分类分级指南》、等保 2.0 等国家指导性文件建立健全安全管理体系，按照组织管理逐层落实企业网络安全责任，有效施行企业网络安全监督考核机制，积极开展应急预案与演练、工业数据分类分级等工作，通过组织培训等措施增强员工安全意识和突发事件处理能力。

（二）持续开展检查评估，逐步提升工业互联网网络安全保障能力

企业可邀请专业机构的检测评估队伍进行评估和经验交流，开展针对工业互联网相关平台、应用、设施的评估工作，检验企业在安全保障措施、安全管理制度、安全应急预案、安全设备配置、外包服务等方面工作是否有效落实，及时发现存在的风险隐患，在专业机构的指导下对存在问题查漏补缺，提升企业自身的网络安全保障能力。

（三）加强安全检测，全面提高关键核心技术应用的数据安全性

企业在运营中可加强与网络安全厂商、外包服务商等的协同联动，部署有效安全技术防护手段，积极对工业互联网设备、网络、平台、工业 APP 等工业数据的载体进行安全检测，对存在的安全风险及时进行整改修复，建立从设备安全配置到边界安全防护再到网络安全态势感知的闭环管控，防止工业数据被窃取。积极引入专业人才对数据载体进行管理和安全加固，做到专人专岗，专事专做。

近些年来，深圳稳步推进工业互联网的政策体系、产业生态和应用模式建设，工业互联网在深圳地区各行业和企业的应用效果显著，涌现出华为、华星光电、富士康、迈瑞医疗、赢领智尚等一批工业互联网应用标杆企业（深圳市龙头标杆企业在工业互联网中的应用实践及安全标准制定情况详见附录 2）。通过发展工业互联网，实现了生产全链条互联互通，大大提升了企业市场反应速度，降低了生产成本，企业效益和竞争力取得明显提升。下一步，应发挥工业互联网安全标准的保障作用和桥梁作用，联合工业互联网产业链各方力量，共同打

造工业互联网安全生态。

附录 1：工业互联网安全标准明细梳理表

总序号	分序号	标准名称	标准号/计划号	对应国际标准号	归口单位	状态/备注
（一）总体类标准						
术语定义						
1	1	电气安全术语	GB/T 4776-2017		TC 25	已发布
2	2	信息安全技术 术语	GB/T 25069-2010		TC 260	已发布
3	3	机械安全 术语	GB/T 30174-2013		TC 208	已发布
4	4	工业通信网络 网络和系统安全 术语、概述和模型	20170373-T-604		TC 124	正在批准
5	5	信息安全技术 术语	20170573-T-469		TC 260	正在审查
6	6	公共安全术语标准	20075940-T-469		TC 351	正在起草
7	7	移动通信网安全术语集	YD/T 2258-2011		CCSA	行业标准 通信
体系架构						
8	1	信息技术 安全技术 IT 网络安全 第 2 部分：网络安全体系结构	GB/T 25068.2-2012	ISO/IEC 18028-2:2006(IDT)	TC 260	已发布
9	2	信息安全技术 可信计算规范 可信连接架构	GB/T 29828-2013		TC 260	已发布
10	3	信息安全技术 移动智能终端安全架构	GB/T 32927-2016		TC 260	已发布
11	4	信息安全技术 云计算安全参考架构	GB/T 35279-2017		TC 260	已发布
12	5	智能制造 系统架构	20173704-T-604		TC 124	正在批准

13	6	信息技术 安全技术 信息安全管理体系审核指南	20190913-T-469		TC 260	正在批准
14	7	信息化和工业化融合生态系统参考架构	20191077-T-339		TC 573	正在批准
15	8	工控系统动态重构主动防御体系架构规范	20190644-T-604		TC 159	正在征求意见
（二）基础共性类标准						
密码技术						
16	1	信息技术 安全技术 实体鉴别 第 4 部分: 采用密码校验函数的机制	GB/T 15843.4-2008	ISO/IEC 9798-4:1999(IDT)	TC 28	已发布
17	2	信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制	GB/T 15852.1-2008	ISO/IEC 9797-1:1999(IDT)	TC 260	已发布
18	3	识别卡 集成电路卡 第 15 部分：密码信息应用	GB/T 16649.15-2010	ISO/IEC 7816-15:2004(IDT)	TC 28	已发布
19	4	信息安全技术 分组密码算法的工作模式	GB/T 17964-2008		TC 260	已发布
20	5	信息技术 安全技术 散列函数 第 2 部分:采用 n 位块密码的散列函数	GB/T 18238.2-2002	ISO/IEC 10118-2:2000(IDT)	TC 260	已发布
21	6	信息安全技术 可信计算密码支撑平台功能与接口规范	GB/T 29829-2013		TC 260	已发布
22	7	信息安全技术 SM3 密码杂凑算法	GB/T 32905-2016		TC 260	已发布
23	8	信息安全技术 SM4 分组密码算法	GB/T 32907-2016		TC 260	已发布
24	9	信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则	GB/T 32918.1-2016		TC 260	已发布
25	10	信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法	GB/T 32918.2-2016		TC 260	已发布
26	11	信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议	GB/T 32918.3-2016		TC 260	已发布

27	12	信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法	GB/T 32918.4-2016		TC 260	已发布
28	13	信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义	GB/T 32918.5-2017		TC 260	已发布
29	14	信息安全技术 祖冲之序列密码算法 第 1 部分：算法描述	GB/T 33133.1-2016		TC 260	已发布
30	15	信息安全技术 密码应用标识规范	GB/T 33560-2017		TC 260	已发布
31	16	信息安全技术 SM2 密码算法加密签名消息语法规范	GB/T 35275-2017		TC 260	已发布
32	17	信息安全技术 SM2 密码算法使用规范	GB/T 35276-2017		TC 260	已发布
33	18	信息安全技术 密码设备应用接口规范	GB/T 36322-2018		TC 260	已发布
34	19	信息安全技术 射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别	GB/T 37033.1-2018		TC 260	已发布
35	20	信息安全技术 射频识别系统密码应用技术要求 第 2 部分：电子标签与读写器及其通信密码应用技术要求	GB/T 37033.2-2018		TC 260	已发布
36	21	信息安全技术 射频识别系统密码应用技术要求 第 3 部分：密钥管理技术要求	GB/T 37033.3-2018		TC 260	已发布
37	22	信息安全技术 密码模块安全要求	GB/T 37092-2018		TC 260	已发布
38	23	信息安全技术 安全电子签章密码技术规范	GB/T 38540-2020		TC 260	即将实施
39	24	信息安全技术 电子文件密码应用指南	GB/T 38541-2020		TC 260	即将实施
40	25	信息安全技术 动态口令密码应用技术规范	GB/T 38556-2020		TC 260	即将实施
41	26	信息安全技术 密码模块安全检测要求	GB/T 38625-2020	ISO/IEC 24759:2017(NEQ)	TC 260	即将实施
42	27	信息安全技术 SM9 标识密码算法 第 1 部分：总则	GB/T 38635.1-2020		TC 260	即将实施
43	28	信息安全技术 SM9 标识密码算法 第 2 部分：算法	GB/T 38635.2-2020		TC 260	即将实施

44	29	信息安全技术 传输层密码协议（TLCP）	GB/T 38636-2020		TC 260	即将实施
45	30	信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制	20190911-T-469	ISO/IEC 9797-1:2011 (MOD)	TC 260	正在批准
46	31	信息安全技术 信息系统密码应用基本要求	20190902-T-469		TC 260	正在审查
47	32	信息安全技术 SM9 密码算法使用规范	20202624-T-469		TC 260	正在征求意见
48	33	信息安全技术 分组密码算法的工作模式	20201696-T-469		TC 260	正在征求意见
49	34	信息安全技术 祖冲之序列密码算法第 2 部分：保密性算法	20190904-T-469		TC 260	正在征求意见
50	35	信息安全技术 祖冲之序列密码算法 第 3 部分：完整性算法	20190903-T-469		TC 260	正在征求意见
51	36	信息安全技术 可信计算密码支撑平台功能与接口规范	20201695-T-469		TC 260	正在征求意见
52	37	SM3 密码杂凑算法	GM/T 0004-2012		密码行业标准化技术委员会	行业标准 国密
53	38	SM2 密码算法使用规范	GM/T 0009-2012		密码行业标准化技术委员会	行业标准 国密
54	39	可信计算 可信密码支撑平台功能与接口规范	GM/T 0011-2012		密码行业标准化技术委员会	行业标准 国密
55	40	数字证书认证系统密码协议规范	GM/T 0014-2012		密码行业标准化技术委员会	行业标准 国密
56	41	密码设备应用接口规范	GM/T 0018-2012		密码行业标准化技术委员会	行业标准 国密
57	42	密码模块安全技术要求	GM/T 0028-2014		密码行业标准化技术委员会	行业标准 国密
58	43	安全电子签章密码技术规范	GM/T 0031-2014		密码行业标准	行业标准 国密

					化技术委员会	
59	44	基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范	GM/T 0034-2014		密码行业标准化技术委员会	行业标准 国密
60	45	射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别	GM/T 0035.1-2014		密码行业标准化技术委员会	行业标准 国密
61	46	射频识别系统密码应用技术要求 第 2 部分：电子标签芯片密码应用技术要求	GM/T 0035.2-2014		密码行业标准化技术委员会	行业标准 国密
62	47	射频识别系统密码应用技术要求 第 3 部分：读写器密码应用技术要求	GM/T 0035.3-2014		密码行业标准化技术委员会	行业标准 国密
63	48	射频识别系统密码应用技术要求 第 4 部分：电子标签与读写器通信密码应用技术要求	GM/T 0035.4-2014		密码行业标准化技术委员会	行业标准 国密
64	49	射频识别系统密码应用技术要求 第 5 部分：密钥管理技术要求	GM/T 0035.5-2014		密码行业标准化技术委员会	行业标准 国密
65	50	密码模块安全检测要求	GM/T 0039-2015		密码行业标准化技术委员会	行业标准 国密
66	51	射频识别标签模块密码检测准则	GM/T 0040-2015		密码行业标准化技术委员会	行业标准 国密
67	52	智能 IC 卡密码检测规范	GM/T 0041-2015		密码行业标准化技术委员会	行业标准 国密
68	53	三元对等密码安全协议测试规范	GM/T 0042-2015		密码行业标准化技术委员会	行业标准 国密
69	54	SM9 标识密码算法	GM/T 0044-2016		密码行业标准化技术委员会	行业标准 国密
70	55	安全电子签章密码检测规范	GM/T 0047-2016		密码行业标准	行业标准 国密

					化技术委员会	
71	56	密码键盘密码检测规范	GM/T 0049-2016		密码行业标准化技术委员会	行业标准 国密
72	57	信息系统密码应用基本要求	GM/T 0054-2018		密码行业标准化技术委员会	行业标准 国密
73	58	多应用载体密码应用接口规范	GM/T 0056-2018		密码行业标准化技术委员会	行业标准 国密
74	59	动态口令密码应用检测规范	GM/T 0061-2018		密码行业标准化技术委员会	行业标准 国密
75	60	商用密码产品生产和保障能力建设规范	GM/T 0065-2019		密码行业标准化技术委员会	行业标准 国密
76	61	电子保单密码应用技术要求	GM/T 0070-2019		密码行业标准化技术委员会	行业标准 国密
77	62	电子文件密码应用指南	GM/T 0071-2019		密码行业标准化技术委员会	行业标准 国密
鉴别机制						
78	1	信息技术 安全技术 实体鉴别 第 1 部分：总则	GB/T 15843.1-2017	ISO/IEC 9798-1:2010(IDT)	TC 260	已发布
79	2	信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制	GB/T 15843.2-2017	ISO/IEC 9798-2:2008(IDT)	TC 260	已发布
80	3	信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制	GB/T 15843.3-2016	ISO/IEC 9798-3:1998/AMD.1:2010(IDT)	TC 260	已发布

81	4	信息技术 安全技术 实体鉴别 第 4 部分: 采用密码校验函数的机制	GB/T 15843.4-2008	ISO/IEC 9798-4:1999(IDT)	TC 260	已发布
82	5	信息技术 安全技术 实体鉴别 第 5 部分:使用零知识技术的机制	GB/T 15843.5-2005	ISO/IEC 9798-5:1999(IDT)	TC 260	已发布
83	6	信息技术 安全技术 实体鉴别 第 6 部分：采用人工数据传递的机制	GB/T 15843.6-2018	ISO/IEC 9798-6:2010(IDT)	TC 260	已发布
84	7	信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制	GB/T 15852.2-2012	ISO/IEC 9797-2:2002(MOD)	TC 260	已发布
85	8	信息技术 安全技术 消息鉴别码 第 3 部分：采用泛杂凑函数的机制	GB/T 15852.3-2019	ISO/IEC 9797-3:2011(MOD)	TC 260	已发布
86	9	信息技术 开放系统互连 开放系统安全框架 第 2 部分: 鉴别框架	GB/T 18794.2-2002	ISO/IEC 10181-2:1996(IDT)	TC 28	已发布
87	10	信息安全技术 引入可信第三方的实体鉴别及接入架构规范	GB/T 28455-2012		TC 260	已发布
88	11	信息技术 安全技术 匿名实体鉴别 第 1 部分：总则	GB/T 34953.1-2017	ISO/IEC 20009-1:2013(IDT)	TC 260	已发布
89	12	信息技术 安全技术 可鉴别的加密机制	GB/T 36624-2018	ISO/IEC 19772:2009(MOD)	TC 260	已发布
90	13	信息安全技术 网络用户身份鉴别技术指南	GB/T 36633-2018		TC 260	已发布
91	14	信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架	GB/T 36651-2018		TC 260	已发布
92	15	信息安全技术 鉴别与授权 访问控制中间件框架与接口	GB/T 36960-2018		TC 260	已发布
93	16	信息安全技术 鉴别与授权 认证中间件框架与接口规范	GB/T 30275-2013		TC 260	已发布

94	17	信息技术 安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的机制	GB/T 34953.4-2020	ISO/IEC 20009-4:2017(MOD)	TC 260	即将实施
95	18	信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架	GB/T 38542-2020		TC 260	即将实施
96	19	信息安全技术 轻量级鉴别与访问控制机制	20130328-T-469		TC 260	正在批准
97	20	信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制	20190911-T-469	ISO/IEC 9797-1:2011(MOD)	TC 260	正在批准
98	21	信息安全技术 实体鉴别保障框架	20193255-T-469		TC 260	正在征求意见
授权机制						
99	1	信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范	GB/T 25062-2010		TC260	已发布
100	2	信息安全技术 鉴别与授权 安全断言标记语言	GB/T 29242-2012		TC260	已发布
101	3	信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言	GB/T 30280-2013		TC260	已发布
102	4	信息安全技术 鉴别与授权 可扩展访问控制标记语言	GB/T 30281-2013		TC260	已发布
103	5	信息安全技术 鉴别与授权 授权应用程序判定接口规范	GB/T 31501-2015		TC260	已发布
104	6	信息安全技术 鉴别与授权 数字身份信息服务框架规范	GB/T 31504-2015		TC260	已发布
105	7	域名系统授权体系技术要求	YD/T 2136-2010		CCSA	行业标准 通信
106	8	移动互联网应用编程接口的授权技术要求	YD/T 2912-2015		CCSA	行业标准 通信
107	9	面向移动互联网的公共认证授权体系技术要求	YD/T 3149-2016		CCSA	行业标准 通信
108	10	基于角色的授权管理与访问控制技术规范	GM/T 0032-2014		密码行业标准化技术委员会	行业标准 国密
109	11	开放的第三方资源授权协议框架	GM/T 0068-2019		密码行业标准化技术委员会	行业标准 国密

110	12	信息安全技术 非授权外联监测产品安全技术要求	GA/T 1144-2014		公安部	行业标准 公共安全
电子签名						
111	1	信息技术 安全技术 带附录的数字签名 第 3 部分:基于证书的机制	GB/T 17902.3-2005	ISO/IEC 14888-3:1998(IDT)	TC260	已发布
112	2	信息技术 安全技术 匿名数字签名 第 2 部分：采用群组公钥的机制	GB/T 38647.2-2020	ISO/IEC 20008-2:2013(MOD)	TC260	即将实施
113	3	保险电子签名技术应用规范	JR/T 0161-2018		中国人民银行	行业标准 金融
114	4	取证与鉴定文书电子签名	GA/T 977-2012		公安部	行业标准 公共安全
公钥基础设施						
115	1	信息技术 安全技术 公钥基础设施 在线证书状态协议	GB/T 19713-2005		TC260	已发布
116	2	信息技术 安全技术 公钥基础设施 证书管理协议	GB/T 19714-2005		TC260	已发布
117	3	信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范	GB/T 19771-2005		TC260	已发布
118	4	信息安全技术 公钥基础设施 数字证书格式	GB/T 20518-2018		TC260	已发布
119	5	信息安全技术 公钥基础设施 时间戳规范	GB/T 20520-2006		TC260	已发布
120	6	信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求	GB/T 21053-2007		TC260	已发布
121	7	信息安全技术 公钥基础设施 XML 数字签名语法与处理规范	GB/T 25061-2010		TC260	已发布
122	8	信息安全技术 公钥基础设施 电子签名格式规范	GB/T 25064-2010		TC260	已发布
123	9	信息安全技术 公钥基础设施 签名生成应用程序的安全要求	GB/T 25065-2010		TC260	已发布

124	10	信息安全技术 公钥基础设施 证书策略与认证业务声明框架	GB/T 26855-2011		TC260	已发布
125	11	信息安全技术 公钥基础设施 PKI 互操作性评估准则	GB/T 29241-2012		TC260	已发布
126	12	信息安全技术 公钥基础设施 桥 CA 体系证书分级规范	GB/T 29767-2013		TC260	已发布
127	13	信息安全技术 公钥基础设施 标准一致性测试评价指南	GB/T 30272-2013		TC260	已发布
128	14	信息安全技术 公钥基础设施 数字证书策略分类分级规范	GB/T 31508-2015		TC260	已发布
129	15	信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范	GB/T 32213-2015		TC260	已发布
130	16	信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求	GB/T 35285-2017		TC260	已发布
131	17	信息安全技术 公钥基础设施安全技术要求	GA/T 687-2007		公安部	行业标准 公共安全
通信安全技术						
132	1	电力系统管理及其信息交换 数据和通信安全 第 1 部分：通信网络和系统安全 安全问题介绍	GB/Z 25320.1-2010	IEC TS 62351-1：2007(IDT)	TC 82	已发布
133	2	电力系统管理及其信息交换 数据和通信安全 第 2 部分：术语	GB/Z 25320.2-2013	IEC/TS 62351-2:2008(IDT)	TC 82	已发布
134	3	电力系统管理及其信息交换 数据和通信安全 第 3 部分：通信网络和系统安全 包含 TCP/IP 的协议集	GB/Z 25320.3-2010	IEC TS 62351-3:2007(IDT)	TC 82	已发布
135	4	电力系统管理及其信息交换 数据和通信安全 第 4 部分：包含 MMS 的协议集	GB/Z 25320.4-2010	IEC TS 62351-4：2007(IDT)	TC 82	已发布
136	5	电力系统管理及其信息交换 数据和通信安全 第 5 部分：GB/T 18657 等及其衍生标准的安全	GB/Z 25320.5-2013	IEC/TS 62351-5:2009(IDT)	TC 82	已发布

137	6	电力系统管理及其信息交换 数据和通信安全 第 6 部分：IEC 61850 的安全	GB/Z 25320.6-2011	IEC TS 62351-6:2007(IDT)	TC 82	已发布
138	7	电力系统管理及其信息交换 数据和通信安全 第 7 部分：网络和系统管理（NSM）的数据对象模型	GB/Z 25320.7-2015	IEC/TS 62351-7:2010(IDT)	TC 82	已发布
139	8	通信安全防护名词术语	YD/T 1765-2008		CCSA	行业标准 通信
140	9	数据网络与开放系统通信安全 端到端通信系统安全架构	YD/T 2386-2011		CCSA	行业标准 通信
141	10	软交换网络通信安全	YD/T 2253-2011		CCSA	行业标准 通信
142	11	基于 LTE 的车联网通信安全技术要求	YD/T 3594-2019		CCSA	行业标准 通信
143	12	基于 LTE 的邻近通信安全技术要求	YD/T 3697-2020		CCSA	行业标准 通信
144	13	电力系统控制及其通信数据和通信安全	DL/Z 981-2005		全国电力系统控制及其通信标准化技术委员会	行业标准 电力
（三）安全防护类标准						
设备安全						
145	1	工业互联网设备安全防护要求				待制定
146	2	工业以太网交换机安全技术要求				待制定
147	3	工业路由器设备安全技术要求				待制定
148	4	工业互联网时间敏感网络交换机安全技术要求				待制定
149	5	工业互联网无源光网络（PON）设备安全技术要求				待制定
150	6	信息技术设备 安全 第 1 部分：通用要求	GB 4943.1-2011	IEC 60950-1:2005(MOD)	工业和信息化部	已发布
151	7	信息技术设备 安全 第 22 部分：室外安装设备	GB 4943.22-2019	IEC 60950-22:2005(MOD)	工业和信息化部（电子）	已发布

152	8	信息技术设备 安全 第 23 部分：大型数据存储设备	GB 4943.23-2012	IEC 60950-23:2005(IDT)	工业和信息化部	已发布
153	9	音频、视频及类似电子设备 安全要求	GB 8898-2011	IEC 60065:2005(MOD)	工业和信息化部	已发布
154	10	电气设备的安全 人体工程的安全指南	GB/T 34137-2017		TC 25	已发布
155	11	机械安全 生产设备安全通则	GB/T 35076-2018		TC 208	已发布
156	12	机械安全 机械设备安全升级指南	GB/T 38272-2019		TC 208	已发布
157	13	信息安全技术 移动通信智能终端操作系统安全技术要求	GB/T 30284-2020		TC 260	即将实施
158	14	与通信网络电气连接的电子设备的安全	GB 38189-2019	IEC 62151:2000(IDT)	工业和信息化部（电子）	即将实施
159	15	信息安全技术 办公设备安全测试方法	GB/T 38558-2020		TC 260	即将实施
160	16	信息安全技术 智能联网设备口令保护指南	GB/T 38626-2020		TC 260	即将实施
161	17	信息安全技术 智能音视频采集设备应用安全要求	GB/T 38632-2020		TC 260	即将实施
162	18	信息安全技术 蓝牙安全指南	GB/T 38648-2020		TC 260	即将实施
163	19	国家电气设备安全技术规范	20141750-Q-469		TC 25	正在批准
164	20	电动汽车供电设备安全要求及试验规范	20150669-T-524		中国电力企业联合会	正在批准
165	21	工业电池充电设备	20091644-T-604		TC 60	正在批准
166	22	网络关键设备安全技术要求 交换机设备	20190764-T-339		TC 485	正在审查
167	23	网络关键设备安全技术要求 路由器设备	20190769-T-339		TC 485	正在审查
168	24	安全防范报警设备 安全要求和试验方法	20140174-Q-312		TC 100	正在审查
169	25	音视频、信息技术和通信技术设备 第 1 部分：安全要求	20140168-Q-339		工信部	正在审查
170	26	网络关键设备安全检测方法 交换机设备	20190765-T-339		TC 485	正在征求意见

171	27	网络关键设备安全检测方法 路由器设备	20190768-T-339		TC 485	正在征求意见
172	28	信息安全技术 云计算安全综合防御产品安全技术要求	GA/T 1527-2018		公安部	行业标准 公共安全
173	29	信息安全技术 移动智能终端安全监测产品安全技术要求	GA/T 1528-2018		公安部	行业标准 公共安全
174	30	信息安全技术 网络设备信息探测产品安全技术要求	GA/T 1543-2019		公安部	行业标准 公共安全
175	31	信息安全技术 网络及安全设备配置检查产品安全技术要求	GA/T 1545-2019		公安部	行业标准 公共安全
176	32	信息安全技术 工业控制系统主机安全防护与审计监控产品安全技术要求	GA/T 1560-2019		公安部	行业标准 公共安全
177	33	信息安全技术 工业控制系统边界安全专用网关产品安全技术要求	GA/T 1562-2019		公安部	行业标准 公共安全
178	34	信息安全技术 数据库安全加固产品安全技术要求	GA/T 1574-2019		公安部	行业标准 公共安全
179	35	信息安全技术 大数据平台安全管理产品安全技术要求	GA/T 1718-2020		公安部	行业标准 公共安全
控制系统安全						
180	1	工业互联网控制安全要求				待制定
181	2	机械安全 控制系统安全相关部件 第 1 部分：设计通则	GB/T 16855.1-2018		TC 208	已发布
182	3	机械安全 控制系统安全相关部件 第 2 部分：确认	GB/T 16855.2-2015		TC 208	已发布
183	4	工业过程测量和控制 系统评估中系统特性的评定 第 7 部分：系统安全性评估	GB/T 18272.7-2006	IEC 61069-7:1999(IDT)	TC 124	已发布

184	5	信息技术 开放系统互连 开放系统安全框架 第 3 部分: 访问控制框架	GB/T 18794.3-2003	ISO/IEC 10181-3:1996(IDT)	TC 28	已发布
185	6	电力系统安全稳定控制系统检验规范	GB/T 22384-2008		中国电力企业联合会	已发布
186	7	电力系统安全稳定控制技术导则	GB/T 26399-2011		中国电力企业联合会	已发布
187	8	工业控制系统信息安全 第 2 部分：验收规范	GB/T 30976.2-2014		TC 124	已发布
188	9	信息安全技术 工业控制系统安全控制应用指南	GB/T 32919-2016		TC 260	已发布
189	10	工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序	GB/T 33007-2016	IEC 62443-2-1:2010(IDT)	TC 124	已发布
190	11	工业自动化和控制系统网络安全 可编程序控制器（PLC） 第 1 部分：系统要求	GB/T 33008.1-2016		TC 124	已发布
191	12	工业自动化和控制系统网络安全 集散控制系统（DCS）第 1 部分：防护要求	GB/T 33009.1-2016		TC 124	已发布
192	13	工业自动化和控制系统网络安全 集散控制系统（DCS）第 2 部分：管理要求	GB/T 33009.2-2016		TC 124	已发布
193	14	工业自动化和控制系统网络安全 集散控制系统（DCS）第 3 部分：评估指南	GB/T 33009.3-2016		TC 124	已发布
194	15	工业自动化和控制系统网络安全 集散控制系统（DCS）第 4 部分：风险与脆弱性检测要求	GB/T 33009.4-2016		TC 124	已发布
195	16	控制与通信网络 CIP Safety 规范	GB/Z 34066-2017		TC 124	已发布
196	17	控制与通信网络 Safety-over-EtherCAT 规范	GB/T 36006-2018	IEC 61784-3-12：2010(IDT)	TC 124	已发布
197	18	信息安全技术 工业控制系统安全管理基本要求	GB/T 36323-2018		TC 260	已发布

198	19	信息安全技术 工业控制系统信息安全分级规范	GB/T 36324-2018		TC 260	已发布
199	20	信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求	GB/T 37934-2019		TC 260	已发布
200	21	信息安全技术 工业控制网络监测安全技术要求及测试评价方法	GB/T 37953-2019		TC 260	已发布
201	22	信息安全技术 数控网络安全技术要求	GB/T 37955-2019		TC 260	已发布
202	23	信息安全技术 工业控制系统安全检查指南	GB/T 37980-2019		TC 260	已发布
203	24	信息安全技术 移动通信智能终端操作系统安全技术要求	GB/T 30284-2020		TC 260	即将实施
204	25	工业机器人力控制技术规范	GB/T 38559-2020		TC 159	即将实施
205	26	工业互联网标识体系 Ecode 标识系统安全机制	GB/T 38660-2020		TC 287	即将实施
206	27	工业过程测量控制和自动化 系统评估中系统特性的评定 第 1 部分：术语和基本概念	GB/T 38852.1-2020		TC 124	即将实施
207	28	工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术	20170374-T-604		TC 124	正在批准
208	29	信息安全技术 系统安全工程 能力成熟度模型	20193258-T-469		TC 260	正在批准
209	30	信息安全技术 工业控制系统安全防护技术要求和测试评价方法	20171744-T-469		TC 260	正在审查
210	31	电力系统安全稳定控制策略描述规范	20184611-T-524		TC 446	正在征求意见
211	32	信息安全技术 信息系统等级保护安全设计技术要求 第 5 部分：工业控制系统	20171111-T-469		TC 260	正在起草
212	33	工业控制系统产品信息安全 第 2 部分：安全功能要求	20171279-T-469		TC 260	正在起草
213	34	工业控制系统产品信息安全 第 3 部分：安全保障要求	20171280-T-469		TC 260	正在起草
214	35	工业过程控制系统用时间比例控制器性能评定方法	JB/T 8221-2014		全国工业过程测量和控制标	行业标准 机械

					准化技术委员会	
215	36	工业过程测量和控制安全 网络和系统安全	JB/T 11960-2014		全国工业过程测量和控制标准化技术委员会	行业标准 机械
216	37	工业通信网络 网络和系统安全 术语、概念和模型	JB/T 11961-2014		全国工业过程测量和控制标准化技术委员会	行业标准 机械
217	38	工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术	JB/T 11962-2014		全国工业过程测量和控制标准化技术委员会	行业标准 机械
218	39	电力系统安全稳定控制技术导则	DL/T 723-2000		国家经济贸易委员会	行业标准 电力
219	40	电力系统安全稳定控制系统通用技术条件	DL/T 1092-2008		电力行业继电保护标准化技术委员会	行业标准 电力
220	41	信息安全技术 工业控制系统安全管理平台安全技术要求	GA/T 1350-2017		公安部	行业标准 公共安全
221	42	信息安全技术 网络安全等级保护基本要求 第 5 部分：工业控制系统安全扩展要求	GA/T 1390.5-2017		公安部	行业标准 公共安全
222	43	油气输送管道监控与数据采集（SCADA）系统安全防护规范	SY/T 7037-2016		国家能源局	行业标准 石油天然气

网络安全						
223	1	信息安全技术 网络安全等级保护基本要求	GB/T 22239-2019		TC 260	已发布
224	2	信息安全技术 网络安全等级保护实施指南	GB/T 25058-2019		TC 260	已发布
225	3	信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理	GB/T 25068.1-2012	ISO/IEC 18028-1:2006(IDT)	TC 260	已发布
226	4	信息技术 安全技术 IT 网络安全 第 2 部分：网络安全体系结构	GB/T 25068.2-2012	ISO/IEC 18028-2:2006(IDT)	TC 260	已发布
227	5	信息技术 安全技术 IT 网络安全 第 3 部分：使用安全网关的网间通信安全保护	GB/T 25068.3-2010	ISO/IEC 18028-3:2005(IDT)	TC 260	已发布
228	6	信息技术 安全技术 IT 网络安全 第 4 部分：远程接入的安全保护	GB/T 25068.4-2010	ISO/IEC 18028-4:2005(IDT)	TC 260	已发布
229	7	信息技术 安全技术 IT 网络安全 第 5 部分：使用虚拟专用网的跨网通信安全保护	GB/T 25068.5-2010	ISO/IEC 18028-5:2006(IDT)	TC 260	已发布
230	8	信息安全技术 网络安全等级保护安全设计技术要求	GB/T 25070-2019		TC 260	已发布
231	9	工业控制网络安全风险评估规范	GB/T 26333-2010		TC 124	已发布
232	10	信息安全技术 网络安全等级保护测评要求	GB/T 28448-2019		TC 260	已发布
233	11	信息安全技术 网络安全等级保护测评过程指南	GB/T 28449-2018		TC 260	已发布
234	12	网络安全事件描述和交换格式	GB/T 28517-2012		工业和信息化部（通信）	已发布
235	13	信息安全技术 网络安全预警指南	GB/T 32924-2016		TC 260	已发布
236	14	信息安全技术 基于 IPSec 的 IP 存储网络安全技术要求	GB/T 33131-2016		TC 260	已发布
237	15	电力监控系统网络安全防护导则	GB/T 36572-2018		TC 82	已发布
238	16	信息安全技术 网络安全等级保护测试评估技术指南	GB/T 36627-2018		TC 260	已发布
239	17	信息安全技术 网络安全监测基本要求与实施指南	GB/T 36635-2018		TC 260	已发布

240	18	信息安全技术 网络安全威胁信息格式规范	GB/T 36643-2018		TC 260	已发布
241	19	电力监控系统网络安全评估指南	GB/T 38318-2019		TC 82	已发布
242	20	信息安全技术 网络安全等级保护定级指南	GB/T 22240-2020		TC 260	即将实施
243	21	信息安全技术 网络安全管理支撑系统技术要求	GB/T 38561-2020		TC 260	即将实施
244	22	信息安全技术 汽车电子系统网络安全指南	GB/T 38628-2020		TC 260	即将实施
245	23	信息安全技术 网络安全事件应急演练指南	GB/T 38645-2020		TC 260	即将实施
246	24	信息安全技术 重要工业控制系统网络安全防护导则	20121629-T-524		TC 260	正在批准
247	25	信息安全技术 关键信息基础设施网络安全保护基本要求	20173585-T-469		TC 260	正在批准
248	26	信息技术 安全技术 网络安全 第 1 部分：综述和概念	20173861-T-469	ISO/IEC 27033-1:2015(IDT)	TC 260	正在批准
249	27	信息技术 安全技术 网络安全 第 2 部分：网络安全设计和实现指南	20173860-T-469	ISO/IEC 27033-2:2012(IDT)	TC 260	正在批准
250	28	信息技术 安全技术 网络安全 第 5 部分：使用虚拟专用网的跨网通信安全保护	20152013-T-469	ISO/IEC 27033-5:2013(MOD)	TC 260	正在批准
251	29	信息安全技术 网络安全漏洞分类分级指南	20190906-T-469		TC 260	正在批准
252	30	信息安全技术 网络安全漏洞标识与描述规范	20190910-T-469		TC 260	正在批准
253	31	信息安全技术 网络安全漏洞管理规范	20190912-T-469		TC 260	正在批准
254	32	信息技术 安全技术 网络安全 第 3 部分：参考网络场景——风险、设计技术和控制要素	20201688-T-469	ISO/IEC 27033-3:2010	TC 260	正在征求意见
255	33	信息技术 安全技术 网络安全 第 4 部分：使用安全网关的网间通信安全保护	20201689-T-469	ISO/IEC 27033-4:2014(IDT)	TC 260	正在征求意见
256	34	关键信息基础设施网络安全框架	20160645-T-469		TC 260	正在起草
257	35	信息安全技术 网络安全漏洞发现与报告管理指南	20173859-T-469		TC 260	正在起草
258	36	信息安全技术 网络安全专用产品安全技术要求	20201946-Q-312		公安部	正在起草

259	37	国家网络安全应急处理平台安全信息获取接口要求	YD/T 2251-2011		CCSA	行业标准 通信
260	38	网络安全监控系统技术要求	YD/T 2387-2011		CCSA	行业标准 通信
261	39	IP 存储网络安全技术要求	YD/T 2391-2011		CCSA	行业标准 通信
262	40	IP 存储网络安全测试方法	YD/T 2392-2011		CCSA	行业标准 通信
263	41	LTE 无线网络安全网关技术要求	YD/T 2853-2015		工业和信息化部	行业标准 通信
264	42	LTE 无线网络安全网关测试方法	YD/T 2874-2015		工业和信息化部	行业标准 通信
265	43	SDN 网络安全能力要求	YD/T 3489-2019		CCSA	行业标准 通信
266	44	SDN 网络安全能力检测要求	YD/T 3490-2019		CCSA	行业标准 通信
267	45	工业互联网 网络安全总体要求	2017-0960T-YD		CCSA	行业标准 通信
268	46	工业互联网 安全接入技术要求	2018-0179T-YD		CCSA	行业标准 通信
269	47	工业互联网工厂内安全接入要求	待制定		CCSA	行业标准 通信
270	48	信息安全技术 网络安全等级保护专用知识库接口规范	GA/T 1349-2017		公安部	行业标准 公共安全
271	49	信息安全技术 网络安全事件通报预警 第 1 部分：术语	GA/T 1717.1-2020		公安部	行业标准 公共安全
272	50	信息安全技术 网络安全事件通报预警 第 2 部分：通报预警流程规范	GA/T 1717.2-2020		公安部	行业标准 公共安全
273	51	信息安全技术 网络安全事件通报预警 第 3 部分：数据分类编码与标记标签技术体系技术规范	GA/T 1717.3-2020		公安部	行业标准 公共安全
274	52	电力 LTE 无线通信网络安全防护要求	DL/T 1931-2018		中国电力企业联合会	行业标准 电力

275	53	可再生能源发电站电力监控系统网络安全防护技术规范	DL/T 1941-2018		中国电力企业联合会	行业标准 电力
276	54	烟草行业工业控制系统网络安全基线技术规范	YC/T 580—2019		国家烟草专卖局	行业标准 烟草
平台安全						
277	1	信息安全技术 工业互联网平台安全要求及评估规范				待制定
278	2	工业互联网平台 安全接入风险分析及技术要求				待制定
279	3	工业互联网平台 安全防护检测要求				待制定
280	4	工业互联网平台 安全风险评估规范				待制定
281	5	工业互联网平台 安全防护要求				待制定
282	6	工业互联网平台 安全防护能力评估规范				待制定
283	7	信息安全技术 可信计算密码支撑平台功能与接口规范	GB/T 29829-2013		TC 260	已发布
284	8	电能服务管理平台技术规范 第 5 部分：安全防护规范	GB/T 31991.5-2015		中国电力企业联合会	已发布
285	9	信息安全技术 信息系统安全管理平台技术要求和测试评价方法	GB/T 34990-2017		TC 260	已发布
286	10	信息安全技术 可信计算规范 服务器可信支撑平台	GB/T 36639-2018		TC 260	已发布
287	11	信息安全技术 移动终端安全管理平台技术要求	GB/T 37952-2019		TC 260	已发布
288	12	信息安全技术 网站安全云防护平台技术要求	GB/T 37956-2019		TC 260	已发布
289	13	信息安全技术 蓝牙安全指南	GB/T 38648-2020		TC 260	即将实施
290	14	电子商务数据交易平台 数据接口规范	20154004-T-469		TC 83	正在批准
291	15	工业机器人云服务平台数据交换	20170044-T-604		TC 159	正在批准
292	16	云制造服务平台制造资源接入集成规范	20173695-T-604		TC 159	正在批准
293	17	云制造服务平台安全防护管理要求	20173696-T-604		TC 159	正在批准

294	18	工业机器人可编程控制器软件开发平台程序的 XML 交互规范	20184690-T-604		TC 159	正在批准
295	19	工业机器人云服务平台分类及参考体系结构	20194034-T-604		TC 159	正在批准
296	20	工业互联网 信息共享和交换平台通用要求	20174080-T-469		TC 28	正在审查
297	21	移动通信网络面向物流信息服务的 M2M 平台测试方法	20192074-T-339		TC 485	正在审查
298	22	智慧城市 设备联接管理与服务平台技术要求	20181813-T-469		TC 28	正在征求意见
299	23	信息安全技术 可信计算规范 可信平台控制模块	20192182-T-469		TC 260	正在征求意见
300	24	信息安全技术 可信计算密码支撑平台功能与接口规范	20201695-T-469		TC 260	正在征求意见
301	25	能源互联网数据平台技术规范	20160504-T-524		中国电力企业联合会	正在起草
302	26	智能制造 工业大数据平台通用要求	20182053-T-339		工业和信息化部（电子）	正在起草
303	27	自动化系统与集成 科技资源云平台集成通用要求	20192971-T-604		TC 159	正在起草
304	28	基于工业云平台的个性化定制实施规范	20193187-T-469		TC 28	正在起草
305	29	智能制造 工业技术软件化 工程中间件平台通用要求	20193193-T-469		TC 28	正在起草
306	30	公共安全视频图像共享交换平台技术要求	20202602-T-312		TC 100	正在起草
307	31	公安交通管理综合应用平台安全保护通用技术要求	GA/T 1168-2014		公安部	行业标准 公共安全
308	32	信息安全技术 工业控制系统安全管理平台安全技术要求	GA/T 1350-2017		公安部	行业标准 公共安全
309	33	信息安全技术 智能卡开放平台安全技术要求	GA/T 1526-2018		公安部	行业标准 公共安全
310	34	信息安全技术 大数据平台安全管理产品安全技术要求	GA/T 1718-2020		公安部	行业标准 公共安全

311	35	国家网络安全应急处理平台安全信息获取接口要求	YD/T 2251-2011		CCSA	行业标准 通信
312	36	公有云服务平台安全运维管理要求	YD/T 3671-2020		CCSA	行业标准 通信
应用程序安全						
313	1	工业 APP 安全防护要求				待制定
314	2	工业 APP 安全检测要求				待制定
315	3	工业互联网 工业安全 APP 技术要求				待制定
316	4	信息安全技术 公钥基础设施 签名生成应用程序的安全要求	GB/T 25065-2010		TC 260	已发布
317	5	信息安全技术 鉴别与授权 授权应用程序判定接口规范	GB/T 31501-2015		TC 260	已发布
318	6	信息技术 云计算 平台即服务（PaaS）应用程序管理要求	GB/T 36327-2018		TC 28	已发布
319	7	民用航空移动应用程序安全测评指南	MH/T 0068-2018		中国民航科学技术研究院	行业标准 民用航空
320	8	移动终端设备应用程序开放接口技术要求	YD/T 2743-2014		CCSA	行业标准 通信
321	9	移动互联网应用程序安全加固能力评估要求与测试方法	YD/T 3474-2019		CCSA	行业标准 通信
322	10	基于安卓系统的移动应用程序第三方数字签名技术要求	YD/T 3524-2019		CCSA	行业标准 通信
323	11	移动应用程序代码签名技术要求	YD/T 3646-2020		CCSA	行业标准 通信
324	12	移动应用程序代码签名测试方法	YD/T 3647-2020		CCSA	行业标准 通信
325	13	电子产品安全性名词术语	SJ/T 10720-1996		电子工业部	行业标准 电子
326	14	手持式个人信息处理设备中文应用程序接口规范	SJ/T 11229-2001		信息产业部	行业标准 电子
327	15	集成电路卡通用规范 第 6 部分：安全规范	SJ/T 11232-2001		信息产业部	行业标准 电子
328	16	电子设备的安全	SJ/Z 11266-2002		信息产业部	行业标准 电子
数据安全						

329	1	工业互联网 数据分级技术要求				待制定
330	2	工业互联网 工厂内数据安全防护要求				待制定
331	3	智能交通 数据安全服务	GB/T 37373-2019		TC 268	已发布
332	4	信息安全技术 大数据安全管理指南	GB/T 37973-2019		TC 260	已发布
333	5	信息安全技术 数据安全能力成熟度模型	GB/T 37988-2019		TC 260	已发布
334	6	信息安全技术 政务信息共享 数据安全技术要求	20190907-T-469		TC 260	正在批准
335	7	信息安全技术 健康医疗数据安全指南	20193254-T-469		TC 260	正在审查
336	8	信息安全技术 电信领域大数据安全防护实现指南	20202621-T-469		TC 260	正在起草
337	9	银行卡联网联合技术规范 第 4 部分：数据安全传输控制	JR/T 0055.4-2009		全国金融标准化技术委员会	行业标准 金融
338	10	互联网码号资源公钥基础设施（RPKI）安全运行技术要求 数据安全威胁模型	YD/T 3458-2019		CCSA	行业标准 通信
339	11	面向公有云服务的文件数据安全标记规范	YD/T 3470-2019		CCSA	行业标准 通信
340	12	面向互联网的数据安全能力技术框架	YD/T 3644-2020		CCSA	行业标准 通信
341	13	工业互联网 数据安全保护要求	2018-1369T-YD		CCSA	行业标准 通信
（四）安全管理与服务类标准						
管理能力评估						
342	1	信息安全技术 信息系统安全管理要求	GB/T 20269-2006		TC 260	已发布
343	2	信息技术 安全技术 信息安全管理体系 要求	GB/T 22080-2016	ISO/IEC 27001:2013(IDT)	TC 260	已发布
344	3	信息安全技术 信息安全管理体系审核指南	GB/T 28450-2012		TC 260	已发布
345	4	信息安全技术 信息系统安全管理评估要求	GB/T 28453-2012		TC 260	已发布

346	5	信息技术 安全技术 信息安全管理体系 概述和词汇	GB/T 29246-2017	ISO/IEC 27000:2016（IDT）	TC 260	已发布
347	6	信息技术 安全技术 信息安全管理体系审核和认证机构要求	GB/T 25067-2016	ISO/IEC 27006:2011（IDT）	TC 260	已发布
348	7	信息技术 安全技术 信息安全管理体系实施指南	GB/T 31496-2015	ISO/IEC 27003:2010（IDT）	TC 260	已发布
349	8	信息技术 安全技术 行业间和组织间通信的信息安全管理	GB/T 32920-2016	ISO/IEC 27010:2012（IDT）	TC 260	已发布
350	9	信息安全技术 信息系统安全管理平台技术要求和测试评价方法	GB/T 34990-2017		TC 260	已发布
351	10	信息安全技术 工业控制系统安全管理基本要求	GB/T 36323-2018		TC 260	已发布
352	11	信息安全技术 办公信息系统安全管理要求	GB/T 37094-2018		TC 260	已发布
353	12	信息安全技术 移动终端安全管理平台技术要求	GB/T 37952-2019		TC 260	已发布
354	13	信息安全技术 大数据安全管理指南	GB/T 37973-2019		TC 260	已发布
355	14	供应链安全管理体系 对供应链安全管理体系审核认证机构的要求	GB/T 38701-2020	ISO 28003:2007(IDT)	TC 351	已发布
356	15	信息技术 安全技术 信息安全管理体系审核和认证机构要求	GB/T 25067-2020	ISO/IEC 27006:2015(IDT)	TC 260	即将实施
357	16	信息技术 安全技术 信息安全管理体系审核指南	20190913-T-469	ISO/IEC 27007：2017(IDT)	TC 260	正在批准

358	17	供应链安全管理体系 ISO 28000 实施指南	20081194-T-469	ISO 28004:2007(IDT)	TC 351	正在审查
359	18	食品安全管理体系 审核与认证机构要求	20171122-T-469	ISO/TS 22003:2013(IDT)	TC 313	正在审查
360	19	《信息安全技术 政府部门信息安全管理基本要求》补篇:信息安全管理制度参考模板	20130319-T-469		TC 260	正在起草
361	20	公安工业互联网前端感知汇聚节点安全管理与远程维护技术要求	20130092-T-312		公安部	正在起草
362	21	食品安全管理体系要求	SN/T 1443.1-2004		国家认证认可监督管理委员会	行业标准 出入境检验检疫
363	22	食品安全管理体系审核指南	SN/T 1443.2-2004		国家认证认可监督管理委员会	行业标准 出入境检验检疫
364	23	城市轨道交通消防安全管理	GA/T 579-2005		公安部	行业标准 公共安全
365	24	信息安全技术 移动终端安全管理与接入控制产品安全技术要求	GA/T 1455-2018		公安部	行业标准 公共安全
服务能力认证						
366	1	信息安全技术 信息安全服务能力评估准则	GB/T 30271-2013		TC 260	已发布
367	2	信息安全技术 信息安全服务 分类	GB/T 30283-2013		TC 260	已发布
368	3	信息安全技术 云计算服务安全指南	GB/T 31167-2014		TC 260	已发布
369	4	信息安全技术 云计算服务安全能力要求	GB/T 31168-2014		TC 260	已发布
370	5	信息安全技术 信息安全服务提供方管理要求	GB/T 32914-2016		TC 260	已发布

371	6	信息安全技术 公共域名服务系统安全要求	GB/T 33134-2016		TC 260	已发布
372	7	信息安全技术 云计算服务安全能力评估方法	GB/T 34942-2017		TC 260	已发布
373	8	信息安全技术 大数据服务安全能力要求	GB/T 35274-2017		TC 260	已发布
374	9	信息安全技术 电子认证服务机构服务质量规范	GB/T 35289-2017		TC 260	已发布
375	10	信息安全技术 金融信息服务安全规范	GB/T 36618-2018		TC 260	已发布
376	11	信息安全技术 灾难恢复服务能力评估准则	GB/T 37046-2018		TC 260	已发布
377	12	基于云计算的电子政务公共平台安全规范 第 3 部分：服务安全	20132190-T-339		TC 485	正在批准
378	13	云制造服务平台安全防护管理要求	20173696-T-604		TC 159	正在批准
379	14	信息安全技术 网络产品和服务安全通用要求	20193257-T-469		TC 260	正在批准
380	15	信息技术服务 服务安全要求	20171070-T-469		TC 28	正在审查
381	16	信息技术 工业云服务 服务协议指南	20173827-T-469		TC 28	正在审查
382	17	信息安全技术 信息安全服务 分类	20201691-T-469		TC 260	正在征求意见
383	18	信息安全技术 云计算服务安全能力要求	20201692-T-469		TC 260	正在征求意见
384	19	信息安全技术 云计算服务安全指南	20201693-T-469		TC 260	正在征求意见
385	20	信息安全技术 电子凭据服务安全要求与测评方法	20202598-T-469		TC 260	正在征求意见
386	21	信息安全技术 互联网信息服务安全通用要求	20202619-T-469		TC 260	正在征求意见
387	22	信息安全技术 互联网服务安全评估基本程序及要求	GA 1278-2015		公安部	行业标准 公共安全
388	23	电信网和互联网第三方安全服务能力评定准则	YD/T 2669-2013		CCSA	行业标准 通信
389	24	电信信息服务的安全准则	YD/T 2704-2014		CCSA	行业标准 通信
390	25	公有云服务安全防护要求	YD/T 3157-2016		CCSA	行业标准 通信
391	26	公有云服务安全防护检测要求	YD/T 3158-2016		CCSA	行业标准 通信

392	27	互联网接入服务系统安全防护要求	YD/T 3159-2016		CCSA	行业标准 通信
393	28	互联网接入服务系统安全防护检测要求	YD/T 3160-2016		CCSA	行业标准 通信
394	29	电信网和互联网安全服务实施要求	YD/T 3315-2018		CCSA	行业标准 通信
395	30	公有云服务安全运营技术要求	YD/T 3471-2019		CCSA	行业标准 通信
396	31	公有云服务平台安全运维管理要求	YD/T 3671-2020		CCSA	行业标准 通信
397	32	信息技术服务 服务管理 技术要求	SJ/T 11435-2015		工信部电子工业标准化研究院	行业标准 电子
398	33	信息技术服务 服务级别协议指南	SJ/T 11691-2017		全国信息技术标准化技术委员会	行业标准 电子
安全风险评估						
399	1	机械安全 风险评估 实施指南和方法举例	GB/T 16856-2015	ISO/TR 14121-2:2012。(MOD)	TC 208	已发布
400	2	信息安全技术 信息安全风险评估规范	GB/T 20984-2007		TC 260	已发布
401	3	电气设备的安全 风险评估和风险降低 第 2 部分：风险分析和风险评价	GB/T 22696.2-2008		TC 25	已发布
402	4	电气设备的安全 风险评估和风险降低 第 3 部分：危险、危险处境和危险事件的示例	GB/T 22696.3-2008		TC 25	已发布
403	5	电气设备的安全 风险评估和风险降低 第 5 部分：风险评估和降低风险的方法示例	GB/T 22696.5-2011		TC 25	已发布
404	6	工业控制网络安全风险评估规范	GB/T 26333-2010		TC 124	已发布
405	7	风险管理 风险评估技术	GB/T 27921-2011		TC 310	已发布
406	8	信息安全技术 信息安全风险评估实施指南	GB/T 31509-2015		TC 260	已发布

407	9	汽车产品安全 风险评估与风险控制指南	GB/T 34402-2017		TC 463	已发布
408	10	信息安全技术 工业控制系统风险评估实施指南	GB/T 36466-2018		TC 260	已发布
409	11	信息安全技术 信息安全风险评估规范	20173857-T-469		TC 260	正在审查
410	12	金融信息系统网络安全风险评估规范	20193363-T-320		TC 180	正在起草
411	13	网络与信息安全风险评估服务能力评估方法	YD/T 2252-2011		CCSA	行业标准 通信
412	14	移动通信智能终端安全风险评估要求	YD/T 3663-2020		CCSA	行业标准 通信
413	15	金融行业信息安全等级保护测评服务安全指引	JR/T 0073-2012		全国金融标准化 技术委员会	行业标准 金融
414	16	海关信息系统信息安全风险评估规范	HS/T 28-2010		海关总署	行业标准 海关
415	17	交通运输信息系统安全风险评估指南	JT/T 1275—2019		交通运输部	行业标准 交通
安全态势感知						
暂无相关标准发布						
产品检测认证						
416	1	信息安全技术 服务器安全测评要求	GB/T 25063-2010		TC 260	已发布
417	2	面向制造业信息化的 ASP 平台测评规范	GB/T 25459-2010		TC 159	已发布
418	3	信息安全技术 网络安全等级保护测评要求	GB/T 28448-2019		TC 260	已发布
419	4	信息安全技术 网络安全等级保护测评过程指南	GB/T 28449-2018		TC 260	已发布
420	5	信息安全技术 智能卡通用安全检测指南	GB/T 31507-2015		TC 260	已发布
421	6	信息安全技术 信息技术产品安全检测机构条件和行为准则	GB/T 35280-2017		TC 260	已发布
422	7	信息安全技术 网络安全等级保护测评机构能力要求和评估规范	GB/T 36959-2018		TC 260	已发布
423	8	信息安全技术 密码模块安全检测要求	GB/T 38625-2020	ISO/IEC 24759:2017(NEQ)	TC 260	即将实施

424	9	网络关键设备安全检测方法 交换机设备	20190765-T-339		TC 485	正在征求意见
425	10	网络关键设备安全检测方法 路由器设备	20190768-T-339		TC 485	正在征求意见
426	11	信息安全技术 服务器安全技术要求和测评准则	20190908-T-469		TC 260	正在征求意见
427	12	信息安全技术 电子凭据服务安全要求与测评方法	20202598-T-469		TC 260	正在征求意见
428	13	电力系统控制类软件安全性及其测评技术要求	DL/T 1455-2015		中国电力企业联合会	行业标准 电力
429	14	信息安全技术 信息系统安全管理测评	GA/T 713-2007		公安部	行业标准 公共安全
430	15	信息安全技术 计算机主机安全检测产品测评准则	GA/T 1536-2018		公安部	行业标准 公共安全
431	16	信息安全技术 企业移动终端安全管理产品测评准则	GA/T 1538-2018		公安部	行业标准 公共安全
432	17	信息安全技术 个人移动终端安全管理产品测评准则	GA/T 1540-2018		公安部	行业标准 公共安全
433	18	密码模块安全检测要求	GM/T 0039-2015		密码行业标准化技术委员会	行业标准 国密
434	19	金融行业信息系统信息安全等级保护测评指南	JR/T 0072-2012		全国金融标准化技术委员会	行业标准 金融
435	20	金融行业信息安全等级保护测评服务安全指引	JR/T 0073-2012		全国金融标准化技术委员会	行业标准 金融
436	21	民航 Web 应用系统安全检测指南	MH/T 0067-2018		中国民航科学技术研究院	行业标准 民用航空
（五）垂直行业类标准						
汽车						

437	1	电动汽车 安全要求 第 1 部分：车载可充电储能系统(REESS)	GB/T 18384.1-2015		TC 114	已发布
438	2	电动汽车 安全要求 第 2 部分：操作安全和故障防护	GB/T 18384.2-2015		TC 114	已发布
439	3	电动汽车 安全要求 第 3 部分：人员触电防护	GB/T 18384.3-2015		TC 114	已发布
440	4	燃料电池电动汽车 安全要求	GB/T 24549-2009		TC 114	已发布
441	5	电动汽车用锂离子动力蓄电池包和系统 第 3 部分：安全性要求与测试方法	GB/T 31467.3-2015		TC 114	已发布
442	6	电动汽车用动力蓄电池安全要求及试验方法	GB/T 31485-2015		TC 114	已发布
443	7	电动汽车碰撞后安全要求	GB/T 31498-2015		TC 114	已发布
444	8	汽车产品安全 风险评估与风险控制指南	GB/T 34402-2017		TC 463	已发布
445	9	汽车车轮安全性能要求及试验方法	GB 36581-2018		工业和信息化部	已发布
446	10	电动汽车安全要求	GB 18384-2020		工业和信息化部	即将实施
447	11	电动汽车用动力蓄电池安全要求	GB 38031-2020		工业和信息化部	即将实施
448	12	信息安全技术 汽车电子系统网络安全指南	GB/T 38628-2020		TC 260	即将实施
449	13	汽车爆胎应急安全装置性能要求和试验方法	GB/T 38796-2020		TC 114	即将实施
450	14	燃料电池电动汽车 安全要求	20140520-T-339		TC 114	正在批准
451	15	汽车信息安全通用技术要求	20191065-T-339		TC 114	正在审查
452	16	电动汽车远程服务与管理系统信息安全技术要求	20191066-T-339		TC 114	正在审查
453	17	汽车网关信息安全技术要求	20191070-T-339		TC 114	正在审查
454	18	电动汽车碰撞后安全要求	20192311-T-339		TC 114	正在征求意见
455	19	电动汽车 与外部电源连接的安全要求	20162653-T-339		TC 114	正在起草

456	20	家用汽车产品严重安全性能故障判断指南	20173998-T-469		TC 463	正在起草
457	21	电动汽车充电系统信息安全技术要求	20192313-T-339		TC 114	正在起草
石油化工						
458	1	化工行业能源管理体系实施指南	GB/T 38899-2020		TC 20	即将实施
459	2	化工园区综合评价导则	GB/T 39217-2020		TC 251	即将实施
460	3	智慧化工园区建设指南	20184447-T-469		TC 251	正在批准
461	4	港口石油化工库区作业安全规程	20173656-Q-348		TC 530	正在征求意见
462	5	油气化工码头作业安全规程	20173657-Q-348		交通运输部	正在征求意见
463	6	石油机械制造企业安全生产规范	SY 5445-2017		石油工业安全专业标准化委员会	行业标准 石油天然气
机械制造						
464	1	机械安全 安全防护的实施准则	20194254-T-469		TC 208	正在起草
465	2	机械安全 安全控制系统设计指南	20201657-T-469		TC 208	正在起草
466	3	机械制造企业安全生产标准化规范	AQ/T 7009-2013		全国安全生产标准化技术委员会	行业标准 安全生产
航空航天						
467	1	航天器安全防护通用要求	GB/T 37833-2019		TC 425	已发布
468	2	航天控制工程通用要求	20184488-T-469		TC 425	正在征求意见
469	3	民用航空信息安全事件分类分级指南	MH/T 0041-2013		中国民航科学技术研究院	行业标准 民用航空
470	4	民用航空信息系统安全等级保护实施指南	MH/T 0051-2015		中国民航科学技术研究院	行业标准 民用航空

471	5	民用航空移动应用程序安全测评指南	MH/T 0068-2018		中国民航科学技术研究院	行业标准 民用航空
472	6	民用航空网络安全等级保护定级指南	MH/T 0069-2018		中国民航科学技术研究院	行业标准 民用航空
473	7	民用航空空中交通管理信息系统技术规范 第 2 部分：系统与网络安全	MH/T 4018.2-2004		中国民航科学技术研究院	行业标准 民用航空
474	8	民用航空空中交通管理管理信息系统技术规范 第 7 部分：数据安全	MH/T 4018.7-2012		中国民航科学技术研究院	行业标准 民用航空
电子信息						
475	1	电子信息产品中有毒有害物质的限量要求	SJ/T 11363-2006		中国电子技术标准化研究所	行业标准 电子
476	2	电子信息产品污染控制标识要求	SJ/T 11364-2006		中国电子技术标准化研究所	行业标准 电子
477	3	电子信息产品中有毒有害物质的检测方法	SJ/T 11365-2006		中国电子技术标准化研究所	行业标准 电子
478	4	电子信息行业安全生产标准化评价方法	SJ/T 11442-2012		工信部电子工业标准化研究所	行业标准 电子
479	5	电子信息行业外场及其他临时场所危险作业分类	SJ/T 11443-2012		工信部电子工业标准化研究所	行业标准 电子
480	6	电子信息行业危险源辨识、风险评价和风险控制要求	SJ/T 11444-2012		工信部电子工业标准化研究所	行业标准 电子

附录 2：深圳市龙头标杆企业在工业互联网中的应用实践及标准制定情况

一、华为技术有限公司：5G 让工业互联网成为现实

华为基于 30 年 ICT 技术积累和制造经验打造的工业互联网平台 FusionPlant 为工业互联网引入了三项关键技术：5G、AI、鲲鹏云服务。

5G 在华为云 FusionPlant 联接管理平台中发挥了重要作用，实现产业链上的各个价值要素的互联互通，满足工业领域实时性场景要求。联接产生的大量数据汇聚到华为云，发挥全栈全场景 AI 的领先优势，华为云工业智能体在云上进行模型的大规模训练后，将模型下发到边侧进行推理，极大满足工业企业时延和安全上的要求。工业应用上云需要强大的计算平台的支撑，华为云鲲鹏计算服务为工业应用提供了自主创新的异构算力，全方位赋能工业应用的开发、部署、运行、聚合、集成等各环节。

在华为松山湖生产线，传统测试生产线是半自动化作业，有些环节需要人工参与，例如人力插拔网线，不仅受线缆约束无法流动加工，而且面临着生产效率低、无法满足多产线并行需求等多种问题。有了 5G 的加持，可以实现无线测试，开启全自动化生产模式，测试端产能从 800 片/天的产能提升到 1000 片/天。

安全标准化工作：

华为不仅在公司内部建立成熟高效的安全可信体系，同时积极参与国家、行业安全标准制定工作，至今为止，华为已经参与 TC 28、TC260 等数十个国内外标准组织，支持主流国家标准，至今参与国内外近百项安全相关的标准制修订，涉及云计算、云存储、数据传输、大数据、AI 技术以及音视频解码等技术领域，涵盖公安、交通、园区等行业，贯穿智能安防端到端的产品。

云计算方面：华为先后参与了《信息安全技术可信计算规范 服务器可信支撑平台》、《信息安全技术 云计算安全参考架构》、《信息安全技术 服务器安全技术要求和测评准则》等云计算、云存储、可信服务器领域多个国家标准制定。

《信息安全技术 云计算服务安全指南》、《信息安全技术 云计算服务安全能力要求》（华为云参与制定首批云安全国家标准，获中国标准创新贡献奖）

大数据方面：华为先后参与 GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》、《信息安全技术 数据安全能力成熟度模型》等多个大数据安全标准的编写工作，当前正积极投入《公安大数据安全 总体技术框架》、《公安大数据安全 安全访问平台技术设计要求》、《公安大数据安全 云平台安全技术要求》等公安部大数据标准编写工作中。

二、腾讯科技（深圳）有限公司：在工业互联网领域打造“新基建”样本

腾讯的新基建布局正在加速落地。今年 3 月份，腾讯联合深圳宝安区打造的工业互联网特色产业示范基地，入选第九批“国家新型工业化产业示范基地”，这也是深圳第 4 个国家工业化产业示范基地。

基于工业互联网特色产业示范基地，接下来腾讯将联合宝安区、生态伙伴搭建工业互联网平台，围绕消费类电子、新材料等产业链全面助力提升产业链数字化水平。

在垂直行业领域，腾讯与富士康、三一重工等领军企业深度合作，并协助企业推出了各自的工业互联网平台，一方面满足集团内部集约化管理和服务，实现 IT 基础资源弹性伸缩、工业软件服务共享、软件开发敏捷化、数据互联互通、业务场景创新等，另一方面行业领头羊企业面向产业链上下游中小企业输出自身的工业互联网服务，助力中小企业。

从区域方向上，腾讯积极配合地方政府及工业互联网主管部门，重点发展与当地产业深度结合的区域工业互联网平台，采用 1+N 的搭建方式，1 代表一套云计算基础设施，N 代表多个行业工业互联网平台，全面支撑当地产业的转型升级。目前，腾讯联合产业生态合作伙伴已在烟台、德州、张家港、西安等地落地工业云基地，并搭建了区域工业互联网平台。2020 年，腾讯还将落地 10 家以上的工业云基地，将腾讯的技术和生态开放给广大的中小企业。

腾讯认为工业互联网会成为工业企业数字化升级的新型基础设

施，会加大在这个方向的投入，发展更多的专业合作伙伴，引入更多的工业互联网专业人才，具体从以下几个方向重点发展。

（一）在疫情期间将免费为企业提供复产复工、人员防控、医疗物资互助、在线培训和金融服务等。

（二）一方面打造供应链金融、协同制造、在线培训、工业超市、产业分析等腾讯特色服务，也打造了一个工业 APP 市场，开发更多的实用的工业应用小程序。

（三）新技术日新月异，腾讯将加强 5G+工业互联网的融合应用，积极探索智能工厂、远程运维、车联网等创新应用场景。

（四）重点打造 PaaS 服务能力，打造低代码开发平台、敏捷开发平台、数据中台、机理模型开发平台等，主要培育工业互联网 ISV 开发者生态，开展工业生态伙伴招募计划，期待更多工业领域的合作伙伴加入，一起共建工业互联网生态。

标准化工作：

腾讯高度重视标准化研究与应用的工作，于 2016 年起组建专业的标准化团队，今年 9 月份，发布了《腾讯标准化白皮书（2020）》，白皮书围绕“标准助力新基建”、“规范数据要素”，以及“促进产业互联”三个方面介绍了腾讯在数字经济领域的系统布局和内外标准联动的标准化布局。

以 5G 技术领域为例，腾讯在 R16 5G 架构规范中扮演着重要角色，同时也是 R17 5G 架构规范的积极参与者。在 5G 边缘计算标准、

国内外 V2X 标准等 5G 架构规范中，腾讯贡献了大量有价值提案，帮助 5G 行业应用优化，同时在垂直领域起到积极作用。例如以 5G 网络服务化架构标准提升 5G 网络稳定性，降低网络延迟的前提下，结合 V2X 标准，可满足高等级自动驾驶的需求，实现车路云网的协同，从而推动智能网联和自动驾驶技术的发展。在标准助力新基建方面，腾讯在 5G 标准成果的基础上，向云计算标准化、多媒体标准化，物联网等众多新基建领域开展标准化实践，以标准化为核心逐步完善数字生态。

三、富士康工业互联网股份有限公司：基于 5G 的精密工具智能工厂

富士康紧跟数字化转型升级潮流，于 2017 年成立富士康工业互联网公司，整合旗下网络通信、精密制造、信息科技等板块，打造了 BEACON 工业互联网平台。平台连接、管理 16 类超过 68 万个工业设备，累计工业机理模型 416 中，已开发 1037 个工业 APP。

在精密机构件领域， 5G 模组信号敏感度也推升了产品工艺技术水平、加工精度的要求，工业富联基于多年的制造经验和技术积累，自主研发了“一站式”精密刀具磨削 APP，获得了 2019 首届中国工业互联网大赛冠军，还被工信部评为 2019 年工业互联网 APP 优秀解决方案，引领着产业创新和转型升级，未来也将在 5G 驱动精密机构件加工技术升级突破进程中继续发挥标杆企业的责任与力量。事实上，工业富联推动 5G 行业应用的项目远不止“5G+精密刀具”。

图 2-1 精密工具智能工厂

目前，工业富联正与中国联通推动深圳唯一的“5G+工业互联网”应用省级示范园区建设，运用到自主设计的、全球第一款为工业互联网设计的、独立组网的 5G 小基站，还有 5G 核心网，以覆盖 1000 多条产线、53 栋厂房。同时携手合作伙伴提供 5G 终端设备，并基于 DTU、BBU，连接边缘计算服务器，将 5G 和边缘计算有效地融合在一起。该示范园区已有多个合作项目进入测试阶段，除了“5G+精密刀具”，还有智能仓储、智能运输等。

四、深圳华龙讯达信息技术股份有限公司：木星数字孪生平台

华龙讯达自主研发基于工业互联网平台的木星数字孪生技术在业内具有领先优势，木星数字孪生技术打破“信息孤岛”，促进集成共享，实现跨企业、跨领域、跨产业的广泛互联互通，实现生产资源和服务资源更大范围、更高效率、更加精准的优化，推动一二三产业、大中小企业融通发展，实现全要素、全产业链、全价值链的全面连接，

驱动数据充分流动，实现以数据流带动技术流、资金流、人才流、物资流，构建数据驱动的网络化生产制造、流通体系和服务体系，正在成为传统企业数字化转型的新型基础设施。

图 2-2 木星工业互联网平台生态体系

华龙讯达的核心能力在于全球主流工业设备设施数据自主采集、生产线（车间/工厂）数字孪生系统、场景化的数据模型定制、社交化平台服务等领域，拥有 OT 与 IT 深度融合的核心技术、海量工业机理模型库、全产业链数据的开发利用能力、以及工业互联网创新生态构建优势，形成了有成熟的行业级应用，且可复制、可推广的端到端工业互联网解决方案。

华龙讯达将以木星数字孪生为中心，采取“强平台、壮生态、拓应用、融智能、重行业”的发展战略，进一步加强与国家级研究机构、主流云服务商、高校的战略合作，不断扩大在数字孪生、工业互联网和工业物联网领域的优势，吸引优秀众创团队的参与，丰富和完善工业 APP 的应用，成为“基础领先、平台领先、生态领先、应用领先”的工业互联网平台标杆企业。

标准化工作：

华龙讯达参与制定国家两化融合、物联网和 CPS 标准，入选广东省、云南省工业互联网产业生态供给资源池，是新能源装备、石化、航空、风电、核电、汽车、交通、医药、烟草等行业的工业互联网平台领跑者。提供全球主流工业设备设施数据采集和边缘计算设备“机器宝”、木星数字孪生平台、木星数据建模平台、木星工业物联网平台、木星工业互联网平台、木星智能控制等系列产品，助力传统行业数字化转型升级。

五、TCL 华星光电技术有限公司：电子制造行业工业互联网实践

TCL 华星光电是国家工信部智能制造试点示范项目，2018 年荣获“国家绿色工厂”称号，格创东智作为参与整个项目全程的工业互联网公司，为智能工厂项目自主研发了多个工业互联网智能应用，助力 TCL 华星光电实现生产高度自动化、数字化和智能化。

格创东智广泛服务电子制造行业，先后帮助晶圆制造、新型显示、3C 电子、5G 通信等电子制造企业实现数字化、智能化转型升级。2018 年，格创东智、腾讯云联手，助力华星实现人工智能在 AI 判片的应用，全面承接 t1，t2 和 t6 工厂 ADC 系统（Auto Defect Classification）在一些工艺制程上的落地实施项目。ADC 系统是液晶面板行业首个落地应用的人工智能自动缺陷分类系统。

面板属于精密仪器，对产品良率的要求非常高，但是面板的一些

细微瑕疵微小，不容易被检测出来。在导入 ADC 之前，光学检测机设备会拍摄很多图片，但设备只能拍摄图片，无法分类图片，需要将图片收集起来，技术人员凭人眼分类。人工判片环节存在一定的困扰：一是人员流失严重，且新人需要漫长的培养期；二是每人的经验技术不一样，导致判断结果也会不一样，对图片分类的准确率、覆盖率都有较大影响。

基于此，华星导入了 ADC 系统，设备拍照后，将图片传到存储服务器上，然后通过 ADC 系统对缺陷进行判定。ADC 项目的有形效益明显：替代 50%以上的人力，实现超千万每年的经济效益。无形效益也很显著：AI 识别速度提升 5-10 倍，准确率从人眼的 85%提升到 90%以上。

标准化工作：

近期，TCL 华星主导并参与了全球首个 Mini-LED 商用显示屏团体标准《Mini-LED 商用显示屏通用技术规范》的制定和发布工作，标准为产业链企业研发、生产、销售、安装提供了科学依据，并为科研机构、院校单位、建设单位、设计单位、施工监理及运行管理人员提供了参考。此外，由 TCL 华星提交的《超高清显示器件 AM MINI LED 背光源通用技术要求》也已在近期获得深圳 8K 超高清产业协作联盟同意，作为团体标准立项。

六、深圳市赢领智尚科技有限公司：高端女装智能个性定制

深圳市赢领智尚科技有限公司（以下简称“赢领智尚”）致力于将新一代的 IT 技术、自动化的设备及赢家积累的雄厚技术相融合，以智能化和数字化为核心驱动力，打造全球首个女装全智能供应链平台，开创高级女装智能制造和个性化定制新模式。

2019 年，赢领智尚成功中标工业互联网标识解析二级节点（服装行业应用服务平台）项目，积极开展服装行业的工业互联网标识解析二级节点建设。针对女装行业发展的痛点和瓶颈，利用数字化驱动，实现全程信息化智能管控，重新定义服装行业供应链体系。通过建设智能研发平台体系解决传统设计打板周期长的瓶颈；通过建设智能制造平台解决传统生产制造的短板，实现女装生产多款式、小批量、多批次的柔性、混合性生产模式。

图 2-3 赢领智尚女装智慧工厂

通过深入研究顾客的个性化定制需求，挖掘、设计、生产、智能物流等全流程环节，打通全生命周期的数据流，用数据流带动产品流、

物流，整合资源，实现从生产产品向提供产品和服务的服务型智造转型升级，满足顾客个性化需求，减少品牌商库存，提高生产商效益，降低员工操作难度，实现绿色生产。赢领智尚自主研发，创新的智能供应链平台将带领服装业向智能化、柔性化、服务化延伸发展。

七、深信服科技股份有限公司：赋能 5G 边缘计算新安全

深信服科技股份有限公司（以下简称“深信服”）作为专注于企业级安全、云计算和基础架构的产品和服务供应商，深耕运营商与广电行业领域多年，基于 5G 新基建发展方向，配合运营商整体建设脚步与安全需要，提出了 5G MEC（边缘计算）安全解决方案，为 5G 时代下各行业信息化发展提供了有力的安全保障。

作为新兴的移动通信技术，5G 是万物互联的关键基础，为产业互联网提供了巨大的发展动能，高带宽、广连接、低时延等特性支撑了工业自动化、智慧城市、远程医疗、自动驾驶等多种应用，但也给 5G 系统和应用带来了空口安全风险、网络安全风险、云化安全风险、切片安全风险等诸多安全风险。

深信服立足“立体保护 全局运营”的 5G 场景化安全框架，特别针对站点机房、边缘云和核心云中的各 MEC 节点，进行物理、网络、数据、应用、身份立体保护；通过 5G 场景化安全运营中心，打造集统一运营管理、资产识别和威胁监测、响应编排与价值量化于一体的安全管理门户，并通过和上级平台对接级联，最终实现“能力易集成、最小业务影响、自动化运营”。

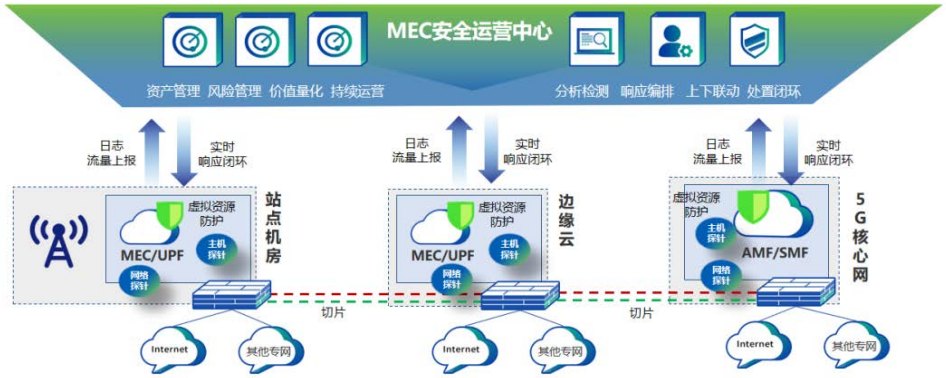

图 2-4 5G 场景化安全框架

5G 发展在“新基建”的催动下势如破竹。应用广、渗透深的 5G 网络建设背后，是随之增加的安全风险。深信服将充分发挥网络安全领域的优势和潜力，敏锐把握在 5G 场景化、行业化落地中的安全需求，保障 MEC 等 5G 关键技术的安全稳定落地，牢牢构筑工业互联网、车联网、智慧城市、物联网、人工智能等飞速发展的安全基石。

安全标准化工作

深信服近年来积极参与安全方面的国家标准化工作，在云安全标准化方面表现突出。2019 年 8 月 30 日，由全国信标委云计算标准工作组归口管理的 12 项云计算国家标准获批正式发布。深信服作为组织会员单位，参与了其中 3 项国家标准的制定，分别是：GB/T 37741-2019《信息技术 云计算 云服务交付要求》、GB/T 37739-2019《信息技术 云计算平台即服务部署要求》、GB/T 37738-2019《信息技术 云计算 云服务质量评价指标》。

在云计算领域，深信服已加入云计算标准和开源推进委员会、信标委云计算标准工作组等组织，与相关标准组织、合作伙伴共同规范

云计算行业发展与推进生态建设。目前，深信服已参与到多个产业白皮书、行业标准、国家标准的制定工作当中，是国内首部《混合云白皮书》主要撰写单位，同时也是《云服务用户数据保护能力参考框架》、《云服务数据保护能力评估方法》等标准的主要起草单位。未来，深信服将持续深耕超融合、云计算、信息安全等领域，利用技术、产品和市场方面的创新与积累，携手业内同行，共同推动云计算产业规范化、标准化地向前发展。

八、深圳奥联信息安全有限公司：国产密码技术保障工业互联网安全

深圳奥联信息安全技术有限公司（以下简称“奥联”）是集算法研制、产品研发、方案实现、标准制定、前瞻性技术研究为一体，具备国际领先的密码领域全面“智造”能力的综合型密码安全企业。其自主研制的《基于标准算法的高效无证书密码系统 ECS》已通过国家密码管理局安全性认证，该系统可应用于物联网、工业互联网、车联网、区块链等领域。

ECS 密码系统无需证书系统管理公钥，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，非常适用工业互联网领域。对标国际上类似方案，ECS 密码系统具有安全性更高、公钥计算速度更快等特点。ECS 采用标识认证机制，去中心化，支持离线认证，无需使用数字证书，免去证书管理的负担，用户私钥是用户自己掌握，满足电子签名法的强签名要

求，不用计算线性对，运算效率高。

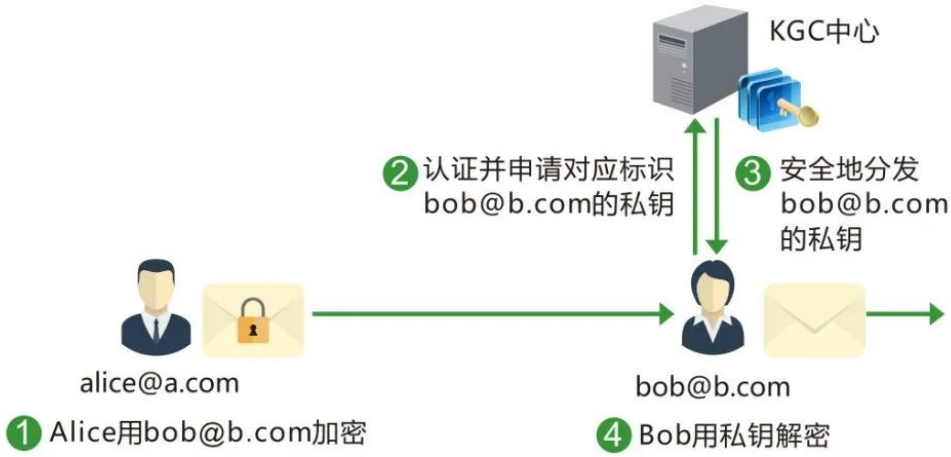

图 2-5 无证书标识密码体系

基于国密算法的工业互联网安全解决方案，采用 SM9 算法结合新一代安全传输协议（NTLS），实现操作人员、设备、云端服务器彼此之间的身份认证，实现工业终端数据、云端服务器数据的加密传输及加密存储，并建设相应的工业信息安全密码支撑系统，从而全面为工业互联网提供安全可靠的网络环境和数据加密服务的整体解决方案，满足工业互联网的双向身份鉴别、精准权限控制、数据传输安全、控制指令防篡改和数据存储安全保护等安全需求。

安全标准化工作：

奥联在 IBC 标识密码技术研究和应用上处于国际领先水平，自主或参与设计的多个标识密码算法已被 ISO、IEEE、3GPP 和 IETF 等国际标准组织采纳为标准算法；目前已主导或参与了国际标准 7 项、国家标准 8 项、行业标准 8 项的制定工作。在算法方面，奥联是国家 SM9 算法重要的原研及标准编制单位，积极推动 SM9 成为第一个全

体系进入 ISO 的非对称国际算法；物联网方面，奥联联合中国电信、华为编制的 X.1365《在电信网络上使用基于身份的密码来支持物联网服务的安全方法》获国际电信联盟（ITU）正式发布，填补国际空白；在政务数据共享方面，奥联牵头制定的《信息安全技术 政务信息共享 数据安全技术要求》国家标准，即将发布。

九、深圳融安网络科技有限公司：网络安全态势感知平台与工业安全评估系统建设

深圳融安网络科技有限公司致力于工业互联网安全技术研发和服务的高科技创新型企业，拥有国际领先、完整自主知识产权的安全测试和防护技术，开发出全面覆盖工业互联网、工业物联网的保护监测、检测、管理、工业安全态势等系列产品，为电力、轨道交通、石化、军工、冶金、燃气、水务、智能制造等国家重点行业客户提供完整的工业互联网安全解决方案。融安网络将秉承持续精进软硬件的创新，为工业智能化——“中国制造 2025”植入安全基因，实现从“工业控制系统的安全”到“安全的工业控制系统”的跨越，构建可持续发展的工业互联网安全防护体系。

融安网络自主研发的电力监控系统网络安全态势感知平台是一套分布式的网络信息安全审计平台，对电力监控系统的运行状态、安全情况通过本系统实现合法性、合规性检测。平台主要实现针对不同监视对象的数据采集；根据监视规则对数据进行分析，根据分析结果产生不同的监视动作。它支持对常见网络安全设备、电力二次安全设

备在运行过程中产生的日志、消息、状态等信息的实时采集，在实时分析的基础上，监测各种软硬件系统的运行状态，发现各种异常事件并发出实时告警，提供对存储的历史日志数据进行数据挖掘和关联分析，通过可视化的界面和报表向管理人员提供准确、详尽的统计分析数据和异常分析报告，将数据转发给上级安全管理系统，协助管理人员及时发现安全漏洞，采取有效措施，提高安全等级。共筑全网统一的网络安全态势感知安全平台，提升整个系统的安全防护能力，保障电力系统的网络安全合法合规和安全运行。

工业安全评估系统为融安网络推出的针对工业现场风险评估而设计的工业控制网络安全工业安全评估系统。系统通过多维度的评估分析方式得到一份全方位的风险评估报告，通过合规性评估分析，资产分析，病毒扫描,流量分析和 U 盘认证全方位满足工业现场风险评估的需求。主要包含合规性评估，资产分析，流量分析，病毒扫描，报告管理等功能。

十、深圳市网安计算机安全检测技术有限公司：网络安全服务平台支撑保障疫情防控和复工复产

深圳市网安计算机安全检测技术有限公司（以下简称“网安检测”）是国内最大的第三方专业“网络安保+审计溯源+保全鉴证”的综合性信息安全服务提供商——网安集团的旗下子公司，其服务项目包括网络安全等级保护测评、商用密码应用安全性评估、数据安全咨询、ISO27001 体系建设咨询、信息系统审计、ICP 评测、APP 个人信息安

全合规评估、信息安全风险评估、一体化创新智能安全防护平台等，迄今为止所服务的政府、金融、医疗、教育、企业单位已超过 1000 家。2018 年，网安检测公司正式列入第一批 27 家商用密码应用安全性测评机构试点单位目录，2019 年 8 月，网安检测公司获准扩大试点范围，面向社会开展密码应用安全性评估。

为做好工业互联网、远程医疗、在线服务、云办公等新型应用的安全保障支撑，充分发挥基础电信企业、网络安全企业作用，工业和信息部网络安全管理局近日组织相关企业，依托网络安全公共服务平台，向党政机关、医疗机构、公共应急、教育教学等疫情联防联控单位以及重点工业互联网企业等用户提供网络安全服务，最大程度降低企业系统遭受网络攻击的风险，支撑疫情防控和复工复产。网安检测公司“安证云”平台作为获推荐的全国 21 家网络安全公共服务平台之一，积极为社会提供网络安全服务。

图 2-6 工信部发布网安公共服务平台企业支撑保障疫情防控和复工复产的通知

安全标准化方面：

（1）深圳网安检测参与发起国内首个“零信任产业标准工作组”

今年 6 月份，深圳网安检测联合公安部第三研究所、腾讯联合国家互联网应急中心等单位共同成立国内首个“零信任产业标准工作组”，覆盖产、学、研、用四大领域，推动零信任系列团体标准的研究、研制与产业化落地，提高零信任技术的应用效率。

零信任产业标准工作组的成立，能够帮助各行业用户基于标准化的方式来评估其安全态势，建立真正有效、合规的网络安全架构，最终提升行业的整体安全水平与企业竞争力。

（2）联合腾讯、深圳市标准技术研究院等推进 AI 安全标准，助力企业复工复产

今年伊始，新冠疫情爆发后，深圳网安检测就联合腾讯、深圳标准院等单位成立标准编制工作组，共同研究《基于 AI 的工作场所非接触式视频安全监测技术指南》的标准制定工作，该团体标准已于今年 5 月 14 日正式发布和实施，是国内首个基于 AI 的科技抗疫团体标准。

《基于 AI 的工作场所非接触式视频安全监测技术指南》（T/SZS 4016-2020）团体标准规定了基于 AI 的工作场所非接触式视频安全监测技术和系统的总体原则、参考架构、接入设备要求和安全要求等，适用于基于 AI 的工作场所非接触式视频安全监测系统的设计、研发、选型测试、运营维护、安全管理等过程，能够为本次疫情或其他社会重大卫生事件情境下，为企业复工复产提升安全防控能力。

参考文献

[1] 于成丽，康双勇.我国工业互联网安全标准情况研究[J].保密科学技术，2019（03）20~24.

[2] 《工业和信息化部国家标准化管理委员会关于印发〈工业互联网综合标准化体系建设指南〉的通知》[R/OL].(2019-03-08)[2019-03-15].

[3] 杜霖，陈诗洋，姜宇泽，李艺. 工业互联网安全关键技术研究[J].信息通信技术与政策，2018(10)：10~13.

[4] 关鸿鹏，李琳，李鑫，姚玉梅，徐克超，王颜山. 工业互联网信息安全标准体系研究[J]. 自动化博览，2018(03) ：50~53.

[5] 工业互联网产业联盟. 《工业互联网安全框架》.2018.

[6] 深圳市工业和信息化局. 《深圳市工业互联网发展白皮书》.2019.

[7] 工业互联网产业联盟. 《工业互联网标识解析—安全风险分析模型研究报告》.2020.

[8] 中国信息通信研究院，IMT-2020(5G)推进组.《5G 安全报告》.2020.

[9] 全国信息安全标准化技术委员会，通信安全标准工作组. 《物联网安全标准化白皮书》（2019 版）.2019.

[10] 中国电子技术标准化研究院，全国信息技术标准化技术委员会大数据标准工作组. 《工业大数据白皮书》（2019 版）.2019.

[11] 中国信息通信研究院. 《云计算发展白皮书》(2020 年).2020.

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

[13] 中国信息通信研究院. 《中国网络安全产业白皮书》（2019 年）.2019.

[14] 国家计算机网络应急技术处理协调中心. 《2019 年中国互联网网络安全报告》. 2020.

[15] 工业互联网产业联盟. 《中国工业互联网安全态势报告》（2019）. 2020.

[16] 深圳市工业和信息化局.《深圳市工业互联网发展白皮书（2019）》.2019.