EcoStruxure™
Innovation At Every Level

SECURE

工业信息安全技术洞察

施耐德电气商业价值研究院与亚信安全联合出品

www.se.com/cn

Schneider Electric 施耐德电气

亚信安全

施耐德电气
商业价值研究院介绍

施耐德电气商业价值研究院成立于2021年5月。遵循严格的方法和为社会做贡献的使命，我们通过对中国经济、产业和商业进行严谨、实用和创造性的研究，为公众和商界提供融合全球智慧的专业洞见，致力于成为推动中国经济、社会和企业可持续发展的领先智库。

我们的研究团队汇集了绿色智能制造、绿色能源管理领域的一线专家、深耕前沿技术的研发工程师、参与行业政策和标准制定的专家学者，也聚集了来自业界各科研院所的学术界领袖、为企业掌舵的管理层，以及来自于通讯、信息安全、互联网、管理咨询、市场研究等领域的生态伙伴专家。

我们的研究内容涵盖行业、技术、宏观等方面，同时基于自身发展以及所提供的企业咨询服务中的积累，将深入探讨企业战略、研发管理、供应链管理、营销、财务、人力资源、品牌推广等话题，并与社会积极分享研究成果。

我们的研究方法结合定性和定量分析，通过一线调研，以数据驱动分析，实现深层价值提炼，进而帮助企业中高管理层把脉宏观，见微知著，助力企业探索可持续发展之道，把握时代机遇，加速变革转型。

目录 CONTENTS

目录 CONTENTS

前言

目前，全球正在经历百年未有过的大变局时代，以5G、大数据、云计算、人工智能等为代表的新一代网络信息技术正在推动着传统经济发展和产业模式的变革，数字经济已经成为世界新格局的重要标志。

但随着数字化进程的快速推进，网络风险也呈现指数级增长，网络漏洞、数据泄露等问题日益凸显，有组织、有目的的网络攻击在不断增多，网络安全防护工作面临严峻挑战。国家工业信息安全发展研究中心监测数据显示，2020年全球工业信息安全事件涉及8大领域、16个细分领域，其中装备制造、能源等行业遭受的网络攻击最为严重，交通运输、电子信息制造、消费品制造、水利等行业网络攻击呈现高发态势[1]。

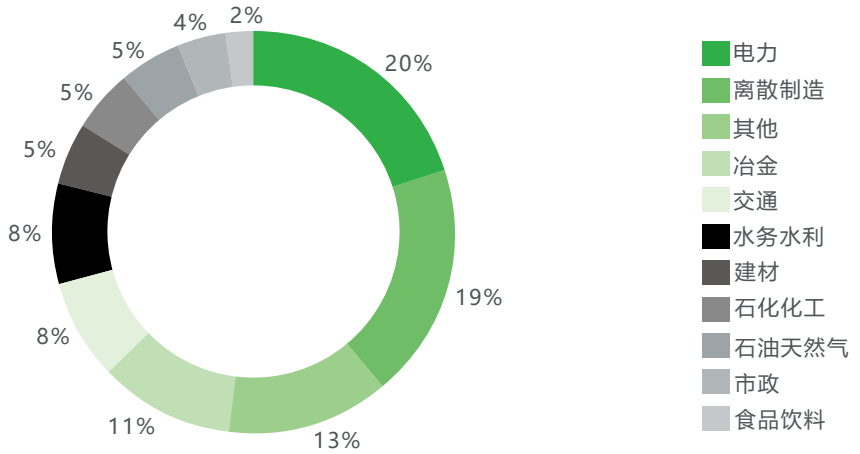
施耐德电气商业价值研究院与亚信安全携手，从中国工业信息安全发展的现状出发，利用线上线下结合的方式针对两百余家工业企业用户展开摸底调研。为了加深认知，我们挑选其中十余家典型行业的企业高管进行深访，以期本洞察的分析和总结，能够带给中国的行业、企业以价值参考。

注 [1]　《工业信息安全发展报告 2020-2021》邬贺铨 2021.08

核心发现

在这次由施耐德电气商业价值研究院联同亚信安全组织的“工业信息安全发展”企业调研中，我们收集了近 200 位工业企业高管和信息安全相关负责人对工业信息安全发展的反馈。这近 200 位的被访者来自十个纵深行业中的代表企业，他们所展示的观点和经验将覆盖大多数中国工业企业对信息安全这一话题的认知现状，由此所总结出的核心发现对众多国内工业企业将具有一定借鉴意义。

企业调研样本分布



三个发现

工业信息安全发展驱动力在增强

随着两化融合工作的快速推进，工业企业数字化转型工作进入到发展新阶段，从监管机构到企业自身都深刻的认识到信息安全保障对于数字化转型工作的重要性。在该背景下，大量的法律法规和监管政策高频推出，工业信息安全领域标准体系持续完善，监管手段日益多样化。同时企业自身也逐渐开始将工业信息安全建设提升到与数字化转型和可持续发展相同的战略高度来推动。

外部监管

- 政策法规高频发布
- 国家标准持续完善
- 监管力度不断提升

内部驱动

- 数字化转型基础保障
- 可持续发展韧性源泉

工业信息安全建设仍面临较大挑战

超半数受访者认为企业对工业信息安全的重视程度还有待完善。资金人力的投入不足成为工业信息安全建设的首要挑战；基础设施陈旧、历史遗留的安全设计缺失所带来的攻击性升级，以及 IT/OT 融合大背景下协同工作的复杂度升级也相应增加了信息安全管理难度。

54%

资金人力投入不足

- **资金：**重视程度不够，整体信息安全投资低于国际公认合理水平，OT领域投资更是偏低
- **人力：**专职信息安全人员不足，OT领域更是几乎缺失，企业选择服务外包缓解人才瓶颈

33%

基础设施环境陈旧

- **设计：**生产运营系统时间久远，安全设计考虑少
- **防护：**存量风险问题多，实施需考虑对生产影响

27%

工业攻击针对性升级

- **风险：**新技术的应用导致攻击面增大，工业控制系统的风险呈持续上升趋势
- **攻击：**工业环境攻击的针对性显著增强，高赎金的勒索攻击对数据安全和持续运营带来严重威胁

26%

IT/OT 融合协同复杂

- **上云：**云技术在IT领域快速发展全面应用，越来越多的企业在OT领域探索并使用云计算和5G技术
- **赋智：**工业大数据平台建设成为未来重点方向，IT/OT共同规划和落地实现整体方案成为趋势

企业工业信息安全建设刚刚起步

参与调研的高管及信息安全负责人表示，尽管工业信息安全发展驱动力正在逐步增强，工业信息安全建设却仍处在“从初步合规开始迈向全面合规”的发展阶段。企业 OT 信息安全成熟度综合评分仅为 2.1 分（满分 5 分），相较 IT 信息安全成熟度水平具有不小的差距，绝大多数被访企业表示未来需要从管理成熟度和技术成熟度两方面着手加强工业信息安全能力的提升。

综合成熟度	管理成熟度	技术成熟度
2.1/5	2/5	2.2/5

四大价值主张赋能最优实施路径

结合代表企业在工业信息安全建设的行业经验，以及施耐德电气的最佳工厂实践和亚信安全的信息安全服务实践，通过厘清最优实施路径的发展思路，施耐德电气商业价值研究院总结出四个价值主张——“自知、合规、着力、迭代”，作为支撑企业工业信息安全建设的路径参考。

01 梳理现状 形成规划

开展信息资产梳理和和合规风险识别，评估信息安全成熟度水平，基于现状和问题，针对性开展战略规划、落地计划规划，制定安全体系框架，输出关键建设任务落地方案。

自知

02 建立基础 保障业务

构建信息安全管理体系，形成完善的管理制度，构建并落实 OT 环境安全基线，规划部署关键安全技术控制，以构建保障业务正常运作所必须的防护体系为目标建立基础安全能力。

合规

着力

03 关注痛点 强化运营

针对资产管理、应用管控、数据安全、安全态势感知、攻击遏止与协同响应等 OT 环境安全痛点难点问题进行专项提升，加强人员团队建设，强化 IOT 协同的安全运营能力建设。

迭代

04 持续改进 拥抱未来

建立信息安全内部常态化评估检查机制，积极参与网络安全等级保护和工业信息安全标准贯标认证工作，主动发现问题不足并及时制定并落实改进方案，持续提升工业信息安全管理水平。

1 外紧内驱：工业信息安全需求日益凸显

1.1 合规监管推动工业信息安全建设

信息安全是信息化社会国家安全的基石，尽管传统的 IT 系统信息安全已经步入市场成熟阶段，并具备不错的成熟度和大量成功案例。但对于工业企业来说，工业信息安全（ICS Cybersecurity）比仅有 IT 系统的传统信息安全更加复杂。

目前，网络空间安全已经上升为国家战略高度，工业信息安全作为国家网络空间安全的重要组成部分，相关的法律法规、指导方针、行动计划、国家标准、行业规范等都已发布或在积极制定过程中，同时国际组织也在推进工业信息安全国际标准的制定，将最佳实践标准化。

1.1.1 安全地位强化

主要政策法规

（图 1）来源：施耐德电气商业价值研究院

- **2010 年，**震网事件后工业信息安全地位得到越来越高的重视，2011 年工信部印发《关于加强工业控制系统信息安全管理的通知》，首次明确了重点领域工业控制系统在连接、组网、配置管理、设备选择与升级管理、数据管理和应急管理等方面的要求。并建立工业控制系统安全测评检查和漏洞发布制度，加强工业控制系统信息安全工作的组织推进。近年来，伴随着监管单位持续强化对网络安全主体责任落实要求，各行业、各领域的网络安全政策供给和标准指引明显加快，尤其是在关键信息基础设施相关的重要行业领域逐渐形成了具备显著行业特征的网络安全政策体系。伴随着工业互联网创新发展大潮，工业信息安全相关政策密集出台。

- **2016 年，**为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》，在充分考虑信息化和工业化融合的不断深入过程中，工业控制系统所面临的威胁风险情况变化以及我国工控安全现状，工信部又印发了《工业控制系统信息安全防护指南》（以下简称《指南》），涵盖工业控制系统设计、选型、建设、测试、运行、检修、废弃等各阶段防护工作要求，提出了具体实施细则指导工业企业开展工控安全防护工作。
- **2017 年，**《网络安全法》正式实施，并对关键信息基础设施的保护提出了明确要求。
- **2019 年，**《信息安全技术网络安全等级保护基本要求》发布新版，进入到结合云计算、移动互联网、物联网、工业控制和大数据等新技术新应用开展综合治理、系统监管、主动防控的等保 2.0 时代，至此工业控制系统被正式纳入保护范围之内，并要求在 “通用要求” 的基础上，符合 “工业控制系统安全扩展要求” 。
- 在当前数字产业化、产业数字化加快发展的大背景下，做好工业信息安全工作对制造强国、网络强国建设具有重要意义，在推动工业互联网加快发展的过程中，工信部在 2018 年和 2021 年连续下发《工业互联网行动发展计划》，其中特别强调推动实施工业互联网安全综合保障能力提升工程，依法落实企业网络安全主体责任，强化网络安全技术保障能力。
- **2021 年，**《关键信息基础设施安全保护条例》发布实施，条例中包含的公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域中大多涉及工业控制系统。
- **2021 年，**《数据安全法》和《个人信息保护法》的发布实施充分体现了数字化时代数据作为新的生产要素的重要性，两部法律的颁布将数据安全工作的重要性提升到了新的高度，数据安全也成为工信部加强网络安全保障体系和能力建设，护航制造强国、网络强国、数字中国建设的重要工作中心。

工业信息安全国家标准体系已初步成形，尤其在工业控制系统安全和工业信息安全防护产品领域，相关标准（如图 2）已涵盖了工控系统安全分级、安全管理、安全功能要求、安全评估准则、信息安全技术、风险评估、安全程序、安全控制应用和工业信息安全防护产品技术要求等多个维度。

安全相关标准

安全分级类国标

- GB/T 36324-2018 信息安全技术 工业控制系统信息安全分级规范

安全要求类国标

- GB/T 36323-2018 信息安全技术 工业控制系统安全管理基本要求
- GB/T 36470-2018 信息安全技术 工业控制系统现场测控设备通用安全功能要求
- GB/T 37933\GBGB/T 37934\GB/T 37941\GB/T 37953\GB/T 37954等多种类型的工业安全防护产品技术要求
- GB/T 37962-2019 信息安全技术 工业控制系统产品信息安全通用评估准则
- GB/T 40218-2021 工业自动化和控制系统信息安全技术等同 IEC/TR 62443-3-1:2009

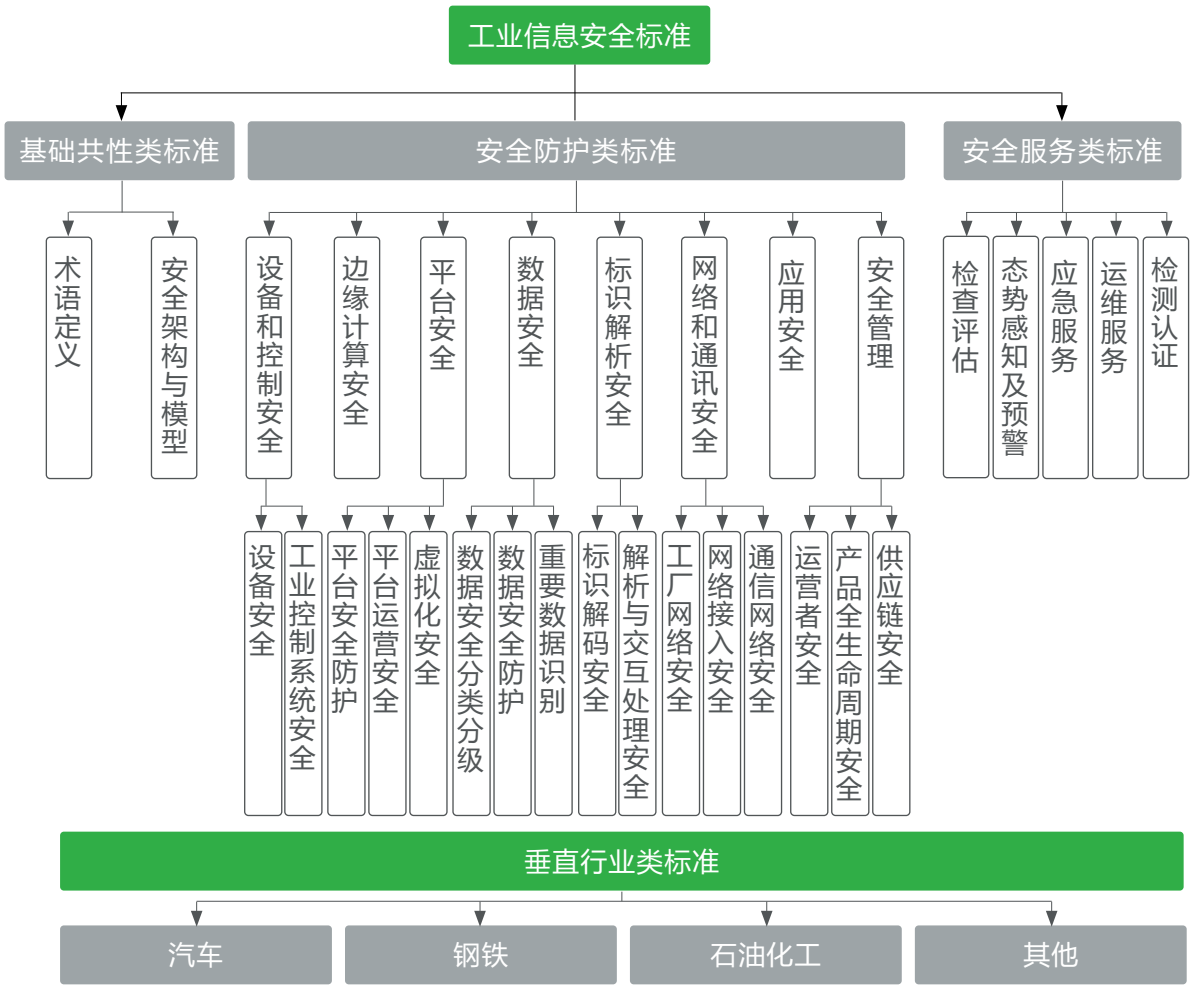
安全实施类国标

- GB/T 26333-2010 工业控制网络安全风险评估规范
- GB/T 33007-2016 建立工业自动化和控制系统安全程序 等同IEC 62443-2-1:2010
- GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南
- GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南
- GB/T 37980-2019 信息安全技术 工业控制系统安全检查指南
- 信息安全技术 工业控制系统信息安全防护建设实施规范（征求意见稿）

（图 2）来源：施耐德电气商业价值研究院

2019 年，工业信息安全产业发展联盟发布的《工业信息安全标准化白皮书》中构建了工业信息安全标准体系框架，覆盖基础共性类、安全防护类、安全服务类和垂直行业类的四大维度以及工业企业、边缘接入、工业云平台、工业应用等层次。

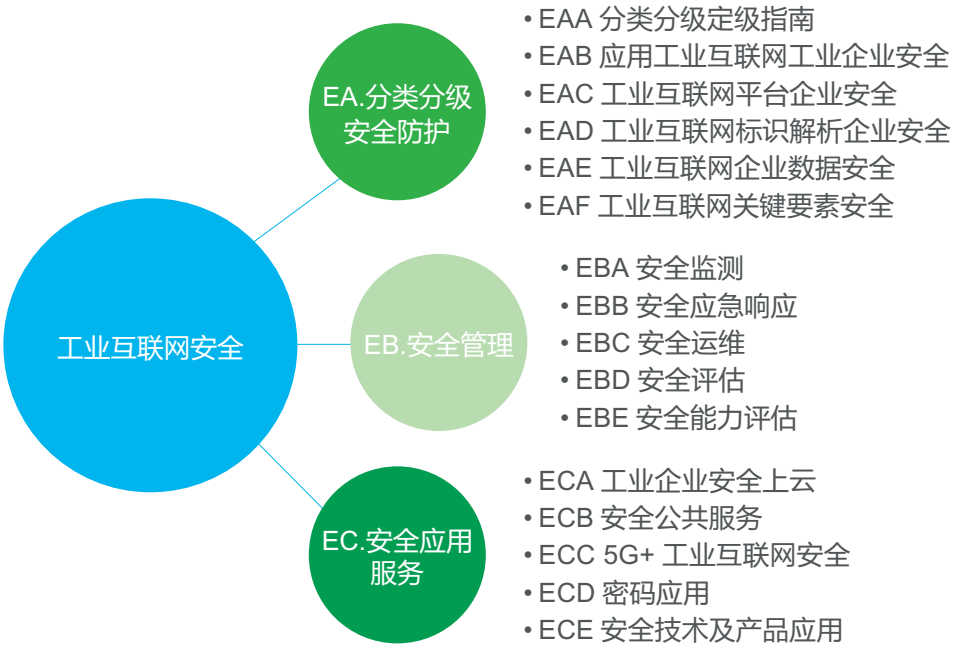
工业信息安全标准体系



（图 3）来源：工业信息安全标准化白皮书（2019 版）- 工业信息安全产业发展联盟

2021 年，工业互联网产业联盟、工业信息安全产业发展联盟、工业和信息化部商用密码应用推进标准工作组共同发布了《工业互联网安全标准体系（2021 年）》，其中包括分类分级安全防护、安全管理、安全应用服务等 3 个类别、16 个细分领域和 76 个具体方向。

工业互联网标准体系



（图 4）数据来源：施耐德电气商业价值研究院

1.1.2 监管手段多样

在相关政策趋于完善、标准逐渐充盈的环境下，工业信息安全的监管方式也更加严格和多样。

- **监管手段多样：**各级网信、公安以及各行业主管单位在职责范围内通过组织建设国家和行业区域级的安全态势感知平台、安全技术保障平台和安全基础资源库，竭力健全和完善安全威胁通报的处理机制，并组织开展网络安全技术应用试点的示范工作，通过数据安全管理等专项工作试点等多种形式的监管手段，积极推进网络安全的保护工作。
- **监管力度升级：**坚持以查促建、以查促管、以查促防、以查促改，加强信息安全的风险隐患排查，通报检查结果并加大整改力度，风险防范及主体责任落实，重点落实行业关键信息基础设施安全防护，对未履行义务或造成重大安全事故的运营单位进行严肃的处理。

1.2 数字化转型促进工业信息安全提速

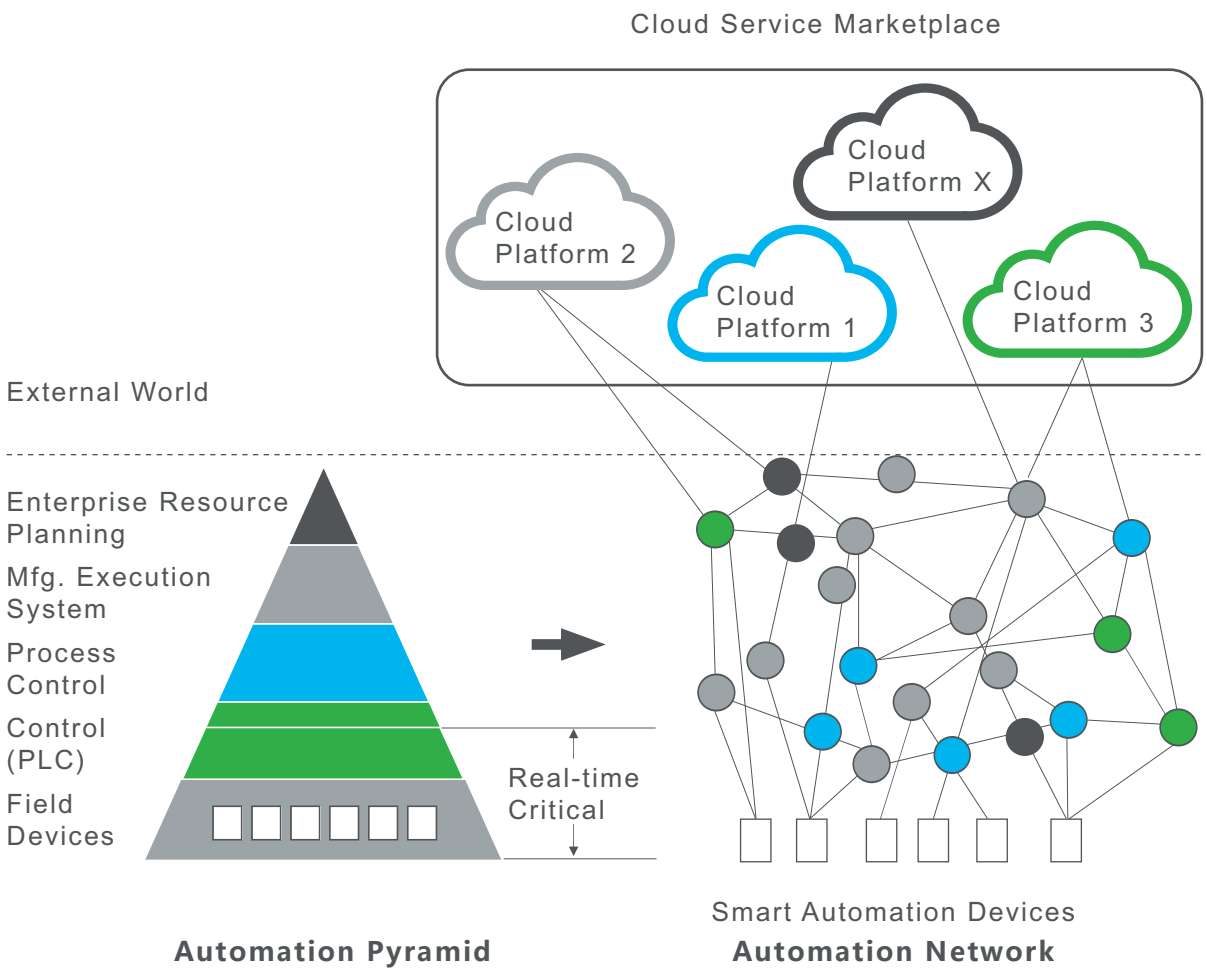
对于工业企业来说，控制系统被广泛应用于我国电力、冶金、水利、市政石油天然气、化工、交通运输、制药，以及大型制造业行业中，涉及国计民生的关键基础设施是依靠工业控制系统来实现自动化作业的。随着 5G、工业互联网等新型基础设施建设的不断推进，工业生产过程开放程度逐步加深，新一代技术与实体工业紧密融合，制造业企业数字化转型持续加速，工业信息安全已然成为支撑转型的重要基础保障。所以，信息安全和数字化两者必须要统一规划、统一实施，做到协调一致，切实防范、控制和化解数字化转型进程中可能产生的安全风险。

1.2.1 护航——数字化转型

全球数字经济正在加速，且与实体产业的融合也在不断深入，对于制造业企业来说，数字化转型成为“必选题”，并呈现出三大特点：

- **从非数字化到数字化：**随着网络技术的快速发展、互联互通的设备大规模的增加，大量的数据被采集汇总，而人工智能等 IT 技术也被用于系统优化、预测性维护等，因此极大地提高了生产力。
- **从封闭到开放：**通用 IT 技术、工业软件以及软件定义网络 (SDN) 逐渐改变着工业控制系统的架构，而传统的工业控制系统架构是由不同功能的产品构成，随着 ISA-95 普渡图架构从分层形态转变为扁平和自由的结构，逐渐趋同于现场设备、边缘及云三层 (如图 5)。在新的架构下，通信接口更加通用化，每个节点和设备的功能增强且独立，更便于访问不同的资源。

工业系统网络的演变



（图 5）来源：Interoperability in Smart Manufacturing: Research Challenges (MDPI)

- **从信息孤岛到互联互通：**可远程连接的智能节点数量随着工业系统架构的改变，呈现出几何级的增长态势。越来越多的生产流程以数字化方式进行监视、操作和控制，因而需要采集、归档、分析和管理大量不同系统的实时、结构化和非结构化数据。在生产工艺流程中，则更加依赖大数据、控制算法和人工智能等技术进行优化，设计资料、生产配方数据、库存信息等重要数据可通过网络进行访问。

曾经作为“孤岛”存在的工业控制系统因数字化而变得更加互联互通、高效灵活，这却导致生产运营过程中遭受信息安全攻击的概率显著提高，攻击对系统的影响的严重性也急剧升高。在这种背景下，数字化程度越高的工业环境，信息安全的“护航”作用就越发明显。

1.2.2 成就——可持续发展

在企业发展的过程中，效率和安全是首要考量因素，所以在提升效率的过程中保障安全才能真正意义上的实现可持续发展。

数字化进程的推进可以有效帮助工业企业提升生产运营效率，但随之而来暴露的工业信息安全问题，也是企业必须要面对和迫切解决的。近些年来，工业信息安全事件频发并有逐步增多的趋势，为工业领域的发展敲响了警钟，系统的可用性、完整性和保密性都受到了严重的威胁。

近年来大型工业信息安全事件

地点	事件
伊朗核电站	震网攻击导致上千台离心机损毁
大型石化企业	3 万台电脑数据被 Shamoon 病毒擦除
德国钢铁厂	高炉控制系统遭受攻击
乌克兰电网	两度被攻破，造成上百万人停电
某半导体厂商	同时遭受勒索病毒攻击，停产三天损失八千万美金，并对芯片供应链造成巨大打击
挪威某铝业巨头	遭受“武器化”的勒索攻击，停产第一周即损失三千万欧元
美国燃油管线运输公司	受到勒索攻击，造成全线管道停运，使多个州的燃油供应中断

（图 6）来源：施耐德电气商业价值研究院

2 迎难而上：工业信息安全建设的挑战和现状

构建信息安全弹性，确保业务韧性。对于积极推进数字化转型、追求可持续发展的企业来说，如果想有效应对信息安全威胁并最大程度的保障数字化转型带来的提质增效成果，就必须加强构建信息安全弹性。要使系统具有预防和适应变化的能力，能够对潜在的威胁进行预测和准备。监视和识别系统的关键功能或部件是否处于被攻击状态，在面对威胁和攻击时能够及时响应，从而能够保持信息基础设施的结构完整和功能稳定，实现对风险的动态适应和共生共存。即使在遭受攻击的情况下，能够有效的维持关键业务运行而不会导致大幅度的性能下降或功能丧失，并能够迅速恢复政策业务，最大程度减少损失，从而持续保持业务正常运转。

在数字化转型提速和监管力度升级的背景下，工业信息安全建设热火朝天。但由于在工业环境中，产品种类型号纷杂繁多，应用场景复杂多样，系统长时间连续不间断运行，工业企业在实践的路上仍然存在很多不确定性和挑战。

为了更好地理解当下工业信息安全建设的现状，施耐德电气商业价值研究院联合亚信安全以**“工业信息安全发展”**为主题，通过线上线下结合的方式进行了深入的调查研究。线上，采用问卷的形式完成了近两百家工业代表企业用户调研；而线下，则与 10 余家典型行业的企业高管或安全工作负责人展开了面对面的交流。本次调研分析，结合了施耐德电气自身在工业领域深耕多年的实践经验，旨在帮助工业企业在充分了解目前工业信息安全发展现状的基础上吸收更多经验，从而提高信息安全的建设效率，切实地为企业数字化转型提供坚实有力的保障。

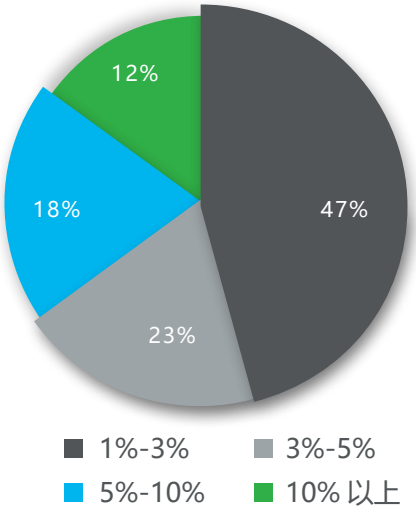
2.1 工业信息安全建设的四大挑战

如核心发现所述，工业企业的信息安全建设存在四大挑战：约 54% 的受访企业表示，资金、人力投入不足成为建设的首要突出问题；约 33% 的受访者认为工业领域暴露出的信息基础设施陈旧不容忽视；与此同时，近年来工业攻击针对性升级和 IT/OT 融合协同的复杂性，更是进一步加大了工业信息安全建设的难度。

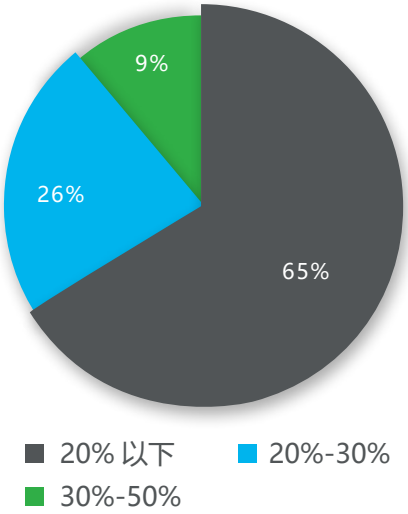
2.1.1 资金人力投入不足

2021 年，工信部发布《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》。该计划在国家政策层面明确提出，重点行业网络安全投入占信息化投入比例达到 10%。但从我们的调研结果来看，近半数受访企业表示 2020 年度针对信息安全投入占信息化总投入的比例低于 3%。其中，有 65% 的受访企业在 OT 领域信息安全投入占整体信息安全投入比例低于 20%。截止目前，所有调研企业在 OT 领域的信息安全投入均少于 IT 领域。

信息安全投入占信息化总投入比例分布



OT 领域信息安全投入占整体信息安全投入比例分布



（图 7）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

信息安全专业人员是安全能力构建的核心要素，且工业信息安全领域人力投入严重不足的问题尤其突出。从调研情况来看，超过 10% 的受访企业暂时没有信息安全专职人员，而 OT 领域没有信息安全专职人员的比例则接近 70%。同时我们也关注到，利用服务外包已经成为缓解自身人才瓶颈而造成的投入不足问题的普遍选择，仅 35% 受访企业没有常驻外包安全服务人员。

信息安全专业人员

超 10%

受访企业表示没有专职信息安全人员

近 70%

受访企业表示没有专职 OT 领域的信息安全人员

仅 35%

受访企业表示没有常驻外包安全服务人员

（图 8）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

“现在最大的挑战，是管理层重视度和投入的问题，如何展现信息安全工作价值，让管理层认识到信息安全的重要性，获得管理层的支持，从而得到相应的资源以开展信息安全工作成为最大的难题。”

—— 云南驰宏锌锗股份有限公司 总部自动化主管 彭俊超

2.1.2 基础设施陈旧

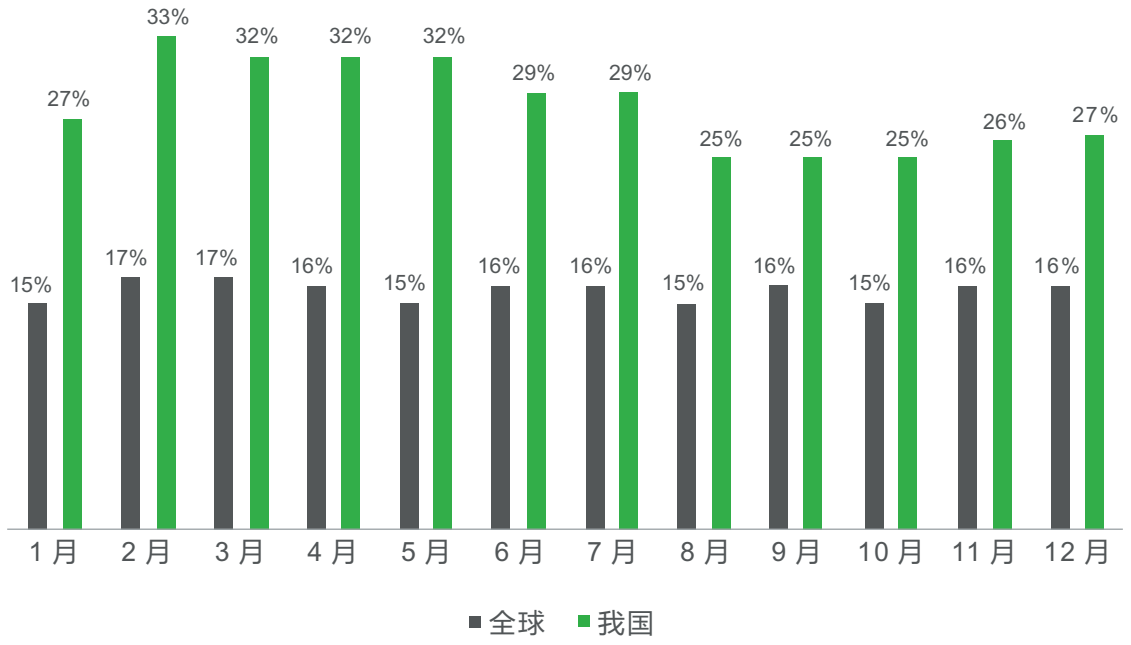
工业领域的生产运营系统生命周期通常较长，在本次调研中发现，在役的多数生产运营系统使用的是 10 多年前甚至是更久的产品或技术，并且在安装时很少会考虑信息安全风险及防护，这样的基础条件给信息安全防护建设带来很大挑战。

对这些运营 10 年以上的存量系统进行信息安全防护，需要充分思考如下方面：第一，考虑对现有系统和在线生产业务可能造成的影响；第二，应对系统组件（控制产品、操作系统、应用程序等）甚至是信息安全防护产品本身长久以来积累以及不断被新发现的漏洞导致的风险，以及防御网络攻击技术发展产生层出不穷的攻击技术和手段；第三，适应工业应用兼容性差、性能和操作限制多的环境特征，匹配工控系统的长生命周期。

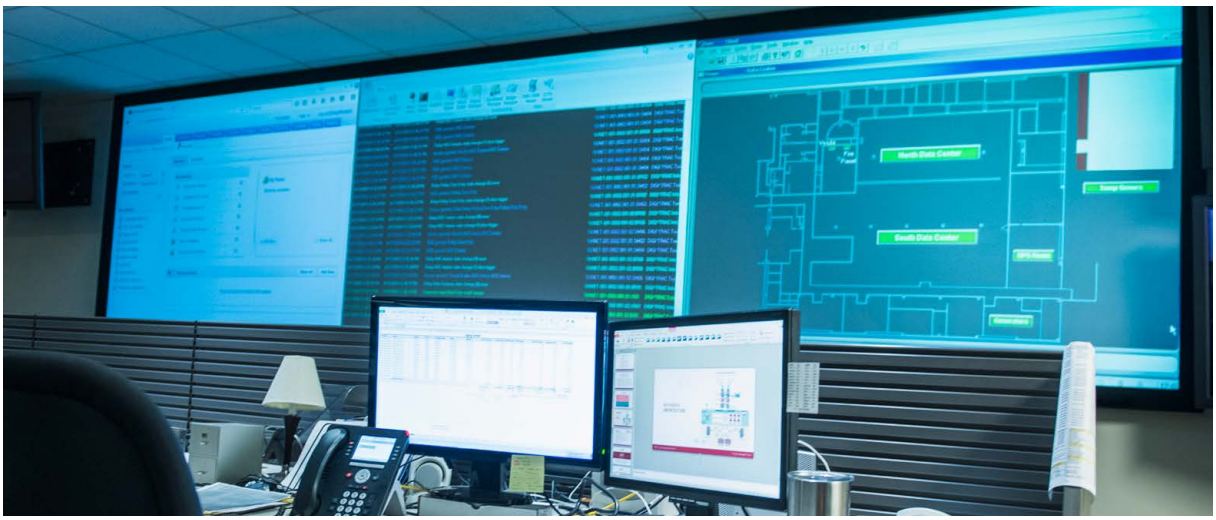
2.1.3 攻击针对性升级

基于国家工业信息安全发展研究中心发布的《2021 年工业信息安全态势报告》，近年来公布的工业信息安全，尤其是工业控制系统漏洞呈持续上升趋势。由于工业环境相较于 IT 环境，其系统安全程序、安全措施不够完善，一旦遭到攻击产生影响较大，更容易被勒索。越来越多的黑客开始将他们的目标，从熟悉的 IT、金融等领域扩展到工业领域，尤其是能源、制造等行业。近年来，工业环境攻击的针对性也显著增强，每次攻击的受害者数量尽管只有几十个甚至个位数，但都集中在高价值对象，由此虽然受攻击主机数量在下降，但产生重大影响的大规模安全事件却显著增加，其中高赎金的勒索软件攻击对企业数据安全和持续运营带来的威胁尤为严重。

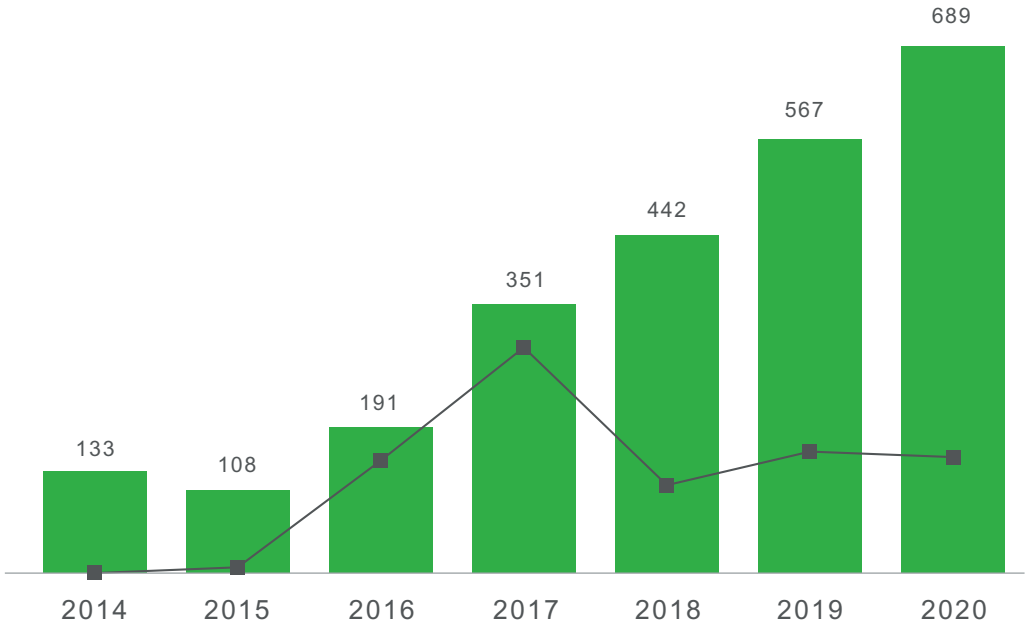
2020年全球及我国受攻击的工业主机比例



（图 9）数据来源：卡巴斯基 ICS-CERT，国家工业信息安全发展研究中心



工业控制系统漏洞新增数量



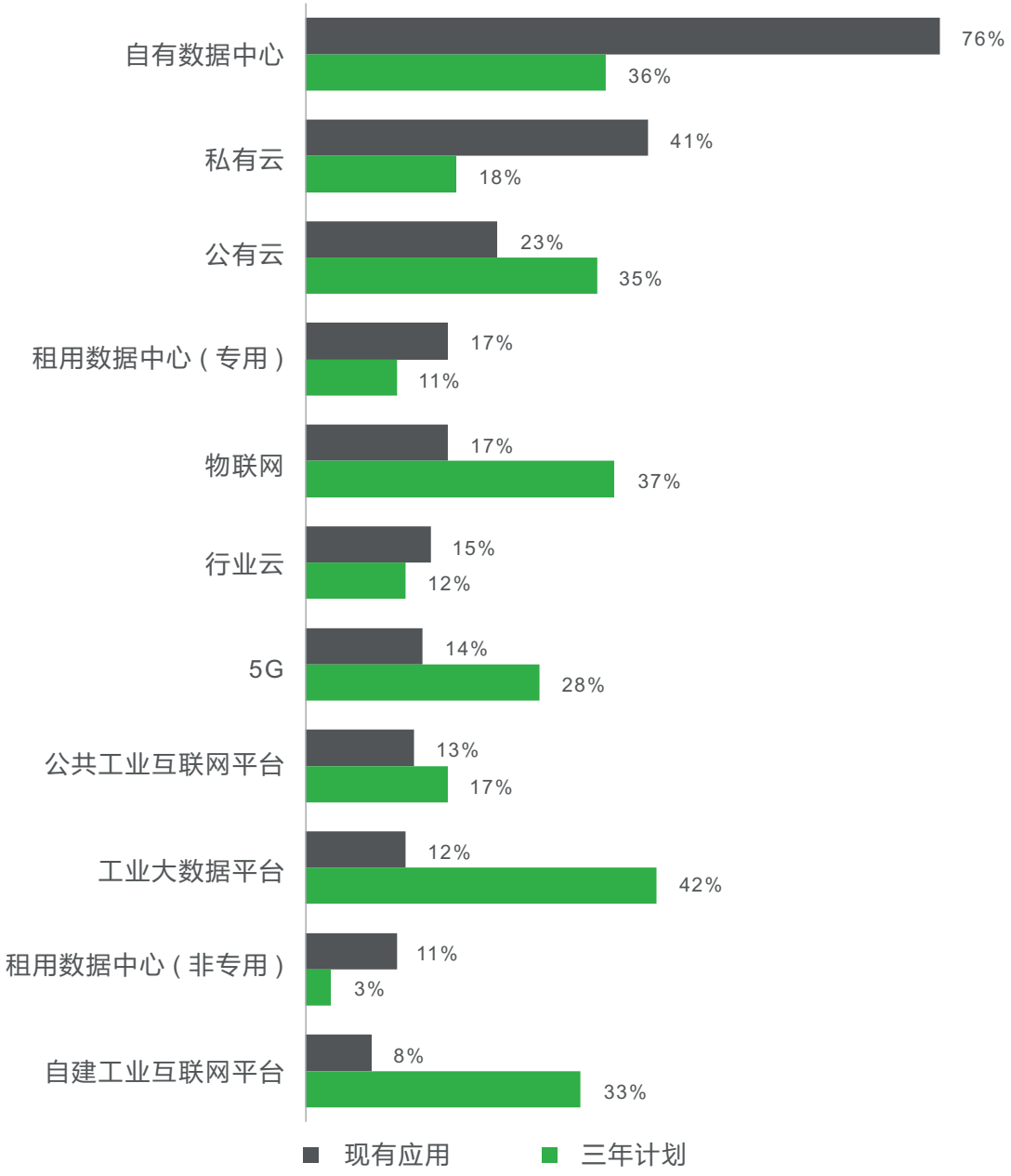
（图 10）数据来源：国家信息安全漏洞共享平台（CNVD）

2.1.4 IT/OT融合协同复杂

IT/OT 融合已经成为当下数字化转型过程中关键的变革趋势，在 IT 领域快速发展、全面应用的基础上，以工业头部企业为先导，越来越多的企业正在 OT 领域持续探索并使用云计算、大数据分析等新一代数字化技术。

本次调研结果显示，在现有技术应用中，其中约 41% 的受访企业表明已经使用私有云，有 23% 和 15% 的企业正在使用公有云和行业云。超过半数的受访企业已经或者计划未来 3 年内进行工业大数据平台建设，对于 5G 技术的使用比率将超过 40%。融合 IT 和 OT 资源需要 IT 和 OT 共同规划和落地，从而实现整体信息化和安全解决方案的全面部署。

技术应用情况



（图 11）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

“IOT 融合在我们现在新的基地和生产线规划时都会重点考虑，这个是未来很明确的趋势，但旧基地基础架构重视度不足的历史遗留仍需要更多的时间和资源去解决。”

—— 圣戈班管道系统有限公司 陈希

2.2 工业信息安全实践的两大现状

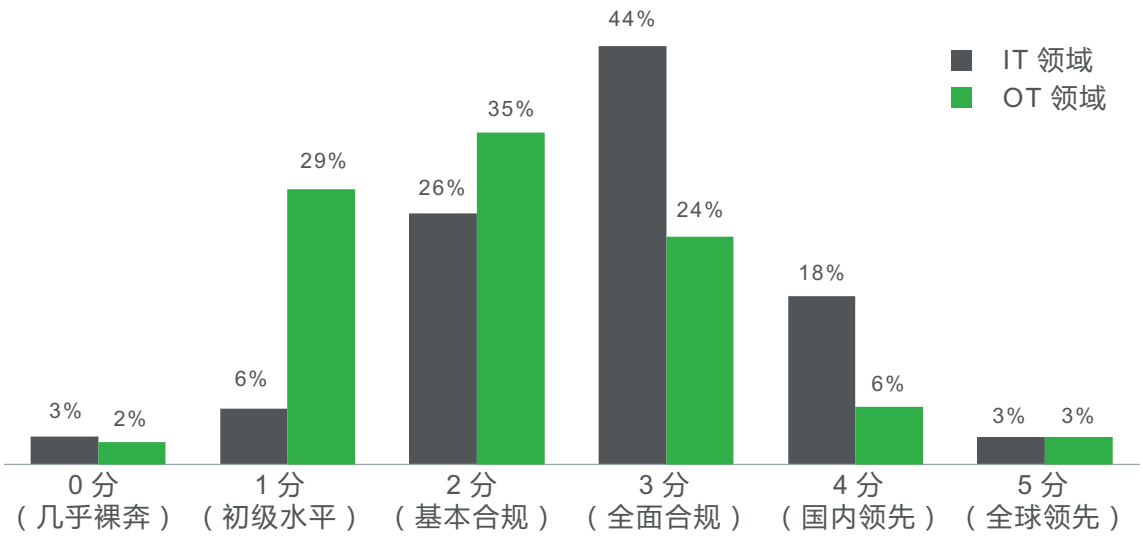
2.2.1 综合管理亟待完备

虽然在多方力量推动下，工业企业信息安全建设逐步受到重视并进入能力提升的快车道，但 OT 领域信息安全成熟度整体仍处在较低水平，尤其是“轻管理、轻运营”的现象较为严重，人员整体安全意识薄弱，距离形成基本完备持续改进的成熟体系尚有一定时日。

2.2.1.1 OT 领域信息安全成熟度较低

从调研结果来看，OT 领域信息安全成熟度水平平均在 2 分 （基本合规），而 IT 领域信息安全成熟度水平整体接近 3 分（全面合规），尤其值得关注的是来自于大、中型工业企业的 IT 领域得分普遍高于 OT 领域，兼顾负责 IT 和 OT 安全职能团队的受访者反馈目前两者的差距比较显著。与此同时，我们横向对比了施耐德电气与亚信安全近年来在不同行业客户 IT/OT 环境的咨询项目中，其现状评估的结论也与本次调研分析结论相呼应。

IT/OT 领域信息安全成熟度自评估得分分布



（图 12）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

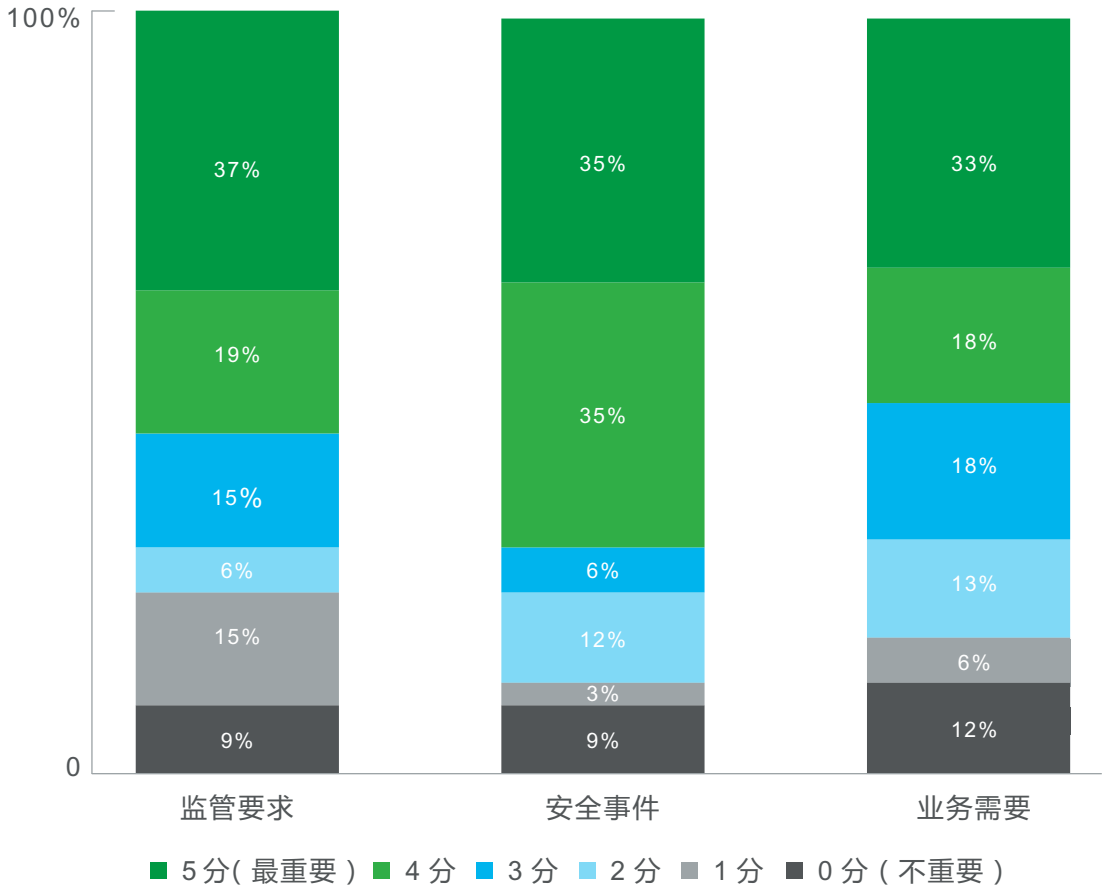
“我们的 IT 信息安全已经开展 10 多年，OT 信息安全刚刚起步，两者成熟度存在差距是必然的，而人才、知识和能力的匮乏是 OT 信息安全的短板。从近期工业信息安全的需求和获得的成果来看，通过培养既懂安全也懂 OT 的人才，快速提升 OT 信息安全水平是完全可行的。”

—— 某国内上市能源公司 数字安全解决方案专家 程苗

2.2.1.2 信息安全投入转向混合驱动

我们认为，当前信息安全工作驱动力主要来源于监管合规压力、安全事件和自身业务需要三个维度。调研结果显示，OT 领域信息安全投入呈现出由事件驱动向混合驱动的变化，但事件驱动仍是 OT 领域信息安全投入最重要的驱动，超过 70% 的受访者对其重要性给出 4 分及以上，同时，选择这三个维度作为最重要的驱动力（5 分）的组织比例几乎相当，这意味着混合驱动的趋势已经相对明显。

信息安全工作驱动力分布

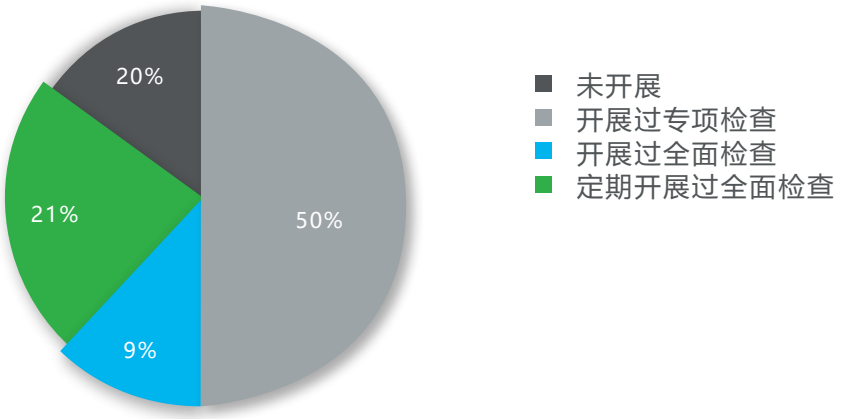


（图 13）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

2.1.1.3 安全管理和运营重视度不足

信息安全建设历来有“三分技术、七分管理”的说法，强调基于风险管理理念的持续改进，但目前 OT 领域整体呈现重视技术能力建设而忽视管理运营改进的情况。从调研结果看，仅有 20% 左右的受访企业能够在 OT 领域定期开展较全面的内部信息安全检查，半数的受访企业仅仅是基于事件响应需要才开展小规模专项检查，甚至有约 20% 的受访企业从未开展过 OT 领域内部信息安全检查，而没有全面开展内部检查的企业几乎都不具备面向 OT 领域完善的信息安全管理制度和运营流程。

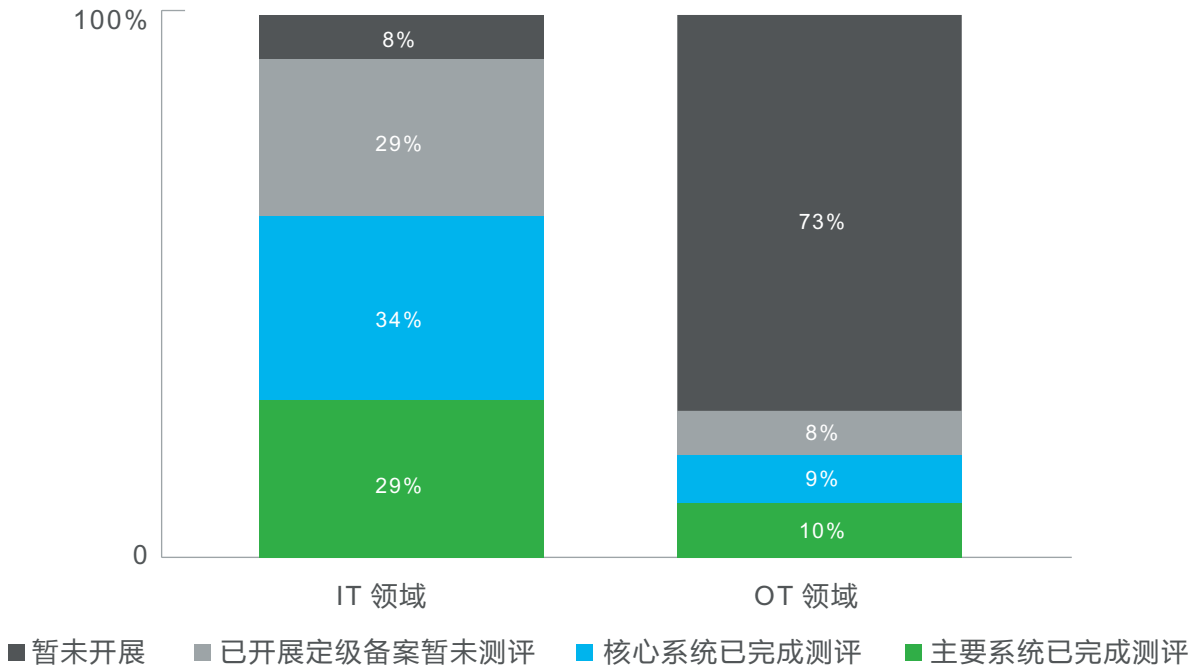
OT 领域内部安全检查工作执行情况分布



（图 14）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

在等保工作推进上，虽然工业控制系统已经纳入等保 2.0 测评范围，但相比较于受访企业 IT 领域主要系统超过 90% 的备案率和超过 60% 的测评完成率来说（主要针对企业主要系统和核心系统测评情况进行调研），工控系统测评率不足 20%，定级备案率也不足 30%，的确存在着显著的差距。

等级保护工作执行情况分布

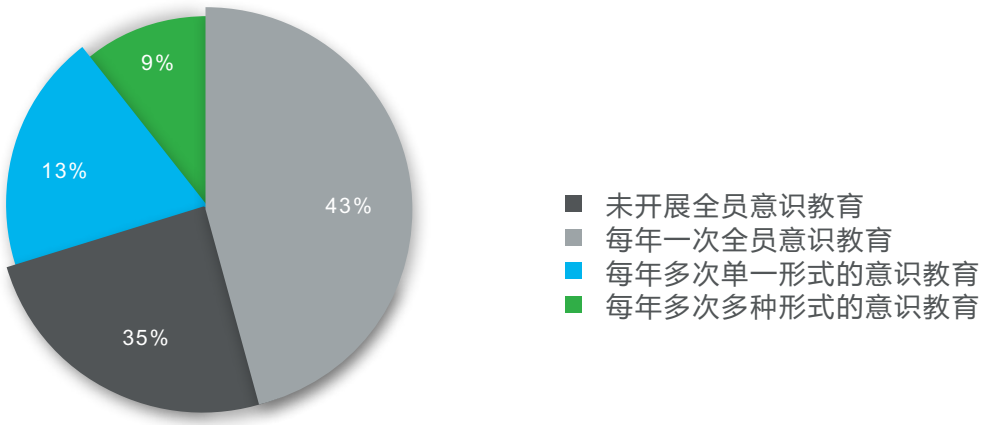


（图 15）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

2.2.1.4 安全教育培训意识薄弱不足

OT 领域信息安全意识教育不足的情况比较严重，这也从侧面反映了企业管理层对工业信息安全领域的重视程度仍显不足。从调研结果看，约 35% 的受访企业没有在 OT 领域开展过全员信息安全意识教育；近半数的受访企业每年固定开展一次意识教育而且多数偏向形式主义，真正能够每年多次多种形式的开展意识教育的受访企业不足 10%。

OT 领域信息安全意识教育开展情况



（图 16）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

这种培训教育不足直接会导致整体安全意识的薄弱，集中体现在工业环境下信息安全的风险认识不足，如使用弱口令、滥用移动设备等错误的行为习惯。

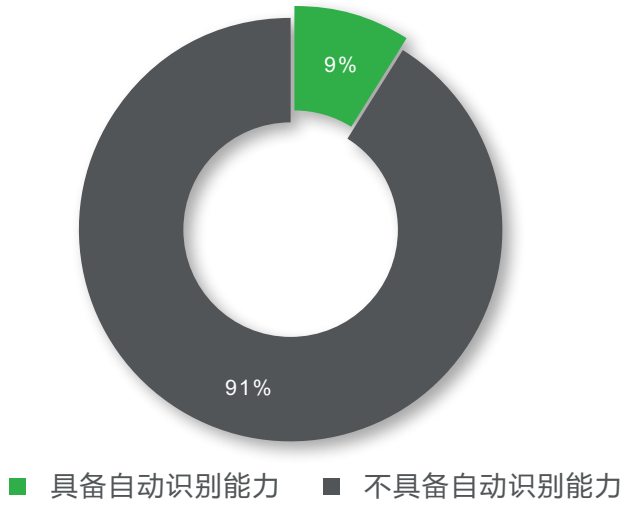
2.2.2 关键技术逐步落地

结合工业环境实际情况及业务合规等需求，配合事件响应过程中的安全强化，相关企业已开始在威胁防护、监测感知和处置恢复等维度推动工业网络、主机设备、控制应用、数据安全等关键控制措施的落地。在网络安全方面，因为一些核心能力和安全策略有效性管控上的不足，整体效果其实受到较大的限制。控制主机和终端安全方面，广泛认同的最佳实践取得一定效果。控制软硬件安全和数据安全方面，受到越来越多的重视，头部企业已开始进入综合态势感知能力建设的高峰期。

2.2.2.1 OT 环境资产和脆弱性识别

参考 IT 环境的经验，资产和脆弱性识别实际是形成针对性安全管控落地和高效安全运营的基础。但从调研情况来看，具备 OT 环境资产和脆弱性识别能力的受访企业占比不足 10%，目前针对管理有诉求的中大规模企业来说，很多还是采用手工方式识别和记录，缺乏即时更新。

OT 环境资产和资产脆弱性自动识别能力



（图 17）施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

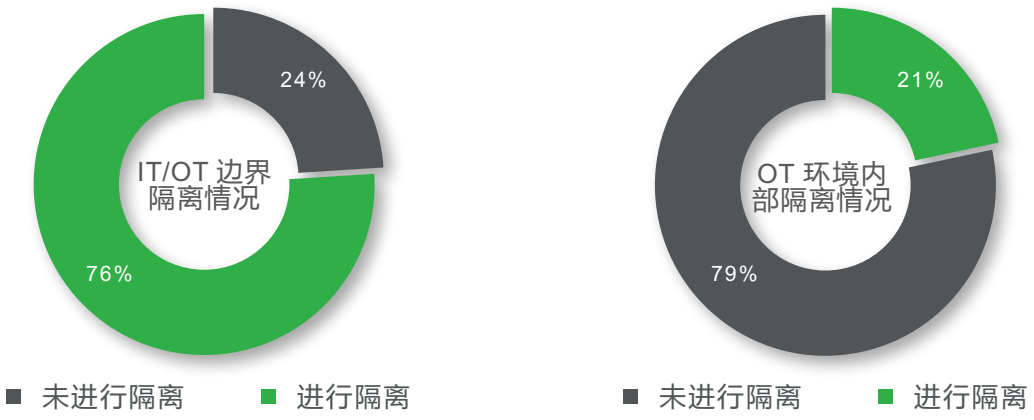
“OT 环境的资产和脆弱性识别难度远大于 IT 环境，一方面环境中资产多样化，可能存在数千种跨厂商的应用组件和控制器。同时，由于生产环境限制我们也很难使用主动探测技术，更多需要依靠基于流量的被动分析来进行识别，因此进一步加大了工作难度。”

—— 中沙（天津）石化有限公司 仪表设备专家 杜佐政

2.2.2.2 网络隔离

大部分受访者表示，网络隔离是开展 OT 信息安全建设的第一步，但策略有效性问题严重制约了此项关键控制真正发挥作用。虽然从调研结果来看，超过 75% 的受访者单位已经通过防火墙、网闸等设备实现了 IT 与 OT 边界的隔离。但结合线下访谈，以及施耐德电气与亚信安全近年来在不同行业客户 IT/OT 环境的咨询项目的现场评估结论，大部分安全设备缺乏有效地配置。针对 OT 内部不同层级或不同系统间，仅有 20% 左右的受访企业进行了进一步的逻辑隔离，此类型的隔离设备策略配置往往较为宽松。

IT/OT 边界隔离情况

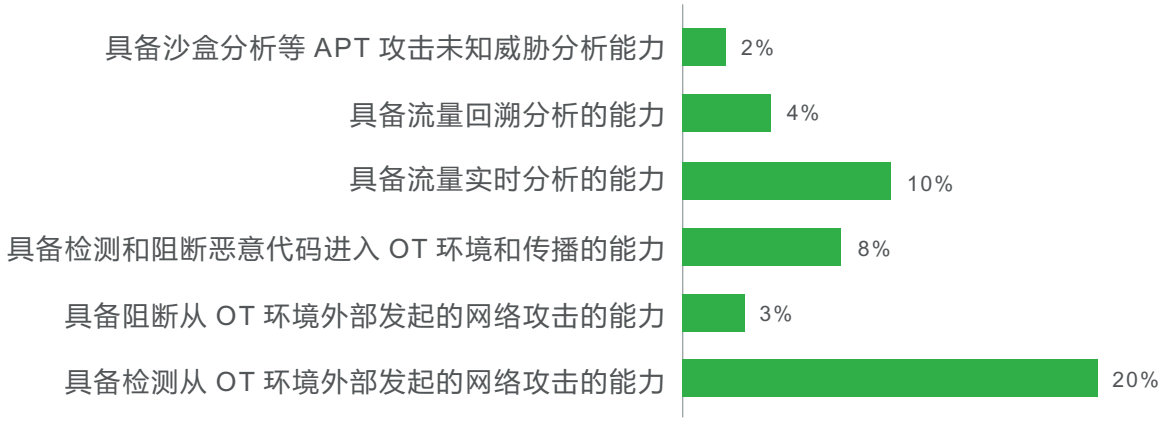


（图 18）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

2.2.2.3 网络攻击检测阻断

检测能力是进行有效响应网络攻击的基础，但 OT 环境下检测能力建设刚刚起步。从调研结果来看，20% 左右的受访企业已经在 OT 环境部署了基于流量分析的攻击检测设备；但考虑到 OT 环境误判情况下对业务正常运作的潜在影响，在防火墙或网闸的网络隔离策略之外，自动化的攻击阻断手段目前极少使用，即使部署相关设备也是处于学习模式而非阻断模式（受访者阻断模式使用率低于 3%）；基于网络侧对恶意代码识别或阻断的部署比例不足 8%，并结合 OT 环境主机终端恶意代码防护部署比例不足 40% 的情况来看，这实际上也是工业环境实质性安全事件中恶意代码类型比例较高的重要原因。大约 10% 的受访企业具备全流量实时审计分析的能力，但具备流量回溯深度分析的受访者企业则仅有约 4%，具备沙盒分析能力的占比更是不足 2%。企业对网络攻击的发现主要依靠规则匹配，对零日攻击的发现能力严重不足。

OT 网络攻击阻断检测能力情况

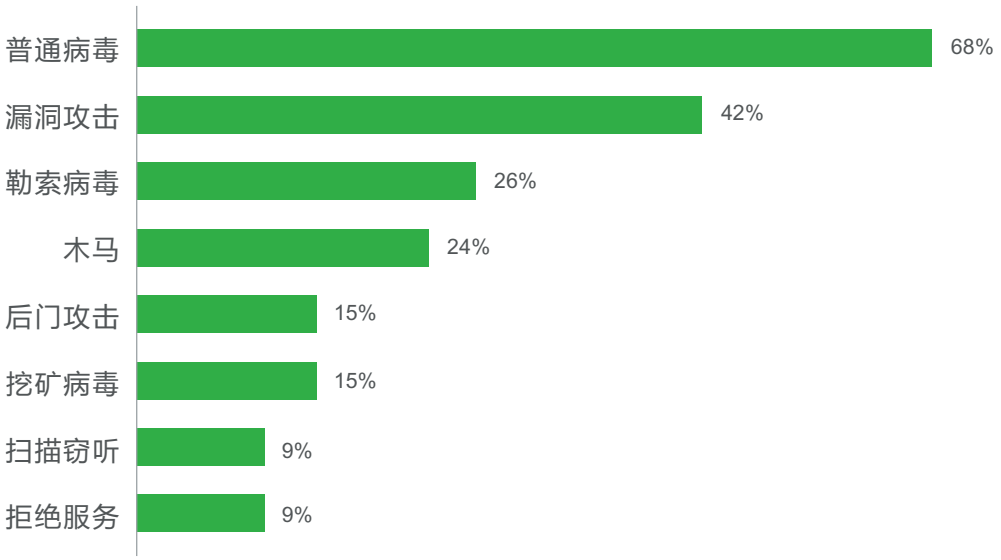


（图 19）施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

虽然有接近半数的受访者表示 OT 领域在过去 3 年未发生过信息安全事件，但进一步分析可看到，在网络和终端部署有检测防御手段的受访者中，超过半数检测到过异常流量或行为，这一比例也接近于施耐德电气与亚信安全工业信息安全解决方案在不同行业客户 OT 环境验证测试和实际使用情况了解的真实数据。由此不难看出，安全事件普遍存在于现实环境，但缺乏有效检测手段部署的企业却处于一种浑然不觉的状态，并没有及时和充分地发现问题。

依据过去 3 年发生过信息安全事件的受访企业反馈，最为常见的普通病毒占比超过 50%，而漏洞攻击的占比也超过40%，但从深度访谈中我们获悉，如何解决勒索病毒是目前安全管理者们在 OT 领域最为棘手的信息安全问题。

OT 领域主要类型信息安全事件发生情况



（图 20）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

“从 OT 安全的特征来讲，对可用性的关注是显著高于 IT 领域的，而勒索病毒恰恰直接影响系统应用的正常使用，若由此造成大面积停工停产的影响是我们所不能承担的。”

—— **中联水泥集团 郭晓斌**

2.2.2.4 主机终端防护

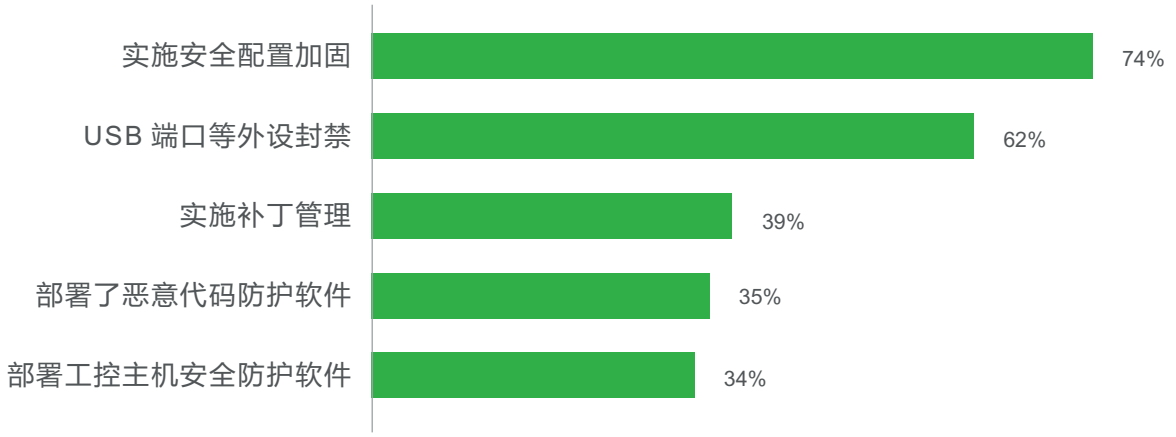
得益于 IT 领域技术积累和安全工作经验较高的可复用性，基于基线管理、外设管理、补丁管理和进程管控的应用，OT 环境主机和控制器终端安全防护能力建设整体成熟度水平相对较高，并且已经初步显现出效果。

从调研结果来看，超过 70% 的主机已经定义安全控制基线进行了标准化配置，尤其是大家普遍认为移动介质使用造成的恶意代码传输是 OT 环境重要的风险因素，基本都通过物理手段或基线配置实施了移动介质访问封禁的配置。

补丁管理工作也受到了较多企业的关注，接近 40% 的受访企业建立和落实了相关流程。相较于 IT 环境，控制系统主机的补丁管理需要更稳定，以此避免影响企业的生产业务。通过对先行使用者的反馈，新兴的虚拟化补丁技术效果甚佳。

超过 30% 的受访企业已经部署安全防护软件强化 OT 环境工控主机和终端的系统安全性，但因为工业现场基础设施环境陈旧的现实情况，软件对老旧操作系统版本的支持就变得尤为重要。基于白名单的应用进程管控，对系统资源占用少，能较好的适配现场工作站配置较低，在应用场景比较单一的客户现场受到广泛认同。我们也关注到，在少量应用场景比较复杂的客户现场，基于白名单的进程管控也会特例性的出现配置不当而影响生产的情况。

OT 环境主机 / 控制器终端安全控制实施情况

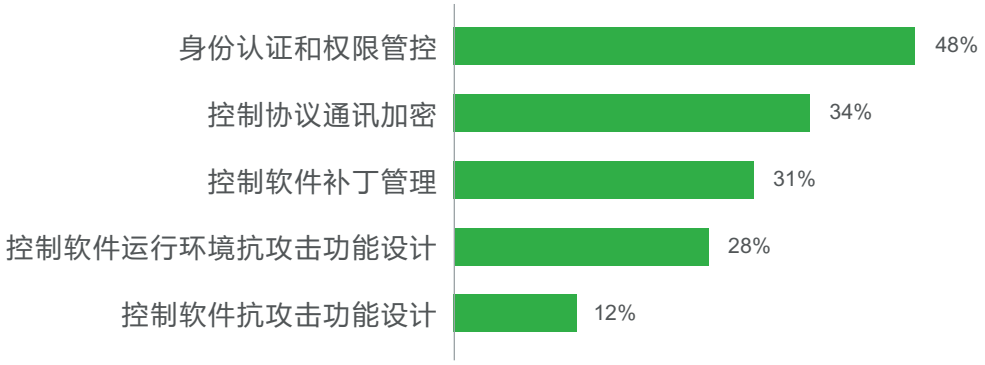


（图 21）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

2.2.2.5 控制软件和智能设备安全

因为工业控制软件和智能设备的特殊性，再加之企业在采购选型时对于自动化解决方案信息安全能力的忽视（调研中仅不足 40% 的受访者会将安全要素纳入综合评价范围），安全功能过往一直呈现受重视程度不足且升级缓慢的特征，尤其是缺乏抗攻击功能的设计和实现。从调研结果来看，即使是最为基础的身份和权限管理功能，也只有不足 50% 的工业控制软件能够较完整的涵盖其功能，受访者使用的智能设备经过厂商内核加固、协议优化等固件安全增强的智能设备的比率不足 10%。结合施耐德电气与亚信安全近年来在不同行业客户 IT/OT 环境的咨询项目中发现，由于生产现场人员安全意识薄弱，弱口令、初始口令、缺乏有效权限管理等情况比较严重。综述，控制软件、智能设备安全能力的提升需要企业提高对供应商的要求，推动安全开发生命周期落地，持续提升产品原生安全能力，并在应用过程中有效运用安全控制措施。

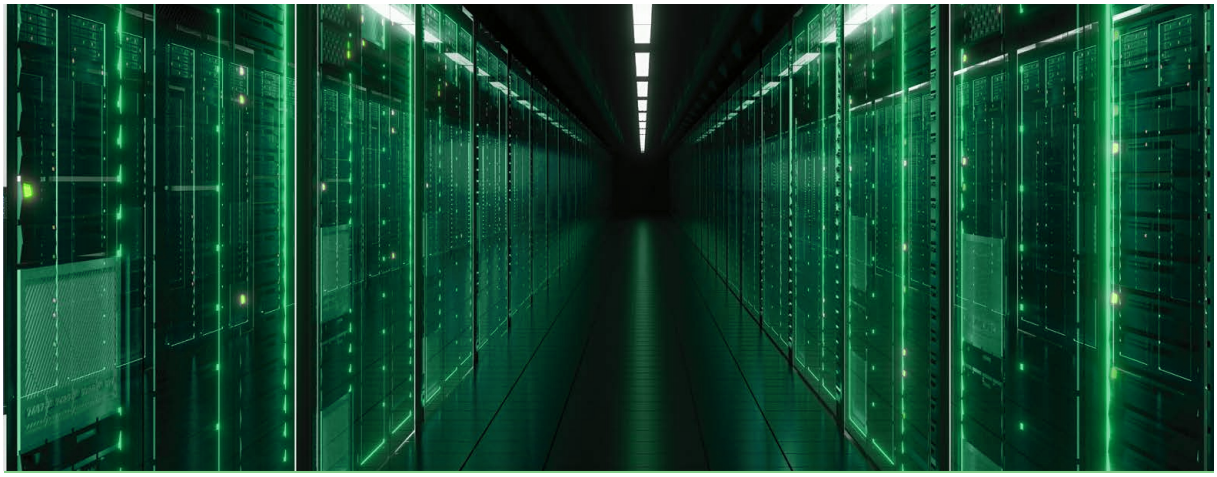
工业控制软件安全控制实施情况



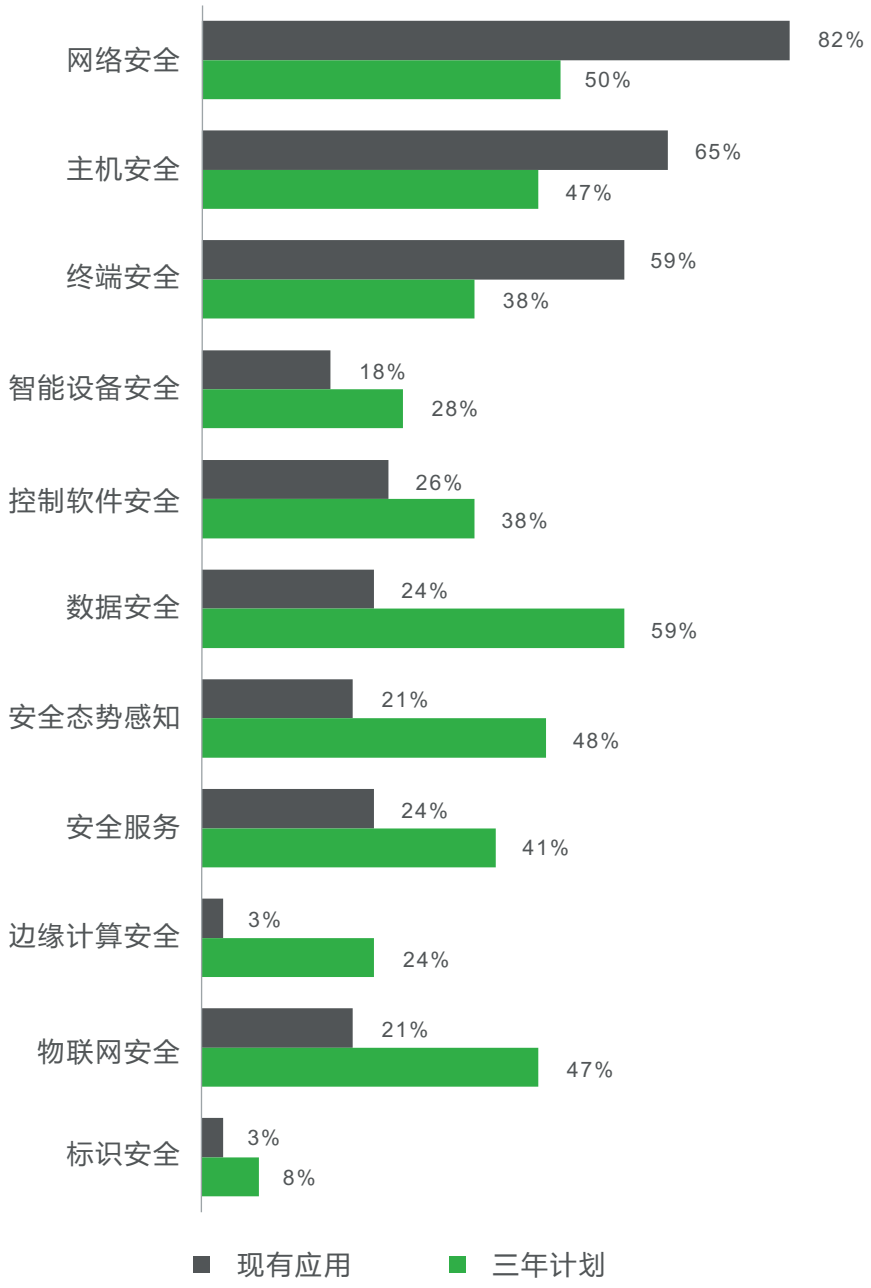
（图 22）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

2.2.2.6 数据安全

数据安全的重要性已经得到充分认识，接近 60% 的受访企业表示未来三年计划将数据安全作为 OT 领域信息安全工作建设的重点方向。



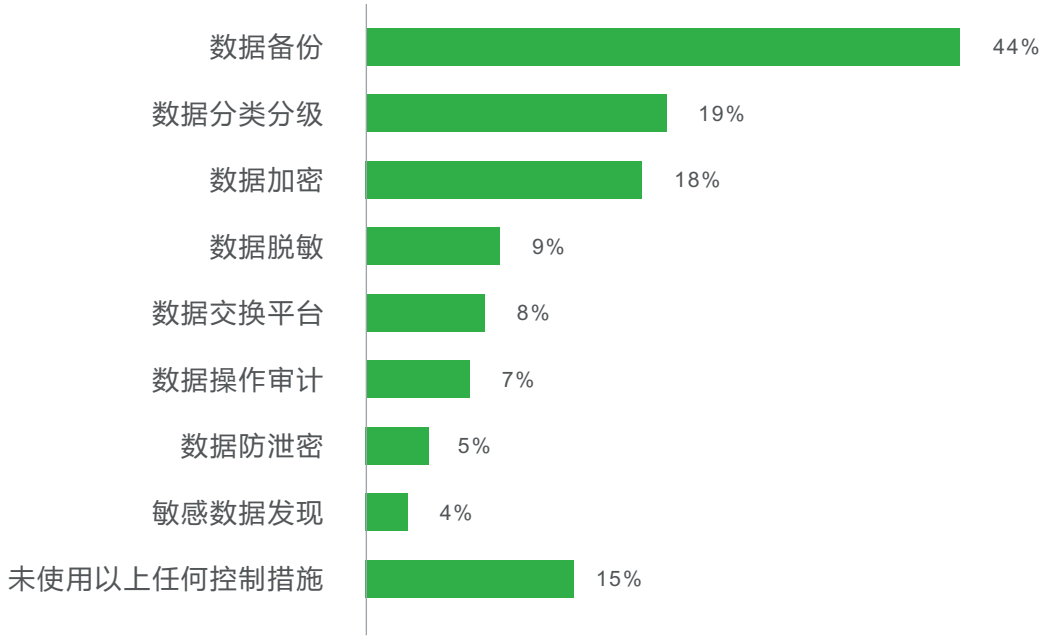
OT 领域投入重点分布



（图 23）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

但与此同时我们也看到，除了预防性的数据备份有 45% 左右的受访者使用外（IT 领域接近 100% 的覆盖），常见的数据安全防护手段仅数据加密在受访单位 OT 环境深度使用的比例达到 20% 左右，且集中于 MES 等信息系统，其他诸如数据脱敏、操作审计、数据防泄漏和安全数据交换手段的深度使用率均低于 10%，更有超过 15% 的受访者表示尚未使用任何数据安全管控措施。结合现场深入访谈，不足 20% 的受访企业已经开展数据分类分级工作，且部署使用敏感数据发现梳理工具的不足 5%，这意味着实际工作开展的效果并不理想。

数据安全控制实施情况



（图 24）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

“现在我们做的最弱同时又最迫切希望提升的能力就是数据安全能力，在 OT 环境尤其如此，数字化转型的核心驱动力是数据挖掘价值，做不好数据安全未来整个转型工作都要受到极大的掣肘，产生根本性的影响。”

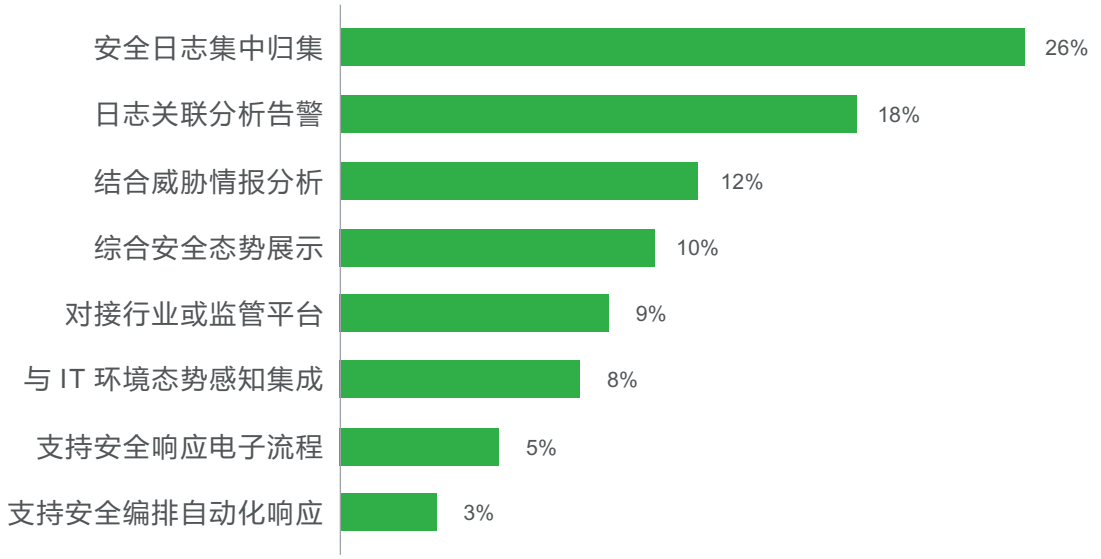
—— 得力集团 生产 IT 部经理 蒋理明

2.2.2.7 态势感知

从调研结果分析来看，未来三年建设规划中，接近半数的受访企业将态势感知能力建设作为 OT 领域信息安全工作的重点方向，仅次于数据安全。

从现状来看，超过 25% 的受访企业已经实现了 OT 环境主要安全日志集中归集，超过 15% 更是进一步实现了日志关联分析告警，同时超过 10% 的企业还引入了威胁情报进行参考。但我们也注意到，相比较于 IT 环境态势感知近年来在综合态势多维展示、安全运营流程支撑和安全编排自动化响应等维度的快速发展，OT 环境态势感知平台在响应支撑上的能力还明显不足。虽然国家工业信息安全发展研究中心联合 31 家支撑机构已经初步建成国家工业信息安全监测预警网络，但企业自身平台对接国家、省级或行业工业态势感知平台的比例仍然较低，调研结果仅在 10% 左右。

工业态势感知平台部署情况



（图 25）数据来源：施耐德电气商业价值研究院“工业信息安全发展”用户研究，2021

“对日趋增多的企业网络安全需求，工业信息安全也应该使用安全态势监测与全网感知整合 OT 和 IT 安全事件。通过对生产企业多数据源接入、智能分析处置，为 OT 安全创建基线，实现可视化检测未知威胁，监测异常活动，与安全生产体系保持一致，为企业安全生产做好工业网络安全保障。“

—— 亚信安全 工业互联网安全事业部总经理 楚鹏

3 躬行实践：以专业能力构筑工业信息安全保障

3.1 施耐德电气最佳工厂实践

施耐德电气连续两年跻身 Gartner 世界供应链榜单第四名，同时作为全球拥有七家灯塔工厂的企业。其中无锡工厂凭借其数字化转型的卓越成就于 2021 年获评为世界经济论坛端到端“灯塔工厂”的称号。在中国施耐德电气已经拥有了 23 家工厂和 7 家物流中心，其中有 15 家已被工信部认定为绿色工厂，同时被评为绿色供应链示范企业。

作为工业先锋之一，施耐德电气充分借鉴国际和业界工业信息安全最佳实践，结合国内监管要求，将施耐德电气制造执行系统及生产控制系统领域的信息安全建设服务充分本地化，形成了具有中国特色的工业信息安全实践范例。

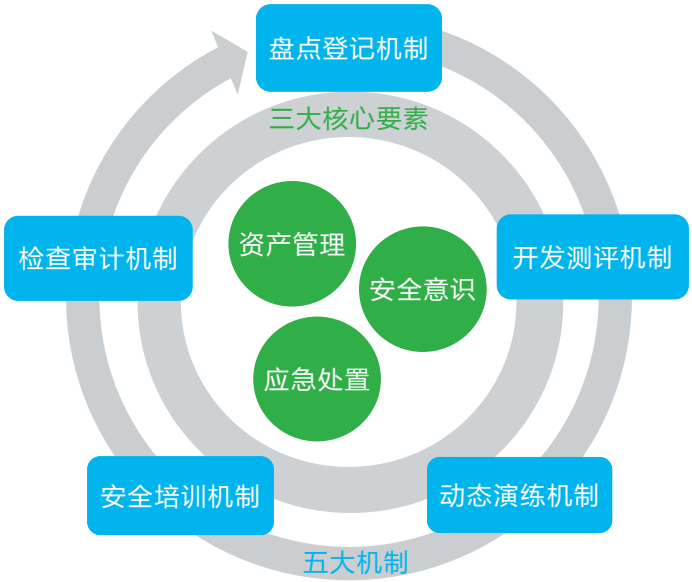
3.1.1 人才——搭建本地组织

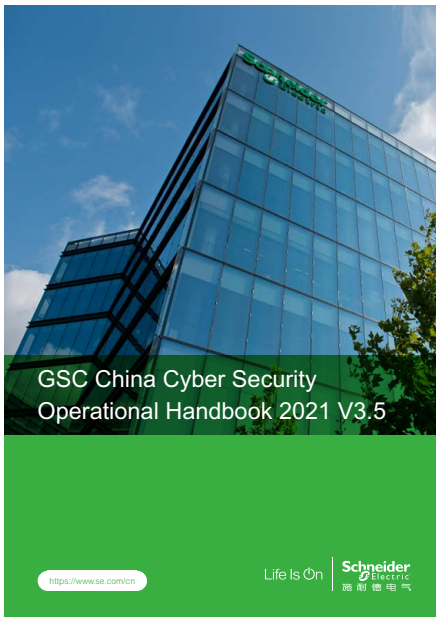
施耐德电气搭建了地区和工厂的本地安全管理的组织架构，配合与全球架构的定期安全会议机制，实现纵向高效的协同联控。在工厂层面，设立了 “安全负责人”认证机制，培训并选拔熟悉工厂业务并具备信息安全专业知识的人员牵头负责各个工厂的信息安全工作，覆盖国内 23 个工厂和 7 个物流中心。工厂安全负责人实行双线汇报机制，除汇报给工厂负责人外，统一汇报给供应链中国网络安全负责人。

3.1.2 管理——建设标准流程

基于施耐德电气的全球标准，并结合国内工厂的特点进行调整，从而构建施耐德电气中国工厂的网络安全分级机制、安全标准和评估体系。同时，依照施耐德电气全球信息安全标准和操作手册，按照国内的安全合规要求进行适当裁剪和完善，已经形成了施耐德电气中国工厂信息安全管理体系，并定期迭代更新。其中，重点落实入网设备动态盘点和登记认领机制、安全开发和准入测评机制、动态安全演练机制、持续安全培训机制、定期安全检查审计机制，以资产管理能力、应急处置能力和安全意识水平为核心要素，持续改进安全管理水平。

施耐德电气中国工厂信息安全管理体系





（图 26）来源：施耐德电气

3.1.3 技术——落实技术控制

施耐德电气中国目前已经实现了国内 IT/OT 网络的统一规划设计和运维管理，通过全面隔离 IT/OT 网络，实现 OT 设备全面覆盖的域控接入，并在高等级的工厂实现了产线级的网络隔离和差异化安全防护。通过构建覆盖 OT 环境全网、关键终端的安全实时监测预警体系和集中安全运维平台，形成全局感知和联动处置能力。

施耐德电气全球安全体系本地化合规实践——工厂 OT 领域

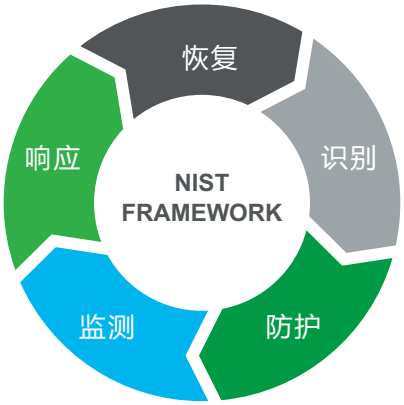
（图 27）来源：施耐德电气

3.2 施耐德电气信息安全服务实践

施耐德电气作为长期在工业自动化及能源管理领域耕耘的专家，具有丰富的 IT 及 OT 信息安全专业知识和工业客户信息安全服务经验。

我们目前采用全球业界内认可的基于业界最佳实践IEC 62443工业控制系统安全系列标准，指导安全制度流程的建立、安全风险评估和安全措施手段的部署，并选取 NIST 安全框架作为全生命周期管理的支撑。

信息安全框架



（图 28）来源：NIST 美国国家标准与技术研究院

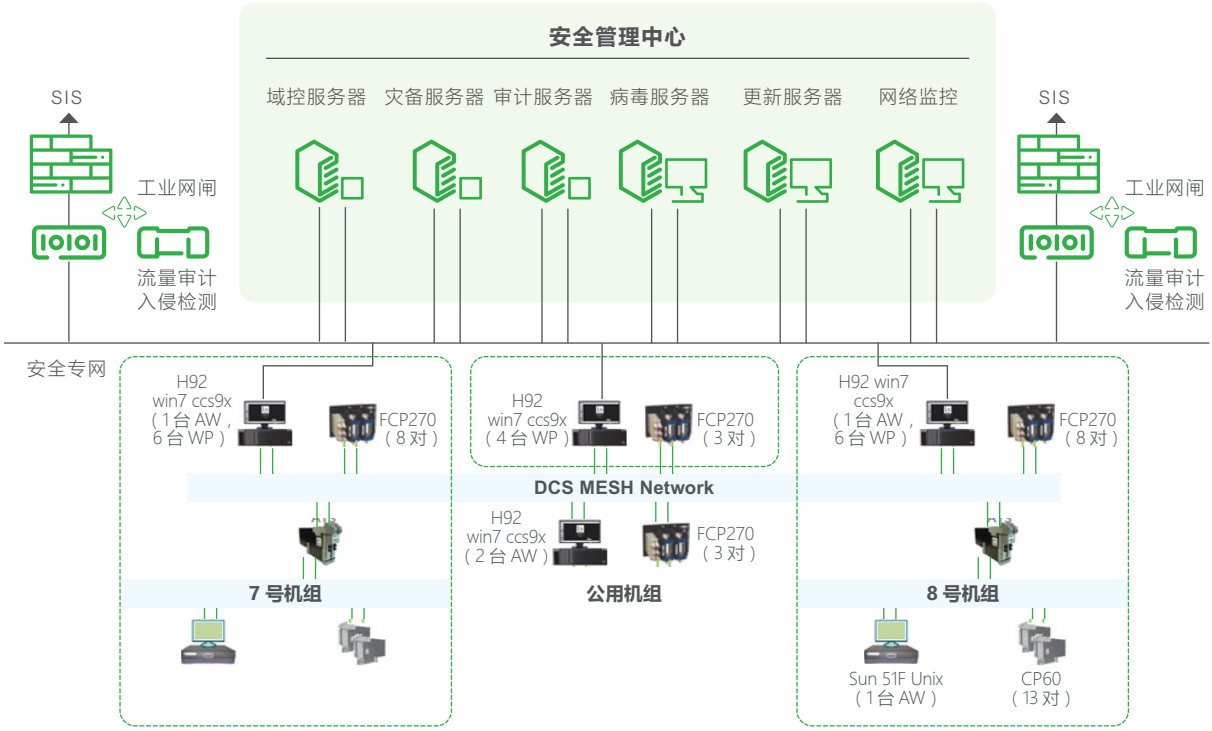
我们在全球以及中国助力工业用户提升其信息安全的防护能力，包括信息安全规划咨询、风险评估、安全防护设计、防护措施实施以及全生命周期的安全运维等服务，行业涵盖石油天然气、化工、电力、食品饮料、市政、楼宇等多个领域，并致力于为全球客户达成业务安全的目标，同时满足当地政府所提出的法律法规要求。

在中国，施耐德电气引入了全球工业信息安全的防护理念、方法论和专业技能，结合多年来积累的行业知识和经验，使用来自于可信赖的信息安全合作伙伴（包括亚信安全在内的国内信息安全厂商领导者）提供的工业信息安全软硬件，打造了符合国内法律法规和国家标准的工业信息安全服务方案综合能力。

> “在应对无处不在并不断演变的信息安全威胁时，没有完美实现零风险的安全方案。如何对公司有形及无形的重要资产进行识别，分析和评估来形成关键威胁风险清单，并以此为目标从人员，管理和技术等不同维度进行有针对性的安全控制已经成为我们每一家企业需要面对的挑战和任务。”
>
> **—— 施耐德电气 首席信息安全官 蒋宇寒**

案例：在某发电企业已经使用长达 15 年之久的 DCS 控制系统中，施耐德电气根据客户现场信息安全的现状和企业对等保 2.0 三级的明确需求，在不改变现有 DCS 控制系统整体网络架构的基础上进行了信息安全的整改设计，并在 2 周停机窗口内实施了信息安全的整改方案：

信息安全整改设计图



（图 29）来源：施耐德电气

- **安全区域边界：**

  电力专用隔离装置隔离网闸：在网络边界通过电力专用隔离装置单向隔离网闸对工控系统进行加强防护

  内部分区隔离：在网络内部针对不同的装置和功能进行内部的安全分区隔离

- **安全网络通信：**

  部署网络监控软件：对工控网络和网络设备的负荷，性能进行实时监控

  部署入侵检测和流量审计系统：在网络边界和核心交换机对通过网络的攻击和非授权访问进行实时检测和审计

- **安全主机环境：**

  工控主机安全加固：安装工业防病毒套件对主机进行“白+黑”防护，同时部署数据防护组件DLP和主机入侵防护组件HIPS

  实时验证系统安全补丁并发布验证后的补丁清单：通过补丁服务器可以为所有工控主机进行及时的补丁修补

  部署灾备系统：对工控主机的系统，应用和数据进行实时数据备份，在受到网络攻击或数据被勒索后可以尽快恢复，对工控系统提供必要的业务连续性保障

- **安全管理中心**

  域控制器统一管理：通过域控制器进行工控系统范围内的统一的身份鉴别、访问控制、行为审计以及安全策略的统一管理

  部署安全专网：对工控系统的所有安全管理相关的数据和通信流量都通过安全管理专网，避免对正常的业务造成不必要的影响

  部署安全日志服务器：对工控网络内的所有工控资产、网络资产和网络安全资产的安全相关的日志进行统一的采集，归档以及关联分析

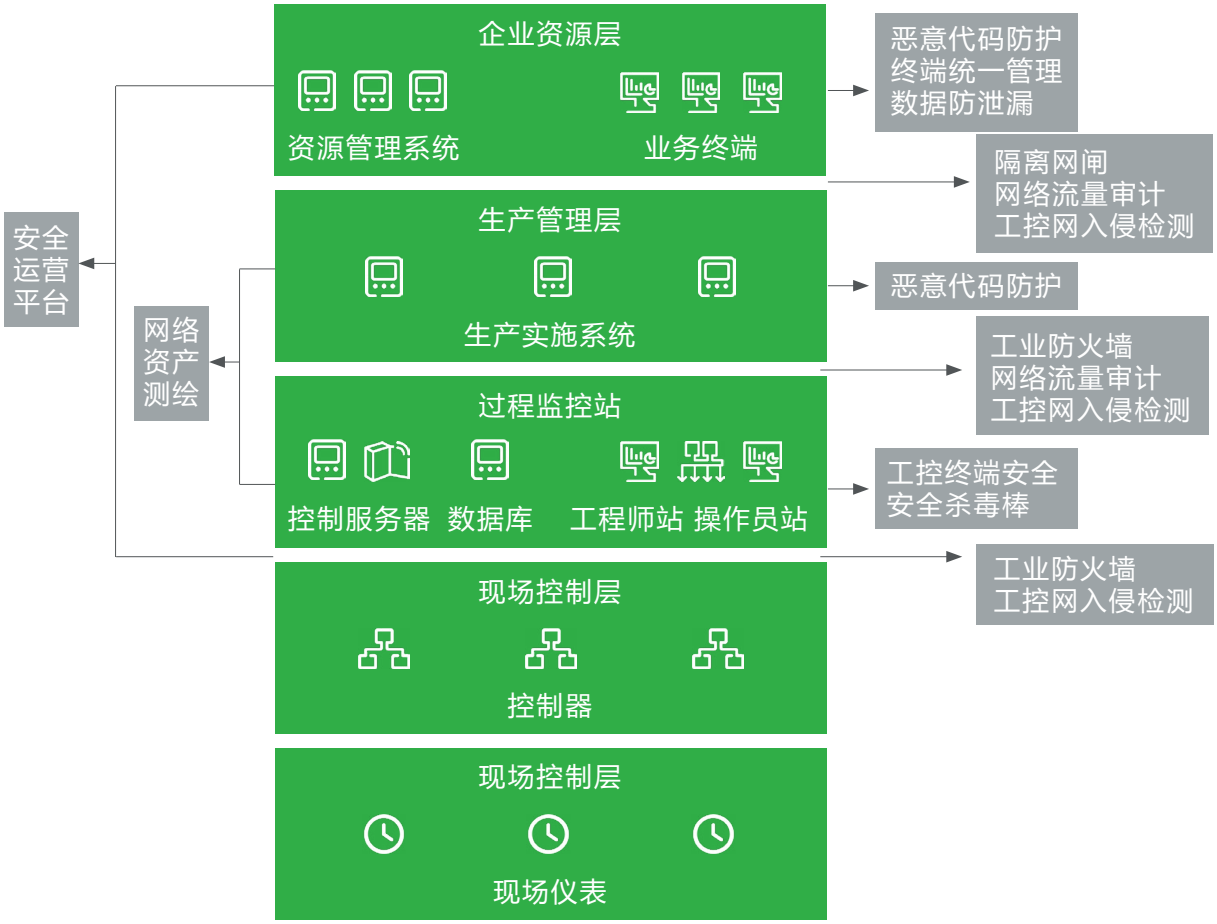
通过工业信息安全整改优化，该企业有效的提高了工控系统的信息安全防护能力和业务保障能力，并顺利以高分通过了等保 2.0 三级的测评，为企业数字化转型提供有力支撑。

3.3 亚信安全工业信息安全服务实践

亚信安全作为国内综合型网络安全厂商的代表企业和 5G 安全研究应用的先行者，能够提供完备的工业信息安全解决方案和服务支撑，支持工业企业客户构建 IOT 环境安全纵深防御和态势感知体系，规范安全日常运维和风险管理并提升安全运营水平，为工业客户数字化转型保驾护航。

案例：某大型工业企业希望设计构建一整套统一的网络安全综合防护平台在其内部多个企业进行规范化应用，实现对组织安全态势的全面监控和典型安全风险的高效处置。亚信安全在对其组织进行全面调研后，结合最佳实践设计了包括防护能力组件和安全运营平台两大模块的整体方案，通过不同的防护能力组件实现基础安全能力落地。并借由安全运营平台实现对整个网络安全的总体风险监测及控制，通过不断的数据采集、事件分析、安全事件形成、防护规则形成、防护规则下发的过程，反复螺旋迭代优化策略，最终实现阻断各种威胁并支持对攻击事件的溯源取证，整套方案在该企业旗下多家工厂部署应用。

网络安全综合防护方案设计



（图 30）来源：亚信安全

企业资源层主要部署管理终端安全能力组件，为企业管理网络中关键岗位的业务终端提供恶意代码防护、终端统一管理和数据防泄露能力。

生产管理层主要面向生产实施系统服务器部署恶意代码防护组件，对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

过程监控层面向控制服务器、数据库和工程师站、操作员站等部署工控终端安全组件，强化对工业生产网络中服务器和操作终端操作系统安全控制能力。同时部署安全杀毒棒，实现无法安装客户端条件下的恶意软件查杀。

在企业资源层、生产管理层、过程监控层和现场控制层边界部署工业防火墙与工控网入侵检测组件，实现有效的网络隔离、访问控制和攻击检测。同时对生产管理层和过程监控层网络中资产进行识别和管理，形成对工业生产网络环境资产状态的全面了解。对企业资源层、生产管理层、过程监控层关键网络节点流量进行审计分析，有效支持事后审计、事件追溯和网络取证。

部署安全运营平台纳管网络安全综合防护平台各安全能力组件和组织环境中原有的关键网络安全设备平台和主机、数据库的日志信息，进行综合分析和可视化展现，支持安全事件研判告警和联动处置，实现企业跨工厂安全运营流程的标准化和企业工厂两级数据对接综合管理。

4 循序渐进：以最优路径支撑工业信息安全未来

针对工业信息面临的风险环境变化，工业企业将如何强化信息安全的综合能力？如何保障数字化转型的顺利推进？我们结合此次调研的两百余家工业企业信息安全建设发展现状分析，并综合施耐德电气多年来在工业信息安全建设运营和服务方面的实践，提出四大价值主张：自知、合规、着力、迭代，用以支撑工业信息安全最优实施路径，赋能未来建设。

4.1 梳理现状，形成规划

工业信息安全能力建设是一个系统性工程，要积极稳妥有序高效的推进此项工作必须真正落地风险管理理念，基于对自我现状尤其是风险的清晰认知开展系统性的规划，积极借鉴最佳实践经验形成适配自身业务发展需要的建设蓝图和演进路线。

在现状梳理过程中，我们认为有几个核心的关注要点：

- **关键业务和资产梳理：**应清晰定义 IT/OT 融合环境下整体业务流及其关键支撑信息基础设施，初步建立关键资产清单。
- **合规风险识别：**应完整识别法律法规、标准规范等各类合规需求，对比组织信息安全管理技术控制落实情况，对合规要求尤其是近期监管重点的符合性进行准确判定，发现不满足事项需要立刻建立待整改清单。
- **信息安全成熟度水平：**应基于管理策略、技术方案、落地流程、人员能力、执行效果等维度，对信息安全控制措施实施水平进行全面评估，识别落地执行不足环节，进而形成改进事项清单。

基于现状梳理结果，结合工作需要构建不同层级的信息安全规划指导工作的开展，我们认为应考虑的规划内容包括四类：

四类规划内容

01	02	03	04
战略发展规划	中期落地规划	安全体系规划	执行方案规划
以支持客户进行数据化转型为整体性战略目标，明确工业信息安全工作战略目标、重点任务和保障措施	通过规划信息安全建设的蓝图及建设路线图，开展优先级分析，明确重点项目，形成实施路径	确定信息安全目标，形成风险控制策略和控制措施矩阵，初步设计安全技术体系、管理体系和运营体系框架	就具体建设任务项目，梳理业务技术环境，细化信息安全需求，输出定制化产品部署落地方案

工业信息安全现状梳理和规划过程中，具备丰富 OT 环境实战经验的安全专家经验尤为重要。如果自身缺乏适宜专业人员储备的组织，可通过专业咨询服务适当借用外部资源，确保科学研判、因地制宜，从而对工业信息安全能力可持续发展发挥重要的指导作用。

4.2 建立基础，保障业务

安全能力的真正提升最终离不开规划的切实落地，实际建设过程中首先应该基于安全体系规划框架规划建立适应组织业务发展需要的信息安全管理体系和运营机制，结合中期落地规划和重点项目执行方案规划部署关键安全技术控制，以构建保障业务正常运作所必须的防护体系为目标建立基础安全能力。

我们认为以下控制措施是工业信息安全能力优先落地的常见选项：

- **建立责任机制：**建立工业信息安全工作机制，明确工业信息安全管理责任人，落实工业信息安全责任制。
- **强化安全教育培训：**落实全员安全意识教育，开展安全管理技术人员职业技能培训。
- **建立安全管理制度：**遵循网络安全等级保护、IEC 62443 和 ISO27001 等标准要求建立工业安全总体策略、安全建设运维全生命周期的管理制度和技术规范，对关键领域内工作进一步细化，形成作业指导书并明确实施各项流程的记录。
- **物理安全防护：**对重要工业控制软硬件所在区域采取物理访问控制、视频监控、专人值守等防护措施。
- **OT 网络隔离：**在 OT 网络与企业 IT 网络或互联网边界部署隔离技术手段并落实有效的访问控制策略，严格禁止工业控制系统面向互联网开通高风险通用网络服务。
- **远程访问管控：**严格限制对 OT 网络设施的远程访问和维护，确需使用的应限定来源和访问者，采用虚拟专用网络（VPN）等方式提供安全可控的访问通道，并确保访问过程和接入后相关操作的可审计性。
- **OT 环境攻击检测：**在 OT 网络与企业网络、互联网边界以及 OT 网络内部重要工业控制设备前端等关键位置，部署攻击检测设备，识别传统网络攻击和基于业务指令的工控系统攻击。
- **安全基线构建：**建立工业控制网络设备和工业主机终端安全配置基线，并进行部署落实，定期实施配置审计。
- **漏洞和补丁管理：**跟踪重大工控安全漏洞和补丁发布，基于严格的安全评估和验证测试进行补丁升级或部署虚拟补丁。
- **OT 主机 / 控制器终端防护：**强化 USB/ 光驱等外设端口管控，建立防病毒和恶意软件入侵防护能力，对业务必须且临时接入的设备落实病毒查杀。
- **资源使用身份认证：**在 OT 主机、工业控制软件等资源使用过程中落实身份认证机制，避免使用默认口令或弱口令，定期更新口令。
- **数据识别及重要数据备份：**分析梳理业务流程和系统设备，识别重要业务数据和个人信息形成数据资产清单，初步构建数据分类分级机制，定期备份关键业务数据和系统配置信，息确保生产连续性。

4.3 关注痛点，强化运营

在完成基础安全能力构建，有效落实关键安全管理和技术控制措施后，进一步提升的重心应转移到残余的关键痛点问题，针对信息安全风险提供纵深防御措，以免其中一种安全措施失效或其中一个脆弱性被利用。同时应以提质增效为目标，强化安全运营能力建设。我们认为以下要点是工业信息安全能力提升阶段的常见选项：

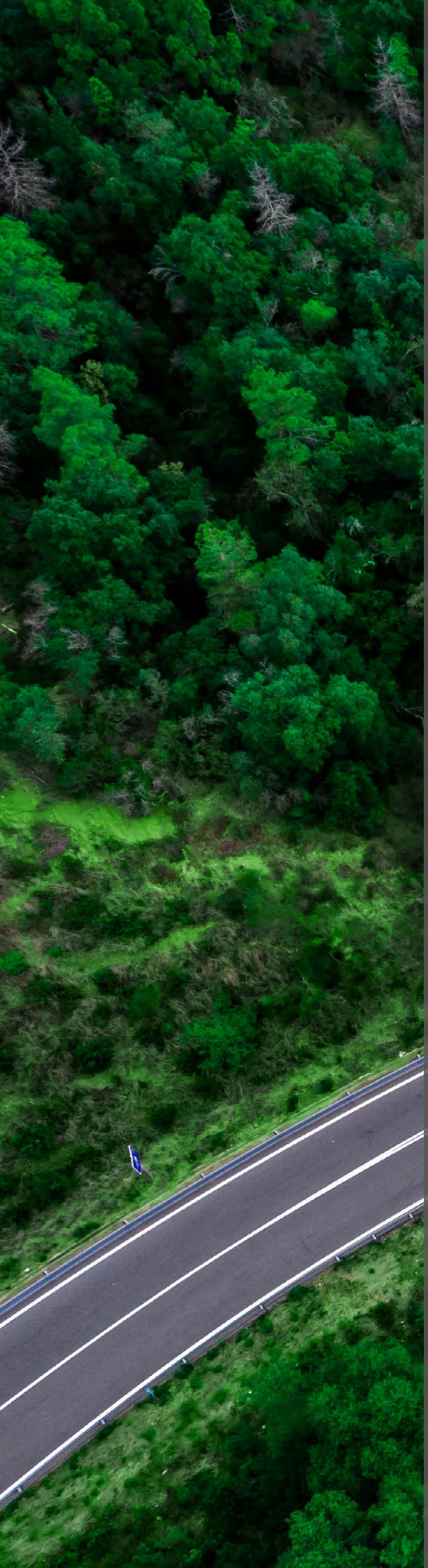
- **高可用提升：**通过对 OT 环境关键组件进行冗余配置等控制措施，保障 OT 系统高可用性，提升业务连续性保障能力。
- **OT 资产和脆弱性管理：**构建 OT 资产和漏洞自动化识别能力，深入了解 OT 网络各类资产信息如厂商、固件版本和高危漏洞等，形成工业网络实时视图。
- **OT 环境内部隔离：**对工业控制网络安全区域之间进行逻辑隔离安全防护。
- **OT 环境攻击遏止：**对已经发生并监测识别到的攻击行为进行遏制，避免攻击行为的持续进行和影响进一步扩大。
- **应用程序控制：**建立安全准入评估机制并综合应用黑白名单手段，确保工业环境主机终端运行的应用程序经过企业自身授权和安全评估。
- **重要数据加密：**对高安全等级工业数据在存储和传输过程中落实数据加密。
- **测试环境和测试数据保护：**分离工业控制系统测试和生产环境，限制真实敏感业务数据在测试环境中的使用。
- **团队建设：**培养 OT 业务和网络安全复合型人才，整合内外部资源，构建工业信息安全专职团队。
- **应急响应：**制定工业环境信息安全事件应急响应预案，定期对工业控制系统的应急响应预案进行演练，并基于结果优化预案。
- **态势感知：**建立工业态势感知平台，综合资产、流量、日志和威胁情报数据进行综合分析多维度量化安全态势，与组织 IT 环境态势感知平台进行集成，构建 IT/OT 联动的安全事件响应流程，建立总部与分支、组织与行业区域工业态势平台的纵向互联，强化多方信息共享和响应协同。

在安全能力建设工程中，应优先注意考虑具备工业自动化和安全防护经验的供应商，优先使用原生信息安全的工控产品，以合同等方式明确服务商应承担的信息安全责任和义务。

4.4 持续改进，拥抱未来

持续改进是信息安全工作永恒的话题。在组织中应培育积极改进的文化和意识，采用风险管理的方法，充分识别改进的机会，有计划地实施改进，具体实施措施包括内部信息安全评估检查、外部认证和测评等。我们认为以下操作是持续改进的关键操作选项：

- **内部信息安全评估检查：**定期开展网络安全全面自查和风险评估，结合安全事件和热门话题组织专项检查，确认信息安全手段按设计正确部署并产生效果，同时保证系统的性能和功能满足业务需要，同时没有因为信息安全升级导致服务降级。针对检查发现的问题和不足，及时制定并落实改进方案。
- **外部认证和测评：**积极开展工业控制系统的等级保护定级备案测评，对等级测评中发现的安全风险隐患，制定整改方案，落实整改措施，消除风险隐患。获取基于 IEC 62443、ISO27001 等国际标准的工业信息安全认证，并通过定期审核以确保持续符合上述标准的要求。



结语：

在当今愈来愈复杂多变的网络空间中，随着云、大数据、物联网等开放式的技术在实际运用中不断普及和发展完善，信息安全所面临的挑战已经由保护某个封闭区域内的资产设备转变为对整体网络安全生态系统的体系化协同保。而此时，只有整个生态链中上 、下游的参加者协同合作，才能让我们应对层出不穷、复杂多变的信息安全威胁。

厂商 作为工业控系统组件的提供者，应使用全生命周期的安全流程，在设计之初就将信息安全作为产品需求的一部分，为用户提供符合法规和应用需求的原生安全的工业产品

用户 作为使用方和信息安全责任主体，应根据具体应用和法律法规要求，系统化的提高对信息安全风险的防控能力，包括建立安全流程机制、重点资产防护、全生命周期的安全管理等，以确保系统的韧性和业务的连续性

安全服务商 作为安全专业服务方，应该深入理解用户特定领域的具体业务需求，如工业企业对环境人身安全、系统可用性和可靠性的需求，与厂商积极配合，有效的协助用户进行信息安全升级、信息安全维护等，以满足合规及业务连续性的需求

基于施耐德电气商业价值研究院和亚信安全联合发起的工业信息安全调研，从合规监管、行业挑战、企业经验、专业服务最佳实践等方面，对不同相关生态方进行访谈分析，我们力争帮助企业对当前工业信息安全状况建立一个更加全面的认识，同时我们也坚信大家的团结协同，才是我们面对这个巨大挑战的最佳应对之术。

携手构筑保障，建设安全未来！

关于作者

王勇

施耐德电气(中国)有限公司
工业自动化业务
中国区工业信息安全负责人

裴渊斗

施耐德电气(中国)有限公司
工业自动化业务
中国区工业自动化信息安全业务负责人

廖双晓

亚信安全科技有限公司
战略发展部
战略咨询专家顾问

洪岩博

施耐德电气(中国)有限公司
战略联盟与创新投资部
中国区生态合作伙伴负责人

施耐德电气商业价值研究院管理委员会

范莉莉

施耐德电气商业价值研究院
知识管理组成员

刘鹤楠

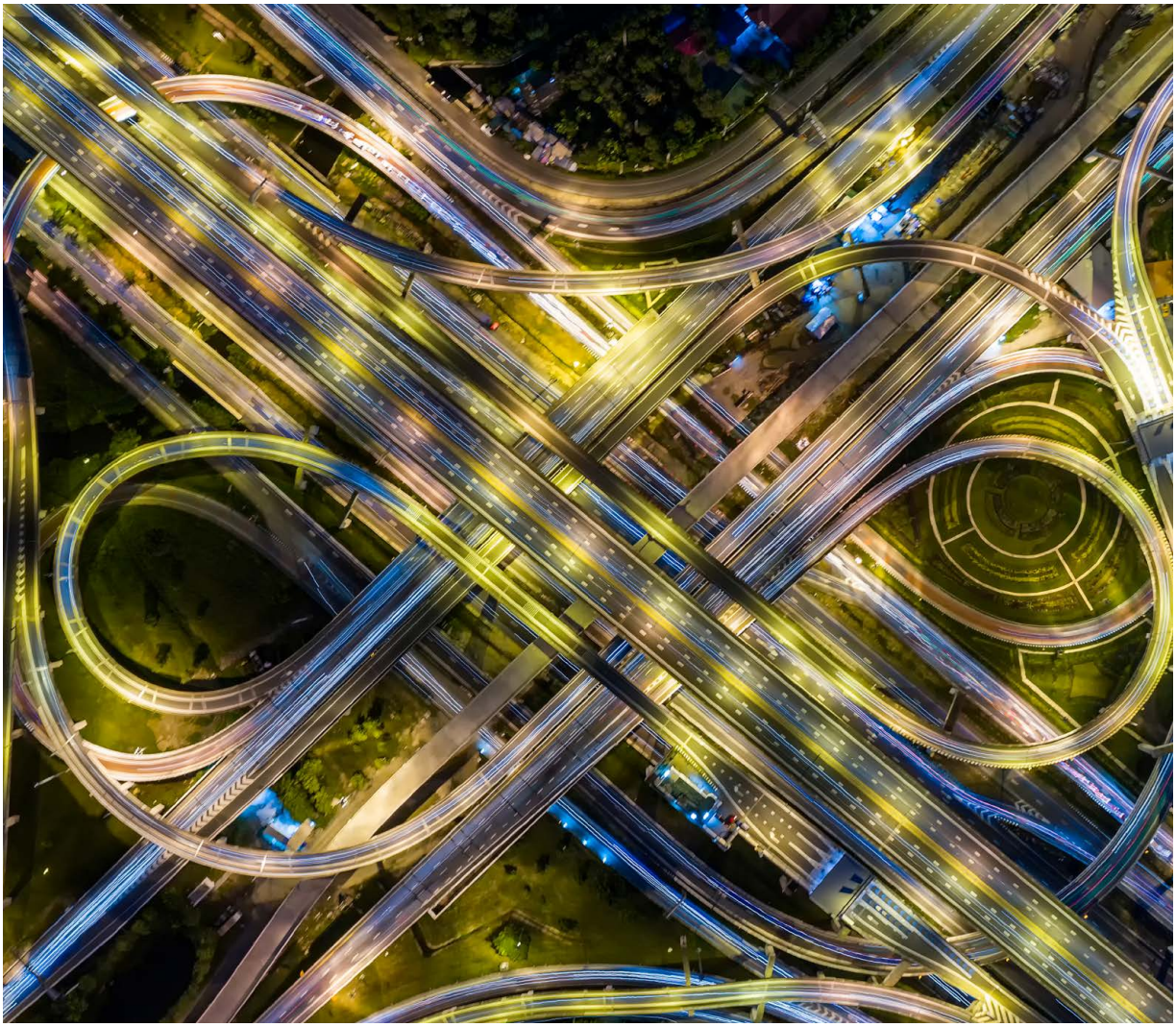
施耐德电气商业价值研究院
知识管理专家

致谢

我们由衷感谢参与本次调研的外部专家，感谢他们抽出时间与我们分享真知灼见。同时，也感谢施耐德电气首席信息安全官蒋宇寒、施耐德电气全球供应链中国区网络安全和IT基础架构负责人王海、亚信安全战略投资与合作部总监曾强，以及战略和市场营销团队在这份报告中的付出和努力。

特别鸣谢*：云南驰宏锌锗股份有限公司、圣戈班管道系统有限公司、中沙（天津）石化有限公司、中联水泥集团、得力集团

*排名不分先后



Life Is On | Schneider Electric 施耐德电气

施耐德电气（中国）有限公司
Schneider Electric(China)Co.,Ltd.

北京市朝阳区望京东路6号
施耐德电气大厦
邮编：100102
电话：(010) 8434 6699
传真：(010) 8450 1130

Schneider Electric Building, No. 6,
East WangJing Rd., Chaoyang District
Beijing 100102 P.R.C.
Tel: (010) 8434 6699
Fax: (010) 8450 1130

2022年4月

998-22047400