



工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

工业互联网平台安全国家标准进展现状

汇报人：中国电子技术标准化研究院、李琳
汇报日期：2019年5月9日

目录

CONTENTS

第一部分



工业互联网发展现状

第二部分



标准化需求与平台安全特点

第三部分



国家标准相关进展

第四部分



下一步工作建议

目录

CONTENTS

第一部分



工业互联网发展现状

第二部分



标准化需求与平台安全特点

第三部分



国家标准相关进展

第四部分



下一步工作建议

1 背景

时代背景

- ⑩ 随着新一代信息技术与制造业深度融合，工业互联网成为推动制造业转型升级、发展实体经济的新型网络基础设施；
- ⑩ 工业互联网平台作为工业互联网的核心，是实体经济全要素连接的枢纽、资源配置的中心和智能制造的大脑；
- ⑩ 工业互联网平台已成为发达国家推进“再工业化”战略、抢占新一轮科技革命和产业变革制高点的必争之地，更是我国工业实现换道超车的重要机遇。

我国政策背景

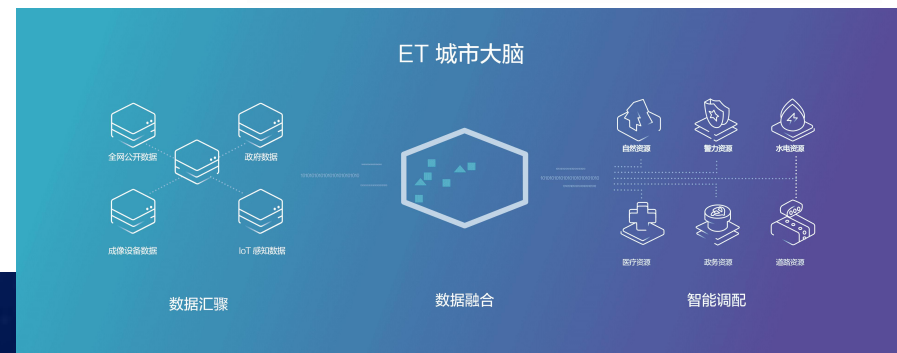
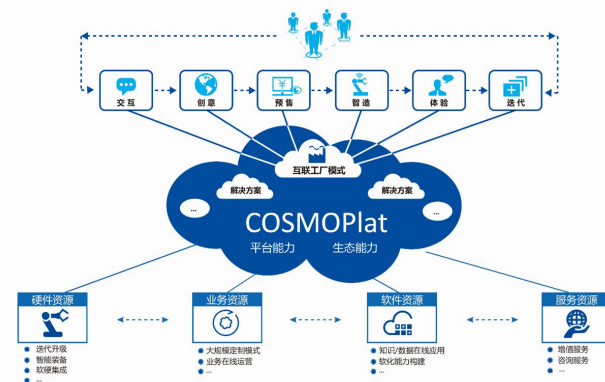
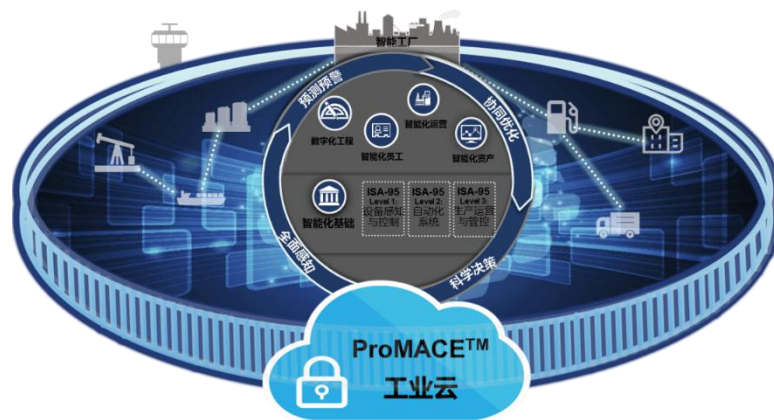
- ⑩ 2017年11月，国务院印发了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》（以下简称：《指导意见》），明确将打造平台体系作为七大任务之一，提出构建工业互联网标准体系，实施标准研制及试验验证工程；
- ⑩ 工业互联网平台标准体系作为工业互联网标准体系的重要组成部分，是打造平台体系的基础技术支撑，有助于统一认识、促进技术成果转化和应用、构建平台发展生态。

国际竞争压力

- ⑩ 美国实施“再工业化”战略，产业界提出了工业互联网，核心功能是将机器、物料、人、信息系统连接起来，结合软件和大数据分析，进行科学决策与智能控制，提高制造资源配置效率，大幅降低生产成本；
- ⑩ 德国在《德国2020高技术战略》中提出工业4.0战略，通过将机器设备、零部件、物料、人等进行数字转化，进行网络连接，实现设备之间、工厂之间横向集成，提高生产效率。

1 发展现状 国内情况

- 近年来，我国工业互联网的发展促进了多产业生态系统的融合，包括先进制造、先进计算、普适感知、泛在网络与智能分析等，在国内引发极大关注。
- 国内外已有大量工业互联网平台，在国内，已有诸如航天云网的INDICS平台、树根互联的根云平台、海尔COSMOPlat平台、华为的OceanConnect IoT平台、和利时的HIACloud平台、石化盈科的ProMace平台、阿里巴巴的阿里云ET工业大脑平台等。
- 总体上，我国工业互联网发展已逐渐从顶层规划迈入应用实施的初级阶段。



1 发展现状

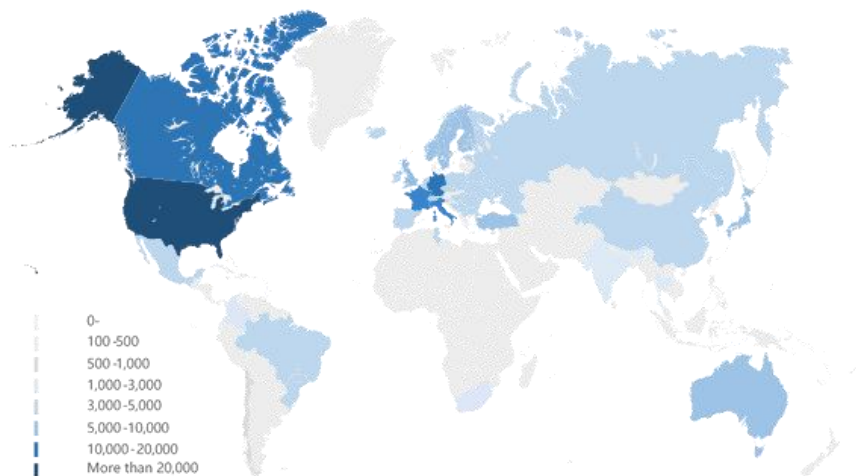
国际情况

- GE联合AT&T、CISCO、IBM、INTEL等企业组建工业互联网联盟(IIC)，发布参考架构IIRA，发挥美国互联网优势，以IT技术和网络技术为主要手段，打造服务于制造业的通用平台，实现多个行业业务的横向集成，促进行业信息融合，提高制造资源的配置效率。
- 德国联邦政府支持相关行业协会建设工业4.0平台，负责工业4.0国家战略的宣传推广、标准制定、人才培养和技术研发等。工业4.0平台发挥了德国传统制造业优势，在深耕专业领域的基础上，借助工业互联网平台，面向不同行业提供定制化解决方案，实现价值从业务需求到设备资产的纵向延伸。
- 目前，全球工业互联网平台数量已经超过150个。

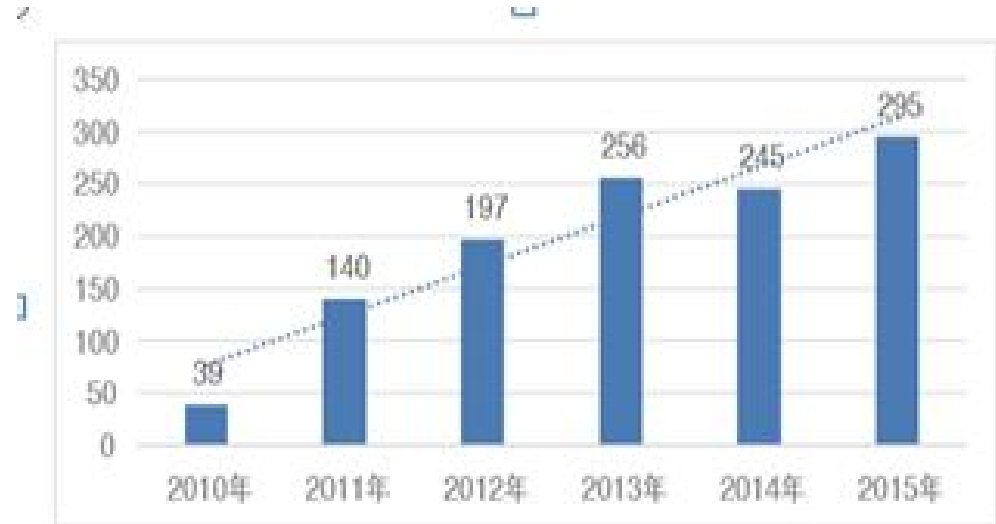
国家	研究内容	成果
 美国	GE Predix主打工业互联网综合平台，采用数据流打通与数据分析衍生价值的结构。	Predix平台
 德国	MindSphere是西门子推出的基于云的开放式物联网操作系统，MindSphere的优势在于能够实现全面的系统集成和数据融合，帮助用户打破“数据孤岛”。	MindSphere平台
 中国	以工业大数据为驱动，以云计算、大数据、物联网技术为核心的工业互联网开放平台，可以实现产品、机器、数据、人的全面互联互通和综合集成。	INDICS平台 “根云”平台 COSMO平台等

1

发展现状 面临的挑战



全球接入互联网的工控系统地域分布图



工业互联网相关安全事件数量统计图

- 工业信息安全事件逐渐上升，随着工业互联网的发展，伴随着协同制造、大规模个性化定制等先进制造需求的提升，大数据、云计算促使工业云的迭代升级，也带来了接入边界安全、数据存储分析安全、控制指令下发、恶意入侵问题。
- 相关工业互联网企业也逐步开展了工业互联网平台安全防护工作，采用边界防护、访问控制、主机安全加固等防护手段。

目录

CONTENTS

第一部分

工业互联网发展现状

第二部分

标准化需求与平台安全特点

第三部分

国家标准相关进展

第四部分

下一步工作建议

2 标准化需求 标准化使命

工业互联网平台标准化的使命是营造可持续发展的工业互联网平台生态，支撑政府、服务产业，发挥“标准化+工业互联网平台”的最大价值，推动互联网和实体经济融合发展。

- 推动互联网和实体经济融合发展 •
- 营造可持续发展的工业互联网平台生态



2

标准化需求 安全保障对象

- 工业企业管理网、控制网和外网的安全；
- 确保传输安全和运行安全。

- 标识解析系统的安全；
- 保障系统安全可靠运行。



- 工业云平台的安全；
- 应加强工业云服务网络安全管理，明确平台管理和运行主体责任。

- 工业生产业务活动中产生、采集、处理和使用的数据的安全；
- 要建立工业数据分类分级管理制度，形成工业互联网数据流动管理机制，解决工业数据流动方向和路径复杂导致的数据安全防护难度增大等问题。

- PLC、SCADA、DCS等工业控制系统安全；
- 提升自主可控的工控系统比例；
- 将安全问题考虑到生产设计中。

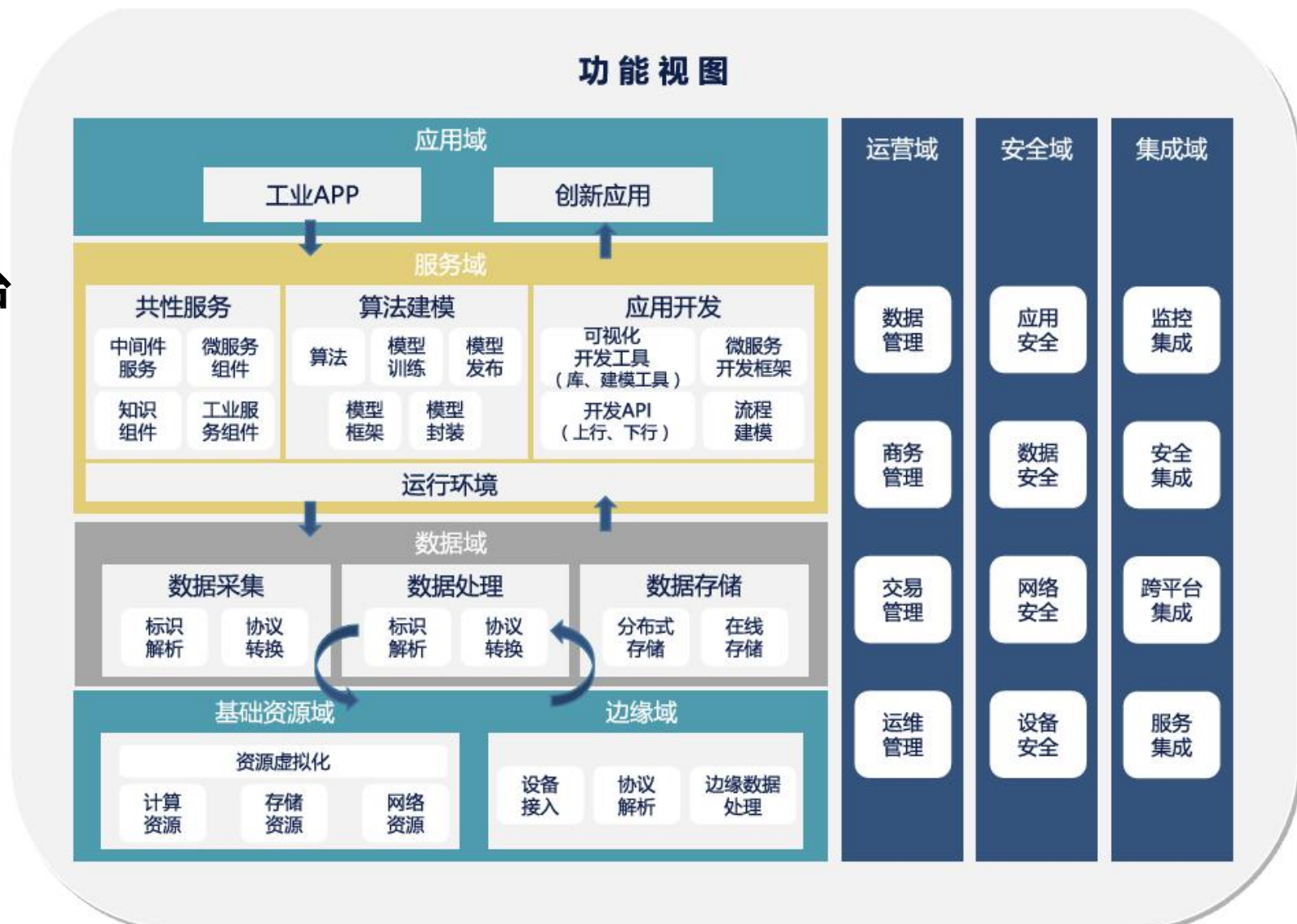
- 接入工业互联网的终端设备的安全；
- 应加强设备自身安全，完善终端接入安全认证。

2

标准化需求 平台功能视图

功能视图描述工业互联网平台的功能框架、功能组件，及其相关关系，共分为八个域，分别为：

- 基础资源域
- 边缘域
- 数据域
- 服务域
- 应用域
- 运营域
- 安全域
- 集成域



2

平台安全特点
安全措施

	工业互联网平台安全特点	工业互联网平台安全措施
工业SaaS层	API恶意代码注入 工业APP安全开发 工业控制命令合法性鉴别	业务应用安全 身份鉴别 工业APP安全 安全审计
工业PaaS层	工业应用开发工具存在漏洞 工业微服务存在漏洞 工业知识恶意获取	微服务组件安全 身份鉴别 容器安全 访问控制 平台应用开发环境安全
工业IaaS层	传统云平台IaaS层安全防护问题	采用《云计算服务安全能力要求》
边缘层	计算资源有限 安全防护能力薄弱 物理分布范围广	网络拓扑结构安全 访问控制 传输保护 入侵防护 网络边界防护 安全审计

目录

CONTENTS

第一部分

工业互联网发展现状

第二部分

标准化需求与平台安全特点

第三部分

国家标准相关进展

第四部分

下一步工作建议

3

国家标准相关进展 在研标准

1	云制造服务平台安全防护要求	20173696-T-604	制定中
2	信息安全技术 工业互联网平台安全要求及评估规范		制定中
3	工业互联网平台 安全接入风险分析及技术要求		待制定
4	工业互联网平台 安全防护检测要求		待制定
5	工业互联网平台 安全风险评估规范		待制定
6	工业互联网平台 安全防护要求	2018-1396T-YD	制定中
7	工业互联网平台 安全防护能力评估规范		待制定

3

《工业互联网平台安全要求与评估规范》

研制过程

2018年1-5月，中国电子技术标准化研究院牵头，联合树根互联、海尔、华为、徐工集团等单位，开展工业互联网平台安全标准化研究，明确标准化需求，形成标准草稿，并联合申报信安标委项目。

2018年5-7月，项目组承接项目后，联系各个参与单位，进行任务分工和任务组织；研究现有国内外工业互联网平台安全相关标准，分析各自特点，学习借鉴。

2018年8月，调研国内工业互联网平台安全现状，学习、研究、讨论国内外相关的标准及研究成果，确定并编写总体框架。

2018年10月，根据各参与单位优势领域，确定标准编写任务分工，开展标准草案初稿编写工作，并在青岛会议周上，就标准内容向与会代表进行了汇报，听取意见建议。

2018年11月-2018年12月，根据青岛会议周专家意见修改标准文本内容。

3

《工业互联网平台安全要求与评估规范》

研制过程

2019年1月，中国电子技术标准化研究院依托工业信息安全产业发展联盟工业信息安全标准工作组，召开标准研讨会，并听取了北航、原神华集团、和利时、中油瑞飞、烽台科技等单位代表意见。

2019年2-3月，项目组依据专家意见建议，进一步修改完善该标准内容。

3

《工业互联网平台安全要求与评估规范》

标准目录

目录 CONTENTS

1

范围、规范性引用文件、术语和定义、缩略语

2

工业互联网平台概述

3

边缘层安全、工业IaaS、PaaS、SaaS
安全要求及评估

4

工业互联网平台安全管理要求

5

工业互联网平台安全评估

3

《工业互联网平台安全要求与评估规范》

标准范围

范围：

本标准针对工业互联网平台安全需求，并针对边缘层、工业IaaS平台层、工业PaaS平台、工业SaaS应用等，提出安全要求，以及安全管理相关要求。在此基础上，提出相应评估流程、评估内容等。

本标准适用于工业互联网平台服务提供商开展工业互联网平台安全防护设计、建设、运维、管理等相关工作，同时也可作为相关第三方评估组织机构面向工业互联网平台，开展安全防护评估工作，提供规范性指导。

术语：

工业云 industrial cloud

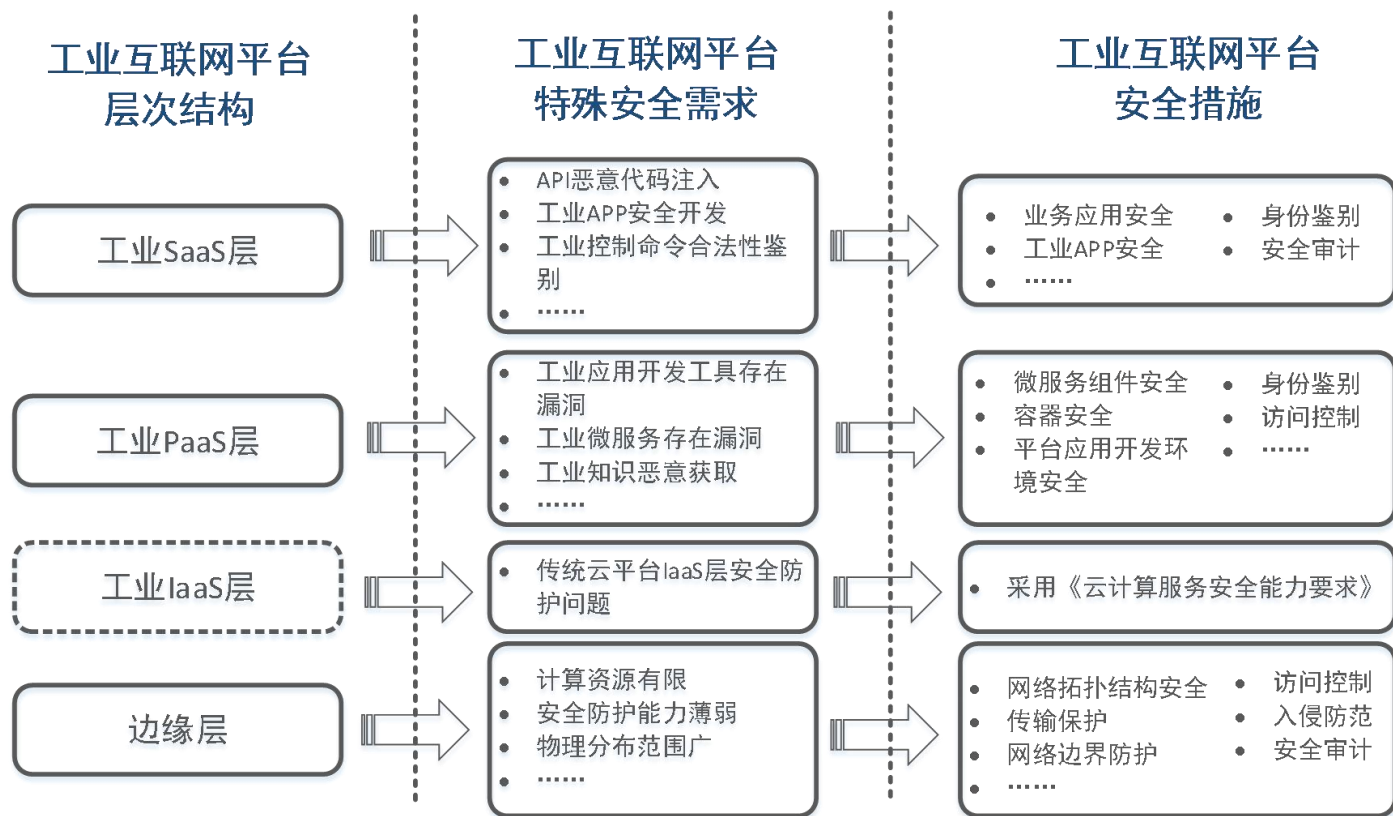
以云计算平台为基础，面向工业的通过网络将弹性的、可共享的资源和业务能力，以按需自服务方式供应和管理的模式。

工业互联网平台 Industrial Internet Platform

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。

3

《工业互联网平台安全要求与评估规范》 标准思路



3

《工业互联网平台安全要求与评估规范》

边缘层安全要求

- 划分安全区域、避免网络直连、多用户隔离



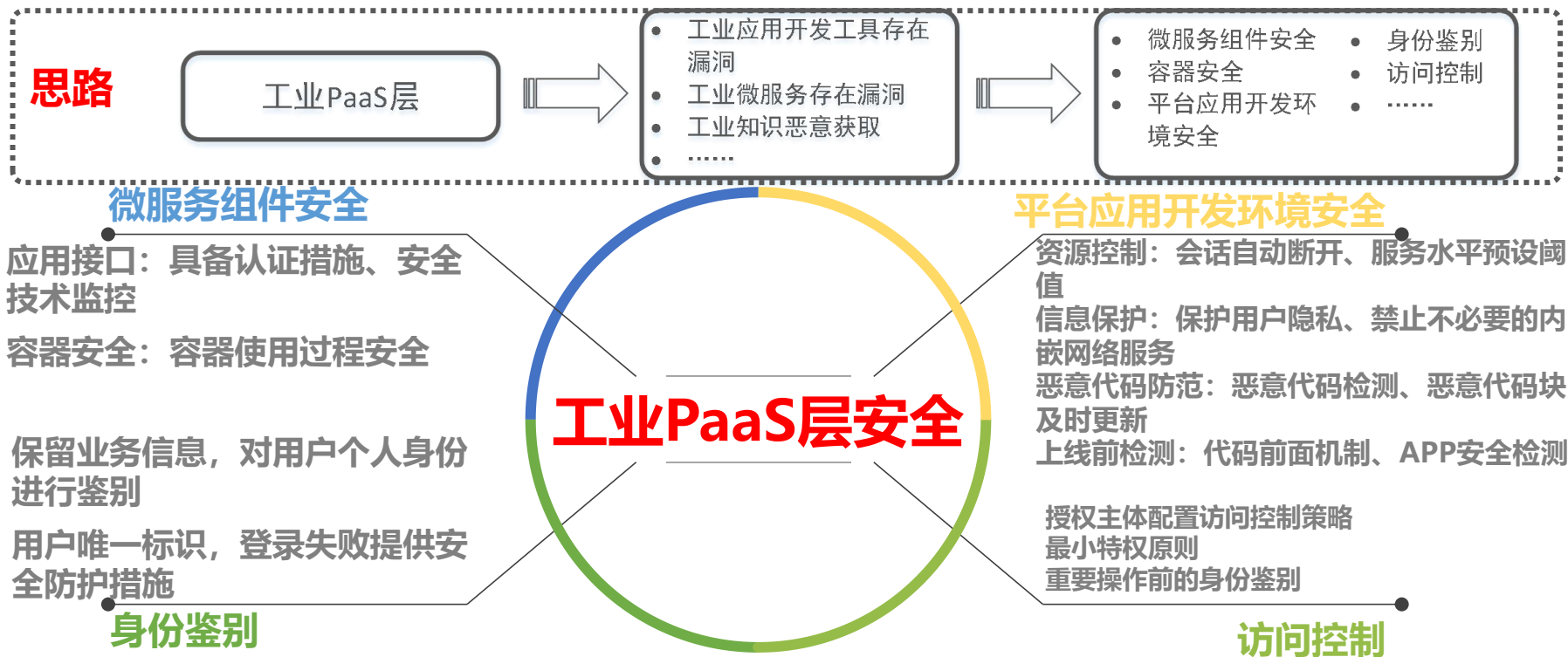
3

《工业互联网平台安全要求与评估规范》 工业IaaS层安全要求

工业互联网平台基于传统云平台建设，其中工业IaaS平台，通过虚拟化技术提供处理、存储、网络和其它基本的计算资源，用户能够部署和运行软件，包括操作系统和应用程序，无需管理或控制任何云计算基础设施，可以控制操作系统的选择、储存空间、部署的应用，以及网络组件（防火墙，负载均衡器等）的控制。工业IaaS平台可采用《信息安全技术 云计算服务安全能力要求》（GB/T 31168 - 2014）开展安全防护工作，同时依据《信息安全技术 云计算服务安全能力评估方法》（GB/T 34942 - 2017），开展安全评估工作。

3

《工业互联网平台安全要求与评估规范》 工业PaaS层安全要求



3

《工业互联网平台安全要求与评估规范》 工业SaaS层安全要求



针对SaaS层具体业务应用，需具有严格的用户访问权限限制功能，多次登录失败处理等；对工业资源使用的控制要求等。

工业互联网相关APP的逻辑安全、应用及后台系统安全、Web安全

对于APP中用户登录等功能，提供唯一标识鉴别等功能

审计覆盖范围：工业APP相关全部用户
审计内容：每个用户的关键操作、重要行为、业务资源使用情况等

3

《工业互联网平台安全要求与评估规范》 工业SaaS层安全要求

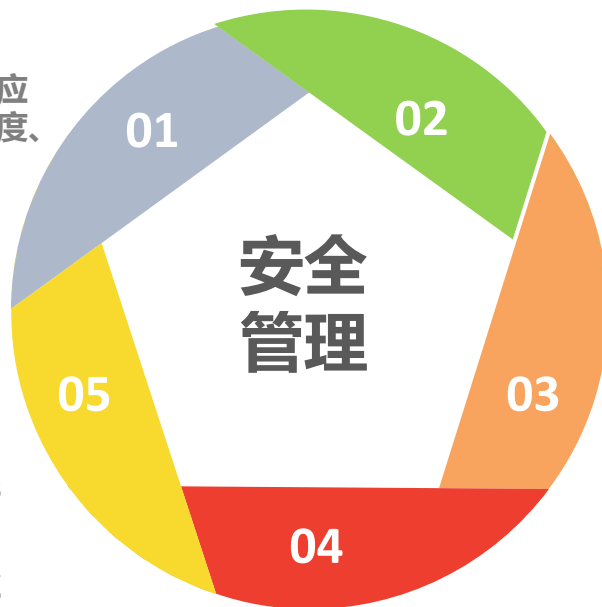
01.组织制度

工业互联网平台运营企业应建立安全安全管理规章制度、成立专门组织。

05.安全评估

风险评估：组织应制定相关计划，定期开展风险评估；

持续监控：组织应对工业互联网平台安全防护措施的效果，开展持续性监控。



02.运维管理

- 受控维护
- 远程维护
- 脆弱性扫描
- 软件、固件、信息完整性
- 缺陷修复
- 安全功能验证

03.事件响应

- 事件处理计划
- 事件处理
- 事件报告
- 事件处理支持
- 安全警报
- 错误处理

04.应急管理

制定应急预案，定期开展应急培训和演练，定期备份关键信息系统

目录

CONTENTS

第一部分



工业互联网发展现状

第二部分



标准化需求与平台安全特点

第三部分



国家标准相关进展

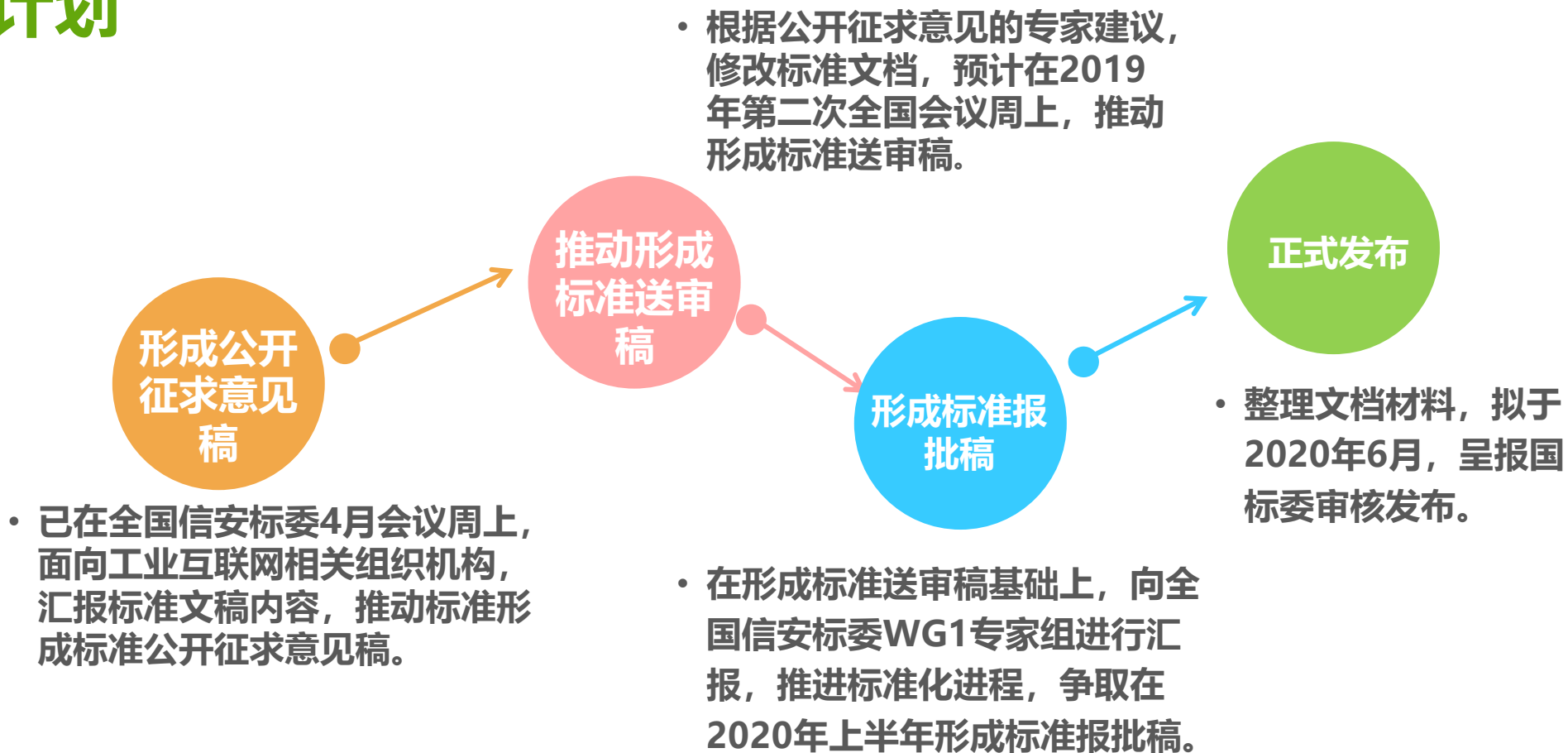
第四部分



下一步工作建议

4

下一步工作 工作计划





工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

谢谢

敬请各位专家批评指导