工业互联网安全框架研究

Research on the Security Framework of Industrial Internet

刘廉如[1]，张　尼[2]，张忠平[1]（1. 宜通世纪物联网研究院（广州）有限公司，广东 广州 510665；2. 中国电子信息产业集团有限公司第六研究所，北京 100083）

Liu Lianru[1]，Zhang Ni[2]，Zhang Zhongping[1]（1. Eastone Century IoT Research Institute（Guangzhou）Co.，Ltd.，Guangzhou 510665，China；2. The 6th Research Institute of China Electronics Corporation，Beijing 100083，China）

摘　要：

工业互联网包括网络、平台和安全三大体系。面对IT和OT的不断渗透融合，工业互联网面临诸多安全挑战，如网络边界模糊化，安全监控管理缺乏，端点增多导致攻击面增大，安全态势可视化不足等。简要介绍了工业互联网安全威胁和标准化进展，以及美德中三国的工业互联网安全框架，并对典型的工业互联网安全防护和运营方案进行了分析。

关键词：

工业互联网；安全框架；防护对象；安全威胁

doi：10.12045/j.issn.1007-3043.2019.04.012

中图分类号：TN915.08

文献标识码：A

文章编号：1007-3043（2019）04-0053-05

Abstract：

The industrial Internet includes three major parts：network，platform and security. As the continuous penetration and integration of IT and OT goes on，the industrial Internet faces many security challenges，such as the blurring of network boundaries，the lack of security monitoring and management，the increase of endpoints leading to larger attack surfaces，the lack of security posture visualization and so on. It briefly introduces the progress of industrial Internet security threats and standardization，as well as the industrial Internet security framework，and analyzes typical industrial Internet security solutions.

Keywords：

Industrial Internet；Security framework；Protection object；Security threats

引用格式：刘廉如，张尼，张忠平. 工业互联网安全框架研究[J]. 邮电设计技术，2019(4)：53-57.

1 概述

伴随着新一代信息技术向传统产业融合渗透，世界范围内新一轮工业革命引发了制造模式、生产方式和组织形态的变革，推动着智能制造、网络制造和服务型制造等新型制造模式涌现，催生出数字驱动和两化融合的工业新业态。世界各国积极抢抓新一轮工业革命的机遇，德国工业4.0、美国先进制造伙伴计划、中国制造2025等一系列国家战略相继推出，工业互联网发展的国际竞争日趋激烈。2017年国务院发布《关于深化“互联网+先进制造业”发展工业互联网的指导意见》后，工业互联网成为中国制造业发展的重要方向，也是建设制造强国的重要抓手。

在市场环境、科技革命和产业转型的综合作用下，制造模式呈现出智能化生产，个性化定制，网络化协同和服务化延伸趋势。系统搭建以网络、平台、安全为核心的功能体系，为建设制造强国网络强国提供关键支撑和重要机遇，为经济转型升级和供给侧结构性改革提供新动能，为制造资源优化配置和效率提升提供新手段。

工业互联网打破了传统工业相对封闭可信的环境，导致病毒、木马和网络攻击等安全风险对工业生产和关键基础设施的威胁日益加剧，一旦受到安全攻击，不仅会造成巨大的经济损失，甚至会危及公众生

收稿日期：2019-02-28

活和国家安全。因此保障工业互联网的安全可控是确保智能制造在生产领域实施的必要前提。

工业互联网的发展面临着多种安全问题，工业互联网安全是全局的、多层次、多维度的系统性安全。从分层结构的角度，安全威胁可分为设备层安全威胁、控制层安全威胁、车间层安全威胁、企业层安全威胁和协同层安全威胁；从体系架构的角度，安全威胁可分为设备层安全威胁、网络层安全威胁、应用层安全威胁、数据层安全威胁、控制层安全威胁、人员管理威胁和高级持续性威胁。

数字化、网络化、智能化生产设备安全，端到端生产模式下的网络安全，生产控制系统安全，应用安全，工业数据和用户数据安全成为工业互联网健康有序发展亟待解决的问题。工业互联网安全保障体系作为支撑智能化生产的安全防护保障以及工业互联网应用安全运行和持续服务的前提条件，具有重要的研究意义。

2 标准体系

标准是指导工业互联网发展的依据和准则，是确保工业互联网健康发展的前提条件。我国工业互联网的发展基础和水平与发达国家相比，存在较大差距，标准体系的不完善是其中重要原因之一。在发展工业互联网的竞争中，标准成为了各国相继争夺的战略制高点。只有形成了科学成熟规范的综合标准体系，才能在技术、产品和服务方面取得系统性推进的优势。

目前，以国际电工委员会（IEC）、美国工业互联网联盟（IIC）、德国电工电子与信息技术标准化委员会（DKE）和中国工业互联网产业联盟（AII）为代表的相关组织均在积极布局和推进工业互联网标准化工作。总体而言，工业互联网标准化还处于起步阶段，将面临长期的探索与研究过程，标准组织多将工作重点放在了顶层设计、参考架构、基础共性、需求用例、关键技术和安全等方面。

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），从产品生命周期/价值链、层级和架构3个维度对工业4.0进行描述。美国工业互联网联盟于2015年6月发布了《工业互联网参考架构》，提出了一套方法论和模型，以业务价值驱动系统设计，以数据驱动端到端的业务优化。2016年8月中国工业互联网产业联盟也推出了《工业互联网体系架构》，涵盖了工业互联网的内涵、业务需求、体系架构、关键要素和实施目标。2016年12月，日本工业价值链促进会（IVI）发布了《日本互联工业价值链的战略实施框架》，提出了新一代工业互联网参考架构（Industrial Value Chain Reference Architecture），成为指导日本产业界发展工业互联网的顶层框架。

2016年9月，美国工业互联网联盟（IIC）发布了《工业互联网安全框架》，定义了工业互联网的五大安全特性，即信息安全、功能安全、可靠性、弹性和隐私安全；从商业、功能和实现角度提出了工业互联网建设和部署实施的指导准则。

为推动工业互联网安全，工信部相继发布了《工业控制系统信息安全防护指南》《工业控制系统信息安全事件应急管理工作指南》《工业控制系统信息安全防护能力评估工作管理办法》和《工业控制系统信息安全行动计划（2018—2020）》等指导文件。

2018年2月，中国工业互联网产业联盟（AII）发布了《工业互联网安全框架（讨论稿）》，为中国工业互联网相关企业构建安全体系提供顶层框架模型，为应对日益增长的安全威胁和实施部署安全防护措施提供有效指导。

中国通信标准化协会（CCSA）已经立项了《工业互联网平台安全防护要求》《工业互联网数据安全保护要求》《工业互联网安全接入技术要求》《工业互联网网络安全总体要求》等相关标准。

中国工业互联网产业联盟（AII）在《工业互联网体系架构（版本1.0）》中提出了工业互联网标准体系建设的总体思路、基本原则、标准体系框架、重点标准化方向，具体如图1所示。在安全标准方面主要包括安全基础支撑标准、安全管理及服务标准、设备安全标准、网络安全标准、控制安全标准、应用安全标准、数据安全标准等。

3 安全框架

安全是保障工业互联网健康有序发展的前提。明确安全防护对象，有效地识别和防范安全威胁，建立贯穿全产业链、全生命周期的安全体系，将安全风险化解于未然，对工业互联网发展具有重要意义。

工业互联网安全框架作为工业互联网安全体系的顶层设计和实施纲要，指导着安全防护措施的部署、实施和评估，促进工业互联网企业的系统性安全

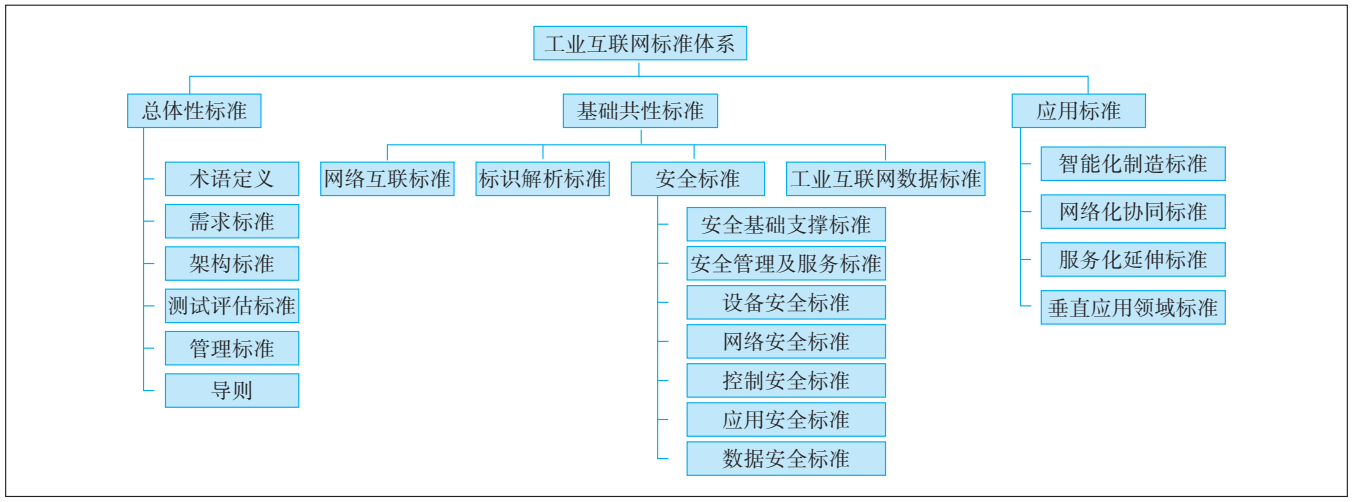

图1　工业互联网安全标准体系

防护能力的提升，为工业互联网数字化、网络化、智能化发展提供安全可信环境。

工业领域的安全可分为信息安全、功能安全和物理安全3个层面。在数字化和网络化阶段，功能安全和物理安全是关注的重点。随着工控系统信息化和智能化不断深化和快速发展，信息安全受到越来越多的重视。需要对工业互联网安全框架的功能安全、物理安全和信息安全进行统筹考虑，建立面向工业需求的安全技术和管理体系。

传统的网络安全框架包括以下内容：

a）OSI安全体系，定义了5类安全服务和8类安全机制。

b）P2DR（Policy Protection Detection Response）模型，从部署安全防护、检测安全风险、响应处置风险3个方面形成一个良性反馈、动态调节的安全循环。

c）信息保障技术框架（Information Assurance Technical Framework）通过对基础设施、计算环境、网络边界等方面的安全防护，保障人、技术和操作3个核心安全要素。

d）IEC62443工业控制系统安全防护标准，按照分层分域分级的控制和管理理念进行安全纵深防御。

e）PC4R（Perception Connection Conversion Cyber Cognition Response）模型由信息感知、数据汇集、转化分析、网络融合、认知预测和响应决策等6个闭环过程组成。

除P2DR、PC4R模型外，其他网络安全框架都侧重静态安全防护，不能满足工业互联网动态防护、过程管控的安全管理需求。

3.1 美国IIC工业互联网安全框架

美国工业互联网联盟在《工业互联网参考架构》中提出了一个标准化的开放式体系架构，定义了业务、用途、功能和执行4个层面的组件，并建议从上述维度综合考虑安全威胁并设计安全系统方案。从业务视角保障业务环境的安全，保护商业数据和关键基础设施是重点考虑因素。从用途视角落实和控制不同端点的能力，保障活动进行过程中端到端的安全管理。从功能视角关注数据流和控制流在控制域、操作域、信息域、应用域和业务域的完整性、保密性和可用性。从执行视角保障端到端的安全包括终端安全、通信安全、数据安全、管理和控制安全、信息交换安全等。

在工业互联网安全的统筹考虑中，应摒弃传统的IT和OT分而治之的思维模式，将两者合而治之，这也是工业互联网参考架构IIRA将IT和OT的功能在一系列的功能域中进行融合的原因所在。

为进一步加强工业互联网安全研究和实施，美国工业互联网联盟（IIC）发布了《工业互联网安全框架》，从功能视角出发，定义了3个层次的6个安全功能（见图2）。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。数据保护层和安全模型策略层主要提供底层支撑。

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

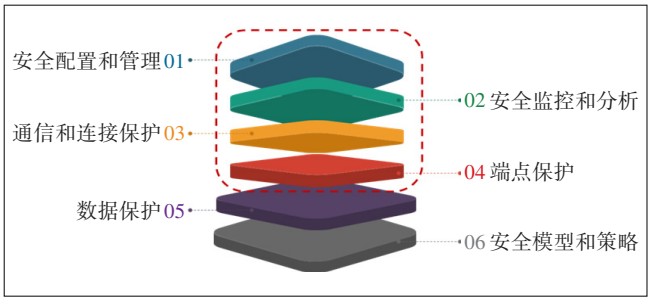

图2　功能视角下的工业互联网安全框架

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，监控与分析和安全配置管理必须在系统层面相应启动。

在安全框架的基础上，美国工业互联网联盟（IIC）发布了《物联网安全成熟度模型：描述与预期用途》，旨在基于治理、支持和强化三大核心要素，提供一套通用的物联网安全成熟度模型用于安全评估，并帮助工业互联网企业定义预期达到的安全成熟目标。

3.2 德国工业4.0架构安全框架

德国工业4.0的战略框架可以归纳为“1438”模型，即1个网络（信息物理系统网络），4大主题（智能工厂、智能生产、智能物流和智能服务），3项集成（横向集成、纵向集成和端到端集成），8大计划（标准化和参考架构、管理复杂系统、综合的工业宽带基础设施、安全和保障、工作的组织和设计、培训和持续的职业发展、监管框架、资源利用效率）。

在工业4.0参考架构（RAMI4.0）中，定义了一个涵盖分层架构、产品生命周期和工厂层级的三维描述模型，如图3所示。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。

工业4.0参考架构的安全框架在分层架构上关注不同层面的安全风险，在产品生命周期上关注不同环节的安全边界，在工厂层级关注物理和数据资产跨域的安全防护。德国RAMI4.0采用了分层管理的方法对防护对象进行保护和管理。未来工业4.0的安全保障框架将采用纵深防御与区域防御相结合、动态主动防御和静态被动防御相结合、预测式防御和响应式防御相结合的方式，实现以数据驱动的多维立体的安全防

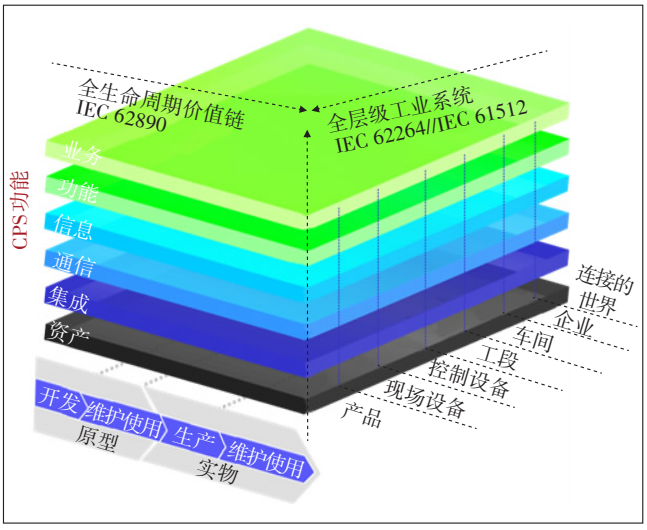

图3　RAMI4.0参考架构模型

御目标。

3.3 中国工业互联网产业联盟安全框架

基于以上国外网络安全框架的分析，归纳出3方面的共性认知：分类分层分级分域部署安全防护措施；具有持续性和反馈性的动态安全模型更适合工业互联网场景；技术和管理手段相结合，物理设备和数字资产保护并重的思路更利于提升安全防护能力。

中国工业互联网产业联盟（AII）发布的《工业互联网安全框架》从明确安全防护对象，落实安全防护措施，提升安全防护管理这3方面构建我国工业互联网安全防护体系。

安全防护对象是开展工业互联网安全防护工作的基础，旨在明确防护的范围和方向，包括设备安全、网络安全、控制安全、应用安全和数据安全。

在安全防护措施方面，包括威胁防护、监测感知和处置恢复三大环节，采用静态被动防护与动态主动防护相结合的方式，形成动态、闭环的机制，在预先设定的安全事件规则触发时，能够及时响应并加以处置，避免安全影响的扩散。

在安全防护管理方面，技术手段和管理手段并用，设定安全目标，实现安全威胁分析和风险评估，制订安全管理原则，配合安全管理方法，搭建科学完备的安全管理流程，配置安全策略，全面指导安全防护能力水平的提升，实现安全防护措施的有效部署。

工业互联网安全框架的3个防护视角相互补充，互为依存，相对独立又彼此关联，以防护对象为核心，辅以防护措施和防护管理策略/流程，形成一个多维立体的防护体系，如图4所示。

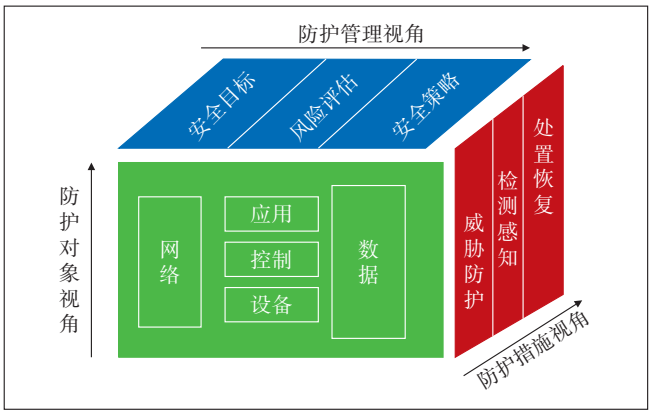

图4　工业互联网安全框架

4 典型方案

随着信息技术和运营技术(IT/OT)一体化的不断深入，工业设备“上云上平台”逐步推进，形成了一个开放式的网络环境。系统安全风险和入侵威胁不断增加，工业互联网面临的安全问题也日渐突出。电子六所、海尔、360企业安全集团、启明星辰等企业纷纷推出工业互联网安全防护和运营方案。

电子六所从态势感知、实时威胁情报与风险通报、漏洞管理到补丁管理及固件升级，均使用自主可信的国产软硬件产品和攻防兼备的安全防护策略，从而构建可检测、可防护、可替代的工业互联网安全深度防护体系。同时，电子六所将进一步攻关物理安全和网络安全、功能安全和信息安全、OT安全和IT安全融合场景下的安全防护难题，构建多层次、自主可信、深度安全的主动防御体系。

海尔为推动工业互联网安全发展，推出了海安盾产品，旨在构建工业互联网生态圈安全态势智能感知、敏捷安全响应的统一平台，实现工业互联网全链条安全可感、可控、可防。海安盾赋能海尔COSMOPlat平台，包括物理安全、基础架构安全、应用安全、数据安全、账号权限和访问、安全事件管理和安全运维。

360企业安全集团提出了数据驱动的工业互联网自适应安全体系的方法论和网络安全滑动标尺动态安全模型，包括架构安全、被动防御、积极防御、威胁情报和进攻反制，逐步构建积极防御能力(安全攻防能力、威胁识别能力、防护响应能力、大数据能力和人才培养能力)。从安全运营角度，针对工业互联网安全需求，建立以安全运营为中心，以威胁情报为驱动，以协同联动为基础的IT-OT融合的安全防护体系。

启明星辰根据工业互联网应用层、网络层和感知层安全威胁分析，及不同层次包括身份鉴别、访问控制、安全审计、入侵防范等综合安全需求，实现由端到云贯穿应用、网络和感知各层次的安全防护保障体系。其安全方案包括安全技术防护和安全服务保障2部分，确保感知层设备的安全性及可视化管理、网络层的安全异常检测和数据流安全分析，在应用层以云安全防护和云数据加密为基础，利用安全态势感知平台实现整体安全的监测、管理、控制和运营，有效构建工业互联网安全运营体系。

5 结束语

工业互联网打通了IT系统和OT系统的边界，传统的安全边界逐渐模糊，网络复杂程度不断提高，海量数据共享与交换的需求日渐增加。工业互联网面临安全威胁高危化，漏洞类型多样化，网络边界模糊化，安全标准空白化，攻击手段多元化、专业化等诸多困难和挑战。随着工业互联网的进一步发展演进，安全保障和防护能力体系需要不断完善，特别是设备内置安全机制、动态网络安全防御机制、信息安全和功能安全融合机制，面向工业应用的灵活安全保障能力和数据分级分类保护机制会给工业智能化发展提供安全可控可信的环境保障。

参考文献：

[1] 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[Z/OL]. [2019-01-19]. http://www.gov.cn/zhengce/content/2017-11/27/content_5242582.htm.
[2] 国务院关于深化制造业与互联网融合发展的指导意见[Z/OL]. [2019-01-19]. http://www.gov.cn/zhengce/content/2016-05/20/content_5075099.htm.
[3] 王建伟. 工业赋能：深度剖析工业互联网时代的机遇和挑战[M]. 北京：人民邮电出版社，2018：21-24.
[4] 陶耀东，李强，李宁. 工业互联网的安全挑战及应对策略[J]. 中兴通讯技术，2016，22(5)：36-41.
[5] 顾旻霞，刘廉如. 物联网商业模式初探[J]. 信息技术与网络安全，2019，38(2)：13-16.

作者简介：
刘廉如，宜通世纪物联网研究院院长助理，工程师，博士后，主要研究方向为工业物联网、泛在网、车联网、未来网络等；张尼，中国电子信息产业集团有限公司第六研究所副所长，教授级高级工程师，博士后，主要研究方向为信息安全、大数据、工控安全等；张忠平，宜通世纪物联网研究院院长，国家“百千万人才工程”有突出贡献中青年专家，享受国务院特殊津贴专家，中国通信学会理事会理事，教授级高级工程师。