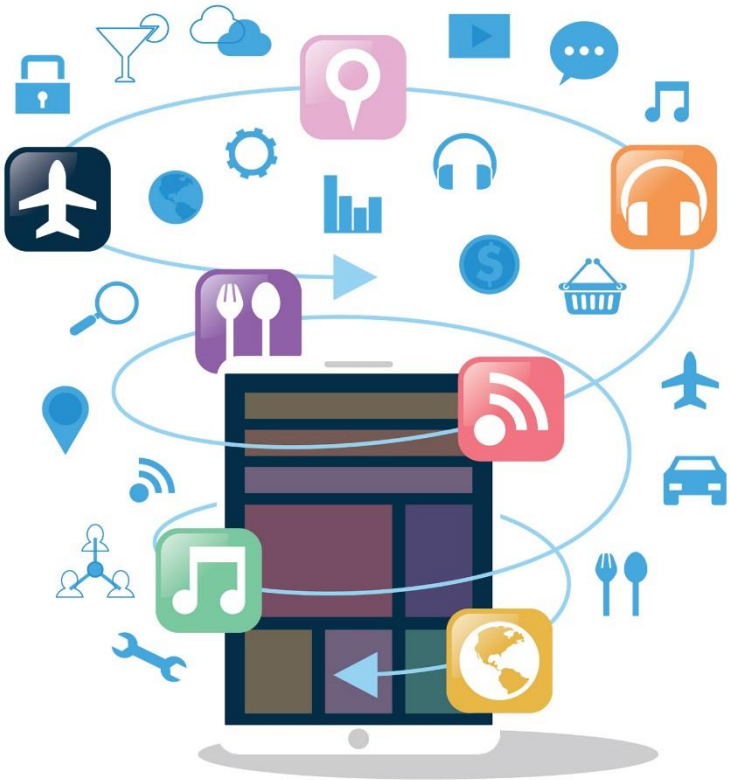
物联网安全标准化白皮书

(2019版)



全国信息安全标准化技术委员会

通信安全标准工作组

2019年10月

编写单位

中国移动通信集团有限公司、中国电子技术标准化研究院、公安部第三研究所、电子科技大学、中国信息安全测评中心、中国信息通信研究院、四川省信息安全测评中心、北京信息安全测评中心、华为技术有限公司、微软（中国）有限公司、广东为辰信息科技有限公司、中电长城网际系统应用有限公司。

编写人员

杨建军、张滨、袁捷、刘贤刚、上官晓丽、于生多、李京春、张峰、邱勤、龚洁中、王军、张伟、孙彦、江为强、赵蓓、武冰梅、李祥军、闵京华、徐思嘉、马洁、孟楠、常玲、于乐、赵章界、顾健、张艳、刘继顺、胡津铭、胡亚兰、彭晋、付俊、杜雪涛、张晨、刘利军、文远、陈欢、张双、柳耀勇、苏郁、赵立君、周剑、谢彦昊、罗蕾、申杰、李允、陈丽蓉、王丹琛、刘冬梅、李冕、黄敏、柳扬。

目 录

一、 导论

1.1 背景及意义

万物互联时代，5G、大数据、人工智能等新技术为物联网（Internet of Things，IoT）带来了创新活力，物联网与个人及家庭生活、工业生产深度融合，为全社会带来深刻变革。我国“十三五”规划将物联网作为战略性新兴产业的重要组成内容，世界各主要国家也纷纷将物联网上升到国家战略高度。全球物联网正进入跨界融合、集成创新和规模化发展的新阶段。

物联网面临着错综复杂的安全风险。从管理角度看，物联网应用涉及国家重要行业、关键基础设施，产业合作链条长、数据采集范围广、业务场景多，各类应用场景的业务规模、责任主体、数据种类、信息传播形态存在差异，为物联网安全管理带来挑战。从技术角度看，物联网涉及通信网络、云计算、移动 APP、WEB 等技术，本身沿袭了传统互联网的安全风险，加之物联网终端规模巨大、部署环境复杂，传统安全问题的危害在物联网环境下会被急剧放大。

我国政府早在 2013 年就将安全能力建设纳入物联网发展规划。近年来，随着物联网技术应用的不断成熟，物联网安全标准化得到进一步重视，成为国家促进关键信息基础设施保护、行业应用安全可控的重要抓手。值此物联网产业发展的关键时期，加快研制应用物联网安全基础标准和关键技术标准，尤其是工业互联网、车联网、智能家居等产业急需的物联网安全服务标准，已成为尤为紧迫的一项工作。

本白皮书梳理了国内外物联网发展现状、法律政策背景、安全标准化进展以及安全防护技术的研究情况，提出了物联网安全标准体系及后续工作建议，旨在为物联网安全监管机构、标准研究及测评认证机构、物联网产业建设和运营商提供参考，推动各相关方在物联网安全领域达成共识，协同完善物联网安全标准研发及应用体系，支撑国家安全监管政策有效落地，促进物联网产业健康持续发展。

1.2 定义及范围

1999 年，美国麻省理工学院提出“物联网”的概念，指将所有

物品通过射频识别等信息传感设备与互联网连接起来，实现智能化识别和管理的网络。2005 年，国际电信联盟(ITU)发布了《ITU 互联网报告 2005：物联网》，对“物联网”的涵义进行了扩展，指出世界上所有的物体都可以通过因特网主动进行信息交换。随着物联网的发展成熟，其内涵和外延也在不断发生变化。

2017 年发布的国家标准《物联网 术语》（GB/T 33745--2017）以及 2018 年发布的国际标准 ISO/IEC 20924:2018《Information technology - Internet of Things – Definition and vocabulary》均给出物联网的定义，即“通过感知设备，按照既定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并做出反应的智能服务系统”。其中，“物”指物理实体。国际标准 ISO/IEC 22417:2017《Internet of things (IoT) - IoT use cases》中提出物联网的应用场景包括交通、家居、公共建筑、办公、工业、农业、渔业、穿戴、机车、智慧城市等 14 个方面。

本白皮书遵照现有 ISO 国际标准及国家标准对物联网的定义，对物联网安全标准化现状及需求进行研究分析。

二、 物联网发展现状与趋势

在万物互联时代，物联网实现了人与物、物与物之间的信息交互和通信，通过与各行业深度融合，催生了智能家居、智慧城市、个人智能穿戴等新兴应用领域，衍生出繁荣多样的物联网业务，使人们获得更为便捷的生产、生活体验。

当前，美、欧等发达国家均将物联网作为国家级战略新兴产业快速推进，中国也在“十三五”规划中明确提出了物联网国家战略，将“物联网应用推广”列为国家八大信息化专项工程之一，物联网时代已到来。

2.1 物联网网络建设初具规模，呈蓬勃发展趋势

根据 GSMA 数据，截至 2019 年 8 月，全球已建成 119 张商用移动物联网（NB-IoT 和 LTE-M），覆盖欧洲、美洲、澳洲、亚洲的大部分地区。

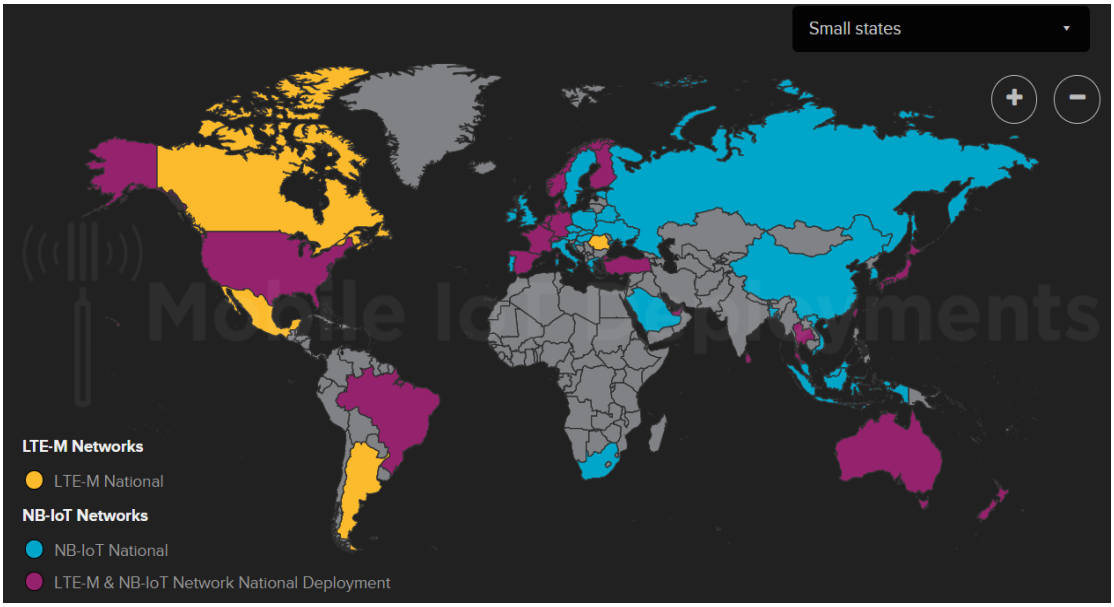


图 2.1 全球移动物联网建设图（来自GSMA）

其中，中国电信、中国移动、中国联通三家运营商均已实现 NB-IoT 的商用部署，共部署超过 70 万 NB-IoT 基站。截至 2018 年年底，中国的授权频段蜂窝物联网连接数为 6.72 亿，占亚太地区的 90%以上、全球物联网连接数的 60%以上。预计到 2025 年，中国的授权频谱蜂窝物联网连接数将增加到 19 亿左右，物联网呈现出蓬勃发展的

趋势。

2.2 物联网催生新应用、新业务，美欧积极推进

物联网网络的大规模建设催生了智能物流、智能停车、智能烟感、智能抄表、智能制造、智慧交通等行业应用，改变了人们的生活方式，带来极大的便利性，同时也为企业创造了新的业务和商业模式，赋能各行各业。以智能物流为例，通过物联网技术实现对货物的检测和运输车辆的跟踪，实现了物流运输、仓储、配送等各个环节的全面感知和分析，提升了物流行业的运输效率和智能化水平。

各国政府也在积极部署推进物联网应用的发展。2015 年，美国政府宣布投入 1.6 亿美元推动智慧城市计划，将物联网应用试验平台的建设作为首要任务。欧盟成立了横跨欧盟及产业界的物联网创新联盟（AIOTI），投入 5000 万欧元，通过咨询委员会和推进委员会统领新的“四横七纵”体系架构，将包括物联网欧洲研究集群（IERC）、地平线 2020 在内的 11 个工作组纳入旗下，统筹原本散落在不同部门和组织的能力资源，协同推进欧盟物联网整体跨越式创新发展。

2.3 我国形成完整的物联网产业链，规划智慧城市建设

目前我国已经初步形成了覆盖芯片和元器件、设备、软件、系统集成、网络运营、物联网服务在内的较为完整的产业链，形成了长三角、珠三角、环渤海和中西部四大物联网产业聚集发展区，在无锡、重庆、杭州建立了三个国家级物联网产业示范基地。

我国有一半以上的城市正在进行“智慧城市”规划，其主要应用项目依次为公共安全、交通、医疗、社区、环保、地下管网监测、水务、教育等，这些应用均以自动感知为基础、数据采集为手段、智能控制为核心、精细管理和服务提升为目的，实现了物联网技术的综合集成应用。

三、 物联网安全威胁与挑战

随着物联网与个人生活及各行各业的深度融合，物联网呈现出与传统网络不同的特性。首先，终端连接数量非常巨大，且终端形态多样，有各类摄像头、传感器等；在通信层面，终端的接入方式多样化，包括 2/3/4/5G、WiFi、蓝牙、Zigbee、LoRa、NB-IoT 等多种无线接入技术；此外，物联网的业务种类繁多，根据具体业务的不同，短信、数据、语音等不同功能进行组合以满足物联网业务需求。新特性带来新挑战，物联网面临复杂的安全风险与挑战。

3.1 传统行业参与多，安全基础较薄弱

大量传统行业，包括交通、医疗、家居、物流、工农业和安防等，借助物联网技术达成产业升级。这些传统行业的 ICT 系统起步较晚，安全保障能力较难应对物联网安全风险挑战。具体来说，安全风险主要集中在平台侧。物联网业务系统和平台使用的基础环境及组件包括虚拟机、云平台、数据库、各类中间件、web 应用等，由于软件本身设计或业务处理流程存在漏洞，存在认证绕过、非授权访问、篡改数据、远程控制、服务中断等安全风险。

3.2 终端能力差异大，安全防护有短板

大部分物联网终端设备的计算资源较低，使得很多适用于通用计算设备的安全防护功能无法实现，抗攻击能力较差。其次，物联网终端物理位置分散，很多设备均处在户外，无人值守，难于统一管理，容易遭受物理攻击，导致设备非法移动、人为破坏、感知节点丢失甚至无法工作，此外，由于物联网终端数量大、部署分散，升级成本高，用户升级意愿低等因素，导致众多物联网终端长期“带病”运行，易被恶意控制。

3.3 连接规模海量化，攻击影响易放大

物联网终端规模巨大，且以集群的方式存在，攻击者容易通过暴力破解、发送恶意数据包、利用已知漏洞等方式控制物联网终端，构建僵尸网络，发动 DDoS 拒绝服务攻击，导致网络拥塞、瘫痪、服务中断，且由于终端数量庞大，这种攻击造成的危害被急剧放大。

3.4 业务场景多样化，安全管理有死角

随着物联网与各行业的深度融合，物联网业务种类多，业务场景和逻辑更加复杂多样，存在业务滥用、防护不足等安全风险。物联网重要业务与普通业务在平台、网络方面未实现分级安全防护，业务防护能力不足，易导致业务系统被攻击。此外，在消费者物联网等领域，物联网终端如智能家居设备、智能穿戴设备等贴近终端销售者和用户，易出现机卡分离，易发生物联网卡被滥用于发送垃圾短信、违规获利等，催生黑色产业链。

3.5 产业合作链条长，安全责任难厘清

物联网业务涉及到的合作伙伴多，合作链条长，涉及到用户、设备制造商、网络运营商、服务提供者等多个利益方，一旦出现安全问题，安全责任界面难以划分。例如，若厂家生产的设备存在安全隐患，则直接影响网络及业务平台的安全，同时联网终端大部分属于广大用户，由用户管理，安全管理要求难以要求用户落实，一旦发生安全事件，存在终端用户、运营商、平台厂商责任不清的风险。

3.6 数据采集范围广，安全保护难度大

物联网采集了大量的个人及行业数据，基于大数据、云计算、AI等技术深挖数据的价值，为个人和行业提供了更高效便捷的服务。数据在物联网时代成为了一项重要的资产。然而，采集的数据不可避免地会包含敏感数据如个人隐私、生产数据、位置信息等，而敏感数据在收集、传输、存储、处理的各个阶段均有被泄露的安全风险。

四、 物联网安全政策和标准

4.1 安全法律政策

4.1.1 美国重视物联网安全，战略、政策、立法协同推进

美国是较为重视物联网安全的国家之一，从战略制定、政策落实、立法方面协同推进物联网安全的建设工作。2016 年美国国土安全部发布了《保障物联网安全战略原则》，制定了物联网安全高级原则，提出要在设计阶段考虑安全问题、加强安全更新和漏洞管理、建立安全操作方法、根据影响优先考虑安全措施、提升透明度、谨慎接入互联网等。2017 年颁布的 13800 号总统行政令《加强联邦网络和关键基础设施的网络安全》提出美国需增强应对僵尸网络及其他自动化和分布式威胁的能力。为落实 13800 号总统令，美国国家电信和信息管理局（NTIA）发布了征求评议文件《促进利益相关者对僵尸网络和其他自动威胁的行动》，以应对物联网安全尤其是僵尸网络分布式拒绝服务（DDoS）攻击威胁。美国国家标准与技术研究所（NIST）也开展了物联网环境下增强网络弹性及应对僵尸网络威胁的解决方案的研究。在立法方面，加州于 2018 年 9 月 28 日批准的《物联网设备网络安全法》，是世界上首部针对物联网设备的网络安全法规，从法律层面规定了物联网设备的安全要求。2019 年 6 月，美国众议院通过了《物联网网络安全改进法案》，除了要求每家企业都提升其制造的联网设备的安全性，该法案还希望对联邦政府使用的任何物联网设备设定最低的安全标准。

4.1.2 欧盟建立物联网安全基线，严格保护个人数据和隐私

欧盟侧重于物联网安全基线的设置及用户数据的保护。2017 年 11 月 20 日，欧盟网络空间安全局（European Union Agency for Cybersecurity）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。

4.1.3 日本关注物联网安全，加强终端设备安全保护

日本针对物联网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，为了减少黑客利用物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物联网设备，将政府人员尝试登录私人物联网设备的行为合法化。2019 年 4 月，日本总务省就《关于物联网设备的安全标准和技术标准合格认证》指南征求意见，以便明确终端设备的安全标准和认证。

4.1.4 我国物联网安全战略明确，安全管理和技术双管齐下

我国政府早在 2013 年就在政策规划中将物联网安全纳入工作体系，并持续推进物联网安全建设工作。2013 年发布的《国务院关于推进物联网有序健康发展的指导意见》中提出应建立健全物联网安全测评、风险评估、安全防范、应急处置等机制。2017 年制定的《物联网“十三五”规划》中明确了构建完善标准体系，提升安全保障能力等具体任务目标。2017 年 5 月，中央网信办、国家质检总局、国家标准委联合发布《“十三五”信息化标准工作指南》，鼓励加快推进物联网等重点技术标准的研制 。2019 年 2 月，全国信安标委印发《全国信息安全标准化技术委员会 2019 年度工作要点》，明确加快工业控制系统安全、汽车网络安全、智能门锁安全等重点领域标准研制。2019 年 8 月，工信部等十部门发布《加强工业互联网安全工作的指导意见》，明确了到 2020 年制定设备、平台、数据等至少 20 项亟需的工业互联网安全标准的工作目标。由此可见，中国物联网安全工作目标逐步细化，安全标准工作有序推进。

此外，相比国外，中国的安全管理和技术保障要求较为严格。2019 年两部委对电信运营商的考核重点之一是物联网、通信能力开放平台相关应用及服务等业务的反诈、数据安全、个人信息保护安全，要求健全安全管理与技术保障措施。近期出台的网络安全等级保护 2.0 相关标准也明确了物联网安全要求，包括感知节点物理防护、感知节点

设备安全、数据融合处理等方面，共划分 4 个等级、8 个控制点、21 个要求项。

在法律方面，我国政府已出台网络安全相关的法律和配套规范性文件，包括《中国人民共和国网络安全法》、《国家网络安全应急预案》、《网络产品和服务安全审查办法》、《网络关键设备和网络安全专用产品目录》等，为物联网行业安全监管提供了法律制度依据。

4.2 国内外安全标准化情况

在安全标准方面，国内外标准组织近年来不断推进物联网安全标准的制定。从标准的分布来看，国内外标准组织由于出发点和利益点不同，各有侧重。国际主要标准化组织中，现有物联网安全标准聚焦在安全体系框架、网络安全、隐私保护、设备安全，侧重于基础框架和技术。产业联盟如 5G 汽车联盟（5GAA）/工业互联网联盟（IIC）也在重点应用领域开展了具体场景下的安全标准研制。我国重视物联网安全监管及技术保障，目前的物联网安全标准化工作已在安全参考模型、感知及无线安全技术、重点行业应用等多个领域开展。

4.2.1 国际标准聚焦安全体系和关键技术

1、ISO/IEC JTC1

ISO/IEC JTC1/SC27（信息技术委员会/安全技术分委员会）主要开展信息安全标准化工作，SC41（物联网及相关技术分委员会）主要开展物联网相关技术标准化工作。此外，SC25（信息技术设备互联分委员会）对智能家居系统、家庭网关等安全也制定了相关标准。

在物联网安全方面，目前的安全标准主要集中在体系架构、安全技术，具体包括加密轻量化、认证、隐私控制等方面。其中，已发布及在研的标准项目有 ISO/IEC 30141:2018《信息技术　物联网参考体系架构》、ISO/IEC 24767《信息技术　家庭网络安全》（由 2 个部分组成）、ISO/IEC 29192《信息技术　安全技术　轻量级加密》（由 8 个部分组成）、ISO/IEC 27030《信息技术　安全技术　物联网安全与隐私保护指南》（在研）、ISO/IEC 27553《信息技术　安全技术　移动设备使用生物特征识别进行鉴别的安全要求》（在研）等。

2、ITU-T

ITU-T 的 SG17（安全研究组）和 SG20（物联网（IoT）和智慧城市与社区（SC&C）研究组）Q6（IoT 和 SC&C 的安全、隐私保护、信任和识别课题组）负责安全标准的制定，SG20 Q6 聚焦于 IoT 和智慧城市的安全标准。SG20 Q6 目前已发布了 ITU-T Y.4103《物联网应用的通用要求》、ITU-T Y.4115《物联网设备能力开放的参考架构》、ITU-T Y.4119《基于物联网的自动应急响应系统的要求和能力框架》和 ITU-T Y.4205《物联网相关众包系统的要求和参考模型》；SG17 规划了物联网安全系列标准 ITU-T X.1360-X.1369，已发布了 ITU-T X.1361《基于网关模型的物联网安全框架》和 ITU-T X.1362《物联网环境的简单加密规程》，并正在开展 ITU-T X.1363《物联网环境中个人可识别信息处理系统的技术框架》、ITU-T X.1364《窄带物联网（NB-IoT）的安全要求和框架》、ITU-T X.1365《电信网络上利用基于身份的密码技术支持物联网服务的安全方法》、ITU-T X.676《基于对象标识符的物联网分组服务解析框架》、ITU-T X.660《物联网对象标识符（OID）使用指南》、ITU-T X.amas-iot《面向物联网环境的具有组鉴别能力的聚合消息鉴别方案》、ITU-T X.elf-iot《物联网安全事件操作错误日志的标准格式》、ITU-T X.iotsec-4《物联网设备和网关的安全要求》、ITU-T X.sc-iot《物联网系统的安全控制措施》、ITU-T X.secup-iot《物联网设备的安全软件更新》、ITU-T X.nb-iot《物联网服务平台的安全要求和框架》等多项标准的研制。

与此同时，ITU-T 积极开展车联网安全标准化工作，由 SG17 Q13 组负责，已发布 ITU-T X.1373《智能交通系统通信设备的安全软件更新能力》，在研的标准项目集中在车联网安全指导原则，车辆外部接入设备安全需求，车内系统入侵检测方法，基于大数据的异常行为检测，数据分类及安全需求，网联车安全需求等方面。

3、ETSI

ETSI 在 2019 年 2 月发布了第一个消费类物联网安全标准 ETSI TS 103 645《消费类物联网安全》，建立了联网消费类设备的安全基线，并为未来物联网认证方案的制定奠定基础。此外，ETSI 还制定了认证授权、量子安全威胁评估以及物联网组认证安全机制分析等标准。

4、IETF

IETF 主要研究了 IP 网络中的授权、认证、审计等协议标准，如 IPSec 协议、IP 安全策略、PKI、传输层安全协议等。针对物联网终端资源有限、低功耗等特性，也提出了相应的协议优化，包括 6LoWPAN，CoAP，TLS/DTLS 等协议标准。

4.2.2 产业联盟在重点安全方向积极探索

1、5GAA

5G 汽车联盟（5GAA）在 2018 年新成立了 ESP 工作组（Efficient Security Provisioning Task Force），专门讨论基于蜂窝网络的车联网（C-V2X）安全相关问题。

目前，5GAA ESP 主要围绕 4 个方向展开项目研究，分别是地区性隐私和安全法规及其需求研究，安全凭据管理系统（SCMS）简化机制研究，SCMS 对 C-V2X 的影响分析研究，以及适用于各地区的车联网简化安全架构研究。其中，前 3 个项目旨在研究全球各地区的隐私及安全法规政策，在 SCMS 的基础上针对 C-V2X 场景研究简化的车联网安全假设及安全机制，最终成为第 4 个项目的输入，形成能够满足全球各地区隐私及安全法规要求的简化的安全架构方案。

2、IIC

工业互联网联盟（IIC）通过建立开放式互通性标准，来促进物理世界和数字世界的融合，推动工业互联网加快落地。

在工业物联网安全方面，IIC 于 2016 年发布了《工业物联网安全参考框架》，旨在推动产业界对于如何保障工业物联网（IIoT）安全达成共识，提供了自身安全性（security）、隐私权（privacy）、弹性（resilience）、可靠性（reliability）、保他安全性（safety）五大特性的细节，有助于定义风险、评估、威胁、评量与性能指标。在此安全框架的基础上，IIC 开发了一种物联网安全成熟度模型，帮助企业利用现有的安全框架达到他们自己定义的物联网安全成熟度目标级别。

3、GSMA

全球移动通信系统协会（GSMA）代表全球运营商的共同权益，就运营商在物联网领域的安全实践进行了积极的探索和研究，目前已

经发布了物联网安全指南文档集，为物联网技术和服务提供者在构建安全产品时提供一系列安全指南，包括《物联网安全指南概述》、《物联网终端生态系统安全指南》、《运营商物联网安全指南》、《物联网服务生态系统安全指南》、《物联网安全评估流程》、《物联网安全评估检查表》等，以确保整个服务周期实施最佳安全实践。

4.2.3 国内标准多点开花、稳步推进

1、TC260

在通用网络安全领域，截至 2019 年 8 月，全国信息安全标准化技术委员会（TC260）已发布 268 项国家信息安全标准，其中，部分通用的安全标准如风险预警、风险处理、漏洞管理、密码算法、密钥管理、PKI、通信协议（IPSec、SSL 等）、安全评估、等级保护相关的安全标准同样适用于广义的物联网安全，详见附录 A.2。

在专门的物联网安全领域，当前 TC260 制定了 GB/T 37044—2018《信息安全技术　物联网安全参考模型及通用要求》、GB/T 37033—2018《信息安全技术　射频识别系统密码应用技术要求》、GB/T 36951—2018《信息安全技术　物联网感知终端应用安全技术要求》、GB/T 37024—2018《信息安全技术　物联网感知层网关安全技术要求》、GB/T 37025—2018《信息安全技术　物联网数据传输安全技术要求》、GB/T 37093—2018《信息安全技术　物联网感知层接入通信网的安全要求》、GB/T 36323—2018《信息安全技术　工业控制系统安全管理基本要求》等国家标准（详见附录 A.1），并启动了医疗行业安全指南、工业互联网平台安全、智慧城市安全体系框架、汽车网络安全技术要求等标准的研究，总体呈现多点开花的形势。

从完整性上看，现有安全标准还未能满足全方位安全保障的需求。例如对企业生产的物联网感控设备还需要建立相应的安全评估标准，以确定其安全风险的大小，从而明确其可以应用的行业和场景范围。

2、CCSA

中国通信标准化协会（CCSA）的物联网安全标准化工作侧重于通信网络和系统，CCSA 中安全领域标准工作主要由 TC5（无线通信技术委员会）的 WG5（无线安全与加密工作组），TC8（网络与信息

安全技术委员会）的 WG1（有线网络安全工作组）、WG2（无线网络安全工作组）、WG3（安全管理工作组）和 WG4（安全基础工作组）来负责制定。目前已完成了 YD/T 3339—2018《面向物联网的蜂窝窄带接入安全技术要求和测试方法》、YDB 171—2017《物联网感知层协议安全技术要求》、YDB 173—2017《物联网终端嵌入式操作系统安全技术要求》、YDB 172—2017《物联网感知通信系统安全等级保护基本要求》等标准。

五、 物联网安全标准化需求

在物联网技术与业务迅速发展的背景下，我国在 ISO 发布了 ISO/IEC 30141:2018《物联网 参考体系架构》，提出了基于实体的物联网参考模型。同时，全国信息安全标准化技术委员会发布的 GB/T 37044—2018《信息安全技术 物联网安全参考模型及通用要求》提出新形势下的物联网安全参考模型。本章参照上述两参考模型，梳理了当前物联网安全需求，并针对重点方向提出物联网安全标准化的主要需求点，为建立物联网安全标准体系提供参考。

5.1 物联网安全参考模型

5.1.1 基于实体的物联网参考模型

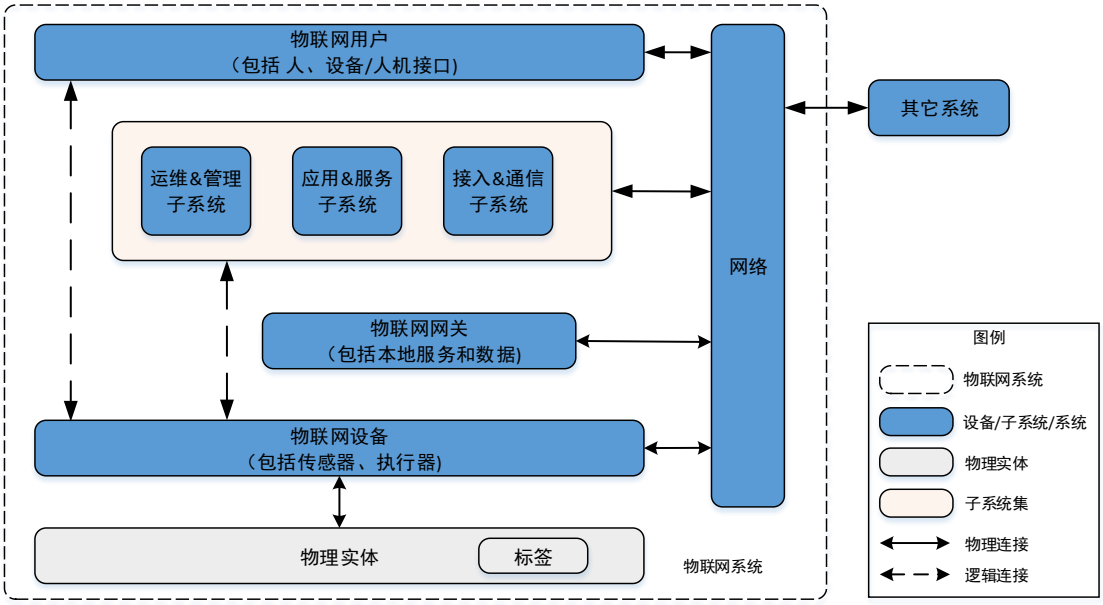


图5.1 基于实体的物联网参考模型[引自ISO/IEC 30141:2018]

ISO/IEC 30141:2018《物联网 参考体系架构》提出的基于实体的物联网参考模型如图 5.1 所示，该图使用箭头线进一步说明了物联网系统中主要实体间的交互关系。

- 物理实体：由物联网设备感知和作用的真实事物，可由各种类型的标签进行监控和识别。
- 物联网设备：通过感知与驱动执行与物理世界进行交互，包括传感器和执行器。
- 网络：物联网设备通过物联网网络进行通信。

- 物联网网关：在本地网络和广域接入网络间形成连接，可包含其它实体提供更广泛的能力。
- 应用&服务子系统：存在于大多数的物联网系统中，有相应的应用程序。应用服务子系统通常能提供设备数据与分析数据存储能力、过程管理能力，分析服务能力等。
- 运维&管理子系统：包含设备管理应用程序，为系统中的物联网设备提供监控和管理功能、提供操作支撑系统、提供物联网系统的监控和管理能力，包括向用户提供的管理能力。
- 接入&通信子系统：为用户和对等系统提供物联网系统的访问能力，为服务功能、管理功能、业务功能提供接口。提供的接入功能因用户而异，取决于访问控制功能管理的权限，并且接入前需进行身份验证和授权。
- 用户：包括人类用户和数字用户。人类用户通常使用某种用户设备与物联网系统交互。数字用户通过 API 与物联网系统交互。
- 其它系统：包括对等的其它物联网系统及非物联网系统，可以是物联网系统的用户或者向物联网系统提供的服务。其它系统通过用户网络与物联网系统交互。

5.1.2 物联网安全参考模型

GB/T 37044—2018《信息安全技术 物联网安全参考模型及通用要求》提出的物联网安全参考模型由物联网系统参考安全分区、系统生存周期、基本安全防护措施三个维度共同描述组成。参考安全分区是从物联网系统的逻辑空间维度出发，生存周期则是从物联网系统存续时间维度出发，配合相应的基本安全防护措施，在整体架构和生存周期层面上为物联网系统提供了一套安全模型，如图 5.2 所示。

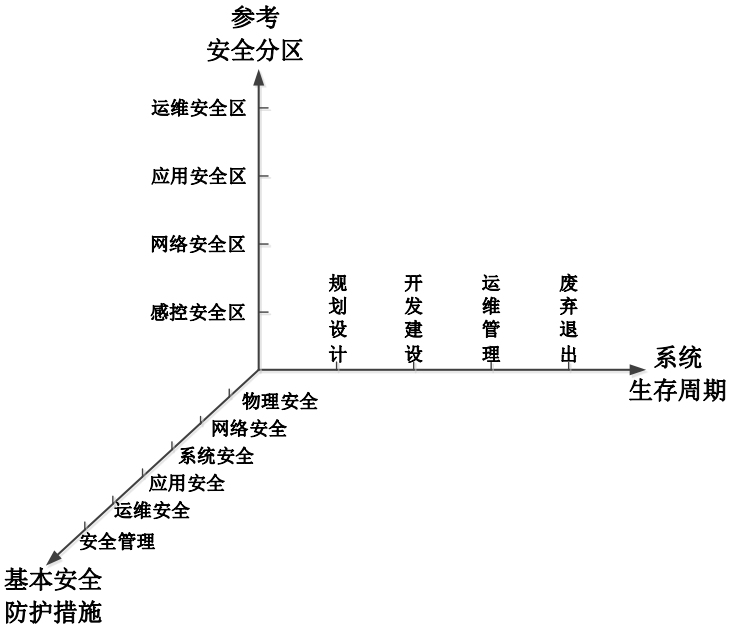


图 5.2 物联网安全参考模型[引自 GB/T 37044—2018]

物联网参考安全分区是基于物联网参考体系结构，依据每一个域及其子域的主要安全风险和威胁，总结出相应的信息安全防护需求，并进行分类整理后而形成的安全责任逻辑分区，见图 5.3。

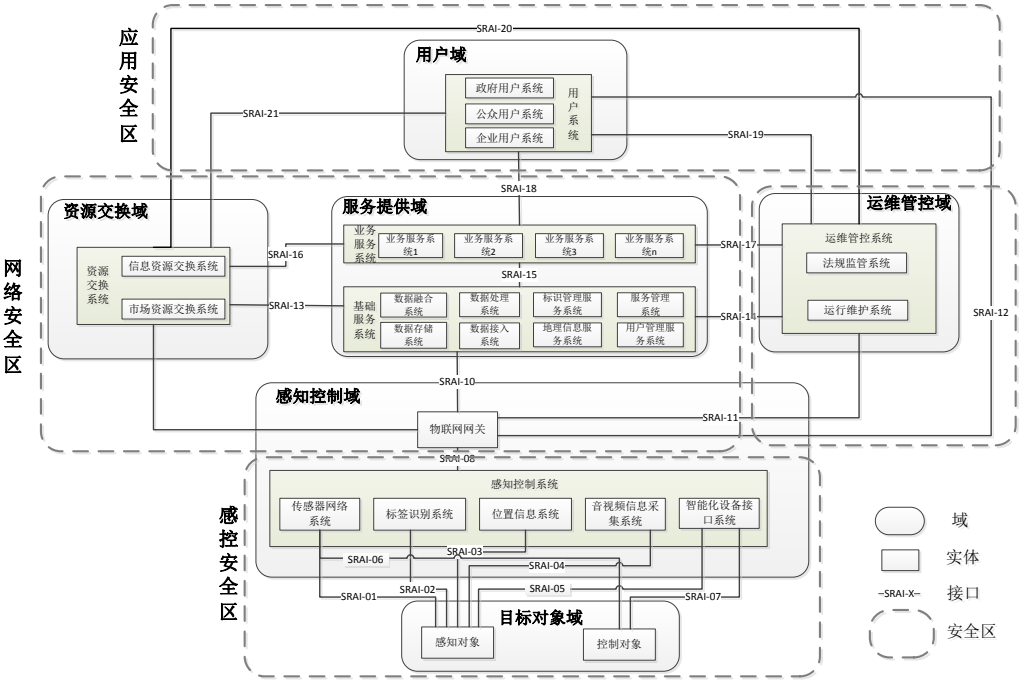


图 5.3 物联网参考安全分区划分[引自 GB/T 37044—2018]

感控安全区：该安全区主要是需要满足感知对象、控制对象（以

下合并简称感知终端）及相应感知控制系统的信息安全需求。由于感知终端的特殊性，在信息安全需求上该安全区与传统互联网差异较大，主要原因表现在感知对象计算资源的有限性、组网方式的多样性、物理终端实体的易接触性等方面。

网络安全区：该安全区主要是需要满足物联网网关、资源交换域及服务提供域的信息安全需求，其安全要求不应低于一般通信网络的安全要求，主要保障数据汇集和预处理的真实性及有效性、网络传输的机密性及可靠性、信息交换共享的隐私性及可认证性。

应用安全区：该安全区主要是需要满足用户域的信息安全需求，负责满足系统用户的身份认证、访问权限控制以及配合必要的运维管理等方面的安全要求，同时需要具备一定的主动防攻击能力，充分保障系统的可靠性。

运维安全区：该安全区主要是需要满足运维管控域的信息安全需求，除了满足基本运行维护所必要的安全管理保障外，更多的是需要符合相关法律法规监管所要求的安全保障功能。

5.2 物联网安全需求

ISO/IEC 30141:2018《物联网　参考体系架构》中将物联网参考模型按实体分为用户、运维&管理子系统、应用&服务子系统、接入&通信子系统、网络、物联网网关、物理实体等。同时，GB/T 37044—2018《信息安全技术　物联网安全参考模型及通用要求》针对感控安全、网络安全、应用安全、运维安全四个参考安全分区均提出相应安全防护措施，涉及物理安全、网络安全、系统安全、应用安全、运维安全、安全管理等方面。通过对 ISO/IEC 30141:2018《物联网　参考体系架构》的实体分类及 GB/T 37044—2018《信息安全技术　物联网安全参考模型及通用要求》中参考模型分区的理解，可合理地将其分别映射物联网感控设备及卡、物联网网络与传输交换、物联网业务应用与服务、物联网安全管理与运维四个方面，如图 5.4 所示。因此，本节将从该四个方面来分析物联网安全需求，从而梳理出后续与安全标准化工作有关的安全需求。

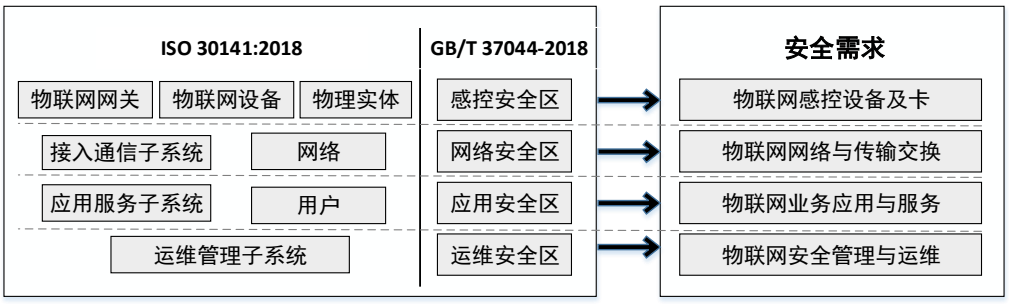


图 5.4 物联网安全需求

一般来说，物联网安全需求主要是保证其可用性、机密性、可鉴别性与可控性。可用性是从体系上来保障物联网的健壮性、鲁棒性与可生存性；机密性是要构建整体的加密体系来保护物联网的数据隐私；可鉴别性是要构建完整的信任体系来保证所有的行为、来源、数据的完整性等都是真实可信的；可控性是物联网的典型特性，是要采取措施来保证物联网不会因为错误而带来控制方面的灾难，包括控制判断的冗余性、控制命令传输渠道的可生存性、控制结果的风险评估能力等。因此，在描述物联网感控设备及卡、网络与传输交换、业务应用与服务、安全管理与运维的安全需求时，需要体现相关系统、设备、业务、服务的以上特性。

5.2.1 物联网感控设备及卡等安全需求

1、感控设备安全需求

感控设备的主要功能是实现对信息的采集、识别和控制，包含感知终端和控制设备，由于感知终端大多处于无人监控且恶劣的环境中，安全风险较为突出，主要防护需求有：（1）可能受自然环境、偷盗、非法移动位置、人为破坏等影响造成感知终端无法工作，需通过关键节点的冗余部署来确保某些节点损坏后能进行网络自愈；（2）攻击者可利用鉴别机制弱点恶意部署同型号或克隆一个相似设备，接入系统进行攻击，需采取基于密码算法的通信前节点间认证的方式解决该问题；（3）攻击者可通过无线电干扰、拒绝服务攻击或攻击感控设备所处网络的路由策略等，导致设备无法正常传输感知数据和接收指令，需通过限制网络发包速度和同一数据包重传次数来阻止利用协议漏洞；（4）攻击者利用物理获取或逻辑攻击的方式，对感控设备进行非授权访问和恶意控制并分析其所存储的敏感信息，造成信息泄露，保

护感控设备的敏感信息安全也是关键需求所在。

2、智能物联网卡安全需求

智能物联网卡指应用于物联网领域的智能卡。它是将具有存储、加密及数据处理能力的集成电路芯片镶嵌于塑料基片上制成的卡片，在智能卡的设计阶段、生产环境、生产流程及使用过程中会遇到各种潜在的威胁。攻击者可能采取各种探测方法以获取硬件安全机制、访问控制机制、鉴别机制、数据保护系统、存储体分区、密码模块程序的设计细节以及初始化数据、私有数据、口令或密码密钥等敏感数据，并可能通过修改智能卡上重要安全数据的方法，非法获得对智能卡的使用权。这些攻击对智能卡的安全构成很大威胁。物联网智能卡的软件形态，主要指的芯片操作系统（COS），主要任务是接收终端请求命令，对命令进行分流并控制其执行，管理芯片内存空间和文件，执行加密算法和应用，对请求命令提供响应结果等。因此，智能卡软件部分安全问题主要存在于攻击者采用重放攻击非法获取智能卡内数据、访问控制机制不完善导致非授权用户随意获取数据等。

对于物联网智能卡的芯片本身而言，针对芯片的攻击主要是在芯片没有工作但电源可能接通的情况下，采用腐蚀剂、高倍显微镜、照相机和探针等设备和材料对智能卡进行分析，从而获取智能卡芯片中的敏感信息。由于该攻击会破坏智能卡的封装，因此也常被称为入侵式攻击。另外，在正常通信的过程中，攻击者可以利用信息采集设备检测和搜集所有与保密数据相关的泄漏信息，经过大量样本的收集从而推算出敏感信息，这种攻击被称为边频攻击。此外，还存在攻击者利用破坏性或是非破坏性技术扰乱芯片加密系统，从而获取密钥的故障攻击手段。

以软件形态嵌入到设备中的智能卡采用基于公众网络的空中写卡技术，将面临假冒、窃听、重放、拒绝服务、非授权访问等常见的网络威胁，包括智能卡数据文件下载失败导致终端无法开通移动通信服务，智能卡管理平台受 DoS 攻击造成服务中断等。此外，软件形态更易造成敏感数据泄露，因而需要采用安全通信机制和存储加密机制实现远程操作和数据交换及存储。

实际应用中，部分物联网设备通过 WIFI、ZigBee 等方式接入物联网，同时，也有部分物联网设备基于电信运营商发行的物联网卡作为网络设备身份标识接入通信网络，使用物联网业务服务。物联网卡从本质上来说也是智能卡的一类。但由于物联网卡存在机卡分离使用情况，在业务开展过程中，存在卡被挪用、滥用、非法获利或用于发送垃圾信息、违规获利等安全风险，需要建立相应的管理规则与监测手段，对违法、违规使用进行监测、预警与处置。

3、安全网关需求

安全网关是为解决现存于物联网中的终端安全问题设计的专用产品。其面向物联网应用场景，可连接传统 PC、智能设备等多种终端。由于安全网关需要支持无线接入功能，对大量的无线设备统一管理，同时支持网络 AP 的发现和识别功能，所以存在被非法接入的风险。此外，由于物联网终端可能采集处理大量敏感数据，若安全网关对上述数据转发未作加密，则易发生数据窃取等问题。因此需要加入双向身份认证机制，同时结合 VPN 技术，防止数据窃取及篡改，保障数据的机密性、完整性及可用性。

5.2.2 物联网网络与传输交换安全需求

1、无线通信安全需求

目前，WiFi、ZigBee、蓝牙、2/3/4/5G 等无线通信技术自身存在的安全问题以及物联网系统中多种无线通信技术并存的复杂性必然导致物联网业务应用面临安全问题。一方面，各类感知终端和接入设备大部分都部署在无人监控的场景下，导致了攻击者很容易接触到这些设备，采用一些技术手段对设备无线通信模块进行逆向分析和攻击；另一方面，物联网中节点数量庞大且数据传输采用无线射频信号进行传输，存在攻击者可通过发射干扰信号造成通信中断，或信号传输过程中劫持、窃听、篡改数据等风险，需要建立安全通道建立信息传输的可靠性保障机制，利用数据校验功能以确保数据传输的完整性，利用加密机制确保数据保密性等。

2、传输交换安全需求

物联网信息传输过程中会经过不同异构性的网络，且物联网中节

点数量庞大并以集群方式存在，当面临海量数据传输需求时，容易导致核心网络堵塞，进而产生各种拒绝服务攻击，需采取多路传输，缓解网络堵塞的压力，并有效抵御拒绝服务攻击。同时，由于在物联网传输层存在不同架构的网络需相互连通，因此传输层也面临异构网络跨网认证等安全问题，可综合利用点到点加密机制和端到端加密机制确保传输层安全。此外，物联网上传输的数据包未加密和签名，易发生被窃听、篡改、伪造以及发送者抵赖等问题，需采用 PGP、SSL/TLS 和 IPSec 等协议，提供通信加密和认证功能，保证通信双方传输交换安全。

5.2.3 物联网业务应用与服务安全需求

物联网业务应用与服务安全需求主要包括业务服务平台安全需求及垂直领域安全需求等。

1、业务服务平台安全需求

物联网业务服务平台可为 SaaS 层和设备层搭建桥梁，为终端层提供设备接入，为 SaaS 层提供应用开发能力，例如阿里的“阿里智能”，腾讯的“物联云”，百度的“物管理”、中国移动 OneNET 等。其安全需求主要涉及接入安全、平台数据安全、应用安全、系统安全等。

接入安全是物联网业务服务平台提供服务的基础，但由于接入设备类型繁多、能力参差不齐，存在身份仿冒、非授权访问等安全风险，需采取相应的安全措施以保证平台接入的安全性。同时，由于物联网业务服务平台中采集、存储及处理大量敏感数据，需保证其不会出现被窃取、被篡改、被伪造、被破坏等现象。

此外，随着对象标识装置的不断普及，出现了各种动态的、富媒体内容的新型业务应用。物联网业务服务平台在向用户提供相关业务及应用时，应注意在实现技术、逻辑、控制等方面的安全威胁，如其业务逻辑设计可能存在安全隐患，业务认证授权、对外开放接口可能存在安全问题等，需要提供相应的安全机制确保业务服务的正常开展。

物联网业务服务平台还应保证其在系统安全方面的安全需求，如系统安全加固及安全审计等。

2、垂直领域安全需求

随着物联网技术产品的不断成熟，物联网应用和产品已渗透到生产和生活中的各个环节，当前其垂直领域主要包括智慧城市、工业互联网、车联网、家庭物联网、智能安防、智慧医疗、公共服务等。

不同的垂直领域由于终端设备、网络结构、业务形态的差异性，面临不同的安全风险与需求。在智慧城市中，其安全需求主要包括感知设备防护能力、多样化网络接入安全性、个人隐私保护等。在工业互联网中，其安全需求主要包括工控设备资产和网络边界的识别、工业网络隔离措施、重要数据的安全保护、威胁感知能力与专业的安全运营能力等。在车联网中，其安全需求主要包括保证传感器数据的合法性、核心控制组件的安全性、接口身份认证的安全性等。家庭物联网、智能安防的安全需求则主要体现在身份认证与鉴权、个人隐私保护、设备安全更新等方面。在智慧医疗和公共服务领域，其安全需求主要包括设备安全、个人隐私保护和数据传输安全等方面。

5.2.4 物联网安全管理与运维安全需求

物联网安全管理与运维安全需求主要包括物联网安全管理相关需求、系统生命周期的运维安全需求等。

1、物联网安全管理相关需求

物联网安全管理涉及物联网安全漏洞管理、物联网安全事件应急响应管理等。物联网安全事件应急响应也是物联网安全的最后一道重要防线，规范的安全应急工作，完备的应急能力，对保障物联网业务正常运行至关重要。同时，由于车联网、工控系统、安防设备、智能家居等物联网应用在终端设备、固件、操作系统、无线协议、专用网络、平台系统等方面具有与通用移动互联网相异的特性，其安全漏洞也及管理形式也有其特性，因此需要研究物联网行业的漏洞安全管理方法，包括漏洞库建设、漏洞标识、共享、设备加固等方法。

2、系统生命周期安全运维需求

物联网系统的一个完整生存周期大致可以分为以下四个阶段：规划设计、开发建设、运维管理、废弃退出。每一个阶段均有不同的任务目标和相应信息安全防护需求，因此应保证在每一个阶段建立相应

的安全防护措施。

5.3 物联网安全标准化需求

根据物联网安全参考模型，物联网安全需求分为四层：感控设备及卡、网络传输与交换、业务应用与服务以及安全运维与管理这四个方面。因此，物联网安全标准应包含以下四个分类：

- 感控设备安全：对应感控设备及卡安全需求，为所有物联网安全标准提供基础的术语定义、角色、模型和框架。
- 网络与交换安全：对应网络传输与交换安全需求，为物联网设备之间、以及物联网设备与平台之间建立安全通信。
- 应用服务安全：对业务应用与服务安全需求，针对物联网应用服务和物联网垂直领域，对涉及终端应用安全、数据安全、业务服务安全等形成安全指南，并指导重要行业和领域相关的物联网安全规划、建设工作。
- 安全管理与运维：对应安全管理与运维安全需求，针对物联网全生命周期安全的日常管理与运维，提出相应安全标准、实施指南，指导安全管理与运维机制建设，并为物联网安全管理与运维提供技术依据和参考。

除此外，物联网安全标准还应有安全模型与术语类，作为物联网领域的基础类标准，支撑感控设备、网络与传输、业务服务、安全运维与管理等细分物联网领域安全标准，包括统一术语及概念定义，通用安全模型和安全框架等，为整个物联网标准体系提供统一的基础框架和指南。

综上，物联网安全标准可分为五类，如图 5.5 所示。

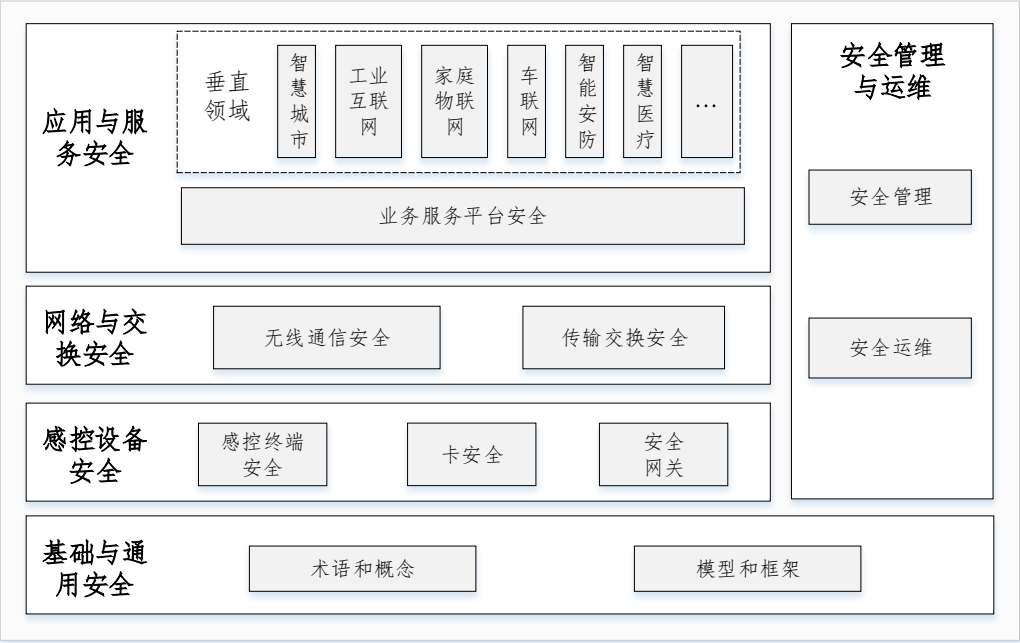


图 5.5 物联网安全标准主题

5.3.1 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。

1、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。

物联网安全模型用于理解物联网安全，表征物联网安全相关的概念以及概念之间的关系。

2、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。物联网安全参考架构需通过借鉴国际上现有的科研成果，针对物联网安全的需求，给出物联网安全参考模型，并作为对物联网安全参考模型的重要补充，给出物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物联网系统安全的组织和个人。

5.3.2 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。

1、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。

具备控制功能的设备通常能够对物理世界直接产生作用，其数据流向多为下行数据，且数据量通常不大，但是对实时性要求不同。可以将控制设备安全标准分成两类：实时控制型控制设备安全标准，如：机器人控制设备；非实时控制型控制设备安全标准，如：智能门锁远程控制。

2、智能物联卡安全

智能物联网卡的主要任务是提供物联网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。

3、安全网关

安全网关是感知层安全能力的“重机枪”，起到承上启下的作用，

大量数据由此转发，包括上行数据和下行数据。安全网关安全能力一般包括：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。

5.3.3 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。

1、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、通讯密钥管理、双向认证、日志审计等方面的要求。尤其是在通讯数据安全方面，应保障通讯数据的机密性、完整性、可用性以及不可否认性。此外，标准的制定还应根据无线通信技术的差异进行区分。

2、传输交换安全

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、中间人攻击等诸多攻击方式以及 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。

5.3.4 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。

1、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。

2、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。

5.3.5 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。

1、安全管理

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。前者主要为物联网安全应急响应提出安全规范及实施指南，对可能发生的安全事件做好事前、事中、事后的安全保障，对安全事件进行分级处置，提升应急响应能力与管理规范，指导相关工作落地。后者主要为物联网安全漏洞管理提供相应管理规范，保证网络产品、服务、系统的漏洞能够及时修补，提高网络安全防护水平，指导各单位、组织建立响应的漏洞修补、防护策略，并建立相应技术管理手段。

2、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。

5.4 物联网安全标准与其它领域标准的关系

物联网本身是个开放的领域，物联网安全标准也与其他领域的标准关系密切。一方面，物联网是在传统的电信与互联网领域发展起来的，5G、云计算与大数据、人工智能、区块链、量子计算等新兴技术的发展能够从通信传输、计算、数据存储等方面快速推动物联网技术的发展。另一方面，物联网安全标准支撑着工业互联网、智慧城市、智慧交通、车联网等垂直领域的发展。因此，物联网安全标准与传统网络安全领域、新技术领域的安全标准，以及与各垂直领域的标准有着密切的联系。

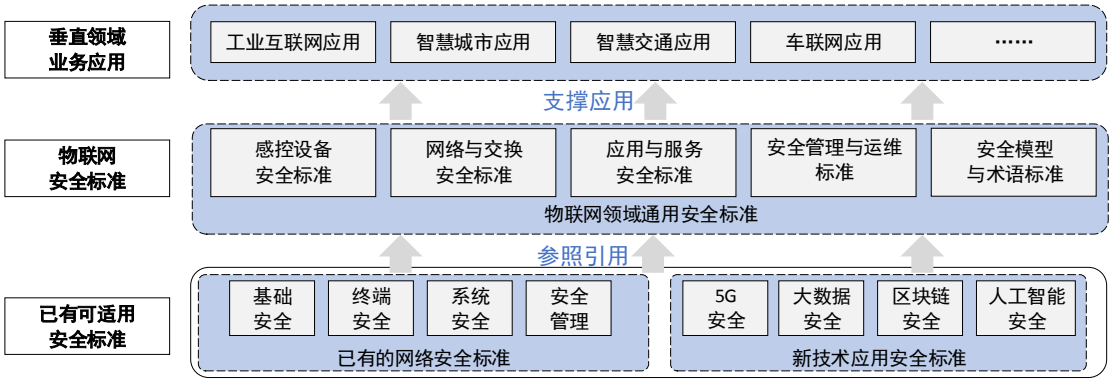


图 5.6 物联网安全标准与其他标准关系图

目前除 TC260 开展物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，物联网领域安全标准还需要引用或参照已有的可适用于物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，达到物联网安全生态的协同发展。

六、 物联网安全标准体系及推进建议

目前我国物联网的发展受到各行业的密切关注，但由于物联网的应用涉及到多种行业和多个领域，呈现跨度大、产业链长且涉及传统行业，导致其安全性控制较其他行业难度更大。因此，尽早对物联网安全标准进行整体布局尤为重要。

6.1 物联网安全标准分类

基于物联网安全标准化需求分析，从标准主题和标准类型两个维度建立物联网安全标准体系。

6.1.1 标准主题分类

根据第四章标准化需求分析，物联网安全标准按主题可以划分为五类，分别是基础与通用安全类、感控设备安全类、网络与交换安全类、应用与服务安全类和安全管控与运维类。

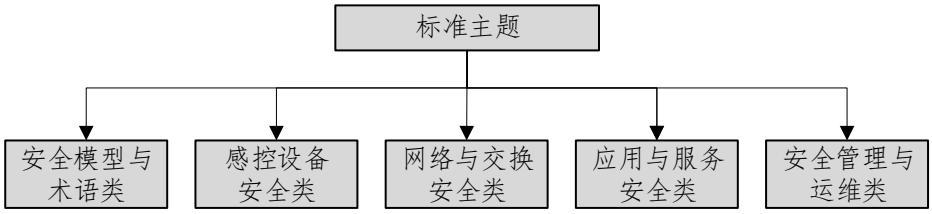


图 6.1 物联网安全标准主题分类

其中，安全模型与术语类标准主要包括术语、概念、模型、框架等相关内容；感控设备安全类标准主要包括感知终端安全、智能物联卡安全以及安全网关等相关内容；网络与交换安全类标准包括无线通信安全及传输交换安全等相关内容；应用与服务安全类标准包括业务服务平台和垂直领域等相关内容；安全管控与运维类标准包括安全漏洞管理、应急响应管理、安全态势感知和新技术应用安全等相关内容。

6.1.2 标准类型分类

物联网安全标准按类型可以划分为：综合类、安全要求类、实施指南类和检测评估类。

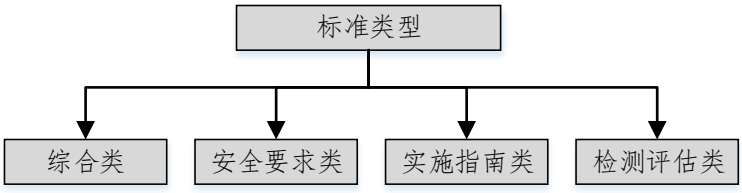


图 6.2 物联网安全标准类型分类图

其中,综合类标准旨在提供基础性的符号、术语、模型、框架等；安全要求类标准主要衔接上位法律法规，围绕物联网安全提出更具体明确的要求；实施指南类标准主要围绕安全要求的落实，基于最佳实践，给出具体的实施指导；检测评估类标准主要围绕评估具体实施是否满足安全要求展开。

6.2 物联网安全标准体系框架

基于物联网安全需求和标准类型，建立物联网安全标准分类体系。基于以上两个维度，通过梳理 TC260 已发布及在研的物联网安全标准和已发布的适用于物联网的通用安全标准，可以梳理物联网安全标准体系框架如图 6.3。相关标准具体信息详见附录 A.1 和 A.2。

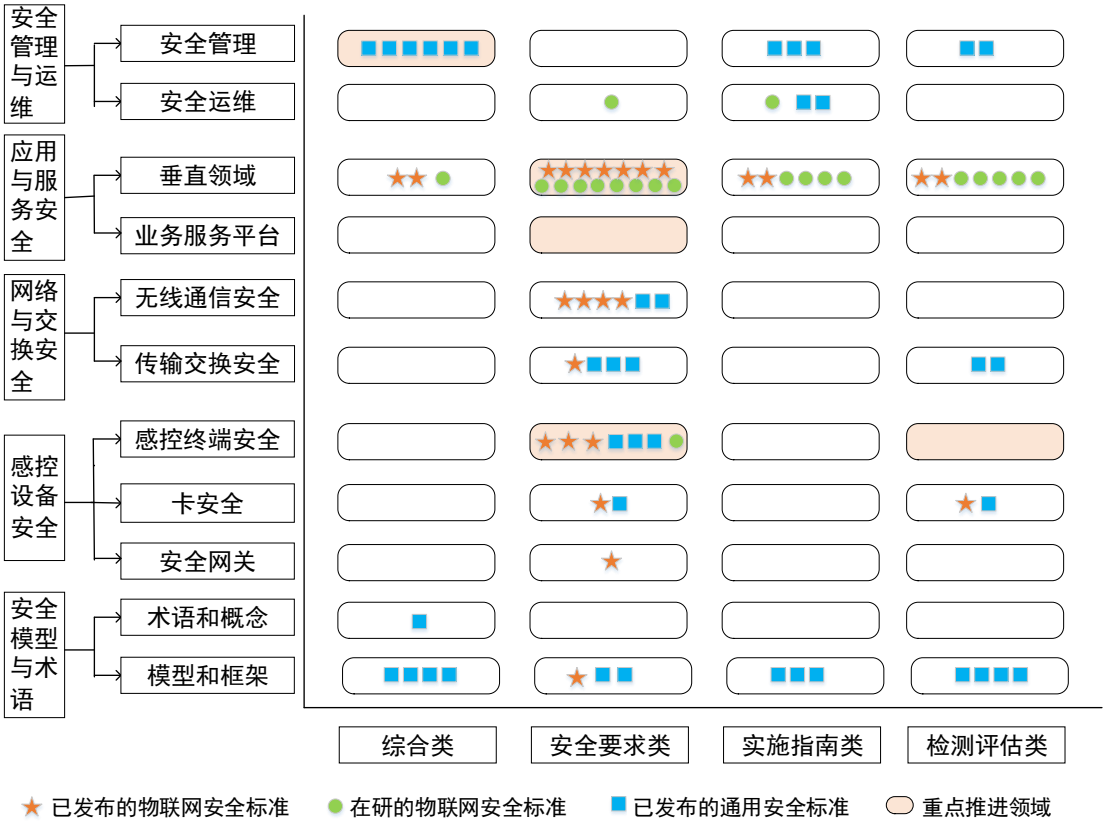


图 6.3 物联网安全标准体系框架

通过梳理物联网安全标准体系框架，可以明确现有标准的定位，并根据物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，更好的推动物联网应用和产业

发展，制定符合中国国情和物联网产业特点的安全标准，促进物联网安全标准研制有序开展。

6.3 标准现状分析

6.3.1 基础与通用类

TC260 已发布相关通用安全标准 14 项，已发布物联网安全模型与术语类标准 1 项，即 GB/T 37044—2018《信息安全技术　物联网安全参考模型及通用要求》。已发布的相关通用安全标准包括 GB/T 22239—2019《信息安全技术　网络安全等级保护基本要求》等系列标准，将物联网、工业控制系统、移动互联等列入了标准规范，并且具有适用性好、可操作性强等特征，能够在物联网领域进行应用。

GB/T 25069—2010《信息安全技术　术语》对信息安全一般概念术语、信息安全技术术语以及信息安全管理术语做出了界定，目前该标准正在修订中，物联网相关的部分术语，如智能卡、传感器等，已收录在最新版本中。随着物联网安全标准不断更新，为适应物联网领域概念体系，建议对 GB/T 25069—2010《信息安全技术　术语》进行持续修订。

6.3.2 感控设备类

TC260 已发布相关通用安全标准 4 项，已发布物联网感控设备类安全标准 6 项，在研 1 物联网安全标准项，为物联网感控设备的标准化工作提供了有意义的参考。

感控设备类标准应主要关注安全要求和检测评估类，现有安全要求类标准较多。鉴于物联网终端设备的特点，感控设备类标准需要在三个方面重点推进：首先，由于物联网终端的快速发展迭代及多样性，建议新增针对物联网新型设备的安全要求类标准，如智能车联设备、智能医疗设备等。其次，由于智能卡计算存储能力受限，需研制轻量化的密码算法和安全协议标准，并新增相应的安全要求类标准。第三个方面，由于智能卡设备涉及软硬件等多方面的安全要求，应在现有安全技术要求及检测指南的基础上新增检测评估类标准，为智能卡设备的安全要求实施提供更有针对性的指导。

6.3.3 网络与交换类

TC260 已发布相关通用安全标准有 7 项，已发布物联网网络与交换类 5 项安全标准。目前已制定的物联网数据传输、感知层协议、近场通信（NFC）、射频识别空中接口协议、感知层网关等安全技术要求相关标准，对物联网传输安全模型、感知层信息传输保护、通讯协议安全模式、密钥管理、通讯流程、算法要求、感知终端接入认证、网络访问控制、数据保护等方面进行了相应要求，并对 NFC、RFID 通讯协议机制、安全交换协议、密钥协商流程、协议规则、参数定义等进行了标准化的要求。

目前网络与交换类共有 11 项，其中 9 项为安全要求类标准。由于物联网设备安全接入方式的涉及多种新型传输协议，建议新增检测评估类安全标准，为物联网网络交换层提供更加细致的实施指导。

6.3.4 应用与服务类

物联网行业涉及众多垂直领域，如智慧城市、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。

TC260 已发布物联网应用与服务类安全标准 13 项、1 项已报批安全标准，包括工业控制系统、智能家居等相关内容。在研标准中，工业互联网和智慧城市行业标准进展较快，且布局较好。工业互联网方向已有在研标准共 9 项，包括通用风险评估、平台、系统、主机等方面。智慧城市方向在研标准共 6 项，包括体系框架、平台及风险评估等方面。各重点领域的安全标准研制呈现较为明显的不均衡现象，车联网领域在 2019 年完成首次安全技术要求的立项，智能安防、智慧农业等领域的安全标准还未启步，需重点推进这些领域安全标准的立项。

随着新一代无线通信技术与物联网场景的深度融合，边缘计算为物联网应用提供了更低的时延和近距离计算、存储能力。同时，边缘计算架构存在存在非授权访问、敏感数据泄露、(D)DoS 攻击等安全风险，建议新增边缘计算场景的安全防护技术要求类标准。

6.3.5 管理与运维类

TC260 已发布相关通用标准 12 项，包括安全管理及安全运维两个子类。

物联网安全管理涉及物联网卡、智能设备、物联网平台、基础资产等，需要进行整体的安全管控和运维，甄别关键威胁、脆弱性并做出智能响应，实现覆盖物联网业务安全的快速预警、统一呈现并对安全风险进行处置，保障物联网端到端的安全、可管、可控，建议重点关注物联网业务系统整体的安全监测、应急响应等问题。特别地，由于物联网与经济生活、社会生活密切相关，甚至直接事关线下人身安全，建议安全应急响应规范中安全处置方法以及处置流程等方面应充分考虑物联网各行业的特殊性。

6.4 近期重点工作方向

为进一步提升物联网安全标准规划体系性与重点聚焦性，适应当前物联网产业快速发展的需要，需进一步调整标准体系布局、加快重点领域规范研制。

6.4.1 完善物联网感控设备安全标准的研制

物联网感控设备存在终端数量大、能力差异大的特点，由于其同时涉及信息技术以外的电子、物理等领域，使其呈现出复杂性、多样性等特征，物联网感控设备安全是物联网安全标准工作的难点之一。同时，由于其计算资源的有限性、组网方式的多样性、物理终端实体的易接触性等，其安全防护需求也最为迫切。建议优先针对关键应用场景研制相应的感控设备安全技术规范，包括无人机设备安全管理要求、智能医疗设备安全技术及测评要求等。

物联网系统中的密码应用问题也与传统 IT 设备有所区别，如感知终端设备由于能量、功耗、存储空间、计算能力受限，无法运行或需要消耗过多的代价运行复杂的密码算法（公钥密码算法）和安全协议（密钥交换协议等）。建议基于上述应用需求，优先针对资源受限物联网设备研制轻量级密码算法（如基于身份的密码算法）的应用实施指南标准。

6.4.2 加快物联网垂直行业的安全标准研制

由于物联网具有广泛的应用性，不同行业和领域的物联网应用具有不同特点，所涉及的业务类型和服务场景因政策环境、行业环境不同存在差异。对重点行业应用的聚焦有利于针对不同的物联网应用场

景提供完善的安全技术标准，有利于解决物联网在行业之间或组织之间的应用服务安全和业务可持续发展问题，支撑行业物联网应用与服务的快速发展。

工业互联网安全是国家关注的重点领域，建议根据十部门《加强工业互联网安全工作的指导意见》等政策，进一步加快工业物联网网络设施安全、平台和工业应用程序（APP）安全、数据安全防护、测试实验环境等方面安全标准的推进。车联网应用发展迅速，目前已经具备一定的安全标准基础，建议重点推进车联网业务平台安全、车联网边缘计算安全等技术要求标准的研制。

6.4.3 推进物联网安全运维与管控标准研制

物联网业务涉及多个利益方，包括用户、设备制造商、网络运营商、服务提供者等，一旦出现安全问题，安全责任界面难以划分。因此，安全运维的过程中有效组织各相关方、及时判断异常行为，将极大提升物联网系统的安全和可靠性。建议在物联网安全运维、事件应急响应等方面加快安全标准研制，推动物联网安全生态的有效协同。

6.4.4 开展物联网通用业务服务平台安全规范研制

物联网生态系统中，有部分的传统行业，例如交通、医疗、物流、家居等，并没有能力打通物联网生态链，业务运营需要借助通用的业务服务平台。这些平台在为企业提供物联网业务助力的同时，如何应对物联网安全风险挑战，实现数据安全防护、身份认证、访问控制等，需要通过相关规范进行明确。建议加快物联网通用业务服务平台安全能力要求、物联网通用业务服务平台安全实现指南等规范的研制，加强平台安全能力，保护各行业在物联网环境下的安全运行。

6.4.5 加强数据安全标准的应用

针对物联网中涉及到的各类数据，包括个人信息、业务数据等，需依据国家相关法律政策及已发布的相关数据安全标准加强管理，做好各种场景下的数据安全管理工作。建议针对工业互联网、智慧城市等关键领域加强数据生命周期安全管理、个人信息以及数据交易等相关标准的应用实施，同时可针对这些领域研制相应的数据安全实现指南等国家标准。

七、 物联网安全标准化工作建议

着眼于物联网未来发展和安全需求，针对物联网未来发展可能面临的网络安全新形势和新需求，建议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，共同打造物联网安全生态，积极推动物联网安全健康发展。

7.1 不断完善安全标准体系

物联网安全标准化是构建物联网安全保障体系的技术保障，新时代网络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。通过安全标准指引，加强物联网全生命周期安全管理，构建覆盖物联网系统建设各环节的安全防护体系。在物联网系统规划、分析、设计、开发、建设、验收、运营维护以及废弃等各环节，明确安全管理要求，使安全融入到物联网系统建设全生命周期中。在开发阶段，严格依据要求和规范进行系统软硬件开发及测试，并阶段性开展安全测试；在建设、验收阶段，严格执行安全管理，在系统建设完成后进行安全风险评估，保障安全防护的有效性和合规性；在运营维护阶段，定期进行安全风险评估，持续跟踪威胁情报和信息，改进安全管理和防护措施；在系统废弃阶段，做好残余信息清理工作，形成全生命周期安全防护管理体系。

7.2 鼓励关键技术标准立项

鼓励安全芯片、安全协议、新的安全技术立项为国家标准。随着物联网技术的发展和应用的创新，未来物联网在服务系统、终端、通信网络等方面都将面临巨大挑战。下一步，我国应着眼于物联网未来发展趋势，引导研发机构、企业在物联网技术体系中关键核心技术的研究和标准制定方面加大力度，以关键共性技术和前沿引领技术的创新作为突破口，加快对高可靠认证、边缘计算、终端安全轻量化防护技术、软件定义边界等新技术新应用的研究和探索，形成安全标准并将其应用于物联网安全防护中，满足物联网未来发展的安全保护需求。

7.3 推动安全标准落地应用

国内已发布 GB/T 37044—2018《信息安全技术 物联网安全参考模型及通用要求》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》等系列国家和行业标准，为设备厂商、服务提供商、安全企业等开展物联网相关工作提供了技术要求和参考规范。下一步应完善安全标准化的运行机制，推动物联网安全标准从高速发展向高质量发展转型，建立健全标准的体系性和配套性，重点解决安全标准研制与应用脱节等问题，大力推进标准的实施应用，强化物联网安全标准试点和推广工作，开展物联网安全合规性评估，促进物联网产业良性发展。

7.4 加强安全标准人才培养

物联网安全标准化的推进需要大量高素质人才的支撑，一方面需要培养物联网安全专业人才，深入开展安全研究；另一方面，需要将已有的安全标准成果向物联网从业人员推广和宣贯，将安全规范成为物联网设计和实施的先天基因。因此，建议在从国家层面加强高等教育及职业教育的安全专业及物联网相关专业的课程规划，加强物联网安全及标准方面的课程设置和人才培养。在高等院校和科研机构，加大对物联网安全及标准化研究项目的支持力度，完善科研评价体系和中青年人才培养方案，优化科研管理，促进物联网安全研究与社会化教育的结合，激发物联网安全研究人员的创新动力。

7.5 打造物联网安全标准与产业生态

发挥物联网安全标准的桥梁作用，联合物联网产业链各方力量，共同打造物联网安全生态。物联网产业具有高度融合、应用多样、发展迅速等特点，其生态覆盖传感器元器件制造、设备集成生产、网络服务提供、软件服务提供、系统集成开发及销售等环节，安全问题更是涉及传感器、芯片、硬件，通信技术、网络服务以及相关行业领域应用等方面，因此构建开放、合作、共赢的安全生态圈是产业发展的必然趋势和要求。未来，我国需要从整机设备、核心芯片、安全运营服务等板块入手加快产业布局，形成产业链上下游协同创新的局面，推进产业转型升级，提升我国物联网安全产业核心竞争力。

附录 A 已发布及在研的相关标准

A.1 TC260 物联网安全相关标准

主题及分类		标准名称	标准编号
安全管理与运维	安全运维	工业控制系统现场安全运维规范	在研
		信息安全技术 工业互联网安全风险评估指南	在研
应用与服务安全	垂直领域	工业控制系统安全管理基本要求	GB/T 36323-2018
		工业控制系统信息安全分级规范	GB/T 36324-2018
		健康医疗信息安全指南	在研
		智慧城市安全体系框架	在研
		智能家居安全通用技术要求	报批
		工业控制系统现场测控设备通用安全功能要求	GB/T 36470-2018
		智慧城市公共支撑与服务平台安全要求	在研
		车载终端安全技术要求	在研
		车载网络设备信息安全技术要求	在研
		工业控制系统安全控制应用指南	GB/T 32919-2016
		工业互联网安全风险评估指南	在研
		工业互联网平台网络安全设计指南	在研
		智慧城市建设信息安全保障指南	在研
		汽车电子系统网络安全指南	在研
		工业控制系统风险评估实施指南	GB/T 36466-2018
		工业互联网安全风险评估规范	在研
		工业互联网平台安全要求及评估规范	在研
		工业互联网平台安全防护评估规范	在研
		工业控制系统主机安全防护系统安全技术要求和测试评价方法	在研
		工业控制系统信息安全防护能力评价方法	在研
		信息安全技术 工业控制系统主机安全防护系统安全技术要求和测试评价方法	在研
		汽车网络的安全技术要求及测评方法	在研
		汽车电子芯片安全技术要求	在研
		工业控制系统专用防火墙技术要求	GB/T 37933-2019
		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

		工业控制系统网络审计产品安全技术要求	GB/T 37941-2019
		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
		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 37954-2019
		工业控制系统产品信息安全通用评估准则	GB/T 37962-2019
		工业控制系统安全检查指南	GB/T 37980-2019
		公安物联网系统信息安全等级保护要求	GB/T 35317-2017
网络与交换安全	无线通信安全	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
		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
		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
		射频识别（RFID）系统通用安全技术要求	GB/T 35290-2017
	传输交换安全	物联网数据传输安全技术要求	GB/T 37025-2018
感控设备安全	感控终端安全	物联网感知设备安全技术要求	20152007-T-469
		物联网感知终端应用安全技术要求	GB/T 36951-2018
		物联网感知层接入通信网的安全要求	GB/T 37093-2018
		公安物联网感知终端安全防护技术要求	GB/T 35318-2017
		公安物联网感知终端接入安全技术要求	GB/T 35592—2017
		信息安全技术 智能门锁安全技术要求和测试评价方法	在研
	卡安全	智能卡安全技术要求（EAL4+）	GB/T 36950-2018
		智能卡通用安全检测指南	GB/T 31507-2015
	安全网关	物联网感知层网关安全技术要求	GB/T 37024-2018
基础与通用安全	模型和框架	物联网安全参考模型及通用要求	GB/T 37044-2018

A.2 TC260 适用于物联网的通用相关标准

主题及分类		标准名称	标准编号
安全管控与运维	安全运维	信息安全技术 信息安全风险处理实施指南	GB/T 33132-2016
		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
	安全管理	信息安全技术 信息安全应急响应计划规范	GB/T 24363-2009
		信息安全技术 网络安全预警指南	GB/T 32924-2016
		信息安全技术 信息安全事件分类分级指南	GB/Z 20986-2007
		信息安全技术 安全漏洞标识与描述规范	GB/T 28458-2012
		信息安全技术 信息安全漏洞管理规范	GB/T 30276-2013
		信息安全技术 安全漏洞等级划分指南	GB/T 30279-2013
		信息安全技术 安全漏洞分类	GB/T 33561-2017
		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
		信息安全技术 网络安全威胁信息格式规范	GB/T 36643-2018
		信息安全技术 统一威胁管理产品技术要求和测试评价方法	GB/T 31499-2015
网络与交换安全	传输交换安全	IPSec 协议应用测试规范	GB/T 28456-2012
		SSL 协议应用测试规范	GB/T 28457-2012
		信息安全技术 IPSec VPN 技术规范	GB/T 36968-2018
		信息安全技术 无线局域网客户端安全技术要求（评估保障级 2 级增强）	GB/T 33563-2017
		信息安全技术 无线局域网接入系统安全技术要求（评估保障级 2 级增强）	GB/T 33565-2017
		公共安全视频监控联网信息安全技术要求	GB 35114—2017
	无线通信安全	近场通信（NFC）安全技术要求 第 1 部分：NFCIP-1 安全服务和协议	GB/T 33746.1-2017
		近场通信（NFC）安全技术要求 第 2 部分：安全机制要求	GB/T 33746.2-2017
感控设备安全	感控终端安全	移动智能终端个人信息保护技术要求	GB/T 34978-2017
		移动智能终端操作系统安全技术要求和测试评价方法	GB/T 34976-2017
		移动智能终端数据存储安全技术要求与测试评价方法	GB/T 34977-2017

	卡安全	信息安全技术 智能卡通用安全检测指南	GB/T 31507-2015
		信息安全技术 智能卡读写机具安全技术要求（EAL4 增强）	GB/T 35101-2017
基础与通信安全	模型和框架	信息安全技术 网络安全等级保护基本要求	GB/T 22239-2019
		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
		信息安全技术 网络安全等级保护测评要求	GB/T 28448-2019
		信息技术 安全技术 信息技术安全性评估方法	GB/T 30270-2013
		信息安全技术 信息系统安全保障通用评估指南	GB/T 30273-2013
		信息技术 安全技术 信息技术安全保障框架 第 1 部分：综述和框架	GB/Z 29830.1-2013
		信息技术 安全技术 信息技术安全保障框架 第 2 部分：保障方法	GB/Z 29830.2-2013
		信息技术 安全技术 信息技术安全保障框架 第 3 部分：保障方法分析	GB/Z 29830.3-2013
		信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南	GB/Z 30286-2013
		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
		信息安全技术 网络安全等级保护测评过程指南	GB/T 28449-2018
		信息安全技术 网络安全等级保护安全管理中心技术要求	GB/T 36958-2018
		信息技术 安全技术 信息安全控制实践指南	GB/T 22081-2016
	术语和概念	信息安全技术 术语	GB/T 25069-2010

A.3 其它组织主要标准

组织	标准名称	编号
ISO/IEC JTC1	Internet of Things (IoT) -Reference architecture 物联网 参考体系架构	ISO/IEC 30141
	Information Technology-Home network security 信息技术 家庭网络安全	ISO/IEC 24767

	Information Security-Lightweight cryptography 信息技术 安全技术 轻量级加密	ISO/IEC 29192
	Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT) 信息技术 安全技术 物联网安全与隐私指南	ISO/IEC 27030
	Information technology — Security techniques — Security requirements for authentication using biometrics on mobile devices 移动设备使用生物特征识别进行鉴别的安全要求	ISO/IEC 27553
ITU-T	Reference architecture for IoT device capability exposure 物联网设备能力开放的参考架构	Y.4115
	Requirements and capability framework for IoT-based automotive emergency response system 基于物联网的自动应急响应系统的要求和能力框架	Y.4119
	Requirements and reference model of IoT-related crowdsourced systems 物联网相关众包系统的要求和参考模型	Y.4205
	Internet of things (IoT) security 物联网安全系列标准	X.1360-X.1369
	Common requirements for Internet of things (IoT) applications 物联网应用的通用要求	Y.4103/ F.748.0
	Requirements and common characteristics of the IoT identifier for the IoT service 物联网服务标识的要求和通用特性	F.748.1
	Secure software update capability for intelligent transportation system communication devices 智能交通系统通信设备的安全软件更新能力	X.1373
	Object identifier-based resolution framework for IoT grouped services 基于对象标识符的物联网分组服务解析框架	X.676(X.orf-gs)
	Security framework for Internet of Things based on the gateway model 基于网关模型的物联网安全架构	X.1361(X.iotsec-2)
	Simple encryption procedure for Internet of Things (IoT) environments 物联网环境的简单加密流程	X.1362(X.iotsec-1)
	Aggregate message authentication scheme with group authentication capability for IoT environment	X.amas-iot

ITU-T	面向物联网环境的具有组鉴别能力的聚合消息鉴别方案	
	Standard format of IoT error logs for security incident operations 物联网安全事件操作错误日志的标准格式	X.elf-iot
	Security framework for use of identity-based cryptography in support of IoT services over Telecom networks 基于电信网络的使用基于标识的密码系统的安全框架	X.ibc-iot
	Technical framework of PII (Personally Identifiable Information) handling system in IoT environment 物联网环境中个人可识别信息处理系统的技术框架	X.iotsec-3
	Security requirements for IoT devices and gateway 物联网设备和网关的安全要求	X.iotsec-4
	Security requirements and framework for narrow band internet of things 物联网服务平台的安全要求和框架	X.nb-iot
	Security controls for Internet of Things (IoT) systems 物联网系统的安全控制措施	X.sc-iot
	Secure software update for IoT devices 物联网设备的安全软件更新	X.secup-iot
	ITU-T X.660 –Supplement on Guidelines for using object identifiers (OID) for the Internet of Things 物联网对象标识符（OID）使用指南增补	X.sup-oid-iot
	Security requirements for vehicle accessible external devices 车辆外接设备的安全要求	X.itssec-3
	Methodologies for intrusion detection system on in-vehicle systems 车内系统的入侵检测系统方法	X.itssec-4
	Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles 基于联网车辆大数据分析的异常行为检测机制	sX.mdcv
	Security threats in connected vehicles 联网车辆的安全威胁	X.stcv
	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks	X.509

	信息技术——开放系统互连——目录:公钥和属性证书框架	
ETSI	Cyber Security for Consumer Internet of Things 消费类物联网安全	ETSI TS 103 645
	options and analyses for the security features and mechanisms providing end-to-end security and group authentication for oneM2M oneM2M 端到端安全及组认证的安全特性和机制分析	ETSI TR 118 512
IETF	6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) 6LoWPAN-GHC: 6LoWPANs 的通用头部压缩	RFC7400
	Use Cases for Authentication and Authorization in Constrained Environments 受限环境下认证和授权的案例	RFC7744
	Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things IoT TLS/DTLS	RFC7925
	CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets 基于 TCP, TLS 和 WebSockets 的 CoAP 协议	RFC8323
	Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation IKEv2 协议	RFC7815
	The Transport Layer Security (TLS) Protocol Version 1.3 传输层安全(TLS)协议 V1.3	RFC 8446
TCG	Hardware Requirements for a Device Identifier Composition Engine 设备标识符组合引擎的硬件要求	Family “2.0” Level 00 Revision 78

附录 B 物联网安全标准应用实践案例

B.1 视频监控领域的应用实践

1、安全实践介绍

由于移动监控具备灵活性强，部署快捷，易应用的特点，具有固定监控不可替代的优势，可以有效弥补固定监控的不足，大大增强动态实时信息的获取能力。近年来，随着音视频编解码、无线宽带通信的技术发展，以及信息化、智能化的推进，移动视频监控已经开始普及，并在多个公共安全应用领域崭露头角。如今，海康、大华、宇视等视频监控行业巨头，围绕智能头盔/眼镜（人/车识别）、车载终端（车牌识别、交通违法抓拍）、无人机、机器人等物联网新兴应用，已经推出了车载高清系统、机器人视觉、多旋翼飞行器、个人可穿戴等多种系列的产品。这些产品为满足公安、交通等行业移动执法取证的需求，普遍采用 H.264、H.265、4K 等编码技术，3G/4G 全网通，并内置 WiFi 等无线通信技术，并将图像采集、车牌识别、车辆特征识别、人脸识别、手机 MAC 地址采集、GPS 定位等集成一体，具有现场执法取证、移动布控、路面巡逻、信息采集、车辆违停取证、全局动态感知等业务功能，实现了移动监控系统智能化管理，极大地提高了一线民警的工作效率，更好的保障了社会安定和人民安全。此外，多种产品满足水平方向 360 度连续旋转的监控需求，实现无死角监控，可快速地捕捉到目标，操作方便灵活。

2、安全标准应用情况

由于视频监控涉及到诸多的敏感信息和个人隐私等问题，和传统固定式视频监控系统一样，移动监控系统存在更多的安全风险。不仅有弱终端、弱密码等终端安全问题，还有开放式环境中的干扰、劫持，数据泄露等诸多安全威胁。而且，每一项威胁都足以对应用产生致命的打击和破坏。

鉴于以上威胁，目前主流的安全方案集中在设备认证、无线通信加密、专用无线信道、后端安全接入系统、系统互连安全系统等方面。技术实施主要以 GB/T 35592—2017《公安物联网感知终端接入安全技术要求》、GB 35114—2017《公共安全视频监控联网信息安全技术

要求》、GB/T 37093—2018《信息安全技术　物联网感知层接入通信网的安全要求》等标准为指导。具体地在移动视频监控终端上部署软/硬件数字证书，采用无线公网专用信道及隧道加密与后端接入系统进行连接，其中采用 SM2 算法用于认证、签名和秘钥协商，采用 SM1、SM4 等算法用于内容加密，采用 SM3 算法用于完整性校验。对于可穿戴或微型设备采用物联网安全网关、安全移动终端为网络中转接入后端的安全接入系统。后端安全接入系统，主要提供强大的宽带网络接入和加解密硬件支持，建立稳定的专用加密信道，提供对整个应用系统的安全保障。

3、安全标准需求及建议

视频图像数据的多部门互通，信息的交换处理是目前形成应用升级的主要途径。因此，突破瓶颈方面，建议考虑制定如下安全标准：视频监控数据敏感标识技术标准（安全分级）、移动视频监控数据的交换和共享安全技术标准（规定可共享程度、范围、技术保障要求、脱敏处理等）等。

B.2 公安核查领域的安全实践

1、安全实践介绍

信息化、动态化社会条件下，人员的流动更加频繁、迅速，虽然公安机关对重点人员的旅客订票信息、旅店住宿登记、网吧上网记录、卡口车辆通行记录、监所关押登记等等动态轨迹信息掌控作用明显，但重点人员的漏管漏控现象依旧严重。移动警务核查核录终端与平台是根据公安一线业务实际，以进一步提升公安机关反恐维稳、重大活动安保和治安防范能力为目标，以情报平台为支撑，所建设的涵盖车站、码头、重大活动场所、固定治安卡点、党政机关、企事业单位以及街面的信息采集暨身份核录系统，该系统依托多样化的信息采集核查终端设备，实时采集和掌握重点区域、部位的重点人员、准重点人员行动轨迹，开展重点人员查询比对等工作，逐步形成覆盖社会面的重点人员信息采集、核查网络，实现重点人员的全方位、立体式管控。

移动核查核录系统是一种典型的物联网系统。系统由移动警务核查核录终端设备、安全接入和后台信息交互三个部分组成，实现了涵

盖现场人员身份核查核录、接入安全管控和移动警务等功能的"云"+"管"+"端" 一体化应用方案和融合服务模式。其技术特点是将传统的人工笔记核录升级为移动终端智能核录，实现了核录过程的智能化、全方位化和高效化，且满足了在线离线双模核录的实战应用。系统采用在 B/S 三层架构基础上扩展的多层架构，数据访问与业务逻辑分离，具备可扩展能力，界面设计中使用了 HTML+CSS+JavaScript 的技术路线，在数据的显示和操作页面中大量的使用了 Jquery 和 Easy UI 等 JavaScript 动态技术，平台比对资源库构建中数据采集与汇聚、信息提取与处理、数据和信息展示与应用采用 ETL 数据集成技术，系统按照功能模块化原则开发，遵循 J2EE 技术标准。具备身份证信息采集核对、高清视频/图像采集、人脸比对、无线数据传输、GPS 定位、信息统计展示、数据分析、通知告警等功能。一线民警通过系统，采集重点场所/位置、关注人员的实时信息，并开展基于数据分析、比对、告警等服务的自动化查询，实现关注人员管控。

2、安全标准应用情况

根据移动核查核录系统本身的组成和开放式应用特点，其基于嵌入式系统平台的终端设备和无线为主的数据通信方式，主要存在终端和用户的非法接入，重要场所、关注人员等敏感实时信息的泄露等问题。由于此类问题一旦发生，容易引起极大的社会关注和治安方面不良影响。因此，必须要有相应的信息安全技术保障。

针对核查核录系统应用的行业特殊性，系统的安全方案是以基于硬件数字证书或安全硬件的 PKI 安全机制基础设施为根本，重点对终端进行安全加固，并在信息化应用前部署安全接入系统。技术实施主要参考 GB/T 35317-2017《公安物联网系统信息安全等级保护要求》、GB/T 35318-2017《公安物联网感知终端安全防护技术要求》、GB/T 35592-2017《公安物联网感知终端接入安全技术要求》等标准。具体地在核查核录终端上部署数字证书和安全加固软件，采用无线公网专用信道及隧道加密与后端接入系统进行连接，其中采用 SM2 算法用于认证、签名和秘钥协商，采用 SM1、SM4 等算法用于内容加密，采用 SM3 算法用于完整性校验。后端安全接入系统，主要提供可靠

的多路接入和快速加解密硬件支持，建立稳定的专用加密信道，安全系统的设备认证、用户管理、数据存储和传输安全。

3、安全标准需求及建议

针对个人身份信息及特征的比对、核实、验证应用方面，建议考虑制定如下安全标准：个人身份信息采集及数据保护技术标准（对应用中产生的数据的安全防护进行规范化）、信息脱敏处理比对技术标准（同态化处理标准化安全机制、数据防碰撞处理要求等）。

B.3 智能家居领域的应用实践

1、安全实践介绍

智能家居是物联网重要应用领域。微软研发的物联网安全应用平台 Azure Sphere 可提供一个端到端的物联网安全解决方案，在智能家居应用中提供安全服务。Azure Sphere 包含了定制的安全微控制器单元、用于开发应用程序的工具和 SDK，以及 Azure Sphere 安全服务，通过该服务应用程序可以安全地连接到云和 web。

Azure Sphere 团队确定了高度安全设备的 7 个属性。Azure Sphere 平台围绕这 7 个属性而设计，见表 B.1。

表 B.1 高安全平台的 7 个属性

属性	描述
基于硬件的信任根	基于硬件的信任根可确保设备及其标识不可分离，从而防止设备伪造或欺骗。Microsoft 设计的 Pluton 安全子系统硬件将生成不可伪造的加密密钥并对此进行保护，将由该密钥标识每个 Azure Sphere MCU。 这可确保从工厂到最终用户均不能篡改硬件信任根，保证其安全可靠。
小型可信计算基	设备的大多数软件仍在可信计算基础范围之外，从而缩小了攻击面。只有安全的安全监视器、Pluton 运行时以及 Pluton 子系统（均由 Microsoft 提供）在可信计算基础上运行。
深度防御	深度防御提供了多层的安全性，因此可以对每个威胁进行多重缓解。Azure Sphere 平台中的每个软件层都会验证其上一层是否安全。
分隔	分隔可限制任何单一故障的范围。 Azure Sphere MCU 具有硬件防火墙等硅应对措施，可防止某一组件的安全漏洞扩散到其他组件。 受约束的“沙盒”运行时环境可防止应用程序损坏受保护的代码或数据。
基于证书的身份验证	相较于密码验证，使用由不可伪造的加密密钥验证的签名证书可提供更安全可靠的身份验证。 Azure Sphere 平台要求对每个软件元素进行签名。 设备到云和云到设备通信要求进行进一步的基于证书的身份验证。
可更新的安全性	设备软件将自动更新以修复已知的漏洞或安全漏洞，无需产品制造商或最终用户的干预。 Azure Sphere 安全服务将自动更新 Azure Sphere OS 和 OEM 应用程序。

故障报告	设备软件或硬件故障是典型的新兴安全攻击；设备故障本身会造成拒绝服务攻击。设备到云的通信提供对潜在故障的早期警告。Azure Sphere 设备可自动报告操作数据和基于云的分析系统故障，并可远程执行更新和维护。

2、安全标准应用情况

针对物联网安全标准的采纳，Azure Sphere 基于证书的身份验证遵从数字证书的国际标准和 TLS 安全连接的标准。此外，为了解决物联网的低成本安全需求,微软在 2016 年启动了一个鲁棒 IoT 项目，今天，同样的概念被标准化为可信计算组（TCG）设备标识符组合引擎的硬件要求（Hardware Requirements for a Device Identifier Composition Engine，DICE），目前微软连接到 Azure 物联网中心云服务的物联网设备亦采纳了 DICE 规范。DICE 提供了一种低成本的方法来保护物联网设备的身份，并验证设备上启动的软件来保证设备软件的完整性，能够从源头上减少安全事件的发生。微软还与工业互联网联盟（Industrial Internet Consortium）合作，创建了一个新的物联网安全成熟度模型，为评估物联网风险概况和规划所需的补救措施提供了清晰的行业最佳实践。

3、安全标准需求及建议

针对物联网安全标准具体建议如下：

在不同行业针对行业的特点，设立行业特有的安全标准和规范，以应对行业的特殊性，支撑行业健康发展。

针对各个行业的共性，参照国际最佳实践设置安全基线类的规范和标准，以规避常见的安全问题，从而将安全风险降到最低。

政府和主管部门能够给出顶层的建议性的安全指南以指导产业协同发展；统一同类的规范，减少产业链中的碎片化现象。

从终端和设备标识出发，逐级建立相应的规范，保证终端和设备的可识别性、可更新、快速可恢复性，从而从源头减少物联网安全风险。

总体上来讲，物联网涉及到广泛的产业链条，构建安全健康的物联网生态需要各方的努力，也离不开政府部门的引导、监管和协调。在制定、更新和维护物联网安全相关指南规范的时候，包括一个具有

广泛代表性的利益攸关方小组对于规范的制定是非常有效的。建议加大政企研的合作，从不同的角度为物联网安全助力，赋能各个行业。

B.4 终端检测领域的应用实践

1、安全实践介绍

IoT 终端种类日益众多，各个厂商的设备具有不同的功能以及实现方式，安全水平参差不齐，难免出现众多安全问题。这些终端一旦被控制，可以被用于影响业务正常运行或向平台及网络发起攻击，甚至进一步影响其他互联网用户。如何在海量终端中快速识别异常终端并隔离，是 IoT 安全解决方案重要的一个技术关注点。

华为公司研发的异常终端检测与隔离技术主要包括以下部分：

- 及时发现：检测设备被劫持、入侵、身份仿冒风险
- 尽早处理：支持对异常设备隔离、强制升级等操作
- 风险可视化：基于租户视角海量设备的安全可视

具体而言，该技术在保护隐私的基础上，结合物联网设备的属性、配置，对设备的告警、行为等进行领域建模、大数据分析，结合外部的情报系统，识别和检测出物联网设备异常，将确定的恶意设备进行隔离，实现对设备正常、可疑状态、确定异常三种状态可视检测，并对确认异常终端处置。

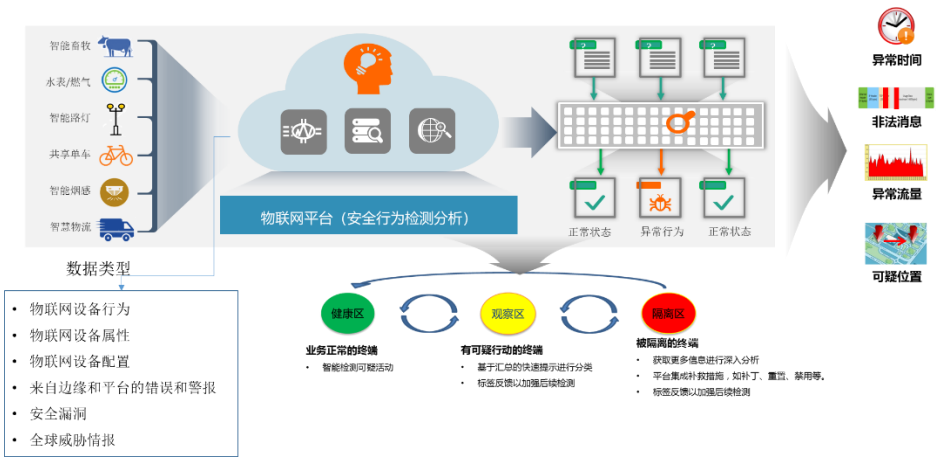


图 B.2 异常终端检测

2、安全标准应用情况

在该技术的使用上，充分参考和结合了 GB/T 37044—2018《信息

安全技术　物联网安全参考模型及通用要求》、GB/T 36951—2018《信息安全技术　物联网感知终端应用安全技术要求》考虑物联网整体架构及物联网终端设备的安全特征，开展了物联网设备安全异常检测。

3、安全标准需求及建议

物联网设备的异常检测和通用的安全检测有类似之处，但是也有物联网自身的安全特征，只有发现这些特征才能更有效的开展物联网终端安全检测。建议可以将物联网终端的安全检测关键要素、接口、检测正确率及异常设备隔离手段等方面进行标准化，提升物联网异常检测的标准化程度。

B.5 安全管理领域的应用实践

1、安全方案实践介绍

由于物联网终端安全能力参差不齐，业务暴露面大，物联网的安全风险分析和管理面临新的挑战。面对物联网行业新的安全风险，中国移动基于中国移动物联网运营大数据，建立安全数据中心、安全分析子平台等，利用异常行为检测、聚类分析、深度学习等技术，研究全方位的物联网安全风险分析技术及管理方案，开展物联网终端、业务、基础资产等方面的安全风险分析与管理，全力保障物联网业务安全运行，全方位提升物联网安全管理及运营能力。

图 B.1 物联网安全风险管理逻辑架构

- 物联网智能终端安全风险管理：通过对终端的脆弱性分析、异常行为分析、异常连接等发现终端感染、受控、僵尸网络、异常访问等威胁，实现物联网智能终端的安全威胁感知，并

进行预警及处置管理。

- 物联网平台安全风险管理：从技术和管理层面协同保障物联网平台安全，通过对流量及设备安全日志等信息进行集中监控分析，建立安全分析模型，实现对物联网平台逻辑安全、数据安全、业务访问安全、威胁情报、APP 安全等方面的安全威胁监控和感知，并进行预警及处置管理。
- 物联网基础资产安全风险管理：通过对物联网基础安全威胁、内部资产及暴露面资产、脆弱性与漏洞、安全溯源等方面进行监测分析，实现物联网基础资产的安全威胁感知，并进行预警及处置管理。

2、安全标准应用情况

在该平台的使用和建设过程中，参考和结合了 GB/T 37044—2018《信息安全技术　物联网安全参考模型及通用要求》、GB/T 37025—2018《信息安全技术　物联网数据传输安全技术要求》、GB/T 36951—2018《信息安全技术　物联网感知终端应用安全技术要求》等安全标准，充分考虑了物联网整体架构及安全特征开展物联网安全威胁感知和管理相关工作。

通过在中国移动物联网安全管理方面的实际运行，其安全风险分析和管理技术在终端、业务等的异常监测和预警处置方面发挥了不可替代的作用。相关成果、实践经验正在推动形成相关行业标准，力争成为最佳实践。

3、安全标准需求及建议

目前国家标准在物联网安全风险分析技术及管理方面，特别是在安全安全管理要求方面比较欠缺，需统一相关要求。建议推进研制物联网终端、物联网平台等安全管理国家标准，推动物联网业务安全健康发展。

附录 C 缩略语

5G	第五代移动通信技术（5th-Generation）
5GAA	5G 汽车协会（5G Automotive Association）
AI	人工智能（Artificial Intelligence）
AII	工业互联网产业联盟（Alliance of Industrial Internet）
AIOTI	物联网创新联盟（Alliance for Internet of Things Innovation）
AP	无线访问接入点（Wireless Access Point）
APN	接入点（Access Point Name）
CCSA	中国通信标准化协会（China Communications Standards Association）
CC	信息技术安全评价通用准则（The Common Criteria for Information Technology security Evaluation）
COS	芯片操作系统（Chip Operating System）
C-V2X	蜂窝式车用无线通信技术（Cellular Vehicle-to-Everything）
DoS	拒绝服务（Denial of Service）
DDoS	布式拒绝服务（Distributed Denial of Service）
DICE	设备标识组件（Device Identifier Composition Engine）
DTLS	数据包传输层安全协议（Datagram Transport Layer Security）
ENISA	欧盟网络空间安全局（European Union Agency for Cybersecurity）
ETSI	欧洲电信标准协会（European Telecommunications Standards Institute）
GSMA	全球移动通讯系统协会（Global System for Mobile Communications Association）
ICT	信息通信技术（Information and Communications Technology）
IEC	国际电工委员会（International Electro technical Commission）
IERC	物联网欧洲研究集群（European Research Cluster on the Internet of Things）
IETF	互联网工程任务组（The Internet Engineering Task Force）
IIC	工业互联网联盟（Industrial Internet Consortium）
IIoT	工业物联网（Industrial Internet of Things）
IP	互联网协议（Internet Protocol）
IPSec	IP 安全协议（Internet Protocol Security protocol）
ISO	国际标准化组织（International Organization for Standardization）
IT	信息技术（Information Technology）
ITU	国际电信联盟（International Telecommunication Union）
NB-IoT	窄带物联网（Narrow Band Internet of Things）

NFC	近场通信（Near Field Communication）
NFV	网络功能虚拟化（Network Virtualization Function）
NIST	美国国家标准与技术研究院（National Institute of Standards and Technology）
NTIA	美国国家电信和信息管理局（National Telecommunications and Information Administration）
P2P	对等计算（peer-to-peer）
PC	个人计算机（Personal Computer）
PGP	良好隐私保护（Pretty Good Privacy）
PKI	公钥基础设施（Public Key Infrastructure）
RFC	互联网技术规范（Request For Comments）
RFID	无线射频识别（Radio Frequency Identification）
SaaS	软件即服务（Software-as-a-Service）
SCMS	安全凭据管理系统（Security Credential Management System）
SDN	软件定义网络（Software Defined Networking）
SIM	用户身份识别模块（Subscriber Identification Module）
SSL	安全套接层协议（Secure Sockets Layer protocol）
TC260	全国信息安全标准化技术委员会
TCG	可信计算组织（Trusted Computing Group）
TEEP	可信执行环境配置（Trusted Execution Environment Provisioning）
TLS	传输层安全协议（Transport Layer Security）
VPN	虚拟专用网（Virtual Private Network）
WiFi	无线保真（Wireless Fidelity）
ZigBee	紫蜂协议

参考文献

[1] 中国信息通信研究院，中国移动通信集团信息安全管理与运行中心.《物联网安全白皮书》. 2018.

[2] 中国移动通信集团公司. 《NB-IoT 安全白皮书》. 2017.

[3] 全国信息安全标准化技术委员会.《信息安全技术 物联网安全参考模型及通用要求》.GB/T 37044—2018.

[4]孙伟. 物联网通信技术的发展现状研究[J]. 中国新通信,2018,20(12):37.

[5]佟浩.探析移动通信技术在物联网中的应用[J]. 中国新通信,2018,(5):9.doi:10.3969/j.issn.1673-4866.2018.05.008.

[6]蒙南,方磊坤. 4G 通信技术在物联网中的应用展望[J]. 中国新通信,2017,(13):85

[7]王武志. 移动通信技术在物联网中的应用探讨[J]. 数字技术与应用,2017,(5):251,254.

[8]李国瑞. 物联网中常用的几种短距离无线通信技术[J]. 信息通信,2017,(10):213-214.doi:10.3969/j.issn.1673-1131.2017.10.101.

[9]范春辉. 物联网短距离无线传输技术研究[J]. 无线互联科技,2017,(19):23-24.doi:10.3969/j.issn.1672-6944.2017.19.010

[10]许洪华. 现场总线与工业以太网技术[M]. 电子工业出版社, 2007.

[11]范红, 邵华, 李程远. 物联网安全技术体系研究[J]. 信息网络安全, 2011(9):5-8.

[12]武传坤.中国的物联网安全：技术发展与政策建议.人民论坛-学术前沿，2016.

[13]全国信息安全标准化技术委员会.《信息技术 安全技术 信息技术安全评估准则》. GB/T 18336—2008

[14]全国信息安全标准化技术委员会.《信息安全技术 物联网安全参考模型及通用要求》. GB/T 37044—2018

[15] ISO/IEC 30141:2018 Internet of Things（IoT）-Reference architecture

[16]NIST Interagency Report(NISTIR) 8200, Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things(IoT), National Institute of Standards and Technology,2018.

[17]NIST SP 800-193: Platform Firmware Resiliency Guidelines.

[18]US Department of Homeland Security. Strategic Principles for Securing the Internet of Things (IoT).2016.

[19]Federal Trade Commission. Internet of Things: Privacy and Security in a Connected World.2015.

[20]Automotive Information Sharing and Analysis Center. Automotive Cybersecurity Best Practices.2016.

[21]European Union Agency For Network And Information Security. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.2017.