工业互联网安全白皮书

2019 年 5 月

上海工业控制安全创新科技有限公司

上海赛博网络安全产业创新研究院

. . .

. . .

前沿

当前，全球工业经济加快数字化转型，工业制造进入 4.0 时代。工业互联网是实现智能制造、推进产业互联网全面发展和培育我国经济增长新动能的必由之路，对于打造我国制造业竞争新优势，实现制造强国具有重要战略意义。然而，安全是发展的前提，安全保障能力已成为工业互联网创新发展的关键因素。2019 年 4 月，工业和信息化部发布了《关于加强工业互联网安全工作的指导意见(征求意见稿)》，明确了建立工业互联网安全保障体系的目标和主要任务，提出建设工业互联网安全保障体系要从制度机制、技术手段、产业发展等方面综合施策，加快部署。

本白皮书在深入分析工业互联网安全挑战的基础上，从功能安全与信息安全融合的角度，提出了工业互联网安全防护总体框架，并梳理了重要垂直领域的安全风险以及应对策略，以期为工业企业、安全企业和监管部门提供工业互联网安全防护思路，促进我国工业互联网的安全部署和推进。

目录

1 工业互联网的发展及安全挑战

1.1 工业互联网的内涵及发展趋势

1.1.1 工业互联网的内涵

工业互联网是服务于工业制造业的数字化、智能化转型需求，基于人、机、物泛在互联和海量数据汇聚分析，与云计算、物联网、大数据、人工智能、数字孪生等新一代信息技术高度融合，通过网络、平台等基础设施构建的实现设计、生产、销售、服务等产品全生命周期和全产业链高效配置、智能决策的系统化应用体系。工业互联网不仅连接工厂内设备、产品、人员，同时打通产业链上下游以及客户，实现工厂内部全面互联、产业之间全面协同，为提高研发、生产效率、高效配置资源、满足客户个性化需求、拓展服务业态提供平台和手段。

工业互联网包括网络互联、数据流动、智能决策和安全保障四大要素。网络互联是前提，通过布局有线、无线网络等网络基础设施，实现工厂内外生产设备、控制系统、工业产品、操作人员、以及物流系统等要素的全面互联。数据流动是基础，通过实现工业大数据的跨系统、跨网络、跨地域的实时采集、传输、存储、交换，为定制、研发、生产、销售、维护等各个环节的高效智能化运行提供依据。智能决策是核心，结合大数据分析、人工智能等技术，通过算法开发，实现数据的深度分析，服务于流程优化、能耗管理、预测性维护等智能化生产目标。安全保障是后盾，是工业互联网稳定、可靠运行的前提，

包括功能安全和信息安全，是本白皮书关注和探讨的主题。

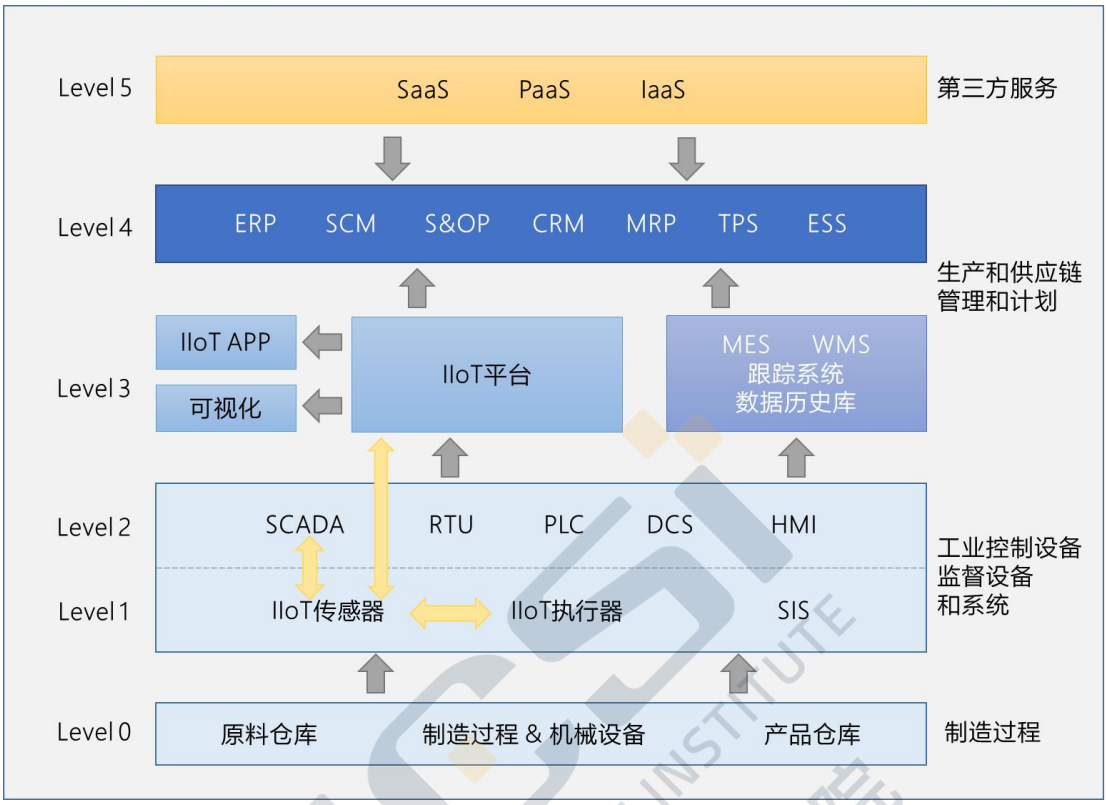

图 1 工业互联网总体功能架构

1.1.2 工业互联网发展趋势

当前全球工业互联网发展处于深入探索和快速落地实践阶段。其中，美、中、德、日等国高度重视工业经济数字化转型，在工业物联网、智能工厂、CPS 系统等技术开发和应用中处于全球领先。

美国推出国家制造创新网络计划（NNMI），现称为美国制造业计划(Manufacturing USA)，围绕科技成果转化，形成了遍布美国的制造创新网络。德国“工业 4.0 战略”由政府主导，侧重于发展基于 CPS 系统的智能工厂和智能制造。日本提出“互联工业”（Connected Industries）战略，宣布推进“通过连接人、设备、技术等实现价值创造的互联工业”。在产业界，美国 IT 和工业自动化巨头积极布局工

业云、工业互联网平台、工业物联网、工业应用等，GE、微软、IBM、思科、霍尼韦尔、PTC 等成立的工业互联网产业联盟（IIC），在标准制定、技术推广、产业协作等方面发挥重要作用。德国工业 4.0 平台由德国机械设备制造业联合会、德国电气和电子制造商协会等发起，在行业内积极推动研发转化、人才培育，德国西门子、大众、博世、SAP、德国电信等先进制造和软件开发企业基于自身优势积极引领产业实践。

我国工业互联网布局早，发展快，机遇大。2017 年，国务院印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，标志着中国工业互联网战略层面的顶层设计正式出台。2018 年 6 月，工业和信息化部发布《工业互联网发展行动计划（2018-2020 年）》，明确了我国工业互联网发展目标和重点任务。当前，我国在工业互联网实践和探索中，应用路径已初步形成，在离散和流程工业中都有一定应用，制造、自动化、IT 企业都积极参与工业互联网建设与推广，产业生态在快速形成，商业模式在积极探索和持续迭代，标准制定、体系架构、安全保障也在快速推进。

未来，全球工业经济转型势头不可逆转，工业互联网作为实现路径，对各国重振工业制造业都意义非凡。科学布局、稳步推进、因地适宜，是在新一轮经济转型发展中制胜的法则。

1.2 工业互联网安全问题分析

随着工业互联网在我国众多行业加快部署，电力、轨交、制造、

钢铁、石化等重要工业领域的关键基础设施、生产设备、控制系统将逐步联网化、数字化、智能化，一旦受到恶意攻击，将有可能造成重大经济损失，甚至威胁人身安全，给环境和国家安全带来重大安全风险。同时，工业领域关键信息基础设施在全球范围内成为黑客重点关注和攻击目标，安全防护压力空前增大。当前，安全保障能力已成为工业互联网创新发展的关键因素。

工业互联网建设面临的安全问题包括：

一、工控系统安全成为掣肘工业互联网安全能力建设的关键。

传统工控系统通常部署在工业现场内网，连接范围有限，地址私有且不与互联网联通，处于网络隔离状态。同时对可靠性和实时性要求高，主要关注功能安全。由于在相对可信环境中信息安全隐患少，以及考虑到对功能安全的影响，设备和控制系统等在设计之初普遍未考虑安全防护问题，极少升级补丁，也缺少认证、授权等安全功能设计，导致工控系统漏洞多，且高危漏洞占比高。然而，随着工业与互联网的不断融合，设备和控制系统将向网络物理系统的方向快速发展，工控系统在信息采集、指令传输、分析挖掘、控制反馈等全生命周期内，将呈现出业务协同化、信息共享化、决策全景化、过程网络化等发展趋势。智能机器人、智能传感器、智能设备将普遍集成嵌入式系统及应用软件，并持续实时将生产现场数据向工业互联网平台集中传输，传统设备也将通过增加通信模组与公共互联网连接。这将极大增加生产控制层的信息安全风险，不仅工控系统自身由于与网络互联以及存在安全漏洞成为攻击目标，攻击源还能通过工业互联网云平台向

生产现场控制系统渗透，对物理安全及功能安全带来极大安全隐患。如何为毫无安全防护措施的工业控制系统构建安全屏障，同时不影响功能安全，是工作互联网安全保障能力建设中的重大挑战。

二、工业互联带来网络基础设施重构及数据规模极速升级。

工业互联对企业网络架构及安全保障提出新的要求。工业领域传统的网络架构无法满足工业互联网发展的数据互通需求，需根据数据流动和业务流程改变传统网络架构，并能适应工业互联网环境下柔性制造对灵活组网的要求。工业网络的持续开放性、企业内网与外网的不断融合、边缘云计算的加快部署等趋势都对网络的安全保障提出更高的要求。同时，传统工业领域网络体系设计之初安全性考虑不足，安全认证、访问控制等手段普遍缺失。

其次，工业互联使得数据规模极速扩张，数据安全问题凸显。工业互联网要通过对工业设备、工控系统、工业产品、工业物料以及人员的实时数据采集、传输、交换、分析、处理，实现对研发、生产、销售、维护等环节的智能化决策和资源优化配置。因此，数据种类和数量大大增加，数据流动路径复杂多变，相对传统工业领域，数据安全的挑战极速升级。

三、工业互联网平台的引入导致安全责任边界不清。

工业互联网平台是实现企业内部高效管理和企业外部互联协同的关键，随着工业上云的推进，工业互联网平台将主要部署在云端。工业互联网平台的引入将导致针对企业内部网络、生产层、控制层的攻击路径大大增加，极大地增加了安全隐患。同时，工业数据、工业

应用等都在一定程度上依赖于工业互联网平台的安全性。这将带来工业企业与平台服务商的安全责任界定问题，工业企业也无法有效掌控平台、数据、应用的安全保障。

四、工业互联网触角外延造成安全覆盖面更为复杂。

工业互联网不仅打通企业内部数据通路，还将覆盖供应链、消费者等企业外部主体，数据流通将跨网络、跨企业、跨平台。与传统工业领域相比，工业互联网安全不仅覆盖企业内部设备安全、控制安全、数据安全和应用安全等方面，还将包括企业外部数据采集及传输、企业外部网络体系安全等方面。在工业互联网时代，安全边界将逐渐融合，安全风险逐渐加大，攻击路径大大增加，安全挑战不断升级。

1.3 工业互联网安全政策与标准

1.3.1 国外政策与标准制定情况

（1） 政策法规

当前，在全球范围内，国家政策主要从工控系统安全和关键基础设施保护层面推进工业互联网安全保障。其中，以美国、欧盟、日本为代表的主要工业国家起步较早，“震网”病毒事件后，各国政府将工控安全问题提升至国家战略层面，发布了一系列战略规划和行动指南，呈现出以下发展趋势：

一是全球共识性。美国的“工业互联网”、德国的“工业 4.0”、日本的“互联工业”，与我国的“中国制造 2025”等相关政策具有高度的一致性。全球范围内，各国针对工控系统的安全政策已经达成了

全球共识。美国在本世纪初就将工控网络安全这一问题提升到国家战略高度，并积极推动在政策、标准、技术、方案等方面引导措施，形成了由国家职能部门协调管理、国家级专业队伍、实验室和科研机构提供技术支撑、用户及厂商共同参与的技术研究体系，并依托模拟仿真平台、综合现场检查测评与实验室测评建立了工业控制系统信息安全和功能安全测评体系。俄罗斯、英国、德国、法国、日本、韩国等其他很多发达国家均将关键基础设施中的工业控制系统作为网络安全战略重点，但这些国家尚未形成比较成熟的指南、准则和法规，且在相关技术支撑方面还比较匮乏。

二是法律保障性。世界各国分别制定了网络空间安全相关法律，并将面向关键基础设施的工控安全作为网络空间安全的重要方面，提供政策落实的法律依据。2014 年，美国发布了《2014 年国家网络安全保护法》，将工控系统网络安全列为网络安全保护对象。同年，日本发布了《网络安全基本法》，重点强调电力等基础设施运营方的网络安全要求。国外工控安全领域的政策指南及相关举措如表 1 所示。

表 1 国外工业互联网安全政策及相关举措

国家	时间	政策及相关举措
美国	1998 年	美国第 63 号总统令《克林顿政府对关键基础设施保护的政策》，将工控安全列为国家间战略制衡的重要手段。
	2003 年	将 SCADA 系统列为国家安全的优先发展领域
	2008 年	将工控系统列入国家重点保护关键基础设施，将工控系统安防提升至国家战略高度。
	2009 年	发布《保护工业控制系统战略》，涵盖能源、电力、交通等 14 个行业的工控安全。
	2009 年	美国国土安全部成立“工控系统网络应急响应小组”（ICS-CERT），研究工控安全事故监控、分析执行漏洞和恶

国家	时间	政策及相关举措
		意代码技术，为事故响应和取证分析提供现场支持。
	2009 年	美国土安全部、能源部联合国际知名工控领域企业，成立“工业控制系统安全评估实验室”，启动控制系统安全项目（CSSP）。
	2011 年	美国国土安全部发布《国家基础设施保护计划》，重点保护工控系统等国家重要基础设施。
	2014 年	发布《2014 年国家网络安全保护法》，将工控系统网络安全列为网络安全保护对象。
	2016 年	美国白宫发布《网络安全国家行动计划》，强调包括工控安全在内的网络空间安全。
欧盟	2010 年	欧盟发布《欧洲 2020：智慧、可持续与包容性的增长战略》，提出工业控制领域旗舰计划“全球化时代的工业政策”。
	2012 年	欧盟发布《未来经济复苏与增长建设一个更强的欧洲工业》，强调提升工控系统的安全防护能力。
	2013 年	欧洲网络与信息安全局(ENISA)发布《工业控制系统网络安全白皮书》，要求采取预防和防范措施，对针对工业控制系统的网络攻击事件和事故做出灵活和综合应对。
	2013 年	创建工控安全与 SCADA 信息安全国际会议（ICS-CSR）。
	2017 年	欧洲网络与信息安全局(ENISA)发布《物联网安全建议：在关键信息基础设施的背景下》
	2018 年	欧洲网络与信息安全局(ENISA)发布《智能制造背景下的物联网安全实践》
	2019 年	欧洲网络与信息安全局(ENISA)发布《工业 4.0-网络安全挑战和建议》
日本	2014 年	发布《网络安全基本法》，强调电力等基础设施运营方的网络安全要求。
	2016 年	成立“工业网络安全促进机构（ICPA）”，抵御关键基础设施攻击。
其他	2016 年	新加坡发布国家网络安全策略，建立强健的基础设施网络。
		澳大利亚发布《澳大利亚网络安全战略》，重视国家重要基础设施。
		以色列发布“前进 2.0”网络安全产业计划，重视工业系统安全。

（2） 标准指南

国际工控系统安全标准制定工作主要由工业过程测量、控制和自动化技术委员会（IEC/TC 65）的网络系统信息安全（WG10）和国际自动化协会（ISA 99）联合负责，发布了 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。该标准包括通用、信息安全程序、系统技术和部件技术四个部分，共包含 12 个文档，分别对资产所有者、系统集成商、组件供应商提出信息安全要求。同时，美国国家标准与技术研究院（NIST）制定了 NIST SP800-82 和 NIST SP800-53 等工控安全标准，重点关注 SCADA 系统等国家关键基础设施安全。

表 2 国外工控安全相关标准指南

制定部门	**标准名称**
国际电工委员会	IEC/TS 62443-1-1：术语、概念和模型 IEC/TS 62443-1-2：术语和缩略语 IEC/TS 62443-1-3：系统信息安全符合性度量
	IEC/TS 62443-2-1：建立 IACS 信息安全程序 IEC/TS 62443-2-2：运行 IACS 信息安全程序 IEC/TS 62443-2-3：IACS 环境中的补丁更新管理 IEC/TS 62443-2-4：对 IACS 制造商信息安全政策与实践的认证
	IEC/TS 62443-3-1：工控系统安全技术 IEC/TS 62443-3-2：区域和通道的信息安全保障等级 IEC 62443-3-3：系统安全保证（SSA）认证要求
	IEC 62443-4-1：产品开发要求 IEC 62443-4-2：对 IACS 产品信息安全技术要求
	IEC 61508：电气/电子/可编程电子安全相关系统的功能安全要求
	IEC 62210：电力系统控制和相关通信：数据和安全通信
	IEC 61531：核电厂以安全为主的系统用仪器仪表和控制： 系统的一般要求
	IEC 60880：核电站安全系统用计算机软件
国际自动化学会	ISA 99：生产控制系统安全

制定部门	标准名称
美国国家标准与技术研究院	NIST SP800-82：工业控制系统安全指南 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 改善关键基础设施网络安全框架 NIST IR 7628：智能电网安全指南 《制造业与工业控制系统安全保障能力评估》草案 《制造业网络安全框架简介》 《保障制造业工业控制系统安全：行为异常监测(草案)》
美国国土安全部	SCADA 和工业控制系统安全 工业控制系统安全评估指南 工业控制系统远程访问配置管理指南 中小规模能源设施风险管理核查事项 控制系统安全一览表：标准推荐
美国天然气协会	AGA Report No.12：SCADA 通信的加密保护
美国能源部	提高 SCADA 系统网络安全 21 步
美国石油协会	API 1164：管道 SCADA 安全 石油工业安全指南
电气和电子工程师学会	IEEE 1686：变电站智能电子设备（IEDs）网络安全标准
北美电力可靠性委员会	NERC CIP 002-009：北美大电力系统可靠性规范
美国核管理委员会	RG 5.71：核设施网络安全措施
德国国际工业流程自动化用户协会	《工业自动化系统的信息技术安全：制造工业中采取的约束措施（NAMURNA115）》
德国机械及制造商协会	《数据保护和工业 4.0》
瑞典民防应急局	《工业控制系统安全加强指南》。

（3） 行业标准

2016 年 9 月，美国工业互联网联盟（IIC）提出《工业互联网安

全框架》，从物理安全（Safety）、信息安全（Security）、可靠性、弹性、隐私性等角度对工业互联网部署提出了安全要求，旨在为工业互联网安全研究和实施提供理论指导。此后，又发布《商业视角下的工业互联网安全概况》、《端安全最佳实践》、《工业物联网安全成熟度模型》等多个安全指导性文件，并举办多次工业互联网安全论坛，推进安全解决方案落地实施。

德国工业 4.0 平台也在推进工业 4.0 进程中关注安全建设，先后发布《工业 4.0 安全指南》、《工业 4.0 中的 IT 安全》、《跨企业安全通信》、《安全身份标识》等指导性文件，提出以网络物理系统平台为核心的分层次安全管理思路。

1.3.2 国内政策与标准制定情况

（1）政策法规

2011 年，工信部发布的《关于加强工业控制系统信息安全管理的通知》，标志着国内工控安全工作的正式启动，在加强重点领域工控信息安全管理、安全测评检查和漏洞发布制度建设、组织领导等方面提出了明确要求，成为相关部门和重点企业推动工业控制系统信息安全工作的指导性文件。此后，国家各部委相继发布扶持政策。同时，随着智能制造、工业互联网等国家战略的推进实施，我国工控安全政策也正不但扩大覆盖范围，逐步囊括工业互联网领域。相关政策法规及相关举措如表 3 所示。

表 3 政策法规及相关举措

时间	内容	政策法规及相关举措

时间	内容	政策法规及相关举措
2011年	工信部	发布《关于加强工业控制系统信息安全管理的通知》（工业和信息化部协[2011]451号），明确工控信息安全建设要求。
2012年	国务院	发布《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发[2012]23号），提出保障工控系统信息安全。
2013年	国家电力监管委员会	发布《电力工控信息安全专项监管工作方案》（办发[2013]50号），加强电力工控系统安全防护监督管理。
2014年	中央网信办	中央网络安全和信息化领导小组成立，将以工控系统为代表的关键基础设施作为安全的重要方面。
	发改委	发布《电力监控系统安全防护规定》（发改委14号令）
	产业联盟	工业控制系统信息安全产业联盟成立。
	国家工程实验室	工业控制系统信息安全技术国家工程实验室成立（电子六所），建设工控系统信息安全模拟平台。
2015年	国务院	发布《国务院关于积极推进“互联网+”行动的指导意见》（国发〔2015〕40号），推动传统装备智能化改造与升级，推动工业软件、工控安全系统关键技术研发及产业化。
		发布《中国制造 2025》，提出要加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系。
2016年	科技部	发布网络空间安全专项“工业控制系统深度安全技术”。
	工信部	发布《工业控制系统信息安全防护指南》，明确提出从11个方面对工控系统信息安全建设内容规范，指导工业企业开展工控系统信息安全防护工作。
	国家研究中心	筹建国家工业信息安全发展研究中心（工信部电子一所），建设监测预警、仿真测试、评估验证等关键共性技术平台。
2017年	科技部	发布网络空间安全专项“工业控制系统安全保护技术应用示范”。
	产业联盟	国家工业信息安全产业发展联盟成立。
	工信部	发布《工业控制系统信息安全事件应急管理工作指南》
	工信部	发布《工业控制系统信息安全防护能力评估工作管理办法》
	工信部	发布《工业控制系统信息安全行动计划》（2018-2020年）征求意见稿，提升自主创新工控安全核心技术和关键产品。

时间	内容	政策法规及相关举措
2019 年	工信部	《关于加强工业互联网安全工作的指导意见(征求意见稿)》，提出到 2020 年底工业互联网安全保障体系初步建立的目标。

目前，国家对工控安全的重视上升为网络空间安全、智能制造、智慧城市关键基础设施等国家战略层面，相关政策的目标、实施对象及预期效果清晰明确。

（2）标准指南

我国工控安全标准体系尚不完善，全国工业过程测量和控制标准化技术委员会（TC 124）、全国信息安全标准化技术委员会（TC 260）、全国电力系统管理及其信息交换标准化技术委员会（TC 82）、全国电力监管标准化技术委员会（TC 296）、全国电网运行与控制标准化技术委员会（TC 446）、全国工业机械电气系统标准化技术委员会（TC 321）等标准化委员会加紧制定工控安全相关标准。同时，工业互联网安全标准体系也正加紧研究和建设中。

已经发布的工控安全相关国家和行业标准如表 4 所示。

表 4 已发布的国家和行业标准

时间	标准
2010 年	GB/T 26333-2010：信息安全技术工业控制网络安全风险评估规范
2014 年	GB/T 30976.1-2014：信息安全技术工业控制系统信息安全第 1 部分：评估规范 GB/T 30976.2-2014：信息安全技术工业控制系统信息安全第 2 部分：验收规范
2016 年	GB/T 32919-2016：信息安全技术工业控制系统安全控制应用指南
2016 年	GB/T33007-2016：工业通信网络系统安全 建立工业自动化

时间	标准
	和控制系统安全程序
2016 年	GB/T33008.1-2016：工业自动化和控制系统网络安全 可编程序控制器（PLC）
2016 年	GB/T33009.1-2016：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/T33009.2-2016：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/T33009.3-2016：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/T33009.4-2016：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
2016 年	GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南

表 5 制定中的工控安全相关国家标准

类型	国家标准
安全要求	信息安全技术 工业控制系统安全管理基本要求
	信息安全技术 工业控制系统测控终端安全要求
	信息安全技术 工业控制系统网络组件安全保障要求
	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
	信息安全技术 工业控制系统网络审计产品安全技术要求
	信息安全技术 工业控制系统专用防火墙技术要求
安全测评	信息安全技术 工业控制网络监测安全技术要求和测试评价方法
	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
	信息安全技术 工业控制系统漏洞检测技术要求及测试评价方法
安全等级	信息安全技术 工业控制系统信息安全分级规范
	信息安全技术 信息系统安全等级保护基本要求 第 5 部分：工业控制系统
	工业控制系统产品信息安全评估准则
安全实施	信息安全技术 工业控制系统风险评估实施指南

类型	国家标准
	信息安全技术 工业控制系统安全检查指南
	信息安全技术 工控 SCADA 系统安全防护管理指南
	信息安全技术 工控 SCADA 系统安全体系
	工业控制系统专业防火墙技术要求
	工业控制系统信息安全实施指南
	工业控制系统网络安全防护导则
	电力监控系统网络安全防护导则

（3）行业标准

2018 年 2 月，我国工业互联网产业联盟（AII）同时发布《工业互联网 安全总体要求》、《工业互联网平台 安全防护要求》两份标准性文件。前者规定了工业互联网应用场景下各组成对象不同安全等级的安全防护要求，对象涵盖工业现场设备、工业控制系统、工业互联网平台及工业应用程序。后者针对工业互联网平台的安全防护需求，规定了工业互联网平台安全防护的总体要求，主要包括边缘层安全、平台 IaaS 层安全、平台 PaaS 层安全、平台 SaaS 层安全等。工业互联网产业联盟后续还将依托产业界，制定《工业互联网 安全接入要求》、《工业互联网 安全能力成熟度评估规范》、《工业互联网 数据安全保护要求》等多项工业互联网安全相关标准。

2 工业互联网安全防护思路

2.1 工业互联网安全总体防护框架

与传统工业控制系统相比，工业互联网的安全覆盖面更为复杂。因此工业互联网安全防护体系建设需从综合安全防护体系的角度进行统筹规划。根据工业互联网的整体实施架构，针对其中的工业设备安全、工业控制安全、工业网络安全、工业数据安全和工业应用安全等各个层面，秉持功能安全与信息安全统筹规划原则，通过安全管理和安全技术综合施策，实现从安全设计、安全防护、安全运营，到威胁预警、威胁监测、威胁防御、应急响应的工业互联网全生命周期安全闭环。

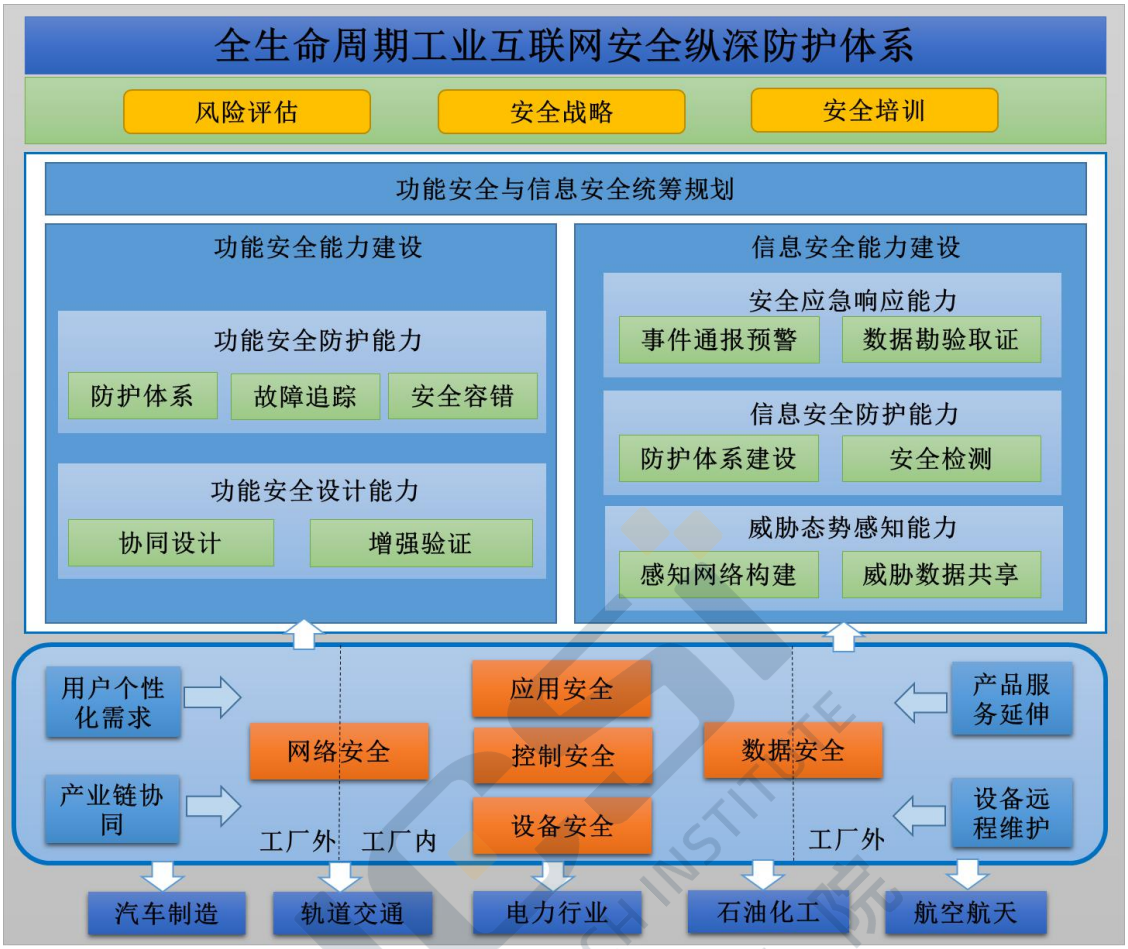

图 2 工业互联网安全总体防护框架

2.2 功能安全与信息安全统筹规划

需将功能安全与信息安全统筹规划原则贯穿于整个工业互联网安全防护能力的建设过程中。

1）基于风险管理思想的融合

在工业互联网安全研究采用风险管理思想时，一方面在风险可接受原则上要与功能安全统一，因为二者针对同一工业互联网研究对象，由不同原因导致的相同安全事件造成的后果严重程度和风险可接受程度应是一致的。如不论是针对工控系统的信息安全事件还是功能安全事件导致的 HSE（Health、Safety、Environment）相关事故，其

风险可接受程度应是一致的。另一方面在脆弱性识别阶段应做到二者有机的结合，功能安全强调系统自身存在的脆弱性导致的系统失效，而信息安全强调威胁主体利用系统自身存在的脆性导致的系统失效，二者都关注系统自身的脆弱性，一个是系统脆弱性易于被人利用，另一个是由于系统自身的不鲁棒性在运行过程中导致的系统失效。因此在系统脆弱性的识别过程中，应该统筹考虑两方面的因素，尽量做到功能安全和信息安全的融合。

2）基于设计原则的融合

工业互联网平台、应用、网络以及物联设备和控制系统在设计开发环节，需将功能安全与信息安全都考虑在内，并形成功能安全和信息安全有机结合的一体化内嵌安全保障，才能有效防护工业互联网各个层面功能的安全可靠运行。例如工业控制系统功能安全在进行安全设计时通常考虑采用冗余、故障安全设计原则等来降低风险。信息安全设计原则通常采用域分离、不可旁路特性等来降低被攻击后的损失。因此功能安全和信息安全在进行安全设计时一方面功能安全要考虑安全设计原则是否存在被攻击者旁路的风险，另一方面信息安全要考虑其自身功能安全特性的失效是否会给系统造成可用性或安全性的风险。

2.3 工业互联网功能安全能力建设

针对工业互联网平台、应用、网络以及物联设备和控制系统，实现逻辑功能可验证、异常故障可处置、标准规范可保障。尤其针对工

业核心控制系统需要求设备的高安全性，即系统需求规定的功能如实完成而不偏离预定目标。

（1）工业互联网功能安全设计能力建设

功能安全软硬件协同设计。建立覆盖系统软硬件全生命周期的安全开发流程；提出系统设计的风险评估与分析的安全手段，形成软硬件分析验证推理的全套保障方法；研究全生命周期各阶段的测试方法的无缝对接与融合，测试数据在各阶段的复用；研究软硬件系统协同可靠性开发方法，形成完备的流程体系并实现其标准化的构架。

功能安全增强及验证机制。研究系统中功能安全等级最高的部件的功能安全的设计方法学，对核心部件应用全数学证明技术；面向工业需求，实现形式化方法的深度安全强化技术，支持工业级别的产品设计。

（2）工业互联网功能安全防护能力建设

面向系统缺陷的功能防护体系。建立系统缺陷的功能防护手段、指南与标准，实现功能防护的冗余备份机制；定制完整的系统功能安全管理机制，例如对工控系统进行合理分层、对工控系统的应用者和应用软件进行分类管理、对访问系统的行为进行多种手段的分析等。

系统功能监控与故障追踪机制。利用云计算、云存储、工业现场总线和传感器等基础设施，为工业互联网和工控系统构建全方位立体在线实时监控环境，建立相关的存储、监测和数据分析方法；建立故障原因分析、故障传递分析、失效分析和软件缺陷定位等多维度、多层次的故障追踪分析体系。

支持工业新环境下的系统容错机制。建立适应工业互联网、工业云环境等新兴工控形态的容错算法和容错机制；设计在线实时冗余备份、现场断点保护和系统断点重启等关键技术；构建工业互联网环境下的系统反馈、系统冗余以及系统在线更新技术，实现工业新业态的纠错与防护体系建设。

2.4 工业互联网信息安全能力建设

针对工业互联网整体实施架构，实现威胁态势可感知、攻击行为可防范、安全事件可控制。部署工业互联网安全在线监测和信息共享平台，提升工业互联网安全主动监测、威胁情报感知共享和分析能力，构建覆盖全生命周期的工业互联网安全主动防御策略和体系。

（1）工业互联网安全威胁态势感知能力建设

面向工业互联网探测识别的感知网络。部署资产自动化发现和可视化、主动异常监测等在线监测手段，扩展工业互联网资产识别种类、提高识别精准度和搜索效率，实现威胁信息自适应聚类提取、工业互联网安全风险信息关联分析、攻击行为智能化溯源。

加强工业漏洞及威胁情报等数据共享。建立工业互联网安全信息共享机制，依托国家工控安全信息共享平台，汇集各方优势资源，加强工业互联网漏洞数据和威胁情报等信息共享，建立威胁来源高效感知、安全态势科学研判的工作体系，实现跨部门、跨区域信息共享。

（2）工业互联网安全防护能力建设

工业互联网安全防护体系及风险评估。构建工业互联网全生命周

期和全方位的安全防护体系，在工业互联网平台、工业 APP、工业网络、工业数据库以及工业设备和控制系统等各个层面部署身份认证、访问控制、安全审计、加密传输、安全网关、安全数据存储等安全技术和管理手段。建立多层次动态化的工业互联网安全风险分析机制，构建工业互联网安全风险评估体系。

工业互联网安全检测技术。建立工业互联网静态和动态安全漏洞分析与挖掘技术，安全漏洞深度利用技术。针对工业互联网攻击机理和工程特征，研究建立工业互联网网络入侵与攻击模型；建立漏洞扫描、健壮性测试、固件深度安全分析等多层次、多维度的工业互联网安全检测技术，提高漏洞扫描分析等检测工具对于不同工业控制系统硬件平台、编译调试软件等应用环境的兼容性。

（3）工业互联网安全应急相应能力建设

工业互联网安全事件通报预警机制。构建工业互联网安全通报预警体系，明确通报预警及应急响应工作流程。依据工业互联网安全事件分级分类，根据行业特征、影响程度、处置难度等，制定工业互联网安全应急处置预案，保证应急预案的连续性、一致性、兼容性和有效性。

工控系统数据勘验取证能力：构建多层次、全方位、全网络的工控系统和设备的数据勘验体系架构，研究分布式远程资源协同调度机制，制定新型信息技术应用环境下的工控系统电子数据取证鉴定标准与规范。

3 国内外工业互联网安全产业发展

3.1 工业互联网安全市场规模快速增长

随着全球不断爆发针对工业企业和关键基础设施的网络攻击事件，以及各国加强工控系统和关键基础设施安全监管，加紧出台各项政策、标准，工控安全市场规模迎来快速增长。据市场研究机构 Market Research Future 分析，2017 年全球工业信息安全市场规模达 130 亿美元左右，预计到 2023 年底，全球工业信息安全市场规模将达到 244.1 亿美元，年复合增长率达 10.97%。市场增长的主要驱动因素将包括：针对工业网络的威胁将成指数级增长，全球积极推进智能制造、工业互联网、工业 4.0 先进制造技术发展，以及政府机构对工控安全产业的大力支持。

3.2 多类企业主体参与市场角逐

强劲的市场需求催生众多市场主体类别涉足工业互联网安全业务，包括大型自动化厂商、传统综合网络安全厂商、以及专注工控安全的初创安全公司。

1. 自动化软硬件厂商

在工业自动化领域，众多百年巨头企业，如西门子、通用电气、霍尼韦尔、罗克韦尔自动化、施耐德电气等，都在力推数字化工厂、工业互联网及工业 4.0 的发展。在工业互联网和工业 4.0 的部署推进中，安全成为不可或缺的重要因素。全球自动化设备供应商、工业软

件供应商都很快在这一点上达成共识，纷纷通过收购工控安全厂商、与工控安全厂商建立合作伙伴关系、自建团队开展工控产品开发等举措开展工业互联网安全业务（表 6），例如美国通用电气于 2014 年 5 月并购了工控安全厂商 Wurldtech，霍尼韦尔公司于 2017 年 6 月收购了工控安全厂商 Nextnine，德国菲尼克斯电气在 2001 年就成立了网络安全子公司，随后又收购和投资了多家工控安全厂商。

这类企业虽也对外提供工业互联网安全产品和服务，但主要还是服务于自家软硬件产品和自动化设备的网络安全保障。在工业物联网设备、工业互联网平台以及工业软件设计之初就将信息安全内嵌其中，不仅可在安全性方面提升产品的优势，免去用户后续部署相关信息安全防护手段的麻烦，同时也是未来数字化时代工业互联网安全的发展趋势。在这一点上其他专业网络安全厂商可能存在面临市场缩小的风险。

此外，自动化企业在将信息安全集成到产品中时，另一个优势是可以较容易地在产品中统筹考虑信息安全与功能安全，实现两者的融合设计。

表 6 全球自动化设备及软件企业开拓安全业务举措

企业名称	国别	安全业务拓展举措
GE	美国	2014 年 5 月收购工控安全厂商 Wurldtech
Honeywell	美国	2017 年 6 月收购工控安全厂商 Nextnine
Rockwell Automation	美国	2017 年 2 月，与工控安全厂商 Claroty 建立合作伙伴关系
Schneider electric	法国	2018 年 1 月，与 Cylance 建立建立合作伙伴关系；2019 年 3 月，与网络安全企业 Vericlave 建立合作伙伴关系

Phoenix Contact	德国	2001 年成立全资网络安全子公司；2008 年 4 月收购工控安全厂商 Innominate；2016 年成为工控安全厂商 SecurityMatters 的股东；
PTC	美国	2019 年 3 月，与网络安全厂商 BlackRidge 建立合作关系。
SAP	德国	2011 年收购安全厂商 SECUDE 的安全产品及资产；
ABB	瑞士	内部拥有网络安全团队，2011 年建立网络安全委员会。
HITACHI SYSTEMS	日本	2015 年收购安全托管服务提供商 ABOVE SECURITY
海天炜业	中国	2009 年将业务延伸到工控安全
力控科技	中国	2009 年成立工控安全子公司力控华康
和利时	中国	2011 年将业务延伸到工控安全

2.传统安全厂商

涉足工业信息安全领域的另一大类市场主体是传统网络安全厂商，包括 Cisco、Fortinet、Palo Alto Networks、Checkpoint 等传统网络安全（Network Security）产品供应商，McAfee、Symantec、Kaspersky Lab 等传统安全软件供应商，Accenture、Deloitte、EY、KPMG 等大型咨询公司，此外，还包括 Leidos Cyber、NCC Group、Darktrace、Forescout 等网络安全企业基于自身的技术专长领域开拓工业互联网安全产品和服务。在国内，也同样出现一波工业互联网安全热潮，传统安全厂商纷纷建立工业信息安全团队，基于 IT 安全产品开发工控安全产品，包括绿盟、启明星辰、奇安信、安天、安恒、圣博润、三零卫士等安全企业。

传统网络安全厂商虽在安全技术方面占有优势，但由于缺乏对工业环境的了解，因此在安全防护产品部署方面可能造成不能真正满足工业企业安全需求，并且容易忽视功能安全与信息安全的融合问题。

3.专业工业互联网安全厂商

近几年国内外涌现了众多专注于工业互联网安全领域的初创企业，例如美国的 Bayshore、Dragos、CyberX，以色列的 Claroty、Indegy、SCADAfence，法国的 Sentryo，以及中国的威努特、长扬科技、安点科技等。这些企业拥有网络安全和工业控制的人才优势，以工业互联网安全为唯一业务领域，在全球开拓了众多能源、制造、化工等领域的客户，是市场里的重要角色，并能以创新性的技术引领整个行业的技术发展趋势。

表 7 国内外工业互联网安全初创企业列表

公司名称	国别	成立时间	主要产品和服务
APERIO Systems	以色列	2016 年	工控数据防篡改(DFP)
Applied Risk	荷兰	2012 年	安全培训、渗透测试、工控安全保险等
Bayshore	美国	2012 年	工控安全态势监控、动态威胁识别、事件应急与响应
Claroty	以色列	2014 年	一体化监控平台：ICS 漏扫、持续威胁监控、访问控制等
Cyberbit	以色列	2015 年	OT 安全平台（SCADAShield）
CyberX	美国	2012 年	工控网络安全监控、事件应急响应
Dragos	美国	2016 年	ICS 安全监控平台与威胁可视化
Firmitas Cyber Solutions	以色列	2014 年	工控系统实时防护产品
HALO Analytics	以色列	2015 年	工控端到端安全、威胁可视化、合规检查
Indegy	美国	2014 年	工控网络安全态势分析、威胁感知产品
SCADAfence	以色列	2014 年	工控网络监控、安全评估
威努特	中国	2014 年	工业防火墙、工控主机卫士、工控漏洞挖掘平台、工控漏洞扫描平台、工业互联网雷达、工控网络攻防演练平台
长扬科技	中国	2017 年	工业防火墙、工业网闸、工控主机卫士、工业监测审计系统、工控等保检查工具箱、工控安全评估系统、统一

			安全管理平台、工业物联网安全态势感知平台
中科兴安	中国	2013 年	工业安全评估系统、工业防火墙系统、工业审计系统、统一安全监管平台、主机安全防护系统
九略智能	中国	2016 年	工业网络智能防护系统、工业主机智能防护系统、工业网络智能监测系统
安点科技	中国	2012 年	工业网闸、工业防火墙、主机威胁免疫系统、网络威胁感知系统、安全审计系统、工业漏洞扫描系统、工业信息安全检查工具集
网藤科技	中国	2016 年	工控行为追溯系统、工控安全防护系统、工控安全审计系统、工业安全隔离网关、网藤账号集中管理与审计系统、网御高级持续性威胁预警系统

3.3 工业互联网安全领域投融资活跃

近年来，工业安全需求催生众多工业互联网安全初创企业涌现，并获得资本市场和现有网络安全企业的青睐。据 Momentum Cyber 初步统计，2017 年全球工业互联网安全企业融资金额达 1.03 亿美元，而 2018 年上半年的融资金额就已达 9000 万美元。国内外工业互联网安全企业获融资情况见表 8。

表 8 国内外工业互联网安全企业获融资情况

企业名称	国别	融资日期	融资金额	融资阶段
Claroty	美国	2018 年 6 月	6000 万美元	B 轮
		2018 年 12 与	未公开	C 轮
PAS	美国	2017 年 4 月	4000 万美元	-
Dragos	美国	2018 年 11 月	3700 万美元	B 轮
Cyberbit	以色列	2018 年 6 月	3000 万美元	-
CyberX	美国	2018 年 2 月	1800 万美元	B 轮
		2019 年 3 月	1800 万美元	C 轮
Indegy	以色列	2018 年 8 月	1800 万美元	B 轮
Nozomi Networks	美国	2018 年 9 月	3000 万美元	C 轮
Radiflow	以色列	2018 年 7 月	1800 万美元	B 轮
Sentryo	法国	2018 年 12 月	1000 万欧元	A 轮
威努特	中国	2018 年 4 月	数亿元	C 轮

长扬科技	中国	2018 年 10 月	数千万元	A 轮
安点科技	中国	2017 年 8 月	4500 万元	B 轮
网藤科技	中国	2017 年 8 月	千万级	A 轮

3.4 安全产品随工业智能化发展快速转型

不仅自动化企业关注工业互联网和工业 4.0 部署中的网络安全问题，安全厂商也都注意到了全球制造业正在发生的数字化和智能化大变革，在工控安全产品和服务开发中更多的开始关注工业物联网、网络物理系统、工业互联网平台、工业 APP、工业互联网等新技术嵌入和设备互联带来的安全风险，并采取技术和战略措施有效管控风险。例如 Symantec 针对工业互联网环境下设备、系统互联互通导致的威胁风险上升趋势，开发了将安全直接嵌入到工业设备中的解决方案。再如美国工业互联网安全专业厂商 Bayshore 建议工业企业在准备部署工业互联网以使工业基础设施和数据互联之前，应确保采取安全措施在工业企业与工业物联网合作伙伴之间建立双向的、访问受到控制的、基于策略进行保护的通信通道。Bayshore 开发的工业网络保护平台可以在网络威胁破坏关键工业资产和系统之前实施阻止，并保护设备安全连接到工业物联网。

4 垂直行业工业互联网安全解决方案

4.1 轨道交通

4.1.1 安全问题分析

轨道交通系统是一线大城市最重要的公共交通系统，具有运力大、安全性高、速度快等特点，是城市中至关重要的关键基础设施。一旦遭受网络攻击，将导致非常严重的社会影响，甚至是人员伤亡的严重安全事件。当前，随着通信、自动控制、交通运输技术水平的不断发展，轨道交通正向无人驾驶的自动化方向发展。同时，随着移动互联网的快速发展，向乘客提供列车和车站的实时信息已成为普遍需求。因此，这些原来采用物理隔离保障的信息系统与互联网的连接越来越紧密，与互联网的通信频次也越来越高，面临的安全挑战也越来越大。此外，轨道交通的安全性主要依赖功能安全标准（IEC 61508）建设，信息安全建设较为薄弱。

1. 综合监控系统安全问题

综合监控系统处于轨道交通系统的控制中心层，与环境控制系统、消防系统、电力 SCADA、乘客信息系统、车站广播系统、信号系统等各类相关子系统相连接，实现对列车整体运营环境的总体监控。综合监控系统的接口多且复杂，安全问题突出。一是普遍未部署工控专用的网络安全设备，缺乏访问控制和异常监测手段。二是普遍采用商用操作系统，无主机审计防护措施。三是应用系统的身份鉴别与授权功

能强度较弱。

2. 轨道交通信号系统安全问题

轨道交通信号系统是负责列车安全运行管理的核心系统，包括自动监控系统、自动保障系统、自动运行系统等。信号系统是列车自动化运行的关键系统，一旦受到攻击，将导致列车停车等重大安全事故。存在的安全问题包括：一是信号系统网络普遍采用安全码机制进行防护，无法实现访问控制和异常监控；二是计算机和服务器无恶意代码防护系统，且不能及时更新补丁。

3. 车地无线网络系统

车地无线网络系统是针对轨道交通系统设计的一种高速移动无线通信系统，可为列车与控制中心之间实时数据传输提供稳定、可靠的无线传输通道。车地无线网络系统受到攻击可造成非常严重的后果，例如导致信号系统中断，列车停止等事故。存在的安全问题包括：一是轨旁 AP 是容易暴露的攻击点，目前普遍存在安全配置弱等问题，极易遭到路边发射设备的攻击；二是无线通信协议加密防护机制缺失，极易被劫持和篡改。

4. 自动售检票系统

城市轨道交通自动售检票系统（AFC）是基于计算机、通信、网络、自动控制等技术，实现轨道交通售票、检票、计费、收费、统计、清算等全过程的自动化系统。AFC 系统自上而下可以分为五层架构：清分中心、线路计算机系统、车站计算机系统、车站终端设备、车票。车站终端设备主要包括自动售票机、闸机、自动验票机、自动增值机

等设备。AFC 系统存在的安全问题包括：一是普遍采用传统 IT 通信网络作为承载，面临与传统 IT 网络一样的安全风险。二是自动售检票机等终端设备无恶意代码防护措施。三是当前“互联网+”与 AFC 系统不断融合，云售票机、云闸机等新型设备可实现移动快捷支付，让购票/乘车更加方便快捷，但安全问题更加严峻，增加了更多攻击路径。

5. 轨道交通电力监控系统

轨道交通电力监控系统（PSCADA）对全线的变电设备进行监控，并采集、分析变电设备的运行数据，为供电系统的调度、维护提供依据，确保牵引供电系统和全线的电力变配电系统安全可靠和经济运行。PSCADA 系统出现信息误报、漏报、误控等情况，将直接影响供电系统的稳定运行和故障判断。存在的安全问题包括：一是主站服务器仅依赖物理隔离保障安全性，无其他安全防护措施。二是主站层网络、光纤环网等通信专网安全防护手段缺失。三是终端层控制器大量采用进口设备，网络模块对抗攻击能力弱，极易成为攻击对象。

4.1.2 应对策略

1. 主机安全

1）在行车调度中心内通信服务器、数据库服务器、应用服务器、接口服务器、RBC 主备接口服务器、本地操作终端等关键主机和服务器上部署工业主机防护系统，阻断蠕虫、木马和恶意程序攻击。使得在物理隔离状态下不能及时更新操作系统补丁的主机，仍能实现对操作系统进程的安全监管。

2）使用安全 U 盘，杜绝蠕虫、木马和恶意程序的传播，行车调度中心、无线闭塞中心内使用安全 U 盘进行数据摆渡，专盘专用。

2.网络通信

1）在行车调度中心、无线闭塞中心边界处部署工业防火墙，实现区域隔离。

2）针对轨道交通综合监控系统、信号系统以及电力监控系统的网络通信安全风险，建立基于白名单的网络访问控制体系，研究面向各个接入系统的大数据流量的态势感知体系。

3）针对车地无线通信系统以及 AFC 系统的的通信网络安全风险，在通信协议中加入密码技术，进一步强化通信保障能力。

4）轨交控制系统对过程通信的实时性要求较高，通过对各个通信环节进行网络安全基线测试和设定，安全可靠地部署信息安全防护措施。

5）实时监测网络内的非正常通信和异常流量，集中监测数据通信网络、列控中心/联锁安全数据通信网络、无线闭塞中心/联锁安全数据通信网络。

6）强化轨旁 AP 设备的网络安全防护建设。

3.应用层安全

对应等级保护要求，加强轨道交通控制系统的应用安全功能研发，包括身份识别、访问控制、应用层通信加密、安全审计、入侵防范等安全功能设计，强化控制系统的应用层安全。

4.安全管理平台

建立安全管理平台，汇总工业防火墙、工业审计系统、工业主机防护系统运行数据，全方位呈现轨道交通控制系统信息安全状况，实现信息安全可视化。

5.加强功能安全与信息安全融合

1）现有的工控信息安全产品，尚未面向功能安全进行设计讨论和功能强化，因此无法进入安全侧开展信息安全防护工作。需面向功能安全要求，重新讨论信息安全产品在此方面的诸如面向安全侧的失效、系统自举自检等功能。

2）加强轨交控制系统的内嵌安全设计，统筹考虑功能安全与信息安全两方面需求，结合功能安全开展面向信息安全保障能力的形式化建模和验证。

4.2 发电系统

4.2.1 安全问题分析

电力工业是国民经济发展中最重要的基础能源和关系国计民生的基础产业。当前，发电行业正在积极利用工业互联网实时掌控设备运行数据，实时呈现工况、产能，达到设备的预见性维护、提高能源利用效率，优化运营水平。但由于安全管理和防护策略不完善，防护技术手段不健全，控制系统存在未知风险和未知漏洞无法检测，使得发电控制系统面临的安全问题非常突出。

电力行业包括发电、输电、配电、变电等各个环节，其中在发电

环节中，火力发电装机容量占我国发电装机总容量的64%左右。当前，火电发电控制系统安全防护存在的主要问题如下：

1）安全防护方案更多的只是通过简单的安全隔离装置、加密认证、防火墙等简单的防护手段加以边界性的防范。

2）对发电工控系统存在的未知风险和未知漏洞无法做到实时检测和积极的主动防御。

3）在信息安全防护方面，技术手段不完善，存在控制系统漏洞、国外设备后门、防护策略不当、病毒库升级不及时等问题。

4）无法体现工控系统安全的核心要素，如本质安全、功能安全、信息安全等。尤其在复杂的发电自动化领域中，如何将信息安全纳入工控安全范畴，以及如何将功能安全、信息安全融合是至关重要的因素。

5）能源互联网、工业互联网等技术发展将对能源电力行业带来新的系统安全问题。

具体而言，火电自动化系统网络结构包括现场设备层、DCS（集散控制系统）实时数据网络、SIS（厂级监控信息系统）网络和MIS（管理信息系统）网络等拓扑结构。各层控制系统的安全问题包括：

（1）现场设备，诸如各种仪器、仪表和现场执行机构、现场总线等存在多种接入方式，非法的接入方式将直接影响设备甚至系统的正常运行，给系统造成严重安全隐患。

（2）DCS集散控制系统组成部件多，协议复杂，系统开发本身基本从功能安全角度出发，为确保实时性一般较少考虑信息安全要求。

系统中基本使用 Windows 为主的国外操作系统，采用的工业协议存在缺乏加密和认证等网络安全的考虑，系统运行环境也存在大量漏洞和隐患并缺乏防护，另外缺少针对工业控制设备的信息安全检测手段、标准和方法。

（3）SIS 监控信息系统体系架构缺乏基本的安全保障，且控制人员缺乏网络安全意识。

（5）火电工控系统的边界针对工控网络威胁的持续防护能力缺失，边界隔离采用传统物理隔离，缺乏相应的访问控制策略，系统直接暴露在互联网上的风险较大。

4.2.2 应对策略

1.基础软件层面

1）针对主流嵌入式操作系统，研究轻量化信息安全加固组件，对嵌入式操作系统进行信息安全加固，提升嵌入式操作系统的安全防护能力。

2）针对实时数据库安全，加强实时数据库数据安全存储、数据安全传输以及安全审计等关键安全技术研究，覆盖数据库应用安全、维护安全、使用安全和存储安全，防止数据泄露。

2.硬件设备

研究嵌入式应用软件的信息安全增强技术，开发一套模拟工具，对即将投入使用的程序代码进行功能及安全防护模拟。

3.应用软件

针对 SCADA 系统监控软件、仿真软件、OPC 软件、网络管理软件

以及在数据服务器、操作员站、工程师站上安装的应用软件（DCS 和 SIS 层），研究白名单技术，安装工控主机防护软件，营造“白环境”。预研内核安全的 DCS 控制器相关的应用软件。

4. 网络通信

1）针对 DCS 层的通信协议，深入研究各种发电工控设备的协议快速识别算法，研制具有鲜明行业特色的工控防火墙，在网络边界和区域边界部署工业防火墙加强访问控制，研制安全型的工业交换机。

2）控制网部署安全审计设备，将包含有设备状态、系统事件、接口状态信息等信息的审计信息存储到本地或远程端，同时加强审计风险防范。

3）针对发电工控系统强实时性传输需求，研究轻量级加密算法，保障传输安全可控。

4.3 石化行业

4.3.1 安全问题分析

石油化工行业是我国国民经济的支柱产业之一，在国民经济发展中有着不可替代的作用。当前，我国石油化工企业正加快数字化转型发展，运用工业物联网、大数据分析、工业云平台等技术实现企业生产方式和管控模式变革，在安全环保、节能减排、降本增效等方面积极探索。然而，目前我国石油石化行业信息安全防护工作虽有一定的建设成果，但仍缺乏足够的重视与技术支持，存在很多安全隐患。对

石油化工行业而言，生产的强连续性、高安全性、环境的特定性使得控制系统安全稳定运行显得尤为重要。

当前石油化工行业存在的安全问题包括：

1）石化生产控制系统在设计之初缺乏信息安全防护设计。

2）安全防护技术不足，包括：控制系统未进行安全域划分，区域间未设置访问控制措施；操作站和服务器操作系统更新困难，存在高危系统漏洞，系统安全配置薄弱；工程师站缺少身份认证和访问控制策略。

3）生产环境内 OT 资产缺乏可见性。IT 安全控制在 OT 设置中使用，而未考虑对 OT 的影响。

4）企业普遍缺乏应急预案以及应急设备。

石化企业的安全需求包括：

1）管理异构控制环境，为来自不同 DCS 供应商的系统提供标准化的视图。

2）实现对网络和服务器状态和配置的自动化、实时视图，并提供变更控制管理，及时识别和阻挡攻击行为。

3）当发现可疑行为或其他问题时，对安全事件作出快速、协同响应。

4）为工业和过程控制系统中的网络和服务器提供安全防护时，不影响 OT 环境的稳定性和正常运行。

4.3.2 应对策略

通过统一的工业防护自动化系统管理平台实现对工厂内所有设

备终端安全事件和状态数据的集成管理和分析，同时确保工业控制系统安全可靠运行。平台应包含的功能包括：资产发现、资产管理、配置变更管理、安全事件监测、事件报告等。平台需采用超低带宽限制和专有协议，以达到不影响工业控制系统安全可靠运行的目的。

（1）资产发现与管理

自动发现资产，快速盘点、搜索和报告环境中的硬件和软件版本，提供控制系统中所有基于 IP 和非 IP 资产的统一拓扑视图。通过自动收集资产配置监测异常状况，降低网络安全风险，按需实施漏洞管理。

（2）配置变更管理

自动收集、规范和报告影响控制系统环境的配置变更，包括 HMI、PLC、RTU 和 IED 等，实现易受攻击资产的快速识别和加固。功能需求包括：远程管理配置规则；更改用户帐户或防火墙规则；禁用不必要的端口和服务；资产配置和变更的集中视图；管理实际配置和基线配置，以消除配置漂移。

（3）安全事件监测

收集控制系统提供的大量信息，并进行标准化和优先次序排列，合并事件日志，检测异常，分流警报，使得安全人员能够监视、跟踪和检查重要的安全事件，提升态势感知能力。

4.4 汽车制造

4.4.1 安全问题分析

汽车制造业是自动化程度最高的行业之一。汽车制造控制系统具

有高度自动化、智能化和网络化，广泛应用了自动化总线技术、PLC、变频器、机器人等汽车制造行业的自动化设备。当前，汽车制造行业正在快速推进工业互联网的落地和实施，通过将信息管理系统、MES系统、生产线自动化控制系统、WMS 物流仓储系统等的互联互通，信息共享，实现生产管理集中管控，解决产线停机等问题，进一步提高效率，降低成本。

虽然汽车制造行业的自动化程度高，但仍存在众多信息安全问题。由于对控制系统实时性和业务连续性要求较高，一旦由于人为错误或恶意网络攻击，未经授权更改工业流程，将极大影响生产效率，造成重大经济损失。

汽车制造行业存在的安全问题包括：

1）工业控制系统主机和服务器系统老旧，处于网络隔离状态无法更新补丁，普遍存在漏洞。

2）工业设备、机器人、PLC 等缺乏可见性，无法实现对工业网络中的恶意攻击行为、误操作行为等的实时检测、预警和记录。

3）工业机器人的网络安全防护能力异常脆弱，存在重大安全隐患，包括存在通信不安全、欠缺身份认证和授权、使用开源软件、默认设置和软件更新不及时等问题。

4）汽车制造行业普遍存在安全意识薄弱问题。

4.4.2 应对策略

1.自动化资产发现

首先需要为工业制造现场设备提供一个完整、详细和自动化的资产清单，这是实现工业制造环境可视化、安全性和可控性的必要条件。资产清单软件需自动发现工厂里所有的设备，包括 PLC、DCS 等控制设备、工作站、HMI、服务器以及机器人等，基于角色对不同类型的资产进行分类，绘制设备之间的关联图谱，同时需要为每个设备列出最新以及精确的状态情况，例如采用 Windows 操作系统的主机的补丁列表，再如 PLC 的背板配置、固件版本等等。其次，需基于每个设备的数据对安全状态进行风险评估，包括基于 Windows 主机的补丁更新情况进行漏洞评估，根据工业控制器上危险的开放端口和默认密码进行风险评估等等。此外，还需实时监控和跟踪状态变更，以发现任何异常行为。

2.网络威胁检测

1）基于策略的威胁检测：根据确定性规则和用户自定义策略识别已知的攻击和风险事件。

2）异常检测：持续“学习”正常的网络行为，创建标准基线，检测偏差并为可疑事件触发警报。

3）基于签名的检测：利用 Suricata 签名和规则来识别已知的威胁和恶意行为。

4）攻击早期预警：监视行为变化和偏离基线的情况，检测恶意攻击行为者的早期探测和侦察活动。

3.自动配置控制

攻击者可通过多种方法对工业控制器执行配置和代码更改，例如

可通过网络进行远程更改，也可通过物理连接在控制器上进行本地更改，还可以通过临时连接到远程网络交换机上进行更改。随着工业流程变得越来越复杂，对控制器的代码和配置更改进行手动管理是不可能的，需开发工具自动跟踪 ICS 环境中的每个配置和代码更改。

1）跟踪远程执行的更改：通过详细的活动细节识别每一个改变控制器配置的远程交互。

2）识别本地执行的更改：检测和跟踪控制器本地执行的更改。

3）版本控制：通过提供完整的控制器代码快照，包括详细的梯形逻辑历史、固件历史、底板硬件配置等，实现版本控制。

4）自动跟踪更改：实时分析通过网络发送的工程工作站命令，提取每个活动的完整上下文，包括指示固件更改、代码更新、强制执行 SFC 和 IO、对设定值执行写入等命令。就违反组织策略的活动向用户发出警报。

4.5 石油开采——海洋石油钻探

4.5.1 安全问题分析

移动式海上钻井平台(MODUs)用于钻井勘探和开采，分为位于浅水海床的自升式平台和用于深水钻井的钻井船和半潜器。标准钻井船和半潜式钻井船通常包括四个主要的独立 OT 网络，每个网络由外部承包商管理，在使用的自动化设备和通信协议方面彼此是不同的。其中发电和配电网为钻井船的所有系统提供电力；动态定位网络通过使用螺旋桨和推进器来维持钻井船的位置和航向；钻井控制网络(DCN)

控制钻井船的钻井活动；防喷网络(BOP)用来封堵、控制和监测油井和气井，防止原油或天然气不受控制地喷射。四个网络分别通过专有协议与钻井船的 IT 网络相连。

当前，钻井平台也正逐步利用物联网、云计算等新一代信息技术实现远程资产监控，避免油气泄露，造成经济损失和人员伤亡。然而钻井船 OT 网络的碎片化和管理使得安全漏洞广泛存在，安全风险及其严峻，具体存在的结构性安全漏洞包括：

1）网络承包商的远程维护活动会引入新的攻击面。攻击者可通过获取享有特权的第三方帐户入侵钻井船的 OT 网络。

2）钻井船的 OT 网络没有做网络隔离，而是直接连接到钻井承包商的 IT 网络（与互联网相连）。

这些结构性漏洞构成了重大网络安全风险。但钻井承包商目前无法有效管理此类风险，原因有二:一是每个网络由其各自的承包商单独管理。因此，在整个 OT 网络环境中缺乏对所有资产的统一视图。二是从技术的角度来看，传统的 IT 安全监控产品不能提供对钻井船网络中资产所使用的所有专有 OT 协议的可见性。因此，钻井平台承包商需要一个安全解决方案，使其能够获得可见性，重新控制其 OT 网络，并更好地解决其所负责的安全和操作风险。

4.5.2 应对策略

1. 部署网络安全集成平台

首先确保网络安全防护措施不会造成任何操作中断。然后将网络安全防护集成平台连接到能够通过 SPAN 端口中继复制流量的托管交

换机。被动监控通过连接到托管交换机上的 SPAN 端口来执行，此配置将复制这些交换机中继的所有流量。在对网络基础设施进行评估以确定要使用的交换机时，需要考虑以下事项：

1）要覆盖直接涉及一级资产(PLC)的所有流量，包括 PLC 与二级资产(工程工作站、HMI)及以上(各种网络服务器)的所有连接。所有直接影响物理进程的流量都要进行复制和监控。

2）完成一级通信覆盖后，搜索二级及以上的通信，包括网络段与工作域的交叉点等重要交换机，例如：IT 和 OT 网络之间的交汇点。

受监控交换机的数量取决于网络拓扑结构。可以从该单点监视聚合所有流量的主交换机的网络。在更加细分的网络中，或者具有独立的一级集群的网络中，对每个相关交换机进行端口镜像。

2. 通过“学习”实现威胁检测

1）平台首先在训练模式下，学习网络的标准行为并建立全面的行为基线。在此期间可汇总网络异常行为，包括不安全的远程连接，不适当的分段或弱密码，以及可能影响运行工作流程的各种网络配置错误。

2）发现网络资产（PLC，HMI，工程师站和网络设备），收集每个资产的详细数据，并描述资产在网络上的通信模式。

3）训练模式完成后，进入运行模式。当检测到与基线的偏差，重大更改（如 PLC 配置下载或模式更改）或明显的恶意活动时，发出威胁警报。同时，在单个屏幕上可查看和控制所有

OT 网络数据，使钻井平台承包商能够跟踪任何变化，并对安全和操作警报做出响应。

4.6 制药行业

4.6.1 安全问题分析

当前，制药行业也正积极推进数字化转型，工业物联网设备在制药行业中的广泛应用带来了许多益处，包括数字化供应链和智能制造流程带来的业务效率提升、定制药品和 3D 打印药品带来的潜在新收入渠道，以及对设备进行预测维修的能力。然而，尽管工业物联网增强了整个制造和供应链流程的数字化能力，但由于攻击面的迅速扩大，导致行业面临新的网络安全风险。

制药行业的首要任务是确保在生产过程中不会发生任何未知或未经批准的篡改，同时，监管部门对制药行业生产数据的留存要求极高，必须确保所有生产数据都被记录下来，并且不会被篡改。

制药行业面临的其他挑战还包括：

1）联网设备的设计仅关注可靠性，未充分考虑安全性；

2）生产设备中大多数操作系统无法及时更新，也无法打补丁；

3）攻击者可通过企业 IT 网络渗透 OT 网络；

4）企业网络和工厂 OT 使用不同的协议和系统，较难实现整体安全性。

这些风险和挑战将会为企业生产带来的影响包括：

1）在企业系统中从事间谍活动；

2）破坏工厂系统，导致设备超压、爆炸或停工；

3）物理危害，例如物质泄漏，进而危害环境和员工健康。

4.6.2 应对策略

通过构建集成多种应用的工业网络防护平台实现对现有资产和风险的可见性，检测并消除高级持续性威胁，实现策略控制的外部互联。

1）在镜像或 SPAN 端口、代理或透明网桥中部署平台，并通过自动发现引擎应用程序捕获、记录流量以供分析，同时对标准工业协议和定制工业协议进行规范化和过滤。

2）通过自动学习引擎应用程序，根据网络流量观察、公共和专有威胁情报、行业最佳实践等，创建初始基线策略建议。

3）通过非破坏性、自动化的标识和资产清单实现对整个 OT 环境中设备、网络和系统的可视性。

4）通过识别资产和流量的变化、基线行为的异常和违反预先建立的策略的行为，进行实时监控，并对工业协议进行深度内容过滤，以提供威胁情报。

5）通过主动报警和选择性地拦截攻击性的通信和命令，防止网络威胁影响目标对象和数据。此外，需以线路速度运行平台，并在细粒度事务级别提供保护，以使授权的流量正常通行，即使当网络攻击发生时，也能允许正常的工作流继续运行。

6）与外部实体建立可信的通信通道，同时控制其中通信的内容，将安全防护功能扩展到工厂之外，实现第三方承包商对特定

机器的远程访问，并通过对其与该机器的交互进行策略保护，防止未经授权的活动。同样，可以建立与外部合作伙伴、供应商和服务提供商之间的安全通信控制，从而实现与工业互联网的安全可靠连接。

5 工业互联网安全发展展望

5.1 工业互联网安全政策将由指导逐步过渡到监管

在当前我国工业互联网发展初级阶段，工业互联网平台、网络物理系统、工业网络架构等工业互联网支撑技术体系仍不成熟并处于快速发展过程中，国家工业互联网安全政策将主要以指南文件对部署工业互联网的工业企业提供指导性参考，并鼓励工业互联网与安全保障同步建设，以及支持工业互联网安全产业生态建设和安全产业快速发展。工业互联网安全标准将主要以行业联盟标准为主。工业互联网发展到一定阶段后，由于工业领域安全事件影响和危害巨大，工业互联网安全将成为国家网络安全法、等级保护条例以及关键信息基础设施保护条例的重要监管对象。

5.2 工业互联网安全产业将迎来增长拐点

由于我国工业制造业自动化程度发展不均衡，普遍在数字化、网络化方面基础较弱，尤其是对于中小企业而言，设备改造和数据采集难度较大，同时工业软件、工业网络等领域的技术基础相对薄弱，因此我国工业互联网发展成熟将是一个长期的过程，需稳步推进，综合部署。由此，工业互联网安全产业在近几年内将不会呈现特别快速的增长，预计在五年后工业互联网在各行业全面铺开时，工业互联网安全产业将迎来增长拐点，呈现爆发式增长。但等保 2.0 以及关键信息基础设施保护条例的出台仍将带动工业互联网安全产业在近年内保

持快速增长，预计从目前到 2023 年，工业互联网安全产业规模将以 30%的速度增长。

5.3 工业互联网安全良好产业生态进一步形成

建设工业互联网安全保障体系需要工业企业、工业自动化企业、工业软件集成商、IT 企业、云服务商以及工业互联网安全企业的协同合作，实现工业互联网平台、工业 APP、工业网络、工业智能设备的安全设计（Security by design），功能安全与信息安全的统筹考虑，以及工业安全需求与网络安全技术能力的对接。预计随着我国工作互联网安全产业政策红利不断释放，多方协作、互利共赢的良好产业生态将逐步形成，产业各类市场将积极展开合作，共同为工业数字化转型提供最佳安全解决方案。

5.4 功能安全与信息安全将进一步融合

OT 环境与 IT 环境具有本质区别，当前针对工控系统的信息安全手段存在与工业环境不兼容问题、与功能安全不兼顾问题。例如信息安全手段会影响工业控制系统的功能正常运行，信息安全威胁也可能导致功能安全失效。工业环境的特殊安全需求将推动工业互联网安全技术进一步提升与工业控制系统和运行环境的兼容性，同时在功能安全与信息安全关联交织的背景下，进一步在安全设计、安全防护等环境增加功能安全与信息安全的统筹考虑。工业互联网安全标准也将既涵盖 OT 和 IT，又涵盖功能安全和信息安全，以全面覆盖工业互联网的安全范畴。

附录 1 国内外工业互联网安全企业一览

一、国外工业互联网安全初创企业介绍

1. Indegy

Indegy 是一家专注于提供工业互联网安全技术和产品的企业，成立于 2014 年，总部设在美国纽约，研发中心设在以色列。Indegy 的创始和研发团队既拥有丰富的网络安全专业技能，又非常了解工业操作技术，很多来自于以色列国防军(IDF)精英网络安全部队。Indegy 的主要产品之一“工业网络安全套件”拥有完整的工业控制系统(ICS)活动和威胁的可见性、安全性和控制能力，结合了混合的、基于策略的检测和网络异常检测，以及独特的设备完整性检查。Indegy 的解决方案广泛用于世界各地的制造业、制药、能源、水力和其他工业组织。Indegy 当前已融资 3 轮，共获得融资 3600 万美元，主要投资人包括 Liberty Technology Venture Capital、Vertex Ventures Israel、Aspect Ventures、Magma Venture Partners 等投资机构。Indegy 的工控安全产品获得众多奖项，并被 Gartner 评为 2017 年“工业 4.0”领域的“酷厂商”。

2. Bayshore

Bayshore 成立于 2012 年，位于美国北卡莱罗纳州达勒姆市。Bayshore 的公司愿景是为 OT 环境提供最健壮、易于部署的主动安全防御解决方案。公司的创始团队认识到传统的企业防火墙不能有效地保护复杂的工业环境，尤其是在普渡模型的较低层级。此外，企业环

境中存在的协议和签名的标准集在 OT 环境中不存在。因此，Bayshore 的创始团队认为需要一种解决方案，将防火墙的传统黑名单功能与白名单功能结合起来。Bayshore 开发的 IT/OT Gateway™专利软件部署在云环境中，使得工业企业能够实现对其 OT 网络的完全可视化。Bayshore 网关软件的特点是对网络流进行粒度检查和过滤、策略构建和实施，以及检测、解析和分割工业协议的能力。2015 年，Bayshore Networks 被 Gartner 评为工控安全领域的酷厂商，并获得“SINET 16 Innovator”称号。当前，Bayshore 的产品和解决方案已广泛应用于制造业、能源、数据中心、制药和化工等行业中。Bayshore 目前融资 3 轮，共融资 1140 万美元。

3. SCADAfence

SCADAfence 专注于工业物联网安全，成立于 2014 年，总部位于以色列特拉维夫，在美国纽约、德国慕尼黑、日本东京都设有办事处。SCADAfence 自称其安全平台是唯一一个专门为支持大规模复杂工业网络的规模和多样性而构建的解决方案，擅长为采用工业物联网和工业 4.0 技术的智能制造企业提供全面覆盖的安全解决方案，例如制药、化工、食品饮料和汽车行业。其解决方案能够提供日常操作的可视性、网络攻击的检测和旨在提高响应能力的取证工具。SCADAfence 的合作伙伴包括 Checkpoint、Fortinet、Demisto、Oracle、Gigamon 等。

4. Dragos

Dragos 是一家工业物联网和工业控制系统安全厂商，成立于 2016 年，总部位于美国马里兰州。Dragos 开发的 Dragos 安全平台，

能够收集、检测和自动化生成资产清单，通过威胁行为分析进行威胁检测，并实现安全运营和事件响应。Dragos 还建设了一个威胁运营中心，为业界提供专用的 ICS 事件响应和威胁搜索服务，以及针对漏洞、威胁和安全事件的行业威胁情报。Dragos 在 2018 年被 Gartner 评为工业物联网安全领域的“酷厂商”，其安全解决方案获得 2019 年 SCawards“最佳 SCADA 安全解决方案”奖。Dragos 当前共融资 3 轮，融资额达到 4820 万美元，投资机构包括 Canaan Partners、National Grid Partners、Schweitzer Engineering Laboratories、Energy Impact Partners 等。2019 年 3 月，Dragos 收购了位于美国亚特兰大的知名工控安全公司 NexDefense，以期利用 NexDefense 的技术能力为工业企业提供资产识别工具。

5.Claroty

Claroty 是一家专注于工业控制系统安全的网络安全初创公司，成立于 2014 年，总部位于美国纽约。Claroty 的综合集成网络安全平台提供了对工业网络（I/O 层）的高度可见性，通过自动发现和监视网络资产和通信模式，为用户提供了一个进入工业控制系统网络的实时窗口。该平台可以主动发现并消除漏洞、错误配置和不安全连接，通过执行细粒度访问策略来管理第三方和员工远程访问，还可以持续监控和检测恶意活动和高风险变化，快速为对网络威胁和事件进行响应。目前 Claroty 共融资累计 9200 万美元，投资机构包括众多全球知名工业自动化企业，例如罗克韦尔、霍尼韦尔、施耐德、西门子、通用电气等。此外，以色列网络安全企业孵化器 Team8 也投资了

Claroty。近两年，Claroty 的客户数量实现了 357%的年增长率，在六大洲的 9 个细分市场拥有大型客户，包括电力、石油和天然气、化工、水力、制造、食品和饮料、采矿和房地产等行业。

二、国内工业互联网安全企业（可替换）

1.安恒信息

安恒是国内领先的网络与信息安全产品和服务提供商，总部设在杭州及北京，在上海、南京、广州、深圳、成都、武汉、重庆、济南、西安等三十多个城市设有分支机构，服务客户包括政府、公安、运营商、金融、教育、企业等多个行业。目前已是享誉国内外的网络安全品牌，于 2016 年成功跻身“全球网络安全 500 强中国区榜首”。安恒的工控安全解决方案实施分层分域防护、集中管理运营的纵深防护体系，通过划分最小安全区域，从访问控制、报文深度过滤等方面入手实施严格的边界防护，在安全域中内部分别从主机层、网络层检测用户行为、控制行为以及网络流量的异常，积极报警与阻止，杜绝网络威胁对生产系统的影响。并通过建立集中的工业安全运营中心，以网络拓扑从空间呈现工控网络内重要资产和安全设备的分布维度，对全网关键节点进行在线监测、威胁量化评级、网络安全态势分析以及预警。工业互联网安全解决方案则从设备与控制安全、网络与数据安全、应用与平台安全，以及安全生命周期管理角度全面增强保障能力。

2.威努特

威努特成立于 2014 年，是国内专注于工控安全领域的国家高新技术企业。威努特以率先独创的“白环境”整体解决方案为核心，深

度结合工控系统安全特点研发了覆盖工控网络安全的 4 大类 20 款自主可控产品，提供工控安全咨询、安全培训、风险评估、安全检测、安全应急、安全建设及运维等全流程服务。拥有核心技术及市场优势，成功为电力、轨道交通、烟草、石油石化、市政、智能制造及军工等五百余家国家重点行业客户提供了全面有效的安全保障。

3. 长杨科技

长扬科技（北京）有限公司是一家北京市国资委和经信局投资、指导下的，专注于工业互联网安全、态势感知和安全大数据应用的创新型高新技术企业。长扬科技公司产品及业务聚焦工业网络安全及安全大数据领域，为客户持续提供覆盖工控系统整个生命周期的网络安全产品、解决方案和安全服务。公司推出安全防护类、监测审计类、漏洞扫描挖掘类、安全检测工具类、工业终端安全类、安全态势感知及工业大数据等七大产品线，既有企业侧的防护、监测类设备，也有基于人工智能和大数据分析技术的工业互联网安全态势感知平台、安全大数据平台。公司产品及解决方案的技术优势在于通过人工智能技术赋予了客户在网络和业务两个层面的安全防护能力。以工控安全数据协同感知与协同处置为核心理念，增强工业安全应用场景化自学习自适配能力，并以 AI 技术赋能工业网络安全态势感知，以工业网络安全数据和关键基础设施行业数据为基础，对工控设备资产指纹，工业漏洞库、安全设备库、物联网传感数据、工业网络安全数据进行建模，实现空间、时间两个维度上的安全大数据分析及态势感知，为客户建设立体式工业互联网安全防护保障体系。

4. 安点科技

安点科技是一家工业网络与工业互联网安全威胁识别与防御技术提供商。安点科技认为多种有效覆盖全业务流程的工业控制网络安全技术的高效联动，可以帮助企业工程师提高对网络安全威胁的识别与应对能力，并有效抵御持续性的网络渗透与压倒性的网络攻击。安点网络微隔离系统采用国际领先的微隔离技术，通过对网络通信行为的细粒度分析，阻止恶意代码的的隐匿渗透。在工业生产过程中，可有效保障生产设备的持续不间断的可靠工作，准确执行生产指令，防止恶意篡改、泄露、仿冒等攻击行为造成的成产中断、技术泄露、人员伤亡等严重生产事故。

5. 观安信息

观安信息是一家以大数据分析为基础，大数据分析+泛安全业务为主线的上海市高新技术企业和软件企业，泛安全业务方向主要包括大数据安全、工控安全、业务安全（风控）、公共安全等。在工控安全领域，观安信息拥有工控安全监测系统、工控安全威胁诱捕感知系统、工业互联网安全态势感知平台等产品，可在不影响业务运行的情况下进行工控系统安全风险自评和工业企业内部威胁快速感知。其中，观安信息以流量采集和深度工控协议包分析为基础，创新性地提出了基于设备的安全行为感知，利用大数据分析建立分析模型，克服了传统的基于规则进行安全分析的不足，可以及时的发现未知威胁并进行报警和通告，实现工业企业的安全运营；观安信息也是国内首家推出工业互联网安全蜜罐产品的企业，该产品可在不影响业务运行的情况

下进行工控系统安全风险自评和工业企业内部威胁快速感知。

附录 2 全球工业互联网典型安全事件

安全事件	日期	事件描述
委内瑞拉停电事件	2019 年 3 月	委内瑞拉古里水电站发生故障，导致委内瑞拉大部分地区断电，委内瑞拉当局设法恢复了该国“许多地区”的电力供应。然而，马杜罗总统表示，该国的电网在周六再次遭受打击，许多恢复的系统再次瘫痪。
台积电病毒攻击事件	2018 年 8 月	8 月 3 日，台积电位于台湾新竹科学园区的 12 寸晶圆厂和营运总部网络遭病毒攻击，导致生产线全数停摆。几小时后，台积电位于台中科学园区的 Fab 15 厂，以及台南科学园区的 Fab 14 厂也陆续遭到病毒攻击，使得台积电在台湾北、中、南三处重要生产基地的核心工厂全部沦陷，产线全部停摆。
恶意软件“TRITON”攻击工控系统安全仪表系统（SIS）	2017 年 12 月	安全研究人员发现了一款针对工控系统安全仪表系统（SIS）的恶意软件“TRITON”，该软件以施耐德电气 Triconex 安全仪表控制系统为目标展开攻击，造成中东多家能源工厂停产，根据对恶意软件样本以及攻击流程、攻击方式的分析，其幕后黑手疑似为国家支持的专业黑客组织。
NotPetya 病毒攻击多国工业企业	2017 年 6 月	2017 年 6 月，俄罗斯最大石油企业 Rosneft 等超过 80 家俄罗斯和乌克兰公司遭到网络袭击，黑客向能源和交通公司、银行业和国家机构等植入病毒并封锁电脑，相关用户被要求支付 300 美元的加密式数字货币以解锁电脑。乌克兰受到的攻击最为严重，乌克兰政府官员报告称，乌克兰电网、银行和政府部门的网络系统遭到严重入侵。此外病毒攻击还波及到英国、俄罗斯等欧洲多国的机场、银行和大型企业的网络系统。美国大型制药企业默克公司、法国建筑巨头圣戈班、俄罗斯石油公司(Rosneft)、丹麦能源和货运公司马士基(Maersk)、西班牙食品巨头 Mondelez 随后相继自曝受网络袭击。
勒索病毒 WannaCry 全球性爆发	2017 年 5 月	这一巨大的全球性网络攻击感染了 150 个国家的 23 万多台电脑，影响了制造商、银行和政府。雷诺(Renault)和本田(Honda)等公司被迫停产。
乌克兰电网遭受两次网络攻击	2015 年 12 月、2016 年 12 月	2015 年 12 月 23 日当地时间 15 时左右，乌克兰首都基辅部分地区和乌克兰西部的 140 万名居民突然遭遇了一次长达数小时的大规模停电，至少三个电力区域被攻击。Kyivoblenergo 电力公司称：公司因遭到入侵，导致 7 个 110KV 的变电站和 23 个 35KV 的变电站出现故障，导致 80000 用户断电。2016 年 12 月 17 日当地时间 23 点多，时隔一年，乌克兰的国家电力部门又一次遭遇了黑客袭击，这次停电持续了 30 分钟左右，受影响的区域是乌克兰首都基辅北部及其周边地区。30 分钟后，

		Ukrenergo 工程师将设备切换为手工模式，并开始恢复供电，75 分钟后完全恢复供电。
化名 Kemuri 的水处理厂遭受网络攻击	2015 年	Kemuri 水公司(KWC)是一家匿名水公司的别名，该公司的水处理厂在2015年遭遇网络攻击。攻击者利用Kemuri水厂互联网客户支付门户的网页漏洞拿到了公司计算机的控制权。攻击方法涉及 SQL 注入和网络钓鱼，获取到了 Kemuri 水厂陈旧的基于 AS/400 商用服务器的工业控制系统。该工业控制系统并未与互联网隔离，下辖一系列可编程逻辑控制器，管理着控制净水系统中水和化学物流动的各个阀门和管道。
德国钢厂遭受网络攻击	2014 年	2014 年 12 月 19 日,德国联邦信息安全办公室(BSI)发布了一份 2014 年的信息安全报告,这份长达 44 页的报告中披露了一起针对 IT 安全关键基础设施的网络攻击，并造成重大物理伤害。受攻击方是德国的一个钢厂，遭受到高级持续性威胁(APT)攻击。攻击者使用鱼叉式钓鱼邮件和社会工程手段，获得钢厂办公网络的访问权。然后利用这个网络，设法进入到钢铁厂的生产网络。攻击者的行为导致工控系统的控制组件和整个生产线被迫停止运转，由于不是正常的关闭炼钢炉,从而给钢厂带来了重大破坏。
欧美能源企业遭受针对 SCADA、PLC 和 DCS 系统的远程访问木马攻击	2014 年	欧洲和美国的能源企业感染了一种名为“蜻蜓”(Dragonfly)的组织开发的新恶意软件。黑客攻击的目标是这些国家的能源网络运营商、主要的发电公司、石油管道运营商和能源工业控制系统设备制造商。攻击者使用了两个主要工具组名为 Backdoor.Oldrea 和 Trojan.Karagany 的远程访问木马（RAT）程序。
沙特阿拉伯石油公司遭受网络攻击	2012 年	这次攻击始于该公司 IT 团队的一名员工打开了一封恶意网络钓鱼邮件，为攻击者提供了一个入口。随后攻击者释放了一种被称为 Shamoon 的病毒。该病毒立即开始在公司的整个 IT 网络中传播，至少感染了该公司 35000 台电脑。尽管攻击只影响了 IT 网络，但它对其他业务流程(如装载汽油卡车)产生了重大影响。
美国一家供水和公用事业公司的 SCADA 系统遭到网络攻击,导致其中一个水泵被毁	2011 年 11 月	美国伊利诺伊州斯普林菲尔德以西一处乡郊的供水设施，约两个月前开始出现系统问题，其中一个水泵被频密开关，后发现控制水泵的监控及数据采集系统（SCADA）疑被黑客入侵。这次攻击始于公用事业公司的 SCADA 软件供应商被黑客攻击，客户系统的用户名和密码列表被窃取。一旦攻击者获得了这些凭证，就可以访问泵的控制系统。