工业互联网安全架构白皮书

（V1.0）

北京六方云信息技术有限公司

2020 年 5 月

版 权 声 明

本白皮书中所出现的材料和信息，除另有特别注明，版权均属北京六方云信息技术有限公司所有，受到有关产权及版权法保护。如需转载使用，需联系北京六方云信息技术有限公司获得书面授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用。北京六方云信息技术有限公司保留对本文档及本声明的最终解释权和修改权。本文档参考或引用的资料无法一一列举在参考资料里面，敬请谅解，如相关作者对版权问题有异议，请及时与我们联系。

免 责 条 款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。北京六方云信息技术有限公司在编写该文档时已尽最大努力使其内容准确可靠，但北京六方云信息技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担任何责任。

北京六方云信息技术有限公司

电话：400-6060-270

邮箱：mkt@6cloudtech.com

目 录

第一章 工业互联网安全的内涵与范畴 1
第二章 工业互联网安全架构的定位与作用. 3
第三章 工业互联网安全总体架构 4
3.1 体系架构设计方法论 4
3.2 体系架构设计原则 4
3.3 工业互联网安全体系架构 5
第四章 工业互联网安全需求. 6
4.1 工业互联网安全现状与问题 6
4.2 工业互联网安全发展趋势 7
第五章 安全业务视图 11
5.1 总体业务视图. 11
5.2 行业维度. 13
5.3 企业维度. 15
5.4 建设维度. 16
5.5 安全能力. 17
第六章 安全功能视图 18
6.1 工业互联网安全特殊性 18
6.2 总体功能视图. 21
6.3 防护对象维度. 22
6.4 防护措施维度. 23
6.5 防护管理维度. 31
第七章 安全实施视图. 34
7.1 安全实施总体框架. 34
7.2 边缘安全防护系统实施 35
7.3 企业安全防护系统实施 43
7.4 企业安全管理平台实施 50
7.5 省/行业级安全平台实施 54
7.6 国家级安全平台实施 57
第八章 安全技术视图 58
8.1 安全技术体系总览 58
8.2 通用安全技术. 61
8.3 工业端点安全. 63

8.4 工业控制安全 74
8.5 工业网络安全 95
8.6 工业边缘系统安全 105
8.7 工业互联网平台安全 106
8.8 工业应用安全 116
8.9 工业人工智能安全 119
8.10 工业大数据安全 128
8.11 工业 5G 安全 147
8.12 工业安全管理 171
第九章 安全标准 183
9.1 工业安全国际标准 183
9.2 工业安全国家标准 187
9.3 云计算安全国际标准 188
9.4 云计算安全国家标准 189
第十章 垂直行业应用实践 190
10.1 钢铁行业：让集团多工厂安全的网络互联以满足个性化制造 190
10.2 能源行业让数字化采油更安全 207
第十一章 工业互联网安全发展展望 216
第十二章 关于六方云 217
12.1 六方云新一代工业互联网安全体系 218
12.2 六方云 5+1 工业互联网安全产品体系 219
参考资料 220

编 写 说 明

“工业互联网”的概念最早由美国通用电气公司（GE）于 2012 年提出，随后其联合另外四家 IT 巨头组建了工业互联网联盟（IIC），将这一概念大力推广开来。“工业互联网”主要目的是使现实世界中的机器、设备和网络能在更深层次与信息世界的大数据和分析连接在一起，带动工业革命和网络革命两大革命性转变。在新一轮科技革命和产业变革的浪潮下，工业产业发展呈现出智能化、网络化、服务化趋势，工业互联网更是工业技术变更发展的必然趋势。

2017 年 11 月 27 日，国务院发布了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，提出要加快发展工业互联网，构建网络、平台、安全三大功能体系，强化工业互联网安全保障。2019 年政府工作报告中明确提出打造工业互联网平台，拓展“智能+”，为制造业转型升级赋能。

习近平总书记在 2019 工业互联网全球峰会致贺信中指出，“中国高度重视工业互联网创新发展，愿同国际社会一道，持续提升工业互联网创新能力，推动工业化与信息化在更广范围、更深程度、更高水平上实现融合发展”。2020 年 3 月，中共中央政治局常务委员会召开会议，强调要加快 5G 网络、工业互联网等新型基础设施建设进度。4 月，国家发改委首次明确将新型基础设施的范围，作为新型基础设施的重要组成部分，工业互联网将会进一步加速发展；而工业互联网安全作为工业互联网的三大体系之一，是国家安全的重要组成部分，它关系到国家关键基础设施建设和经济社会稳定，并且辐射范围广泛，因此工业互联网安全已经成为当前网络安全领域中最为重要的部分之一。

2019 年 7 月，工信部等十部门联合印发《加强工业互联网安全工作的指导意见》，明确指出到 2020 年底，初步建立工业互联网安全保障体系，初步建成国家工业互联网安全技术保障平台、基础资源库和安全测试验证环境。到 2025 年，制度机制健全完善，技术手段能力显著提升，安全产业形成规模，基本建立起较为完备可靠的工业互联网安全保障体系。顺应国家形势，六方云基于自身在工业互联网安全的研究和实践，撰写工业互联网安全架构白皮书。本报告首先简要介绍工业互联网安全的内涵和意义以及工业互联网安全架构的定位和作用，然后从安全业务、安全功能、安全实施、技术体系等四个视图介绍工业互联网安全架构。最后将本报告设计的工业互联网安全架构应用到垂直行业，以期指导垂直行业的工业互联网安全建设。

第一章 工业互联网安全的内涵与范畴

面对第四次工业革命与新一轮数字化浪潮，全球领先国家无不将制造业数字化作为强化本国未来产业竞争力的战略方向。众多国家在推进制造业数字化的过程中，都提出了工业数字化革命的参考架构，如德国推出工业 4.0 参考架构 RAMI4.0、美国推出工业互联网参考架构 IIRA、日本推出工业价值链参考架构 IVRA，其核心目的是以参考架构来凝聚产业共识与各方力量，指导技术创新和研发产品解决方案，引导制造企业开展应用探索与实践，并组织标准体系建设与标准制定，从而推动一个创新型领域从概念走向落地。中国也提出了中国制造 2025 战略。

《中国制造 2025》的总体思路是坚持走中国特色新型工业化道路，促进制造业创新发展，提质增效，加快新一代信息技术与制造业融合，推进智能制造，满足经济社会发展和国防建设对重大技术装备需求。《中国制造 2025》提出，通过“三步走”实现制造强国的战略目标。

在新一代信息技术与制造技术深度融合的背景下，以及在工业数字化、网络化、智能化转型需求的带动下，以泛在互联、全面感知、智能优化、安全稳固为特征的工业互联网应运而生。工业互联网作为全新工业生态、关键基础设施和新型应用模式，通过人、机、物的全面互联，实现人、物品、机器、车间、企业等全要素以及设计、研发、生产、管理、服务等全产业链各环节的泛在互联。为缩短产品上市周期的产品价值链，提高生产率的业务价值链，提升业务灵活性的资产价值链等全价值链的全面连接，工业互联网正在全球范围内不断颠覆传统制造模式、生产组织方式和产业形态，推动传统产业加快转型升级、新兴产业加速发展壮大。因此，工业互联网是实体经济数字化转型的关键支撑，也是实现工业革命的重要基石。

2017 年 11 月 27 日，国务院发布了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，提出要加快发展工业互联网，构建网络、平台、安全三大功能体系，强化工业互联网安全保障。《指导意见》突出强调了工业互联网安全的基础性和战略性地位，为今后我国工业互联网安全工作制定了时间表和路线图。《指导意见》提出“三步走战略”，即到 2020 年初步建立工业互联网安全保障体系，到 2025 年基本建立起较为完备可靠的工业互联网安全保障体系，到 2035 年安全保障能力全面提升。根据国务院发布的《指导意见》，工业互联网包括网络、平台和安全三大体系。网络体系是基础，平台体系是核心，安全体系是保障。

工业互联网三大核心要素包括智能设备、智能系统、智能决策。（1）智能设备：安装了各种传感器，能够收集生产过程中产生的数据；（2）智能系统：包括许多传统的网络系统，同时也包括在机队和网络间广泛部署且内置软件的机械装置的组合，随着加入工业互联网的机床和设备增加，机械装置在机队和网络间的协同效应就可以实现。智能系统需具备四大特征：网络协同、更优维修、智能恢复和智能学习；（3）智能决策：是工业互联网的长期愿景，它是工业互联网的元素按设备、按系统组合的过程中所收集知识的顶点。

工业互联网的网络体系将连接对象延伸到机器设备、工业产品和工业服务中，可以实现人、机器、车间、企业等主体，以及设计、研发、生产、管理、服务等产业链各环节的全要素的泛在互联及数据的顺畅流通，形成了工业智能化的“血液循环系统”。工业互联网平台是工业互联网三大核心要素之一的智能决策的承载者，是工业全要素链接的枢纽与工业资源配置的核心，在工业互联网体系架构中具有至关重要的地位。目前工业互联网平台的发展正处于规模化扩张期，以美、德为代表的世界主要国家纷纷将工业互联网平台作为战略重点，各国领军企业通过发展工业互联网平台，不断巩固和强化他们在制造业的地位。工业互联网安全是工业信息安全的核心，直接决定工业生产安全，更关乎经济发展、社会稳定乃至国家安全。工业互联网安全从三大核心要素的角度来看，包括智能设备安全、智能系统安全和智能决策安全。其中智能决策安全主要体现在工业互联网平台安全。

在“工业 4.0”及《中国制造 2025》的大潮下，工业控制系统正朝着高度信息化方向发展，越来越多的工控系统及设备接入互联网，让更多的网络攻击手段有了可乘之机，网络空间的安全问题开始延伸到工控系统中。网络、平台、安全是工业互联网三大功能体系，而工业互联网安全是工业互联网业务目标达成、功能正常运行、建设顺利实施的重要保障。

新一代信息技术在加速信息化与工业化深度融合发展的同时，也带来了日趋严峻的信息安全问题。工业信息化、自动化、网络化、智能化等基础设施是工业的核心组成部分，是工业各行业、企业的神经中枢。工业互联网安全的核心任务就是要确保这些工业神经中枢的安全。工业互联网安全事关经济发展、社会稳定和国家安全，是网络安全的重要组成。

从内容来看，工业互联网安全涉及工业领域各个环节，包括工业控制系统信息安全（简称工控安全）、工业大数据安全、工业云安全、工业电子商务安全等内容。

随着 IT 与 OT 加速融合一体化，工业互联网的快速发展为工业信息系统的整体安全防护带来更大的挑战。目前，工业互联网平台安全、工业网络基础设施安全、工业数据安全以及

IT/OT 的融合安全等领域的技术研究和产品应用均处于起步阶段，但随着防护对象保障需求的变化，工业信息安全产业的边界也将不断延伸扩展。

第二章 工业互联网安全架构的定位与作用

工业互联网安全是工业互联网保障体系。

2015 年，面对第四次工业革命与新一轮数字化浪潮，中国提出了《中国制造 2025》战略，明确工业互联网是实体经济数字化转型的关键支撑，也是实现工业革命的重要基石。

2017 年，国务院发布了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，提出要加快发展工业互联网，构建网络、平台、安全三大功能体系，强化工业互联网安全保障，并突出强调了工业互联网安全的基础性和战略性地位，为今后我国工业互联网安全工作制定了时间表和路线图。

2018 年，中国工业互联网产业联盟发布了《工业互联网安全框架》。美国工业互联网联盟从工业物联网系统 IIOT、工业功能 IIRA、工业安全框架 IISF 三个角度来梳理构建工业互联网，IISF 即《Industrial Internet of Things Volume G4:Security Framework》，从防护对象、防护管理和防护措施三个角度系统分别阐述了工业互联网安全框架。防护对象包括设备终端、网络、应用、数据等，防护措施包括威胁防护、监测感知、处置恢复等，防护管理包括安全目标、风险评估和安全策略配置等。

随着工业互联网的发展，工业互联网面临越来越严峻的安全挑战，工业互联网安全架构也需要重新定义与构建。鉴于一般以参考架构来凝聚产业共识与各方力量、指导技术创新和产品解决方案研发、引导制造企业开展应用探索与实践、组织标准体系建设与标准制定，从而推动一个创新型领域从概念走向落地，六方云结合自身对工业互联网以及工业信息安全的深刻理解，参考了中国工业互联网产业联盟发布的《工业互联网体系架构（版本 2.0）》及《工业互联网安全框架》，美国工业互联网安全参考架构（IIRA G4）和美国国土安全部发布《物联网安全指导原则》，发布本工业互联网安全架构白皮书。其核心目的是以工业互联网安全参考架构来凝聚产业共识与各方力量，指导工业互联网安全技术创新和产品解决方案研发，助力工业互联网从概念走向落地，引导工业企业在开展工业互联网建设的同时实现安全保障同步规划、同步建设与同步实施。

第三章 工业互联网安全总体架构

3.1 体系架构设计方法论

本工业互联网安全架构白皮书的体系架构，参考了主流的安全架构设计方法论，包括以 ISO、IEC、IEEE 42010 和 TOGAF 为代表的系统与软件工程架构方法论，美国提出的 PDRR 模型、P2DR 模型、IATF 框架、黄金标准框架方法论，Gartner 提出的 Adaptive Security Architecture 模型（CARTA 属于自适应架构 3.0），Forrester 提出的 Zero Trust 模型及 MITRE ATT&CK 框架为代表的安全架构方法论；同时借鉴了安全相关参考架构的设计理念和关键要素，包括联盟发布的工业互联网架构 2.0 为代表的工业互联网架构，美国工业互联网安全参考架构（IIRA G4）为代表的工业互联网安全架构，IEC 62443 为代表的工业通信网络信息安全标准，工业和信息化部印发《工业控制系统信息安全事件应急管理工作指南》，中国等级保护 2.0 标准等。

3.2 体系架构设计原则

本工业互联网安全架构白皮书的体系架构设计原则，总体上遵循等级保护 2.0 技术要求和关键信息基础设施保护要求。

等保 2.0 提出“分等级保护、突出重点、积极防御、综合防护”的基本原则，建立具有动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控六大安全能力的“打防管控”一体化网络安全综合防御体系。

关键信息基础设施的安全保护提出“重点保护、整体防护、动态风控、协同参与”的基本原则，建立网络安全综合防御体系。重点保护是指关键信息基础设施网络安全保护应首先符合网络安全等级保护政策及 GB/T 22239-2019 等标准相关要求，在此基础上加强关键信息基础设施关键业务的安全保护；整体防护是指基于关键信息基础设施承载的业务，对业务所涉及的多个网络和信息系统（含工业控制系统）等进行全面防护；动态风控是指以风险管理为指导思想，根据关键信息基础设施所面临的安全风险对其安全控制措施进行调整，以及时有效的防范应对安全风险；协同参与是指关键信息基础设施安全保护所涉及的利益相关方，共同参与关键

信息基础设施的安全保护工作。

3.3 工业互联网安全体系架构

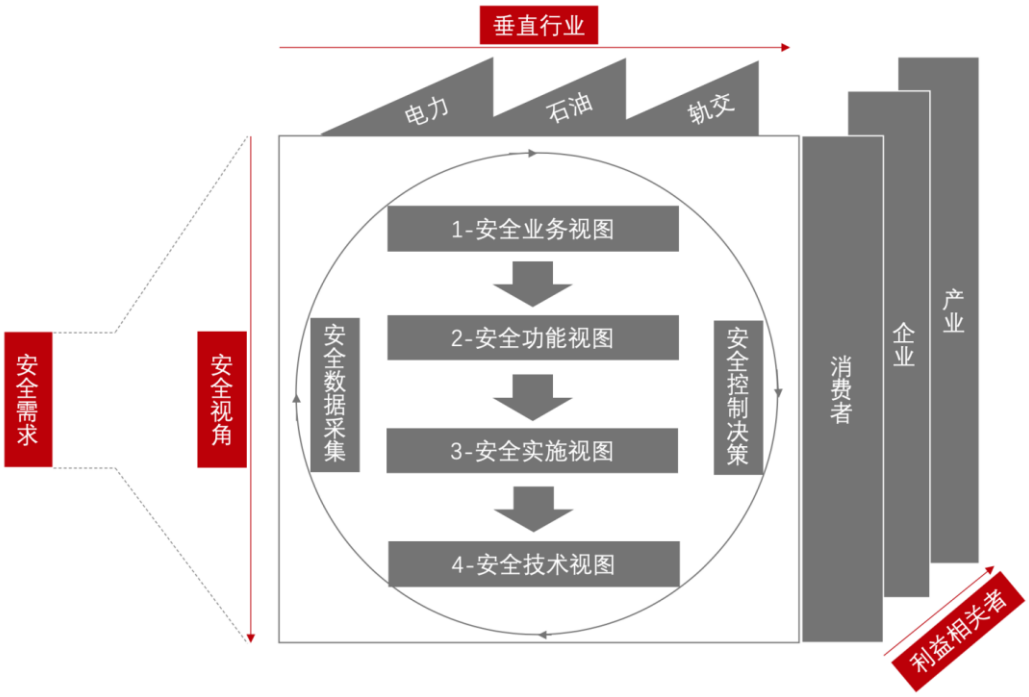

图 3-1 工业互联网安全体系架构

工业互联网安全体系架构参照 ISO/IEC/IEEE 42010 标准以及 TOGAF 架构开发方法，基于安全需求，从利益相关者、垂直行业、安全视角三个角度出发，构建业务、功能、实施、技术四个视图。

从利益相关者角度看，工业互联网安全相关者有产业、企业和工业互联网安全受益消费者。

从垂直行业横向的角度看，工业互联网安全架构指导电力、石油石化、轨交、钢铁生产和高端设备制造等领域的安全建设，同时工业互联网安全架构实施要取得良好效果，也需要将不同行业和地区的人才组织在一个开放的知识框架内，使人才作为垂直行业工业互联网安全创新的核心动力之一。

从安全视角看，可以从安全业务、安全功能、安全实施、安全技术四个视图来构建工业互联网安全体系。

安全业务视图：明确企业在建设工业互联网时在安全体系方面要实现的目标、方向、业务

场景及相应的安全防护能力。安全业务视图主要用于指导企业在商业层面明确工业互联网安全的定位和作用，提出的安全能力需求对于后续功能架构设计有重要指引。

安全功能视图：明确企业在建设工业互联网安全时要实现的核心功能、基本原理和关键要素。安全功能架构主要用于指导企业构建工业互联网安全的支撑能力与核心功能，并为后续工业互联网安全实施框架的制定提供参考。

安全实施视图：描述各项安全功能在企业落地实施的安全层级结构、安全软硬件系统和部署方式。安全实施框架结合联盟在工业互联网架构 2.0 中提出了设备层、边缘层、企业层、产业层四层组成的实施框架层级划分，明确了各层级的安全的系统架构、部署方式以及不同系统之间关系。实施框架主要为企业提供工业互联网安全具体落地的统筹规划与建设方案，进一步可用于指导企业技术选型与系统搭建。

安全技术视图：阐述了工业互联网安全业务、功能、实施所需要的技术体系与技术措施。

第四章 工业互联网安全需求

4.1 工业互联网安全现状与问题

当前，工业系统安全保障体系建设已较为完备，伴随新一代信息通信技术与工业经济的深度融合，工业互联网步入深耕落地阶段，工业互联网安全保障体系建设的重要性越发凸显。世界各主要发达国家均高度重视工业互联网的发展，并将安全放在了突出位置，发布了一系列指导文件和规范指南，为工业互联网相关企业部署安全防护提供了可借鉴的模式，从一定程度上保障了工业互联网的健康有序发展，但随着工业互联网安全攻击日益呈现出的新型化、多样化、复杂化，现有的工业互联网安全保障体系还不够完善，暴露出一些问题：

数据隐私和数据安全防护缺乏有效手段

工业互联网平台采集、存储和利用的数据资源存在数据体量大、种类多、关联性强、价值分布不均等特点，数据隐私与安全主要关注：

（1）数据包含了敏感或个人隐私信息，因此数据在价值挖掘使用和发布的场景中可能会给个人、第三方和国家带来危害和损失，因此对隐私和重要数据的处理、使用、操作、发布、交换等生产流通环节都有安全与合规的要求；

（2）数据需要多方的多维度融合才能创造价值，但往往每方都有自己数据的产权保护、个人数据和重要数据的合规责任，因此需要更安全的数据融合环境；

（3）生产数据的每个环节需要相应的安全控制。工业互联网要健康、顺利的发展，首要要解决企业对数据和隐私的担忧。

OT 与 IT 两个领域人员融合较慢，安全意识亟需提升

工业现场缺乏信息安全专家，对工业系统的信息安全关注度和重视度都不高，信息安全专家在面对生产优先的工业系统往往束手无策、畏手畏脚。大部分工业互联网相关企业重发展轻安全，对网络安全风险认识不足。此外，很多智能工厂内部未部署安全控制器、安全开关、安全光幕、报警装置、防爆产品等，并缺乏针对性的工业生产安全意识培训和操作流程规范，使得人身安全难以得到保证。

工业信息安全存在先天不足，安全防护能力难以快速提升

工控系统和设备在设计之初缺乏安全考虑，自身计算资源和存储空间有限，大部分不能支持复杂的安全防护策略，很难确保系统和设备的安全可靠。同时，当前专业工业信息安全企业和解决方案较少，工业企业风险发现、应急处置等网络安全防护能力普遍较弱。同时，工业生产迭代周期长，安全防护部署滞后整体水平低，存量设备难以快速进行安全防护升级换代，整体安全防护能力提升时间长。

4.2 工业互联网安全发展趋势

总体趋势：传统的安全防御技术已无法抗衡新的安全威胁，防护理念将从被动防护转向主动防御。

融合安全技术成为 OT 与 IT 融合趋势下的必然选择

工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

工业控制系统面临安全事件危害范围扩大、危害程度加深、信息安全与功能安全问题交织等安全风险；控制环境方面表现为信息技术（IT）与操作技术（OT）融合，控制网络由封闭走向开放；控制布局方面表现为控制范围从局部扩展至全局，并伴随着控制监测上移与实时控制下移。

工业互联网安全所采用的技术必须要 IT 安全、OT 安全以及 IT 与 OT 融合安全技术如工业 VPN、工业 NAT、工业入侵检测、工控网络接入控制、无需依赖外部特征库的 AI 智能分析与检测等才能够满足工业互联网安全建设目标，从而使得工业系统既防护 OT 内部威胁，也防护 IT 威胁。

工业互联网未知威胁防范成为难点

新基建筑牢基础并加速工业数字化转型，强化工业互联网建设、催生 5G/IOT 等新场景机会。数字化转型时代，经济利益驱动网络攻击不断升级，关键基础设施和工业互联网保护面临更大挑战。

首先，超大规模泄露已趋于常态化。据报道“每月上亿条信息泄露，涉及政府数据、医疗信息、账户凭证、企业用户信息等敏感数据，平均数据泄露成本高达 392 万美元”。

其次，勒索软件手段升级、加大赌注。勒索软件转向有针对性威胁，80%的攻击针对企业，其中 68%的要钱，并演进为两阶段攻击。攻击目标从盲目感染到针对财务/ERP 等高价值资产，手段从钓鱼方式投递到利用 APT 高危漏洞，套现方式变为先在互联网部分公开窃取数据催缴赎金，获取赎金后，继续贩卖窃取的信息。

最后，关键基础设施面临更大的风险。90%的受访企业在过去两年遭遇过网络攻击，其中一半的网络攻击造成关键基础设施的“停转”。

0 Day 漏洞依然是最有效的攻击工具，一些组织依然不计成本来购买会自己挖掘 0 Day 漏洞来进行攻击，针对 0 Day 漏洞的网络流量入侵，恶意文件攻击检测成为关键。

（1）APT 主要利用未公开的漏洞，来绕过基于已知特征的 IPS 防御。根据美国 Rand 国家智库 2018 年的报道：在 7.6 万 CVE 漏洞中，未公开的漏洞利用工具占 87.2%，贡献了 50%的攻击事件。由于获得和开发漏洞利用工具的成本高，这些未公开的漏洞利用工具主要用于具备高攻击价值的目标。而这些未公开的利用漏洞利用工具都没有 IPS 签名特征，可直接穿透 IPS 设备。

（2）海量恶意软件变异频繁，无法准确检测。据报道，互联网上大约每天 33 万、全年 1.2 亿个恶意软件变种，安全分析人员无法分析海量恶意样本，导致大部分恶意变种都不能检测。

（3）黑客也利用 AI 来发起高效攻击。美国安全企业 ZeroFOX 公司于 2017 年发起了一项实验，希望测试 AI 在发动网络钓鱼攻击方面是否比人类更为擅长。该公司利用 AI 发起鱼叉

式钓鱼，AI 攻击机器监控社交媒体上的用户行为，而后创建并发布自己的钓鱼诱饵，以 6.75 条/分钟的速度向 800 多名用户发送鱼叉式钓鱼推文，快速引诱到 275 名受害者。人类攻击者则以 1.075 条/分钟的速度发送推文，且这种方式仅吸引到 49 名用户。AI 攻击成功率可达到人类攻击者的 6 倍，传统安全防护技术显得力不从心。

在实现态势感知的过程中，对采集的大量安全数据如何进行分析，发现潜在风险一直是个难点，尤其是面对工业互联网平台复杂的架构。面对这一难题，应当引入目前在已经逐渐成熟的机器学习技术，通过 AI 的助力去认知网络、学习现状、总结风险，从而将主动防御这一目标落实，实现更高的安全防护水平。

云平台成为安全防护的重点

未来制造系统将呈现扁平化特征，传统以 ISA-95 为代表的“金字塔”体系结构被逐渐打破，ERP、MES、PLM 等处于不同层次的管理功能基于平台实现集成融合应用，工业互联网平台将成为未来制造系统的中枢与核心环节。借助平台提供的数据流畅传递和业务高效协同能力，能够第一时间将生产现场数据反馈到管理系统进行精准决策，也能够及时将管理决策指令传递到生产现场进行执行，通过高效、直接的扁平化管理实现制造效率的全面提升。

平台作为工业互联网的核心，汇聚了各类工业资源，因而在未来的防护中，对于平台的安全防护将备受重视。平台使用者与提供商之间的安全认证、设备和行为的识别、敏感数据的共享等安全技术将成为刚需。

当前工业互联网平台主要采用云计算和大数据技术搭建而成，针对云平台的保护显得尤为重要。企业工业互联网云平台有如下安全风险或难题需要解决：

（1） 云内更多东西访问，边界防护失效：缺乏威胁隔离机制，网络威胁一旦进入云平台内部，可以肆意横向蔓延；

（2） 流量流向不可视：用户无法直观感受到虚机之间数据流量大小、流向变化；

（3） 威胁态势无感知，虚拟层漏洞不易修复：云内主机成倍增加，横向访问占据 80%以上，安全态势难以全局掌控；

（4） 安全策略调整不灵活：云内 IP 地址动态分配、虚机迁移随时发生，安全策略需自动跟随；

（5） 网络边界消失，硬件设备无法部署：虚机位置不确定、IP 地址动态分配、VLAN 隔离方式太复杂，业务区域边界不确定；

（6） 关键数据被窃取：相较于外部攻击，恶意的内部人员造成的危害风险更大，而缺乏相关审计措施。

内生安全防御和补偿式安全防御将长期并存

内生安全防御通常在设备层面通过对设备芯片与操作系统进行安全加固，并对设备配置进行优化的方式实现应用程序脆弱性分析。可通过引入漏洞挖掘技术，对工业互联网应用及控制系统采取静态挖掘、动态挖掘，实现对自身隐患的常态化排查；各类通信协议安全保障机制可在新版本协议中加入数据加密、身份验证、访问控制等机制提升其安全性。

但另一方面，工业现场还存在大量的不安全控制协议、不安全的工业设备、不可靠的工控网络、不安全的工业软件等，而更新这些系统又显得不现实，而且周期特别长，同时完全采用内生安全防御方式，在某些情况下并非经济高效，所以采用类似网关的补充式安全防御也非常必要。

工业互联网安全防护自动化与智能化将不断发展

未来对于工业互联网安全防护的思维模式将从传统的事件响应式向持续智能响应式转变，旨在构建全面的预测、基础防护、响应和恢复能力，抵御不断演变的高级威胁。工业互联网安全架构的重心也将从被动防护向持续普遍性的监测响应及自动化、智能化的安全防护转移。

对大数据的保护将成为防护热点

工业大数据的不断发展，对数据分类分级保护、审计和流动追溯、大数据分析价值保护、用户隐私保护等提出了更高的要求。未来对于数据的分类分级保护以及审计和流动追溯将成为防护热点。

首先是应用数据领域的安全解决方案。简单讲就是 web 应用 DLP+应用数据对象的安全管理。前者用于发现在各种内部业务人员、外包人员（如客服）、合作伙伴（如加盟网店）必须使用敏感数据的场景下，由这些已经有权限访问敏感数据的人员或主机发起的数据滥用、数据窃取的风险，并能针对泄露事件快速溯源定位到可疑对象，从而建立起威慑能力；后者则用于对应用系统上流动的敏感数据类型、数量、数据载体、涉敏数据接口、暴露面、数据流向、访问者、操作行为多个对象进行识别，监控状态变化、分析变化影响和异常分析，以提供给数据安全管理人员感知企业数据在业务层的流动态势并辅助进行风险评估。

其次是大数据平台安全方案。简单讲就是针对大数据平台（Hadoop 以及相关组件）的 4A（帐号、认证、授权、审计）+数据运维和分析的安全管理。前者提供如账号映射（开源大数

据平台不支持 LDAP）、细粒度权限（可以对表的字段级进行控制）、高危操作识别和拦截、审计等能力，给数据运维和分析场景提供更安全可靠的环境。后者则对用于对数据库和大数据平台及其组件上流动的敏感数据类型、数量、导入和分发数据载体/模型、数据流向、访问者、操作行为多个对象进行识别，监控状态变化、分析变化影响和异常，以提供给数据安全管理人员全面感知企业数据在运维和分析场景的流动态势并辅助进行风险评估。

再次是数据地图。主要围绕隐私合规要求，梳理和识别隐私数据做分类分级、隐私数据的数据流（采集点、存储地域、使用系统和用途、外流去向）、分析隐私数据的授权信息，并按数据主体汇集数据，以提供数据主体权利的支持（这些均是满足 GDPR、个人信息安全规范合规要求的点）。

工业互联网安全态势监测与感知将成为重要技术手段

借助人工智能、大数据分析以及边缘计算等技术，基于协议深度解析及事件关联分析机制，分析工业互联网当前运行状态并预判未来安全走势，实现对工业互联网安全的全局掌控，并在出现安全威胁时通过网络中各类设备的协同联动机制及时进行抑制，阻止安全威胁的继续蔓延。

第五章 安全业务视图

5.1 总体业务视图

安全业务视图包括**行业维度**、**企业维度**、**建设维度**、**安全能力**四个维度。

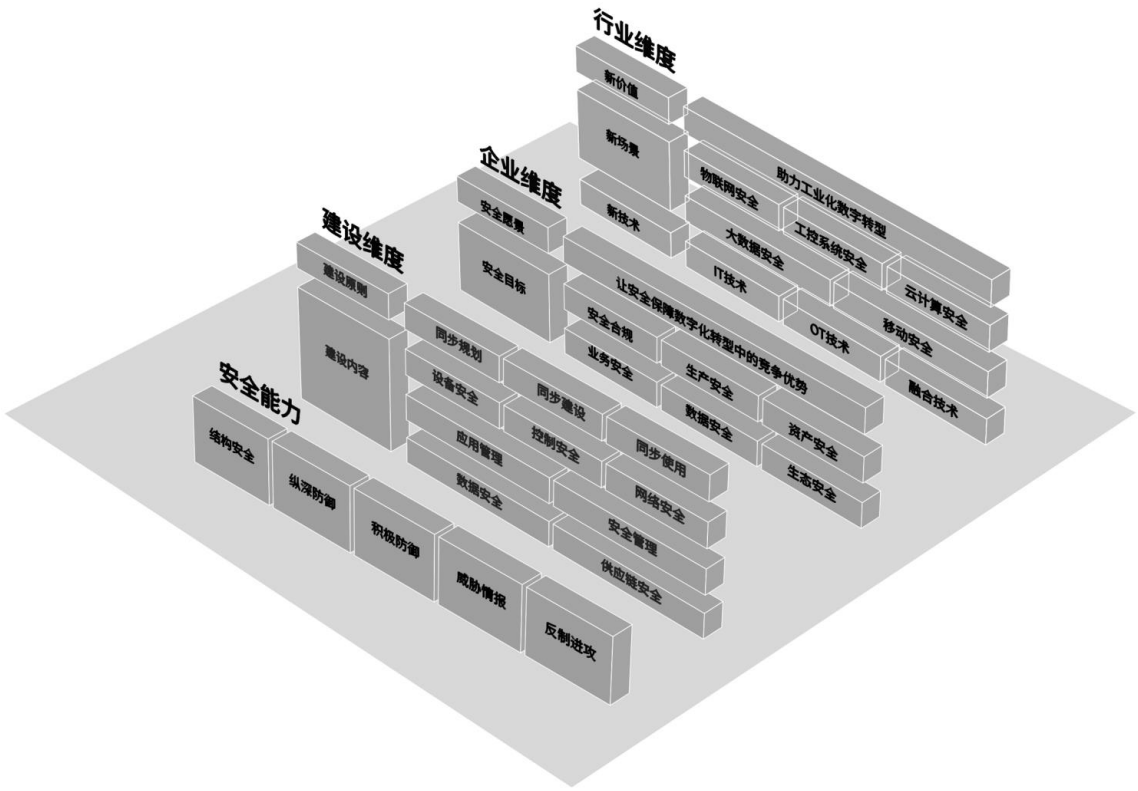

图 5-1 总体安全业务视图

行业维度在面对工业数字化、网络化、智能化的趋势下，要形成一个工业数字技术的新产业，智能化生产、网络化协同、个性化定制、服务化延伸等一系列数字化转型的“新模式”，数字化创新的“新业态”，必须要采用 IT 技术、OT 技术以及 IT 与 OT 融合技术，确保物联网安全、工控系统安全、云计算安全、大数据安全、移动安全等“新场景”安全。

企业维度实现企业各层级要素全面互联，对各类数据进行采集、传输、分析并形成智能反馈，助力企业生产效率、产品质量和运营管理能力提升，加快市场需求响应与交付速度，优化资源要素配置，强化商业模式创新，实现各类生产经营活动目标的提升优化，需要特别关注和确保数据在整个生命周期的安全、业务逻辑安全等。

建设维度关注产品链、价值链、资产链三个核心业务链条的效率与协同，一是需要关注和确保网络互联安全、数据共享安全，二是关注和确保数据在整个业务活动中的流动与使用安全，三是关注和确保资产全生命周期的设计开发安全、运维安全等。

安全能力维度实质表达的是企业在建设工业互联网时需要同步建设达到的工业互联网安全能力。

本报告提出工业互联网安全能力可参考国际知名网络安全研究机构 SANS 提出的网络安全“滑动标尺”模型，此模型正是这样一种网络安全能力模型。该模型将网空安全能力分为五大

类，即结构安全（Architecture）、纵深防御（Defense in Depth）、积极防御（Active Defense）、威胁情报（Intelligence）和反制进攻（Counter）。其中，结构安全、纵深防御、积极防御、威胁情报这 4 类能力是企业在建设工业互联网安全所需要具备的能力，而反制进攻能力则是国家或产业层面所需要具备的能力。

5.2 行业维度

行业维度主要阐述了安全在促进工业互联网发展的主要目标、实现路径与支撑基础。

工业互联网安全的目标是在面临工业数字化、网络化、智能化的趋势下，助力工业数字化成功转型。

工业互联网涉及到物联网、工控、云、大数据、移动访问等新型场景，工业互联网安全需要解决这些新场景下的安全问题。

不仅工业互联网需要信息技术、制造技术和融合技术，工业互联网安全也需要充分利用这三项技术才能够实现目标。一是需要充分利用大数据、云计算、人工智能等信息技术来提升信息安全能力，二是需要充分理解增材制造、现代金属、复合材料等新材料和加工技术以及工业现场操作规范的基础上提高安全防范的效果，三是需要借助工业大数据、工业人工智能等融合技术提升安全防护的自动化和智能化程度。

随着新一代信息技术的快速发展，工业信息安全产业结构不断变化，软硬件产品的界限越发模糊，产品和服务的联系愈加紧密。在借鉴 Gartner 和 ARC 咨询公司对市场主要产品和服务的分类的基础上，结合我国实际情况，基于对产业结构的理解，依据市场主流应用将工业信息安全产业结构分为产品和服务两大类。具体工业互联网安全产业结构如图 5-2 所示。

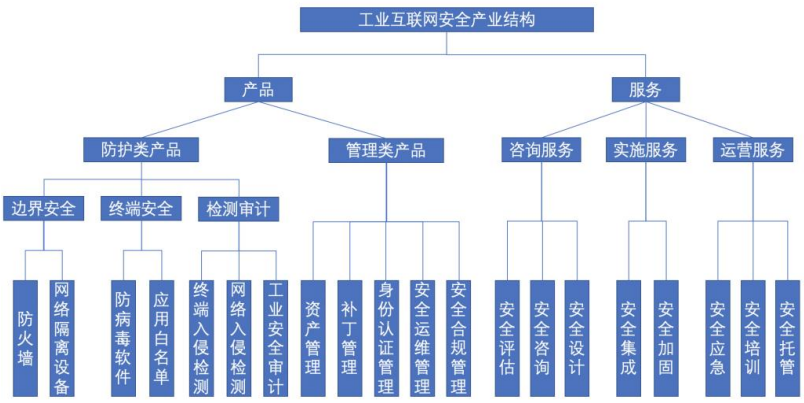

图 5-2 工业互联网安全产业架构

与传统计算机网络安全相比，工业互联网安全在保障对象、安全需求、网络和设备环境、通信协议等方面具有特殊性。识别工业企业信息系统存在的风险与安全隐患，并对应实施相应的安全技术与管理保障策略是确保工业互联网安全的重要手段。从市场发展来看，针对工业企业用户的信息安全需求，工业互联网安全产品类市场主要分为两类：防护类产品与管理类产品。

从技术防护的角度，工业互联网安全防护类产品包括边界安全产品、终端安全产品及监测审计类产品。其中，边界安全产品以工业防火墙和网络隔离设备为代表，主要用于保护工业网络边界并提供区域隔离；终端安全产品涵盖了能够在工业互联网安全环境下，防护所有终端设备的安全产品，如防病毒软件、应用白名单、端口设备控制、主机加固等；监测审计类产品主要用于监控和评估工业控制系统的完整性，典型产品包括终端入侵检测、网络入侵检测和工业安全审计等。

从安全策略和管理流程的角度，工业互联网安全管理类产品包括资产管理、补丁管理、身份认证管理、安全运维管理和安全合规管理几大类，旨在帮助企业管理和维护工业资产和设备安全态势。由于工业企业用户的安全需求侧重于生产或运行过程的可靠性，工业互联网安全管理产品结合了传统 IT 网络安全管理产品和解决方案，但限制了会对工业生产环境造成影响的功能模块。同时，工业互联网安全管理产品还将覆盖范围扩展到其他工业资产和控制协议。

工业互联网安全服务主要指工业企业购买的第三方安全服务。通过对工业互联网安全服务市场发展驱动因素的分析，根据安全服务对象及企业用户项目管理生命周期，安全服务可以分为三大类。

第一类是以安全评估、安全咨询、安全设计为代表的咨询服务，该类服务主要依托专家的知识体系和行业经验并依据国内外标准和行业监管规范，建立工业信息安全管理体系，为用户提供决策依据和优化方案。

第二类是以安全集成和安全加固为代表的实施服务，该类服务主要采取适当的管理过程和控制措施，通过产品和解决方案将工业信息安全管理体系落地实施。

最后一类是以安全应急、安全培训和安全托管为代表的运营服务，旨在为工业企业提供满足其全生命周期安全运营和管理需求的服务。

5.3 企业维度

企业维度主要明确了企业在建设工业互联网安全时的愿景和安全目标。商业维度主要面向 CEO 等企业高层决策者，用以明确在企业战略层面，安全建设的定位与目标。

对正在进行数字化转型的企业来说，工业互联网安全的目标愿景是确保企业在数字化转型过程中的竞争优势。

工业互联网企业安全目标包括安全合规、生产安全、资产安全、业务安全、数据安全。

企业的安全合规成为近期企业安全建设的重要目标。2017 年 7 月 11 日，国家互联网信息办公室公布备受瞩目的《关键信息基础设施安全保护条例（征求意见稿）》，揭开了中国关键信息基础设施安全保护立法进程的新篇章。2019 年 5 月 13 日，国家市场监督管理局、国家市场监督管理总局、国家标准化管理委员会召开新闻发布会，正式发布了等保 2.0 相关的《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准。2019 年 12 月 1 日，《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）正式实施。2019 年 12 月 3 日，全国信息安全标准化技术委员会（以下简称信安标委）秘书处在北京组织召开了国家标准《信息安全技术关键信息基础设施网络安全保护基本要求》（报批稿）（以下简称《基本要求》）试点工作启动会。

资产安全关注被保护用户拥有所有权或保管责任的财物自身价值的被危害和被损失的情况。此危害或损失可能是因为内外部的恶意攻击或内部管理不善所带来的。从安全建设的角度，则会根据资产的价值维度，设计访问资产的信任体系，检查和识别对资产的非法使用和操作，来达到保全资产安全的目的。

业务安全关注在业务过程中带来的对业务的危害和损失。

生产安全关注在企业生产过程中，由于对生产环境、生产资料和设备、生产工艺环节的问题，可能给企业、员工、外部第三方带来的危害和损失。生产安全风险出现在以下三种情况：

（1）危险环境下作业；

（2）使用具备一定危险度的生产设备和生产资料作业；

（3）生产的产品因为在安全属性方面具有质量缺陷。

生态安全关注企业的上下游供应链和合作伙伴，包括供应链和合作伙伴交付的产品与服务导致的生产安全问题，以及供应链和合作伙伴在合作中获取的信息和数据的安全。

数据安全关注企业生产数据的各个环节的安全、敏感数据泄露、数据隐私被侵犯等。具体讲，需要关注下面三个场景下的数据安全：

（1）数据包含了敏感或个人隐私信息，因此数据在价值挖掘使用和发布的场景中可能会给个人、第三方和国家带来危害和损失，因此对隐私和重要数据的处理、使用、操作、发布、交换等生产流通环节都有安全与合规的要求；

（2）数据需要多方的多维度融合才能创造价值，但往往每方都有自己数据的产权保护、个人数据和重要数据的合规责任，因此需要更安全的数据融合环境；

（3）生产数据的每个环节需要相应的安全控制。

5.4 建设维度

建设维度主要阐释了工业互联网的平台、网络、标识系统所涉及到的供应链安全、数据安全、设备安全、控制安全、网络安全、应用安全以及安全管理。

《网络安全法》第三十三条要求“保证安全技术措施同步规划、同步建设、同步使用”。所以工业互联网的设备安全、控制安全、网络安全、应用安全、数据安全、供应链安全、安全管理等安全技术措施建设需要做到“三同步原则”。

数据安全方面，一是需要关注和确保数据在采集、分析、利用等方面的安全，二是工业模型和数据模型的安全，三是数据在企业间、企业内共享安全等。

供应链安全是工业互联网安全建设过程中非常重要的功能模块。一个典型的工业互联网系统是由多个系统、组件构建而成，系统的可靠性取决于对所有组件的信任、如何集成以及它们如何相互作用。“信任渗透”是指信任在一个系统中从整体使用到所有组件的层次流动。每个系统都有独特的信任渗透。每个元素都有参与者（设计人员、开发人员、制造商、操作员等），他们在创建、集成和使用系统的硬件和软件时执行各种角色。

工业互联网安全建设涉及三类角色：

（1）组件制造商：是硬件供应商、软件发布者和服务发布者，他们提供特定的功能作为标准化的产品或服务；

（2）系统构建者：是系统集成商和解决方案提供者，他们在特定于使用的单个解决方案或服务功能中集成或调整这些构建的组件；

（3）操作用户：是系统所有者/操作员，他们将组件、解决方案或服务用于预期的目的。

信任渗透贯穿整个系统生命周期，从供应链、试运行、供应、运行使用到退役，每个环节和每个角色都必须仔细监控，以确保最初的可信度始终保持不变。

5.5 安全能力

安全能力维度描述了企业通过工业互联网实现业务发展目标所需构建的核心安全能力。能力层主要面向工程师等具体技术人员，帮助其定义企业所需的关键能力并开展实践。

（1）结构安全：是在 IT 与 OT 环境中的基础设施结构组件和应用系统中嵌入/实现的安全能力。具体包括网络分区分域、系统安全（资产、配置、漏洞、补丁管理）、应用开发安全、身份与访问、数据安全、日志采集等。其主要防御意图是收缩 IT 与 OT 环境各个层面的攻击暴露面。

（2）纵深防御：是以层次化方式部署的附加在网络、平台、标识、应用环境等基础架构之上的相对静态、被动、外挂式的安全能力。具体包括工控系统防护、网络边界防护、云边界防护、终端安全防护等。通常无需人员持续介入，其防御思想是通过层次化防御，逐层收缩攻击暴露面来消耗攻击者资源，以阻止中低水平攻击者的攻击活动。

（3）积极防御：是强调持续监控的更加积极、主动、动态的结构化安全能力。具体包括日志聚合、安全事件关联分析、安全编排与自动化等安全能力。通常需要安全分析人员依托托态势感知平台进行安全事件的分析、研判和响应处置。其防御思想是通过体系化监控，及时发现和阻止高级与未知威胁。

（4）威胁情报：是强调引入企业外部威胁情报信息以增强对企业内部网络威胁的识别、理解和预见性的安全能力。具体包括情报收集、情报生产、情报使用、情报共享等安全能力。它既包括引入企业外部威胁情报，也包括生产加工企业内部威胁情报。其防御思想是通过扩大威胁视野（即从企业内部转向企业外部），填补已知威胁的知识缺口并驱动积极防御过程，为更全面及时地发现和阻止高级与未知威胁提供决策支持。

（5）反制进攻：是以自卫为目的针对网络攻击者采取合法反制措施和网络反击行动的能

力。具体包括攻击取证与溯源、攻击链分析、网络渗透等攻击性网络安全能力。其防御思想是采用进攻方式达成防御效果。

这五大能力具体体现在：系统安全可控、日常运维可管、业务安全可信、合规配置可查、安全威胁可防、攻击事件可溯、安全态势可视、情报分析可享八大细分能力。

按照上述工业互联网安全发展愿景、推进方向与业务需求，企业在数字化转型过程中需构建系统安全可控、日常运维可管、业务安全可信、合规配置可查、安全威胁可防、攻击事件可溯、安全态势可视、情报分析可享等工业互联网安全能力，以支撑企业在不同场景下的具体应用实践。具体来说：

一是，构建工业互联网的所有系统组件自身要安全可控；

二是，工业互联网的平台、网络、标识系统日常运维要自主管控；

三是，工业互联网所承载的业务系统自身安全并且可信；

四是，工业互联网平台、网络、标识系统符合国家网络安全相关法律、法规、政策，是否合规要能够自查和审计；

五是，能够就针对工业互联网的安全风险进行评估与排查，安全威胁进行检测、保护、预警与响应处置，以尽可能减少风险与损失；

六是，针对发生的攻击事件可以审计与追溯，以防范再次发生；

七是，能够实现工业企业的安全状态全面呈现，安全风险与威胁趋势可预测；

八是，企业既能够借助第三方威胁情报以提升自身安全防护能力，又能够在企业内部和外部共享威胁情报成果。

第六章 安全功能视图

6.1 工业互联网安全特殊性

历史上，工业系统的安全性依赖于物理隔离和网络隔离。工业系统的设计者和运营者并未考虑到这些系统有一天会暴露在一个全球网络中。在过去的几十年里，越来越便宜的计算能力、无处不在的连接性和不断发展的数据分析技术为控制系统、业务系统和互联网的融合打开了大门。最初融合的规模很小，主要在系统的远程监控和管理方面，但很快扩展到挖掘和分析

操作数据、优化性能、故障预测和远程维护等方面。这种融合提高了现有操作流程的生产率、工作效率和性能，并创造了利用操作数据的新方法，从而在现在和将来提供业务价值。但在获得这些收益的同时也带来了安全风险。最初设计为隔离的系统现在暴露在日益复杂的攻击中，因此原有的制造 OT 系统的设计假设不再适用。对工业系统的成功攻击有可能与严重的工业事故一样严重，造成环境破坏、人员伤亡。在这种攻击中，还存在二次损坏的风险，例如泄露敏感数据、中断操作和破坏系统。对工业系统的攻击结果可能是广泛的，与大型自然灾害相当，但源于恶意意图。这将导致品牌和声誉受损、物质经济损失和潜在损害关键基础设施。因此企业和国家必须要重视这些安全风险，并尽可能确保工业互联网系统安全可信。

工业互联网使原来封闭的工业系统走向开放，IT 系统与 OT 系统走向融合成为必然趋势，因此工业互联网安全最终要满足如下目标：

（1） 功能安全 Safety：功能安全强调一个系统、组织或个人按照自己的机制正常运转的“稳定状态”；

（2） 弹性 Resillience；

（3） 隐私保护 Privacy；

（4） 可靠性 Reliability；

（5） 信息安全 Security：信息安全强调采取必要的措施，免受来自外部或内部“蓄意或恶意”的伤害，确保国家、组织或系统的正常运转。

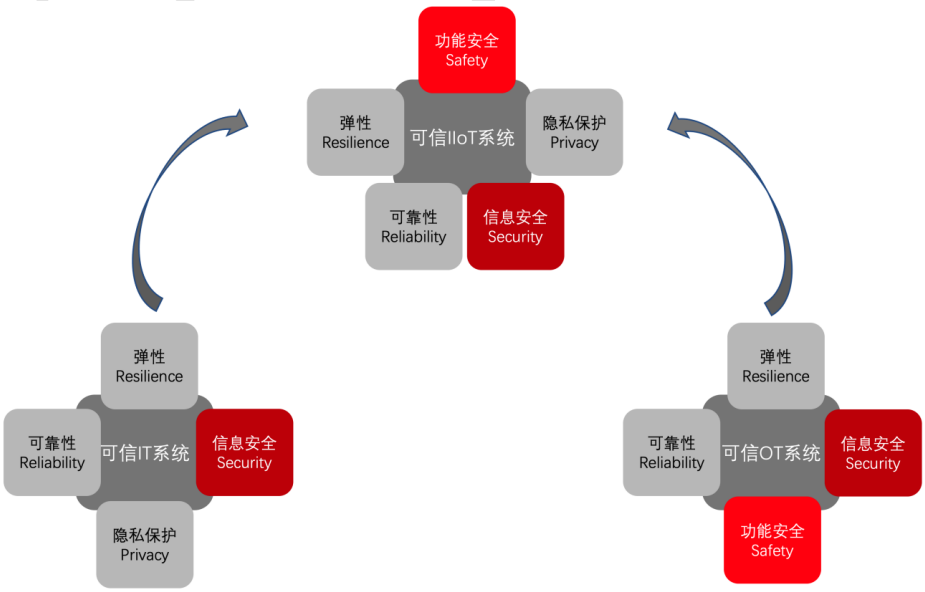

图 6-1 可信 IT 系统、OT 系统融合视图

如何构建工业互联网安全功能是企业、产业以及各个国家的关注重点。工业互联网主要由工业制造 OT 系统和信息 IT 系统构成，在设计工业互联网安全架构之前，首先需要了解 IT 系统与 OT 系统存在的不同之处：

（1） 保护对象不同

传统安全保护的是服务器、个人计算终端（PV、笔记本电脑、手机等），而工控安全保护的是工业控制设备（PLC、SCADA、DCS 及配套上位机、工作站）。

（2） 行业应用的专业性差异

不同的工业场景，工控系统的应用方式区别较大，不同的工控系统、以及相同类工控系统但不同厂家设备，都有较大的差别。例如同样是油气场景，炼化是 DCS、管道是 SCADA、销售终端是 PLC，都不一样；同样是 PLC，西门子、施耐德、GE 的协议就不一样，DCS 也类似。

（3） 工业协议的不同

工业协议大部分是私有协议，如西门子的 S7、GE 的 SRTP 等，都需要深度识别并适配，需要对工业场景和工业协议有深度的理解。

（4） 产生问题造成的后果的不同

传统安全设备一旦出问题，造成的后果是信息丢失或损坏、个人资产被转移、通讯不畅等；而工控系统则不同，由于工控系统广泛应用于国计民生的各个方面，如城市供电供水供气、交通控制、楼宇自动控制、生产制造。一旦出问题，轻则生产停滞造成巨大经济损失，重则城市生活陷于瘫痪、甚至危及生命，后果非常严重。

（5） 设备的操作管理人员不同

传统安全设备的操作对象是 IT 管理人员，大部分具有较好的 TCP/IP 系统的策略配置能力，可以配置较复杂安全规则；而工控安全的操作人员是工业自动化操作人员，不熟悉 IT 操作，所以工控安全设备的操作界面需要非常简单，便于操作。

（6） 工作环境的不同

传统 IT 安全设备一般安装在机房里，恒温恒湿；工控系统则很可能安装在工业现场，会有高温、低温、灰尘等情况，所以要求工控安全设备都是宽温（-40 度到 80 度）、全封闭机箱。

同时 OT 与 IT 两个领域还存在如下不同的特性：

① 在 IT 与 OT 领域从业人员的思维模式不一样：IT 人更喜欢从上向下来分析问题和解决问题；而 OT 人则相反，偏向从下向上，从单点分析和解决问题出发；

② 安全事件造成的损失影响不一样：IT 安全事件造成的损失影响一般情况下还是可以承受的；而 OT 安全事件可能会导致生命、财产、金钱的损失，影响巨大；

③ 安全防护技术不一样：IT 安全防护技术更多是发现和补漏洞；OT 安全防护更多是隐藏漏洞，用虚拟补丁方式让漏洞不被利用；

④ 对安全防护产品的要求不一样：IT 安全产品更多要求做到可视、可管、可控；而 OT 安全产品更多要求做到直接、智能、自动；

⑤ 市场需求认知和重视度不一样：IT 安全已经发展了 20 年，重视和认知度都很高，OT 现场普遍缺少信息安全专家、信息安全责任人或部门；

⑥ 市场需求认知和重视度不一样：IT 安全已经发展了 20 年，重视和认知度都很高，OT 现场普遍缺少信息安全专家、信息安全责任人或部门。

工业互联网还需要面临多种异构网络和海量通信主体接入互联网、天空海地融合的万网互联等场景，因此工业互联网安全需要确保端到端的业务安全可信和网络基础设施安全可信。

6.2 总体功能视图

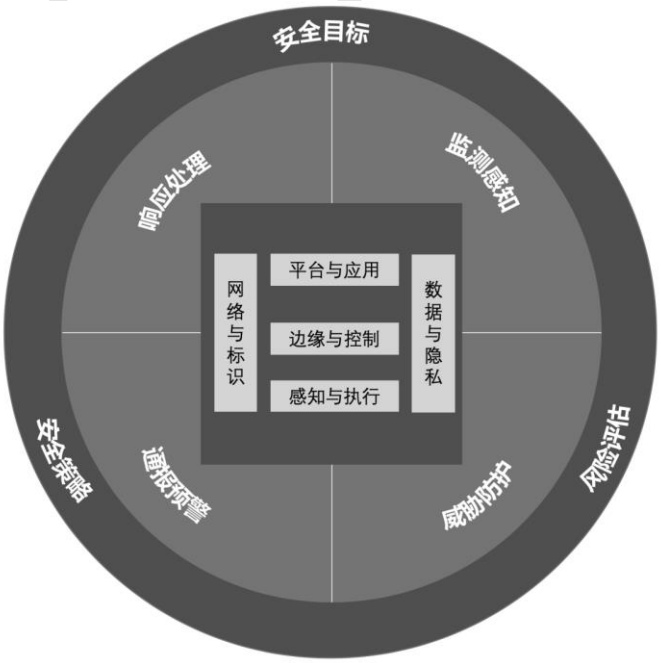

图 6-2 总体功能视图

工业互联网安全功能框架充分考虑了信息安全、功能安全和物理安全，聚焦工业互联网安全所具备的主要特征，包括可靠性、保密性、完整性、可用性、隐私和数据保护。该框架包括防护对象、防护措施和安全管理三个维度。

6.3 防护对象维度

如果我们参照工业 4.0 的核心概念 CPS 来理解工业互联网，工业互联网安全防护对象至少包括 CPS 的 6C：计算 Computing、通信 Communication、控制 Control、上下文 Content、社群 Community、定制化 Customization。如果将 6C 映射到 IT 与 OT 系统，则工业互联网安全防护对象包括感知与执行、边缘与控制、网络与标识、平台与应用、数据与隐私五大防护对象，如图 6-3 所示。

图 6-3 工业 4.0 核心概念 CPS

（1） 感知与执行设备安全

感知与执行设备包括工业控制设备（PLC、RTU 等）、网络和安全设备（工业交换机、工业防火墙等）、智能终端设备（数采网关、视频监控设备及其他物联网相关设备）等智能设备。其安全指围绕工业环境的适用性、硬件安全、系统/固件安全、应用安全、数据安全、接入安

全等。设备安全体现在抗渗透能力、恶意代码防范、抗 DDoS 能力、漏洞隐患情况等方面，可能存在未授权访问、恶意控制、数据窃取以及性能下降或系统崩溃等安全隐患。

（2） 边缘与控制安全

包括控制协议安全、控制软件安全以及控制功能安全。

（3） 网络与标识安全

包括承载工业智能生产和应用的工业控制网络、企业与园区网络、骨干网络及标识解析系统等的安全。

（4） 平台与应用安全

包括工业互联网平台安全与工业应用程序安全。

（5） 数据与隐私安全

包括涉及采集、传输、存储、处理等各个环节的数据以及用户信息的安全。

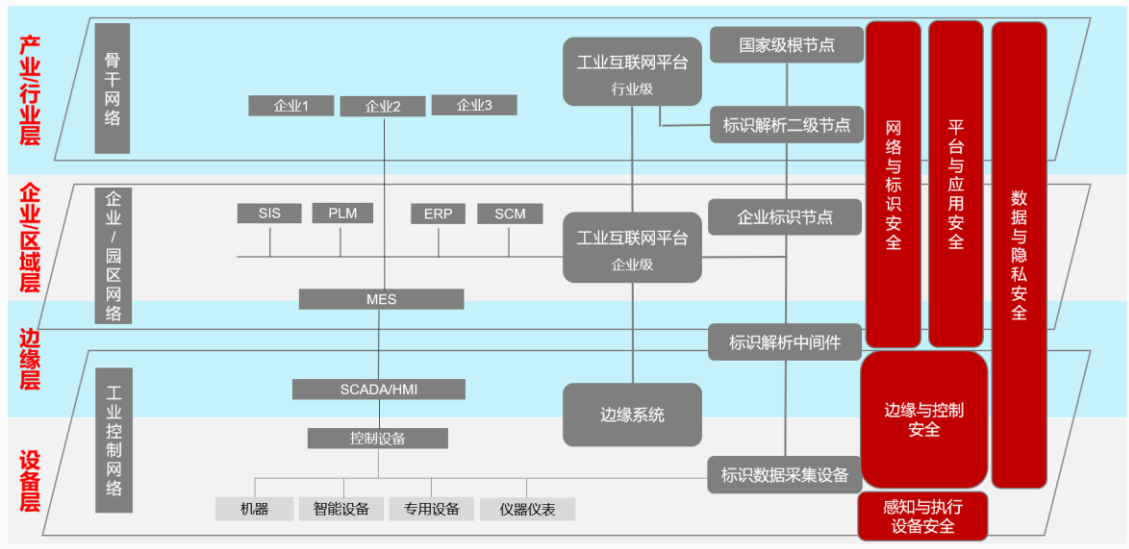

图 6-4 五大防护对象维度

6.4 防护措施维度

总体防护措施框架

工业互联网的核心功能原理是基于数据驱动的物理系统与数字空间全面互联与深度协同，以及在此过程中的智能分析与决策优化。同理，工业互联网安全基于数据整合与分析实现监测感知、威胁防护、预警通报、响应处置四大环节。

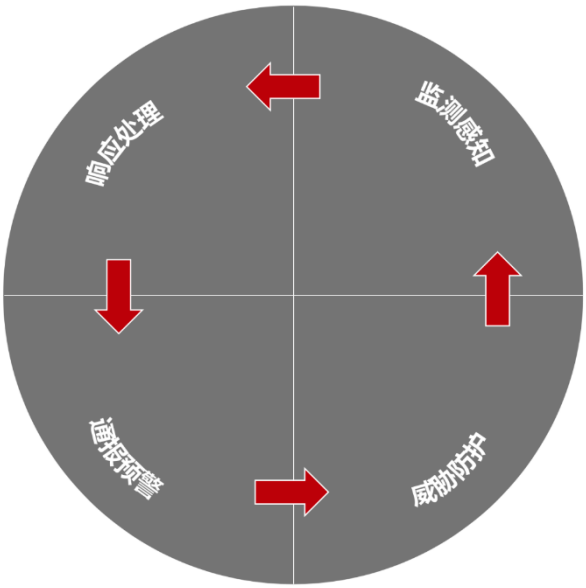

图 6-5 总体防护措施框架

工业互联网安全以数据为核心，包含安全态势感知控制、安全防护数字模型、安全决策优化三个基本层次，以及一个由自下而上的信息流和自上而下的决策流构成的工业安全防护优化闭环。

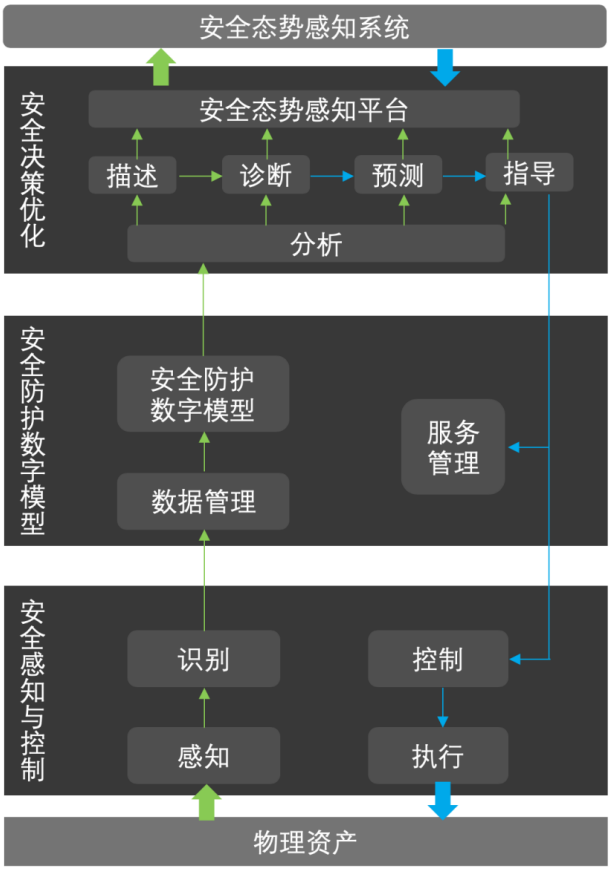

图 6-6 工业互联网基于数据整合与分析的防护措施框架

（1） 安全态势感知控制层

构建安全态势的底层“输入-输出”接口，包含感知、识别和控制、执行四类功能。

① 感知：是利用各类软硬件方法采集蕴含了资产属性、状态及行为等特征的数据，例如用温度传感器采集电机运行中的温度变化数据；

② 识别：是在数据与资产之间建立对应关系，明确数据所代表的对象，例如需要明确定义哪一个传感器所采集的数据代表了特定电机的温度信息；

③ 控制：是将预期目标转化为具体控制信号和指令，例如将工业机器人末端运动转化各个关节处电机的转动角度指令信号；

④ 执行：是按照控制信号和指令来改变物理世界中的资产状态，既包括工业设备机械、电气状态的改变，也包括人员、供应链等操作流程和组织形式的改变。

（2） 安全防护数字模型层

强化数据、知识、资产等的虚拟映射与管理组织，提供支撑安全态势感知的基础资源与关键工具，包含数据集成与管理、安全防护数据模型构建、信息交互三类功能。数据集成与管理将原来分散、杂乱的海量多源异构数据整合成统一、有序的新数据源，为后续分析优化提供高质量数据资源，涉及到数据库、数据湖、数据清洗、元数据等技术产品应用。安全防护数据模型构建是综合利用大数据、人工智能等数据方法和物理、化学、材料等各类工业经验知识，对资产行为特征和因果关系进行抽象化描述，形成各类模型库和算法库。信息交互是通过不同资产之间数据的互联互通和模型的交互协同，构建出覆盖范围更广、智能化程度更高的“系统之系统”。

（3） 安全决策优化层

聚焦数据挖掘分析与价值转化，形成安全态势感知核心功能，主要包括分析、描述、诊断、预测、指导及应用开发。

① 分析功能：借助各类模型和算法的支持将数据背后隐藏的规律显性化，为诊断、预测和优化功能的实现提供支撑，常用的数据分析方法包括统计数学、大数据、人工智能等；

② 描述功能：通过数据分析和对比形成对当前现状、存在问题等状态的基本展示，例如

在数据异常的情况下向现场工作人员传递信息，帮助工作人员迅速了解问题类型和内容；

③ 诊断功能：主要是基于数据的分析对资产当前状态进行评估，及时发现问题并提供解决建议，例如能够在数控机床发生故障的第一时间就进行报警，并提示运维人员进行维修；

④ 预测功能：是在数据分析的基础上预测资产未来的状态，在问题还未发生的时候就提前介入，例如预测风机核心零部件寿命，避免因为零部件老化导致的停机故障；

⑤ 指导功能：则是利用数据分析来发现并帮助改进资产运行中存在的不合理、低效率问题，例如分析高功耗设备运行数据，合理设置启停时间，降低能源消耗。

自下而上的信息流和自上而下的决策流形成了工业互联网安全的优化闭环。其中，信息流是从数据感知出发，通过数据的集成和建模分析，将物理空间中的资产信息和状态向上传递到虚拟空间，为决策优化提供依据。决策流则是将虚拟空间中决策优化后所形成的指令信息向下反馈到控制与执行环节，用于改进和提升物理空间中资产的功能和性能。优化闭环就是在信息流与决策流的双向作用下，连接底层资产与上层业务，以数据分析决策为核心，形成面向不同工业场景的工业互联网安全态势感知解决方案。

监测感知

监测感知是指部署相应的监测措施，主动发现来自系统内外部的安全风险，具体措施包括数据采集、收集汇聚、特征提取、关联分析、状态感知等。

（1） 数据采集

数据采集指对工业现场网络及工业互联网平台中各类数据进行采集，为网络异常分析、设备预测性维护等提供数据来源。

（2） 收集汇聚

对于数据的收集汇聚主要分为两个方面。一是对 SCADA、MES、ERP 等工业控制系统及应用系统所产生的关键工业互联网数据进行汇聚，包括产品全生命周期的各类数据的同步采集、管理、存储及查询，为后续过程提供数据来源；二是对全网流量进行监听，并将监听过程中采集到的数据进行汇聚。

（3） 特征提取

特征提取是指对数据特征进行提取、筛选、分类、优先级排序、可读等处理，从而实现从数据到信息的转化过程，该过程主要是针对单个设备或单个网络的纵向数据分析。信息主要包括内容和情景两方面，内容指工业互联网中的设备信号处理结果、监控传输特性、性能曲线、健康状况、报警信息、DNC 及 SCADA 网络流量等情景指设备的运行工况、维护保养记录、人员操作指令、人员访问状态、生产任务目标、行业销售机理等。

（4） 关联分析

关联分析基于大数据进行横向大数据分析和多维分析，通过将运行机理、运行环境、操作内容、外部威胁情报等有机结合，利用群体经验预测单个设备的安全情况，或根据历史状况和当前状态的差异进行关联分析，进而发现网络及系统的异常状态。

（5） 状态感知

状态感知基于关联分析过程，实现对工业互联网相关企业网络运行规律、异常情况、安全目标、安全态势、业务背景等的监测感知，确定安全基线，结合大数据分析等相关技术，发现潜在安全威胁、预测黑客攻击行为。

威胁防护

威胁防护措施针对五大防护对象，部署主被动防护措施，阻止外部入侵，构建安全运行环境，消减潜在安全风险。

威胁防护措施主要包括：

（1） 设备安全：主要指接入工业互联网的终端设备的安全，重点是加强设备自身安全、完善终端接入安全认证。

（2） 控制安全：主要指 PLC、SCADA、DCS 等工业控制系统安全，一方面要提升自主可控工控系统比例，另一方面要解决控制系统在生产设计时缺少安全考虑这一“先天”问题。

（3） 平台安全：主要指工业 IaaS、PaaS、SaaS 的安全，重点是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。

（4） 数据安全：主要指工业生产业务活动中产生、采集、处理、存储、传输和使用的数据安全，要建立工业数据分级分类管理制度，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。

（5） 网络安全：主要指工业企业管理网、控制网和外网的安全，要做好网络安全态势感知，确保传输安全和运行安全。

在 OT 与 IT 融合趋势下，威胁防护需要做到：

（1） OT 与 IT 检测引擎一体化；

（2） OT 与 IT 入侵特征库一体化；

（3） OT 与 IT 防护功能一体化。

通报预警

通报预警监测感知到的安全威胁及时告警并通报到相关人。

网络安全通报预警需要结合具体业务要求、等级保护的要求及其他法律法规的要求，通常工作信息量大、任务繁重、时间紧迫。所面临的主要问题还是缺乏自动化、标准化、流程化、智能化的电子工具。

网络安全通报预警需以网络安全事件通报、等级保护为核心，对企事业、成员单位及其信息系统的安全事件、等保等情况进行汇总、管理，包括信息系统信息管理、安全通报、安全事件处置、安全年度检查、安全考核评分、知识库等。以模板定制、在线上报、事件工单、自动统计分析等形式，将网络安全工作、等级保护工作融入日常信息安全管理工作中，有效促进各行业网络安全工作简洁化、自动化、智能化和常态化。实现网上报送系统，保障信息安全情况能够及时、有效地得到统一收集、汇总，并定期在系统上公布一些信息安全情况和信息安全事件，将网络安全工作人员从重复的繁琐的统计、汇总、督促、检查、盯梢等工作中解放出来，降低网络安全人员工作量，减少人力投入，提升网络安全通报预警的效率。

响应处置

响应处置措施建立响应恢复机制，及时应对安全威胁，并及时优化防护措施，形成闭环防御。

处置恢复机制是确保落实工业互联网信息安全管理，支撑工业互联网系统与服务持续运行的保障。通过处置恢复机制，在风险发生时灾备恢复组织能根据预案及时采取措施进行应对，及时恢复现场设备、工业控制系统、网络、工业互联网平台、工业应用程序等的正常运行，防止重要数据丢失，并通过数据收集与分析机制，及时更新优化防护措施，形成持续改进的防御闭环。处置恢复机制主要包括响应决策、备份恢复、分析评估等。

（1） 响应决策

对于工业互联网灾难恢复过程中的决策与响应，需预先制定相应的处置策略，针对不同风险等级制定相应预案措施。处置恢复工作需要在处置恢复组织的领导下进行，通过实时监测工

业互联网系统各类数据，在突发灾难时通过相应机制进行应对。

① 处置恢复组织架构

- 处置恢复规划领导组：是实施处置恢复规划工作的组织领导机构，应由单位高层领导担任组长，领导和决策处置恢复规划中的重大事宜。
- 处置恢复现场实施组：负责对处置恢复工作进行需求分析、规划并确立处置恢复策略，制订处置恢复预案。
- 处置恢复日常运行组：负责灾难备份中心日常管理，处置恢复预案的教育、培训、演练、维护和管理，突发事件发生时的损失控制和损害评估，灾难发生后恢复技术支持及外部协作等。

② 灾难风险分析与管理

工业互联网较传统信息系统架构更为复杂，处置恢复组织应根据工业互联网系统架构进行风险识别，并对风险按照类别与等级、风险影响程度、风险发生几率和风险时长等因素进行评估，依照风险处置优先级别制定防范措施与解决预案，将实际情况与之进行匹配，并进行适当的调整以满足实施的有效性。

③ 灾难数据监测

工业互联网系统架构包括多个层级与数据接口，针对可能发生的风险所在的层级，应采取相应的措施降低灾难发生的几率。处置恢复日常运行组可以通过对设备层、网络层、控制层、应用层、数据层等部署监测机制，对工业互联网系统运行中的数据状态进行定期监测，感知潜在的安全风险与系统异常，由处置恢复实施组通过恢复策略进行相应处置。

④ 灾难恢复决策

应建立灾难恢复的处理决策与异常处置规则，当发生突发灾难事件时，若灾难事件超出解决范围或响应时间过长，处置恢复实施组应遵循规则向上级组织进行汇报与处理。针对异常的灾难恢复事件，处置恢复领导小组应召集专业人员评估突发事件，确认突发事件对工业互联网系统造成的影响程度，进而确定下一步采取的措施，并将最新信息通知给处置恢复实施组，确保处置恢复工作的及时性。

⑤ 灾难恢复响应

应建立灾难恢复的响应规则，在事件发生时，处置恢复实施组收到处置恢复领导小组的决策后根据相应的处置恢复策略及时做出响应，迅速进行灾难恢复工作。当处置恢复实施组无法

进行响应或响应时间过长时，应及时向处置恢复领导小组进行汇报，保障灾难恢复工作的持续性。

（2） 备份恢复

为确保工业互联网平台持续运作，应对重要系统进行灾难备份。企业应根据系统备份能力进行分级，按需求目标制订相应的备份恢复预案。为确保备份恢复预案顺利进行，企业可建立专门的灾难备份中心与处置恢复组织，根据处置恢复策略进行维护管理，并定期进行灾难恢复预案演练，确保预案的有效性。

① 备份能力等级的定义

根据企业不同的业务类型与系统特点，对备份能力等级进行划分，依照等级的不同采取不同的备份策略与应对措施。

② 备份能力的需求确立

企业通过对其业务影响程度的分析与风险评估，确定工业互联网系统的备份能力等级需求及备份前所需的资源。

③ 备份恢复策略制定

依据企业现有的或行业通用规范准则制定适合自身的备份恢复策略，有条件的情况下可对制定的策略进行有效性与实用性方面的验证。

④ 灾难备份中心的建设、运行和维护管理

有条件的企业可建立专门的灾难备份中心，在灾难发生时迅速进行备份恢复工作，确保将损害降到最低。企业根据业务需求成立专职的或兼职的灾难备份中心的运行和维护管理团队，进行日常维护或危机处理。

⑤ 处置恢复预案的演练与管理

企业应定期对制定的处置恢复计划进行验证及防灾演习，来不断适应环境或技术的变化，确保计划的有效性。

（3） 分析评估

分析评估风险是工业互联网系统优化防护措施、形成闭环防御不可缺少的一个重要环节。通过分析识别系统面临的风险来制定相应的响应预案，并依据安全事件处理评估结果进行持续修正，从而达到改进处置恢复策略的目的。

① 风险分析

企业可采用定性或定量的分析方法对安全事件造成的各种影响进行等级判断：

- 定量分析：以量化方法，评估业务功能的中断可能给企业带来的直接经济损失和间接经济损失。
- 定性分析：运用归纳与演绎、分析与综合以及抽象等方法评估业务功能的中断可能给企业带来的非经济损失，包括企业声誉、顾客忠诚度、社会与政治影响等。

② 风险定义与预案制定

通过对工业互联网系统面临的内外部风险进行识别和定义，结合企业自身安全框架分析评估风险发生的可能性，从而制定适合企业自身需要的处置恢复机制。

③ 处置恢复效果评估

当企业发生安全事件后，要及时分析事件的影响范围与程度，评估企业处置恢复方案的适用性与有效性。

④ 处置恢复方案改进

通过分析结果，对工业互联网系统面临的风险进行确认，分析总结此次事件处置恢复所消耗的资源成本以及风险造成的损失，检验处置恢复预案的落实与管理是否符合处置恢复目标的要求，并通过实际案例的处理经验不断改进处置恢复准则。

6.5 防护管理维度

防护管理维度的设立，旨在指导企业构建持续改进的安全防护管理方针，在明确防护对象及其所需要达到的安全目标后，对于其可能面临的安全风险进行评估，找出当前与安全目标之间存在的差距，制定相应的安全防护策略，提升安全防护能力，并在此过程中不断对管理流程进行改进。

安全目标

为确保工业互联网的正常运转和安全可信，应对工业互联网设定合理的安全目标，并根据相应的安全目标进行风险评估和安全策略的选择实施。工业互联网安全目标并非是单一的，需要结合工业互联网不同的安全需求进行明确。工业互联网安全包括保密性、完整性、可用性、可靠性、弹性和隐私安全六大目标，这些目标相互补充，共同构成了保障工业互联网安全的关键特性。

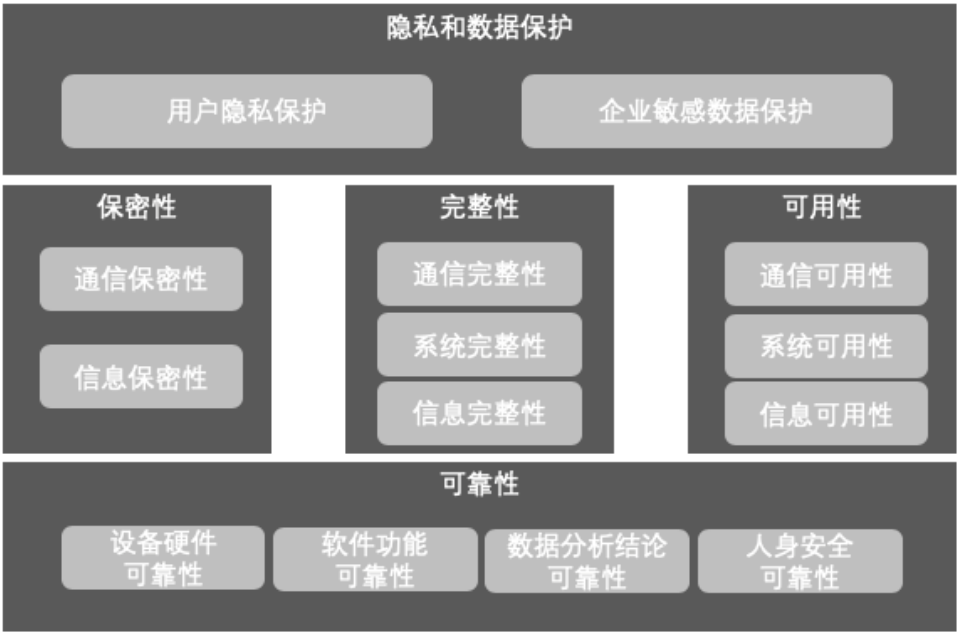

图 6-7 工业互联网安全目标

（1） 保密性：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体；

（2） 完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性；

（3） 可用性：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠、及时地访问信息及资源；

（4） 可靠性：确保工业互联网系统在其寿命区间内以及在正常运行条件下能够正确执行指定功能；

（5） 弹性：确保工业互联网系统在受到攻击或破坏后恢复正常功能；

（6） 隐私安全：确保工业互联网系统内用户的隐私安全。

风险评估

所谓风险，即不确定性对目标的影响，考虑的是一个事件发生的可能性以及该事件发生后的影响。由于不可能消除系统中的所有风险，因此我们必须管理风险，在安全投资与不良后果的影响之间做平衡。

为管控风险，必须定期对工业互联网系统的各安全要素进行风险评估。对应工业互联网整体安全目标，分析整个工业互联网系统的资产、脆弱性和威胁，评估安全隐患导致安全事件的可能性及影响，结合资产价值，明确风险的处置措施，包括预防、转移、接受、补偿、分散等，确保在工业互联网数据私密性、数据传输安全性、设备接入安全性、平台访问控制安全性、

平台攻击防范安全性等方面提供可信服务，并最终形成风险评估报告。

安全风险可以通过多种方式解决：

（1） 风险规避：试图完全消除风险，以避免所有的风险。通常，完全的风险规避只能通过删除导致风险的功能来实现；

（2） 风险缓解：实施补偿措施以减少不可避免的威胁的影响。当风险规避无法实现时，缓解是最适用的策略；

（3） 风险转移：风险由第三方接受并支付。转移风险是高影响、低频率事件的常见技术，这些事件的缓解成本往往高得令人无法接受；

（4） 接受风险：当缓解措施的成本超过不利事件的成本时（如果发生不利事件），通常采用这种策略。

剩余风险是在所有应对措施实施后仍然存在的风险。当所有已知的漏洞被删除后，仍然存在未知的漏洞。由于对系统安全性或可信人员的错误假设，风险可能仍然存在。必须跟踪剩余风险，以确定附加的安全操作的优先级，证明所做的安全选择的合理性，并确定何时在安全控制的成本与有效性之间取得平衡。

安全策略

工业互联网安全防护的总体策略，是要构建一个能覆盖安全业务全生命周期的，以安全事件为核心，实现对安全事件“预警、监测、处置、防护”动态的防御体系。能够在攻击发生前进行有效的预警和防护，在攻击中进行有效的攻击检测，在攻击后能快速定位故障，进行有效响应，避免实质损失的发生。

工业互联网系统制造商、系统集成商、所有者和操作人员应该建立和维护一个安全策略，为组织的安全活动提供治理、规划和支持。安全风险以及安全投资成本和收益必须告知业务决策者，以便于有效决策。

此安全策略必须确保企业在工业互联网方面的投资免受损害。这些损害包括生产中断、系统被破坏以及泄露敏感的业务和个人数据，从而导致知识产权的损失、商业声誉的损害以及客户的损失。当然，加强安全可能会带来更多的投资和更长的部署时间，因此可能会对用户体验产生负面影响。这些额外的成本必须通过利益相关者所承担的业务风险和避免损害所节省的成本来证明其合理性。

安全策略中描述了工业互联网总体的安全考虑，并定义了保证工业互联网日常正常运行

的指导方针及安全模型。通过结合安全目标以及风险评估结果，明确当前工业互联网各方面的安全策略，包括对设备、控制、网络、应用、数据等防护对象应采取的防护措施，监测响应及处置恢复措施等。同时，为打造持续安全的工业互联网，面对不断出现的新的威胁，需不断完善安全策略。

第七章 安全实施视图

7.1 安全实施总体框架

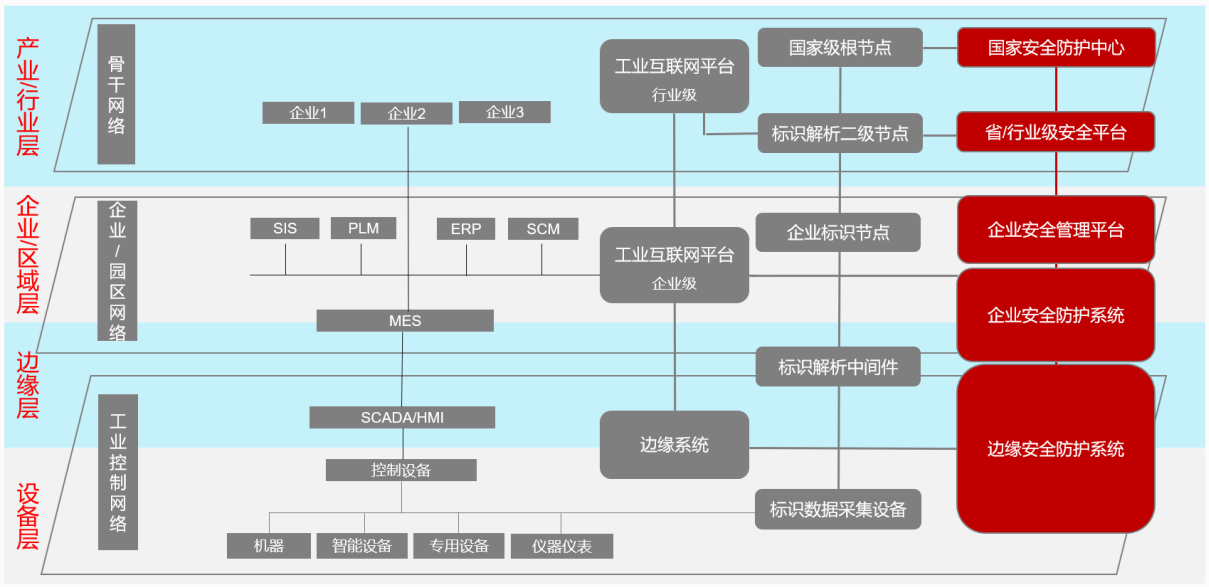

图 7-1 安全实施总体框架

根据 Saltzer 和 Schroeder，实施者在为其工业互联网实施安全功能之前，应遵循八个设计原则：

（1） 经济性原则：尽量保持设计简单、小巧；

（2） 设置故障安全原则：出现故障或错误时，系统仍维持在安全状态运行或过渡到另一种安全状态；

（3） 完全调解原则：必须检查每个对象的每个访问的权限；

（4） 开放设计原则：设计不应是秘密的。这种机制不应依赖于对潜在攻击者的无知，而应依赖于拥有特定的、更容易保护的密钥或密码；

（5） 特权分离原则：在可行的情况下，需要两个密钥才能解锁的保护机制比只允许访问

一个密钥的机制更为健壮和灵活；

（6） 最小权限原则：系统的每个程序和每个用户都应使用完成任务所需的最小权限集进行操作；

（7） 最小共同机制原则：尽量减少一个以上用户共同使用并由所有用户依赖的机制数量；

（8） 心理可接受性原则：人机界面的设计必须便于使用，以便用户能够正常、自动地正确应用保护机制。

美国国土安全部（DHS）的工业控制系统紧急应变小组（ICS-CERT）发布了有效防御工业控制系统的 7 项措施，98%的安全事件可以避免：

（1） 建置应用程序白名单，可以缓解 38%的问题；

（2） 确保正确配置与管理补丁，可以缓解 29%的问题；

（3） 降低易受攻击面，可以缓解 17%的问题；

（4） 建立可防御的环境，可缓解 9%问题；

（5） 认证管理，可缓解 4%问题；

（6） 远程访问控制，可缓解 1%问题；

（7） 监测与响应机制，可缓解 2%问题。

7.2 边缘安全防护系统实施

边缘安全防护系统致力于面向实体实施分层分域安全策略，构建多技术融合安全防护体系，从而实现边缘安全防护。部署的关键在于确保工业互联网边缘侧的设备安全、控制安全、网络安全。

边缘安全防护系统实施需要涵盖安全功能视图中边缘层和设备层的各项功能。首先，保障设备安全，通过采取设备身份鉴别与访问控制、固件安全增强、漏洞修复等安全策略，确保工厂内生产设备、单点智能装备器件与产品，以及成套智能终端等智能设备的安全。其次，保障控制安全，通过采取控制协议安全机制、控制软件安全加固、指令安全审计、故障保护等安全策略，确保控制软件安全和控制协议安全。最后，保障边缘侧网络安全，通过采取通信和传输保护、边界隔离（工业防火墙）、接入认证授权等安全策略，确保生产控制网络、标识解析安全等。

在部署方式上，边缘安全防护系统主要位于设备层和边缘层，具体实施方式如下：

设备安全

可采取设备身份鉴别与访问控制、固件安全增强、漏洞修复等安全策略。设备身份鉴别与访问控制方面，对于接入工业互联网的现场设备，应支持基于硬件特征的唯一标识符，为包括工业互联网平台在内的上层应用提供基于硬件标识的身份鉴别与访问控制能力，确保只有合法的设备能够接入工业互联网并根据既定的访问控制规则向其他设备或上层应用发送或读取数据。固件安全增强方面，工业互联网设备供应商需要采取措施对设备固件进行安全增强，阻止恶意代码传播与运行。工业互联网设备供应商可从操作系统内核、协议栈等方面进行安全增强，并力争实现对于设备固件的自主可控。漏洞修复方面，设备操作系统与应用软件中出现的漏洞对于设备来说是最直接也是最致命的威胁。设备供应商应对工业现场中常见的设备与装置进行漏洞扫描与挖掘，发现操作系统与应用软件中存在的安全漏洞，并及时对其进行修复。

（1） 操作系统/应用软件安全

① 固件安全增强

工业互联网设备供应商需要采取措施对设备固件进行安全增强，阻止恶意代码传播与运行。工业互联网设备供应商可从操作系统内核、协议栈等方面进行安全增强，并力争实现对于设备固件的自主可控。

② 漏洞修复加固

设备操作系统与应用软件中出现的漏洞对于设备来说是最直接也是最致命的威胁。设备供应商应对工业现场中常见的设备与装置进行漏洞扫描与挖掘，发现操作系统与应用软件中存在的安全漏洞，并及时对其进行修复。

③ 补丁升级管理

工业互联网企业应密切关注重大工业互联网现场设备的安全漏洞及补丁发布，及时采取补丁升级措施，并在补丁安装前对补丁进行严格的安全评估和测试验证。

（2） 硬件安全

① 硬件安全增强

对于接入工业互联网的现场设备，应支持基于硬件特征的唯一标识符，为包括工业互联网平台在内的上层应用提供基于硬件标识的身份鉴别与访问控制能力，确保只有合法的设备能

够接入工业互联网并根据既定的访问控制规则向其他设备或上层应用发送或读取数据。此外，应支持将硬件级部件（安全芯片或安全固件）作为系统信任根，为现场设备的安全启动以及数据传输机密性和完整性保护提供支持。

② 运维管控

工业互联网企业应在工业现场网络重要控制系统（如机组主控 DCS 系统）的工程师站、操作员站和历史站部署运维管控系统，实现对外部存储器（如 U 盘）、键盘和鼠标等使用 USB 接口的硬件设备的识别，对外部存储器的使用进行严格控制。同时，注意部署的运维管控系统不能影响生产控制区各系统的正常运行。

控制安全

可采取控制协议安全机制、控制软件安全加固、指令安全审计、故障保护等安全策略。控制协议安全机制方面，为了确保控制系统执行的控制命令来自合法用户，必须对使用系统的用户进行身份认证，未经认证的用户所发出的控制命令不被执行。在控制协议通信过程中，一定要加入认证方面的约束，避免攻击者通过截获报文获取合法地址建立会话，影响控制过程安全。不同的操作类型需要不同权限的认证用户来操作，如果没有基于角色的访问机制，没有对用户权限进行划分，会导致任意用户可以执行任意功能。在控制协议设计时，应根据具体情况，采用适当的加密措施，保证通信双方的信息不被第三方非法获取。

控制软件安全加固方面，控制软件的供应商应及时对控制软件中出现的漏洞进行修复或提供其他替代解决方案，如关闭可能被利用的端口等。指令安全审计方面，通过对控制软件进行安全监测审计可及时发现网络安全事件，避免发生安全事故，并可以为安全事故的调查提供详实的数据支持。目前许多安全产品厂商已推出了各自的监测审计平台，可实现协议深度解析、攻击异常检测、无流量异常检测、重要操作行为审计、告警日志审计等功能。

故障保护方面，确定控制软件与其他设备或软件以及与其他智能化系统之间相互作用所产生的危险状况和伤害事件，确定引发事故的事件类型。明确操作人员在对智能化系统执行操作过程中可能产生的合理可预见的误用以及智能化系统对于人员恶意攻击操作的防护能力。智能化装备和智能化系统对于外界实物、电、磁场、辐射、火灾、地震等情况的抵抗或切断能力，以及在发生异常扰动或中断时的检测和处理能力。

（1） 控制协议安全

① 身份认证

为了确保控制系统执行的控制命令来自合法用户，必须对使用系统的用户进行身份认证，未经认证的用户所发出的控制命令不被执行。在控制协议通信过程中，一定要加入认证方面的约束，避免攻击者通过截获报文获取合法地址建立会话，影响控制过程安全。

② 访问控制

不同的操作类型需要不同权限的认证用户来操作，如果没有基于角色的访问机制，没有对用户权限进行划分，会导致任意用户可以执行任意功能。

③ 传输加密

在控制协议设计时，应根据具体情况，采用适当的加密措施，保证通信双方的信息不被第三方非法获取。

④ 健壮性测试

控制协议在应用到工业现场之前应通过健壮性测试工具的测试，测试内容可包括风暴测试、饱和测试、语法测试、模糊测试等。

（2） 控制软件安全

① 软件防篡改

工业互联网中的控制软件可归纳为数据采集软件、组态软件、过程监督与控制软件、单元监控软件、过程仿真软件、过程优化软件、专家系统、人工智能软件等类型。软件防篡改是保障控制软件安全的重要环节，具体措施包括以下几种：

- 控制软件在投入使用前应进行代码测试，以检查软件中的公共缺陷；
- 采用完整性校验措施对控制软件进行校验，及时发现软件中存在的篡改情况；
- 对控制软件中的部分代码进行加密；
- 做好控制软件和组态程序的备份工作。

② 认证授权

控制软件的应用要根据使用对象的不同设置不同的权限，以最小的权限完成各自的任务。

③ 恶意软件防护

对于控制软件应采取恶意代码检测、预防和恢复的控制措施。控制软件恶意代码防护具体措施包括：

- 在控制软件上安装恶意代码防护软件或独立部署恶意代码防护设备，并及时更新恶意代码软件和修复软件版本和恶意代码库，更新前应进行安全性和兼容性测试。防护软件包括病毒防护、入侵检测、入侵防御等具有病毒查杀和阻止入侵行为的软件；防护设备包括防火墙、网闸、入侵检测系统、入侵防御系统等具有防护功能的设备。应注意防止在实施维护和紧急规程期间引入恶意代码。
- 建议控制软件的主要生产厂商采用特定的防病毒工具。在某些情况下，控制软件的供应商需要对其产品线的防病毒工具版本进行回归测试，并提供相关的安装和配置文档。
- 采用具有白名单机制的产品，构建可信环境，抵御零日漏洞和有针对性地攻击。

④ 补丁升级更新

控制软件的变更和升级需要在测试系统中经过仔细的测试，并制定详细的回退计划。对重要的补丁需尽快测试和部署。对于服务包和一般补丁，仅对必要的补丁进行测试和部署。

⑤ 漏洞修复加固

控制软件的供应商应及时对控制软件中出现的漏洞进行修复或提供其他替代解决方案，如关闭可能被利用的端口等。

⑥ 协议过滤

采用工业防火墙对协议进行深度过滤，对控制软件与设备间的通信内容进行实时跟踪，同时确保协议过滤不得影响通信性能。

⑦ 安全监测审计

通过对工业互联网中的控制软件进行安全监测审计可及时发现网络安全事件，避免发生安全事故，并可以为安全事故的调查提供详实的数据支持。目前许多安全产品厂商已推出了各自的监测审计平台，可实现协议深度解析、攻击异常检测、无流量异常检测、重要操作行为审计、告警日志审计等功能。

（3） 控制功能安全

要考虑功能安全和信息安全的协调能力，使得信息安全不影响功能安全，功能安全在信息安全的防护下更好地执行安全功能。现阶段功能安全具体措施主要包括：

① 确定可能的危险源、危险状况和伤害事件，获取已确定危险的信息（如持续时间、

强度、毒性、暴露限度、机械力、爆炸条件、反应性、易燃性、脆弱性、信息丢失等）；

② 确定控制软件与其他设备或软件（已安装的或将被安装的）以及与其他智能化系统（已安装的或将被安装的）之间相互作用所产生的危险状况和伤害事件，确定引发事故的事件类型（如元器件失效、程序故障、人为错误，以及能导致危险事件发生的相关失效机制）；

③ 结合典型生产工艺、加工制造过程、质量管控等方面的特征，分析安全影响；

④ 考虑自动化、一体化、信息化可能导致的安全失控状态，确定需要采用的监测、预警或报警机制、故障诊断与恢复机制、数据收集与记录机制等；

⑤ 明确操作人员在对智能化系统执行操作过程中可能产生的合理可预见的误用以及智能化系统对于人员恶意攻击操作的防护能力；

⑥ 智能化装备和智能化系统对于外界实物、电、磁场、辐射、火灾、地震等情况的抵抗或切断能力，以及在发生异常扰动或中断时的检测和处理能力。

控制安全措施实施需要遵循以下原则：

（1） 重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

（2） 适度安全原则

任何信息系统都不能做到绝对的安全，过多的安全要求必将造成易用性降低和运行的复杂性，因此要在安全需求、安全风险和易用性之间进行平衡和折中。

（3） 风险管理原则

进行安全风险管理，确认可能影响信息系统的安全风险，正确的识别风险、合理的管理风险，并让信息系统的安全风险降低到可以接受的水平以内。

（4） 分权制衡原则

在信息系统中，对所有权限应该进行适当地划分，使每个授权主体只能拥有其中的一部分权限，使他们之间相互制约、相互监督，共同保证信息系统的安全。

（5） 标准化原则

在方案设计和设备选型方面必须遵循国家以及行业内的相关标准，并充分考虑不同产品

之间的兼容性。

（6） 统一安全管理原则

在方案设计中主机、网络设备、安全设备、应用系统、数据库等必须遵循统一安全管理的要求。

网络与标识安全

可采取通信和传输保护、边界隔离（工业防火墙）、接入认证授权等安全策略。通信和传输保护方面，采用相关技术手段来保证通信过程中的机密性、完整性和有效性，防止数据在网络传输过程中被窃取或篡改，并保证合法用户对信息和资源的有效使用。同时，在标识解析体系的建设过程中，需要对解析节点中存储以及在解析过程中传输的数据进行安全保护。边界隔离（工业防火墙）方面，在 OT 安全域之间采用网络边界控制设备（工业防火墙），以逻辑串接的方式进行部署，对安全域边界进行监视，识别边界上的入侵行为并进行有效阻断。接入认证授权方面，接入网络的设备与标识解析节点应该具有唯一性标识，网络应对接入的设备与标识解析节点进行身份认证，保证合法接入和合法连接，对非法设备与标识解析节点的接入行为进行阻断与告警，形成网络可信接入机制。网络接入认证可采用基于数字证书的身份认证等机制来实现。

工业互联网的发展使得工厂内部网络呈现出 IP 化、无线化、组网方式灵活化与全局化的特点，工厂外网呈现出信息网络与控制网络逐渐融合、企业专网与互联网逐渐融合以及产品服务日益互联网化的特点。这就造成传统互联网中的网络安全问题开始向工业互联网蔓延，具体表现为以下几个方面：

① 工业互联协议由专有协议向以太网/IP 协议转变，导致攻击门槛极大降低；

② 现有一些 10M/100M 工业以太网交换机（通常是非管理型交换机）缺乏抵御日益严重的 DDoS 攻击的能力；

③ 工厂网络互联、生成、运营逐渐由静态转变为动态，安全策略面临严峻挑战等。此外，随着工厂业务的拓展和新技术的不断应用，今后还会面临 5G/SDN 等新技术引入、工厂内外网互联互通进一步深化等带来的安全风险。

工业互联网网络安全防护应面向工业控制网络、企业与园区网络、骨干网络及标识解析系统等方面，具体包括网络结构优化、边界安全防护、接入认证、通信内容防护、通信设备防护、

安全监测审计等多种防护措施，构筑全面高效的网络安全防护体系。

（1） 优化网络结构设计

在网络规划阶段，需设计合理的网络结构。一方面通过在关键网络节点和标识解析节点采用双机热备和负载均衡等技术，应对业务高峰时期突发的大数据流量和意外故障引发的业务连续性问题，确保网络长期稳定可靠运行。另一方面通过合理的网络结构和设置提高网络的灵活性和可扩展性，为后续网络扩容做好准备。

（2） 网络边界安全

根据工业互联网中网络设备和业务系统的重要程度将整个网络划分成不同的安全域，形成纵深防御体系。安全域是一个逻辑区域，同一安全域中的设备资产具有相同或相近的安全属性，如安全级别、安全威胁、安全脆弱性等，同一安全域内的系统相互信任。在安全域之间采用网络边界控制设备，以逻辑串接的方式进行部署，对安全域边界进行监视，识别边界上的入侵行为并进行有效阻断。

（3） 网络接入认证

接入网络的设备与标识解析节点应该具有唯一性标识，网络应对接入的设备与标识解析节点进行身份认证，保证合法接入和合法连接，对非法设备与标识解析节点的接入行为进行阻断与告警，形成网络可信接入机制。网络接入认证可采用基于数字证书的身份认证等机制来实现。

（4） 通信和传输保护

通信和传输保护是指采用相关技术手段来保证通信过程中的机密性、完整性和有效性，防止数据在网络传输过程中被窃取或篡改，并保证合法用户对信息和资源的有效使用。同时，在标识解析体系的建设过程中，需要对解析节点中存储以及在解析过程中传输的数据进行安全保护。具体包括：

① 通过加密等方式保证非法窃取的网络传输数据无法被非法用户识别和提取有效信息，确保数据加密不会对任何其他工业互联网系统的性能产生负面影响。在标识解析体系的各类解析节点与标识查询节点之间建立解析数据安全传输通道，采用国密局批准使用的加密算法及加密设备，为标识解析请求及解析结果的传输提供机密性与完整性保障；

② 网络传输的数据采取校验机制，确保被篡改的信息能够被接收方有效鉴别；

③ 应确保接收方能够接收到网络数据，并且能够被合法用户正常使用。

（5） 网络设备安全防护

为了提高网络设备与标识解析节点自身的安全性，保障其正常运行，网络设备与标识解析节点需要采取一系列安全防护措施，主要包括：

① 对登录网络设备与标识解析节点进行运维的用户进行身份鉴别，并确保身份鉴别信息不易被破解与冒用；

② 对远程登录网络设备与标识解析节点的源地址进行限制；

③ 对网络设备与标识解析节点的登录过程采取完备的登录失败处理措施；

④ 启用安全的登录方式（如 SSH 或 HTTPS 等）。

（6） 安全监测审计

网络安全监测指通过漏洞扫描工具等方式探测网络设备与标识解析节点的漏洞情况，并及时提供预警信息。网络安全审计指通过镜像或代理等方式分析网络与标识解析系统中的流量，并记录网络与标识解析系统中的系统活动和用户活动等各类操作行为以及设备运行信息，发现系统中现有的和潜在的安全威胁，实时分析网络与标识解析系统中发生的安全事件并告警。同时记录内部人员的错误操作和越权操作，并进行及时告警，减少内部非恶意操作导致的安全隐患。

7.3 企业安全防护系统实施

企业安全防护系统实施致力于从防护技术策略角度出发，提升企业安全防护水平，降低安全攻击风险。部署的关键在于确保工业互联网企业侧的网络安全、应用安全、数据安全。

企业安全防护系统实施需要涵盖安全功能视图中企业层中相关防护技术。首先，保障企业侧网络安全，通过采取通信和传输保护、边界隔离（防火墙）、网络攻击防护等安全策略，确保企业与园区网络安全、标识解析安全等。其次，保障应用安全，通过采取用户授权和管理、虚拟化安全、代码安全等安全策略，确保平台安全、本地应用安全、云化应用安全等。最后，保障数据安全，通过采取数据防泄漏、数据加密、数据备份恢复等安全策略，确保包括数据收集安全、数据传输安全、数据存储安全、数据处理安全、数据销毁安全、数据备份恢复安全

在内的数据全生命周期各环节的安全。在部署方式上，企业安全防护系统主要位于企业层。

网络安全

可采取通信和传输保护、边界隔离（防火墙）、网络攻击防护等安全策略。通信和传输保护方面，与边缘安全防护系统中的针对网络安全的通信和传输保护的具体策略一致。边界隔离（防火墙）方面，在 IT 安全域之间采用网络边界控制设备（防火墙），以逻辑串接的方式进行部署，对安全域边界进行监视，识别边界上的入侵行为并进行有效阻断。网络攻击防护方面，为保障网络设备与标识解析节点正常运行，对登录网络设备与标识解析节点进行运维的用户进行身份鉴别，并确保身份鉴别信息不易被破解与冒用；对远程登录网络设备与标识解析节点的源地址进行限制；对网络设备与标识解析节点的登录过程采取完备的登录失败处理措施等。

平台与应用安全

可采取用户授权和管理、虚拟化安全、代码安全等安全策略。用户授权和管理方面，工业互联网平台用户分属不同企业，需要采取严格的认证授权机制保证不同用户能够访问不同的数据资产。同时，认证授权需要采用更加灵活的方式，确保用户间可以通过多种方式将数据资产分模块分享给不同的合作伙伴。虚拟化安全方面，虚拟化是边缘计算和云计算的基础，为避免虚拟化出现安全问题影响上层平台的安全，在平台的安全防护中要充分考虑虚拟化安全。虚拟化安全的核心是实现不同层次及不同用户的有效隔离，其安全增强可以通过采用虚拟化加固等防护措施来实现。代码安全方面，主要通过代码审计检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。

工业互联网应用主要包括工业互联网平台与工业应用程序两大类，其范围覆盖智能化生产、网络化协同、个性化定制、服务化延伸等方面。目前工业互联网平台面临的安全风险主要包括数据泄露、篡改、丢失、权限控制异常、系统漏洞利用、账户劫持、设备接入安全等。对工业应用程序而言，最大的风险来自安全漏洞，包括开发过程中编码不符合安全规范而导致的软件本身的漏洞以及由于使用不安全的第三方库而出现的漏洞等。

相应地，工业互联网应用安全也应从工业互联网平台安全与工业应用程序安全两方面进行防护。对于工业互联网平台，可采取的安全措施包括安全审计、认证授权、DDOS 攻击防护等。对于工业应用程序，建议采用全生命周期的安全防护，在应用程序的开发过程中进行代码审计并对开发人员进行培训，以减少漏洞的引入；对运行中的应用程序定期进行漏洞排查，对应用程序的内部流程进行审核和测试，并对公开漏洞和后门加以修补；对应用程序的行为进行

实时监测，以发现可疑行为并进行阻止，从而降低未公开漏洞带来的危害。

（1） 平台安全

① 安全审计

安全审计主要是指对平台中与安全有关的活动的相关信息进行识别、记录、存储和分析。平台建设过程中应考虑具备一定的安全审计功能，将平台与安全有关的信息进行有效识别、充分记录、长时间的存储和自动分析。能对平台的安全状况做到持续、动态、实时、有依据的安全审计，并向用户提供安全审计的标准和结果。

② 认证授权

工业互联网平台用户分属不同企业，需要采取严格的认证授权机制保证不同用户能够访问不同的数据资产。同时，认证授权需要采用更加灵活的方式，确保用户间可以通过多种方式将数据资产分模块分享给不同的合作伙伴。

③ DDoS 防御

部署 DDoS 防御系统，在遭受 DDoS 攻击时，保证平台用户的正常使用。平台抗 DDoS 的能力应在用户协议中作为产品技术参数的一部分明确指出。

④ 安全隔离

平台不同用户之间应当采取必要的措施实现充分隔离，防止蠕虫病毒等安全威胁通过平台向不同用户扩散。平台不同应用之间也要采用严格的隔离措施，防止单个应用的漏洞影响其他应用甚至整个平台的安全。

⑤ 安全监测

应对平台实施集中、实时的安全监测，监测内容包括各种物理和虚拟资源的运行状态等。通过对系统运行参数（如网络流量、主机资源和存储等）以及各类日志进行分析，确保工业互联网平台提供商可执行故障管理、性能管理和自动检修管理，从而实现平台运行状态的实时监测。

⑥ 补丁升级

工业互联网平台搭建在众多底层软件和组件基础之上。由于工业生产对于运行连续性的要求较高，中断平台运行进行补丁升级的代价较大。因此平台在设计之初就应当充分考虑如

何对平台进行补丁升级的问题。

⑦ 虚拟化安全

虚拟化是边缘计算和云计算的基础，为避免虚拟化出现安全问题影响上层平台的安全，在平台的安全防护中要充分考虑虚拟化安全。虚拟化安全的核心是实现不同层次及不同用户的有效隔离，其安全增强可以通过采用虚拟化加固等防护措施来实现。

（2） 工业应用程序安全

① 代码审计

代码审计指检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。工业应用程序在开发过程中应该进行必要的代码审计，发现代码中存在的安全缺陷并给出相应的修补建议。

② 人员培训

企业应对工业应用程序开发者进行软件源代码安全培训，包括了解应用程序安全开发生命周期（SDL）的每个环节，如何对应用程序进行安全架构设计，具备所使用编程语言的安全编码常识，了解常见源代码安全漏洞的产生机理、导致后果及防范措施，熟悉安全开发标准，指导开发人员进行安全开发，减少开发者引入的漏洞和缺陷等，从而提高工业应用程序安全水平。

③ 漏洞发现

漏洞发现是指基于漏洞数据库，通过扫描等手段对指定工业应用程序的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。在应用程序上线前和运行过程中，要定期对其进行漏洞发现，及时发现漏洞并采取补救措施。

④ 审核测试

⑤ 对工业应用程序进行审核测试是为了发现功能和逻辑上的问题。在上线前对其进行必要的审核测试，有效避免信息泄露、资源浪费或其他影响应用程序可用性的安全隐患。

⑥ 行为监测和异常阻止

对工业应用程序进行实时的行为监测，通过静态行为规则匹配或者机器学习的方法，发现

异常行为，发出警告或者阻止高危行为，从而降低影响。

数据安全

可采取数据防泄漏、数据加密、数据备份恢复等安全策略。数据防泄漏方面，为防止数据在传输过程中被窃听而泄露，工业互联网服务提供商应根据不同的数据类型以及业务部署情况，采用有效手段防止数据泄露。例如通过 SSL 保证网络传输数据信息的机密性、完整性与可用性，实现对工业现场设备与工业互联网平台之间、工业互联网平台中虚拟机之间、虚拟机与存储资源之间以及主机与网络设备之间的数据安全传输，并为平台的维护管理提供数据加密通道，保障维护管理过程的数据传输安全。数据加密方面，工业互联网平台运营商可根据数据敏感度采用分等级的加密存储措施（如不加密、部分加密、完全加密等）。

建议平台运营商按照国家密码管理有关规定使用和管理密码设施，并按规定生成、使用和管理密钥。同时针对数据在工业互联网平台之外加密之后再传输到工业互联网平台中存储的场景，应确保工业互联网平台运营商或任何第三方无法对客户的数据进行解密。数据备份方面，用户数据作为用户托管在工业互联网服务提供商的数据资产，服务提供商有妥善保管的义务。应当采取技术措施和其他必要措施，在发生或者可能发生个人信息泄露、毁损、丢失的情况时，立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。工业互联网服务提供商应当根据用户业务需求与用户签订的服务协议制定必要的数据备份策略，定期对数据进行备份。当发生数据丢失事故时能及时恢复一定时间前备份的数据，从而降低用户的损失。

工业互联网相关的数据按照其属性或特征，可以分为四大类设备数据、业务系统数据、知识库数据、用户个人数据。根据数据敏感程度的不同，可将工业互联网数据分为一般数据、重要数据和敏感数据三种。工业互联网数据涉及数据采集、传输、存储、处理等各个环节。随着工厂数据由少量、单一、单向向大量、多维、双向转变，工业互联网数据体量不断增大、种类不断增多、结构日趋复杂，并出现数据在工厂内部与外部网络之间的双向流动共享。由此带来的安全风险主要包括数据泄露、非授权分析、用户个人信息泄露等。

对于工业互联网的数据安全防护，应采取明示用途、数据加密、访问控制、业务隔离、接入认证、数据脱敏等多种防护措施，覆盖包括数据收集、传输、存储、处理等在内的全生命周期的各个环节。

（1） 数据收集

工业互联网平台应遵循合法、正当、必要的原则收集与使用数据及用户信息，公开数据收

集和使用的规则，向用户明示收集使用数据的目的、方式和范围，经过用户的明确授权同意并签署相关协议后才能收集相关数据。授权协议必须遵循用户意愿，不得以拒绝提供服务等形式强迫用户同意数据采集协议。

另外，工业互联网平台不得收集与其提供的服务无关的数据及用户信息，不得违反法律、行政法规的规定和双方约定收集、使用数据及用户信息，并应当依照法律、行政法规的规定和与用户的约定处理其保存的数据及个人信息。

（2） 数据传输

为防止数据在传输过程中被窃听而泄露，工业互联网服务提供商应根据不同的数据类型以及业务部署情况，采用有效手段确保数据传输安全。例如通过 SSL 保证网络传输数据信息的机密性、完整性与可用性，实现对工业现场设备与工业互联网平台之间、工业互联网平台中虚拟机之间、虚拟机与存储资源之间以及主机与网络设备之间的数据安全传输，并为平台的维护管理提供数据加密通道，保障维护管理过程的数据传输安全。

（3） 数据存储

① 访问控制

数据访问控制需要保证不同安全域之间的数据不可直接访问，避免存储节点的非授权接入，同时避免对虚拟化环境数据的非授权访问。

- 存储业务的隔离

借助交换机，将数据根据访问逻辑划分到不同的区域内，使得不同区域中的设备相互间不能直接访问，从而实现网络中设备之间的相互隔离。

- 存储节点接入认证

对于存储节点的接入认证可通过成熟的标准技术，包括 ISCSI 协议本身的资源隔离、CHAP（Challenge Handshake Authentication Protocol）等，也可通过在网络层面划分 VLAN 或设置访问控制列表等来实现。

- 虚拟化环境数据访问控制

在虚拟化系统上对每个卷定义不同的访问策略，以保障没有访问该卷权限的用户不能访问，各个卷之间互相隔离。

② 存储加密

工业互联网平台运营商可根据数据敏感度采用分等级的加密存储措施（如不加密、部分加

密、完全加密等）。建议平台运营商按照国家密码管理有关规定使用和管理密码设施，并按规定生成、使用和管理密钥。同时针对数据在工业互联网平台之外加密之后再传输到工业互联网平台中存储的场景，应确保工业互联网平台运营商或任何第三方无法对客户的数据进行解密。

③ 备份和恢复

用户数据作为用户托管在工业互联网服务提供商的数据资产，服务提供商有妥善保管的义务。应当采取技术措施和其他必要措施，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

工业互联网服务提供商应当根据用户业务需求、与用户签订的服务协议制定必要的数据备份策略，定期对数据进行备份。当发生数据丢失事故时能及时恢复一定时间前备份的数据，从而降低用户的损失。

（4） 数据处理

① 使用授权

数据处理过程中，工业互联网服务提供商要严格按照法律法规以及在与用户约定的范围内处理相关数据，不得擅自扩大数据使用范围，使用中要采取必要的措施防止用户数据泄露。如果处理过程中发生大规模用户数据泄露的安全事件，应当及时告知用户和上级主管部门，对于造成用户经济损失的应当给予赔偿。

② 数据销毁

在资源重新分配给新的租户之前，必须对存储空间中的数据进行彻底擦除，防止被非法恶意恢复。应根据不同的数据类型以及业务部署情况，选择采用如下操作方式：

- 在逻辑卷回收时对逻辑卷的所有 bit 位进行清零，并利用“0”或随机数进行多次覆写；
- 在非高安全场景，系统默认将逻辑卷的关键信息（如元数据、索引项、卷前 10M 等）进行清零；在涉及敏感数据的高安全场景，当数据中心的物理硬盘需要更换时系统管理员可采用消磁或物理粉碎等措施保证数据彻底清除。

③ 数据脱敏

当工业互联网平台中存储的工业互联网数据与用户个人信息需要从平台中输出或与第三

方应用进行共享时，应当在输出或共享前对这些数据进行脱敏处理。脱敏应采取不可恢复的手段，避免数据分析方通过其他手段对敏感数据复原。此外数据脱敏后不应影响业务连续性，避免对系统性能造成较大影响。

7.4 企业安全管理平台实施

企业安全综合管理平台实施致力于从防护管理策略角度出发，以安全风险可知、可视、可控作为安全防护体系建设的主要目标，强化企业综合安全管理能力。部署的关键在于对企业网络口及企业内安全风险进行监测，在平台网络出口建设流量探针，实现对企业的安全信息采集、资产识别管理、安全审计、安全告警、安全处置跟踪以及数据治理等功能，并与省/行业级安全平台的对接。

企业安全综合管理平台实施需要涵盖安全功能视图中企业层中相关防护管理。安全信息采集指实时地对企业内部的安全动态信息进行有效采集，并进行有效汇总。资产识别管理指通过平台网络出口的流量探针对企业内网进行扫描识别，发现并统计企业内网的资产并进行集中管理。安全审计指通过记录和分析历史操作事件及数据，发现能够改进系统性能和系统安全的地方，防止有意或无意的人为错误，防范和发现网络犯罪活动。安全告警指及时发现资产中的安全威胁、实时掌握资产的安全态势。安全处置跟踪指根据安全事件或安全资产溯源到相关责任人。数据治理指对收集到的相关数据进行分析统计，为企业做出相关研判提供依据。

在部署方式上，企业安全综合管理平台系统主要位于企业层，一方面保障企业内部安全管理有序进行，实现对企业的安全信息采集、资产识别管理、安全审计、安全告警、安全处置跟踪以及数据治理等功能；另一方面与省/行业级安全平台实现有效协同，将监测到的数据及时有效地上报给省/行业级安全平台。

企业安全管理平台至少具有如下功能：

实时监控

实时监控完成系统中安全设备（工业防火墙、工业审计、工业卫士终端）的实时状态、安全日志等信息的实时监控。并对近 7 天安全日志进行趋势展示，包括 X-Y 趋势图及饼状图。另外，还能实时显示安全设备和系统所有设备的在线设备数量。

统计报表

安全事件统计，以时间、设备、区域等不同维度对安全事件进行统计。

安全策略管理

主要是对安全设备进行安全策略管理，包括策略复制、策略下发、策略备份等操作。支持批量对多台设备进行集中定制与策略下发、策略增量下发。支持定时备份安全策略、定时下发安全策略等功能，简化用户对多台设备进行管理的维护成本，提高维护效率。

安全域管理

以按照设备划分不同的安全域，实现安全域的管理，帮助管理人员提高工作效率，降低操作风险。

安全事件管理

（1） 安全事件库维护

建立安全事件库，并提供安全事件库的维护功能，安全事件库内容包括：事件名称、事件类型、事件级别、事件描述和事件特征；安全事件库支持工业控制协议（Modbus、OPC 等）和工业控制系统的安全事件。

（2） 安全事件分析

对收集的审计日志进行分析，从中提取安全事件。

（3） 潜在危害分析

通过设定单类事件累计发生次数或发生频率的阈值，当统计分析表明此类事件超出阈值时则表明工业控制系统出现了潜在的危害。

（4） 异常行为分析

对工控系统中的行为进行定义，能够发现并记录异常行为。

拓扑管理

自动发现网络拓扑，并以直观的形式呈现网络功能拓扑视图。专业的工业控制网络拓扑构建和管理工具，自动发现网络拓扑，并以直观的形式呈现网络功能拓扑视图。专业的工业控制网络拓扑构建和管理工具，提供丰富的资产信息展示功能，呈现丰富的功能视图，帮助用户最大化的了解自身工业控制网络。

网络拓扑显示监控网络的网络拓扑情况，并且可以查询网络拓扑中设备的详细信息。

日志管理

对于保护终端所产生的安全事件和平台系统事件进行行为进行记录，为分析从源头事件

到结果事件的整个过程提供依据。

全面记录工控网络中的监控终端设备日志和网络中其他发现设备的 syslog 日志，便于安全事件分析和调查取证。

对于自身及相关工控安全终端设备产生的日志进行行为分析的功能，其中包括系统日志、操作日志、配置下发日志、配置备份日志、配置操作日志等。

可以转发安全设备的 syslog 到其他设备，如态势感知平台。

设备管理

统一管理工控网络中的设备，可按照重要程度或者设备物理位置不同进行的分区，每个分区可能采取的安全策略有所侧重，分而治之。

当前国际网络安全形式日益严峻，网络攻击集团化、国家化的趋势日益明显。从已曝光的 APT 攻击案例可以看出，大量具备高度经济价值或特殊政治地位的机构成为 APT 攻击的目标，例如伊朗的核电站、乌克兰电网、台积电、委内瑞拉水电站等工业基础设施和大型企业。针对工业领域和关键基础设施领域的攻击层出不穷，其中大部分为有组织有计划的高级威胁，并普遍采用 0 day 漏洞等攻击方式，此种攻击对于传统防御系统来说无法事先预知，形成未知威胁的防御盲区。

传统的防御总是轻易被绕过，新的攻击方式层出不穷，依靠现有已知的攻击方法，并不能预测未知的攻击手段。由于 APT 攻击具有攻击方法多样化、攻击技术复杂先进、攻击持续时间长等特点，传统基于特征匹配、威胁情报的安全防范措施对于未被披露的攻击方式束手无策。

最近比较热门基于大数据和深度学习的恶意流量行为检测技术，有区分正常/恶意的二分类检测，也有检测多种 APT 攻击的多分类检测。同传统的统计分析方法相比，深度学习能够让计算机自动学习恶意样本和正常样本的分界线，并将特征学习融入到建立模型的过程中，从而减少了人为设计特征引发的不完备。虽然深度学习方法有诸多优点，但也有其局限性：模型的准确度完全依赖恶意样本。对于完全未知的、不在训练集中的 APT 攻击，深度学习也就无从学习其特征。

面对日新月异的网络攻防态势，需要更加智能的手段去应对，有必要使用数学和人工智能算法，对现实网络中的设备资产的全流量进行实时在线的机器学习，通过与每台资产的历史行为对比，以及与同类资产的横向对比，发现异常、已知和未知威胁行为。至少具备如下功能：

（1） 资产互访关系深度透析

从流量中准确发现客户资产，辅助资产管理；使用无监督算法大规模的分析资产之间的通信关系，发现不同业务群集及网络层次关系，实现资产、网络、拓扑的三维可视化。

（2） 深度资产行为聚类

采取无监督学习算法，构建异常算法体系，为网络中的用户和设备建立行为模型，区分正常流量与高级或未知的攻击行为。

（3） 未知威胁检测及防护

高级威胁与未知威胁全面检测，支持单个资产攻击链维度呈现被攻击状态，点击资产拓扑中的单个资产，展示攻击链包括扫描探测、入侵尝试、内网渗透和数据窃取四个阶段，点击展示各自阶段日志，提示攻击事件是否成功。

（4） 风险主机威胁可视

只有“看见”，才能够更好防范威胁，支持包括：异常访问、僵尸网络、黑产挖矿、失陷主机、信息探测、横向扩散、密码爆破、恶意域名访问、非法通信隧道和流量速率异常在内的诸多异常行为。

（5） 威胁情报联动预测

支持根据攻击源 IP、Domain、URL、MD5 值等维度进行威胁情报溯源，包括攻击者背景分析、攻击源属性和 IP 信息分析等联动分析。

（6） 完整还原攻击过程

对攻击事件过程的还原，包括攻击发起时间、攻击 IP、攻击次数、攻击手法、受攻击资产、攻击状态、攻击影响、安全处置建议等诸多还原指标；实时记录攻击报文，可在线查看、下载，第一时间掌握入侵证据。

企业安全上云

近期，各省市地区密集出台企业上云计划。“企业上云”是指以云计算和云平台技术为支撑，将企业的基础系统、管理及业务部署到云端，在网络上便捷地按需使用资源，包括计算资源、存储资源、应用软件等，以此提高企业信息化应用水平，促进经济转型升级。推进“企业上云”是积极创建国家信息经济示范区和国家“两化”融合示范区的重要抓手，结合《中国制造 2025》试点示范要求，以“政府+运营商+企业”的推广模式，部署推动基础系统上云、管理上云和业务上云。

因此需要针对工业企业云基础设施，特别是工业私有云的安全防护显得非常必要，需要从

工业云边界、工业云网络、工业云主机、工业云安全运维管理等多维度，基于微隔离零信任理念，采用 CWPP、CASB 等技术，提供如下基本功能：

（1） 云网络病毒横向扩散，云网络入侵横向移动；

（2） 云内东西向流量安全检测与审计；

（3） 云系统漏洞利用与入侵；

（4） 云应用入侵防御；

（5） 云数据防泄漏；

（6） 基于云内流量及日志的 AI 分析，发现 APT 攻击等未知威胁。

同时，鉴于工业生产优先原则，所以云安全防护措施需要具有满足如下安全原则：

（1） 零打扰：简便快捷的安装部署方式，做到安全部署业务零打扰；

（2） 零信任：云内灵活划分安全域且微隔离，做到云内资产零信任安全防护；

（3） 零中断：控制器和安全组件全面高可靠，做到客户业务零中断；

（4） 全面可视：云内资产能够全面立体的安全可视化，提供清晰的云内资产、云内流量、云内应用的安全态势，易于管理员全面掌握云内资产运行及安全状况；

（5） 全面防护：能够在零信任体系内实现 2-7 层的全面防护和安全管理。

7.5 省/行业级安全平台实施

省/行业级安全平台实施致力于通过工业资产探测、流量分析、风险识别、态势分析、预警通报、应急处置等方式保障省/行业级平台安全运行。

省/行业级安全平台实施需要涵盖安全功能视图中产业层的下边缘相关功能要素。通过接入本地移动网、固网（采样）数据，实现工业资产探测、流量分析、风险识别、态势分析、预警通报、应急处置。

在部署方式上，省/行业级安全平台主要位于产业层，一方面保障本省/行业平台的安全运行，另一方面与国家级安全平台和企业安全综合管理平台实现对接，重点覆盖企业工业互联网平台，实现企业基础数据管理功能、策略/指令下发、情报库共享、信息推送等功能。

省级或行业级安全平台一般部署实施安全态势感知系统，态势感知系统通常采用分层架构设计，分别为数据采集层、数据汇聚层（预处理/存储）、态势认知层、态势理解层、态势预

测层和决策响应层。

（1） 数据采集层

负责采集与安全相关的海量异构数据，包括工业主机的木马、病毒、蠕虫和系统漏洞、工业主机行为监控等信息；工业控制网络的工业协议、工业协议异常、网络入侵、网络接入等信息；工业控制器如 PLC、DCS、SCADA 等设备的识别、漏洞信息、网络入侵、远程接入、非法远程调试接入等信息；工业应用系统如 Mess 等系统的病毒、升级补丁、目标、系统漏洞等信息；工业互联网络的总部与分支的纵向访问与入侵，以及产业链合作伙伴企业间横向访问与非法入侵。

（2） 数据汇聚层

实现对采集数据的进行归一化、索引和存储预处理和存储，将数据分别送至分布式文件系统和内存中供大数据分析使用。同时数据汇聚层提供大数据分析基础架构，能够基于云计算的特性实现按需使用、高密度计算、统一资源调配管理，满足跨中心部署需求。

（3） 态势认知层

对预处理后的数据进行实时分析，了解当前的状态，进行攻击识别、攻击确认，对态势认知所需信息来源和素材的质量评价，同时安全大数据可视化框架。

（4） 态势理解层

态势理解层基于态势认知层的结果，对确认发生的攻击进行深入分析，了解攻击的影响、攻击者（对手）的行为和当前态势发生的原因及方式。简单可概括为：损害评估、行为分析（攻击行为的趋势与意图分析）和因果分析（包括溯源分析和取证分析）。

（5） 态势预测层

态势预测层采用神经网络、灰色理论、时间序列分析和支持向量机等多预测方法，对态势发展情况的预测评估，跟踪安全态势演化过程，基于情境推演的方法进行影响评估，对未来安全态势进行预测。

（6） 态势决策层

一方面是自动态势决策，即通过协同防护技术，对已出现的或预测到新攻击、新威胁、异常情况自动生成安全策略，并下发给区域内的各个安全设备，同区域内的安全设备形成统一的纵深协同防护圈；另一方面，人工态势决策，态势理解和预测的结果进行图形或报表可视化，通过长时间的机器学习和积累并形成适合本区域系统的安全知识库，为决策者提供决策依据。

作为工业互联网安全态势感知系统，必须要深入结合工业场景，具有针对性的工业安全状态与趋势的数据采集、分析、预测与决策：

（1） 工业资产画像：类别、脆弱性、风险、异常、沦陷等；

（2） 工控网络：控制系统网络拓扑、厂级网络拓扑、集团网络拓扑等；

（3） 工业协议流量：工控协议类别、吞吐、速率、时延、抖动、流向、异常等；

（4） 工控设备：类别、状态、脆弱性、风险等；

（5） 工业应用：类别、承载的资产风险状态、操作日志、运行日志、应用风险等；

（6） 安全暴露面：哪些暴露在互联网、哪些可能被攻击等；

（7） 合规性状态；

（8） 综合趋势：业务视角、资产视角、威胁视角、运维视角、决策视角等；

（9） 响应处置：策略管理、通报预警、协同联动、应急处置等。

同时工业互联网安全态势感知系统还应该能够基于非结构化数据进行高级与未知威胁检测发现能力：

非结构化数据中包含的信息更为丰富，基于非结构化数据的威胁检测，其第一步就是进行非结构化数据的特征提取，需要根据检测威胁模型的特点，选取非结构化数据不同维度的信息并由特征工程提取出来，再采用机器学习或深度学习进行模型建立。机器学习是基于经验的学习，而非结构化数据中提取出的特征就是先验数据。常见的机器学习算法可分为监督学习和无监督学习两大类。

监督学习通过已有的训练样本（即已知数据以及其对应的输出）来训练，从而得到一个最优模型，再利用这个模型将所有新的数据样本映射为相应的输出结果，对输出结果进行简单的判断从而实现分类的目的，那么这个最优模型也就具有了对未知数据进行分类的能力。其代表就是分类和回归。监督学习的典型例子就是决策树、神经网络。

神经网络作为目前最热门的机器学习算法，在高级威胁检测的多个场景下取得了良好效果。神经网络是一种运算模型，由大量的节点（或称神经元）之间相互联接构成。每个节点代表一种特定的输出函数，称为激励函数。每两个节点间的连接都代表一个对于通过该连接信号的加权值，称之为权重，相当于人工神经网络的记忆。网络的输出依据网络的连接方式、权重值和激励函数的不同而不同。而网络自身通常都是对自然界某种算法或者函数的逼近，也可能是对一种逻辑策略的表达。人工神经网络模型主要考虑网络连接的拓扑结构、神经元的特征、

学习规则等。目前，已有近 40 种神经网络模型，其中有反传网络、感知器、自组织映射、Hopfield 网络、波耳兹曼机、适应谐振理论等。神经网络具有自学习、联想功能以及高速寻找最优解的优势，其将非结构化数据中提取的特征进一步高维化和归一化，而不再是简单的结构化数据，因此相较于传统的检测方式在容错性、预测性和进化性上取得了长足的进步，是非结构化数据特征提取和检测的合适方法。神经网络能在先验数据的基础上，进行学习和预测，进而在面对高级威胁检测时，取得良好的检测效果。

无监督学习事先没有任何训练数据样本，需要直接对数据进行建模。通过循环和递减运算来减小误差，达到分类的目的。无监督学习的典型例子就是聚类。聚类是将物理或抽象对象的集合分成由类似的对象组成的多个类的过程。聚类分析算法主要有划分方法、层次方法、基于密度的方法、基于网格的方法和基于模型的方法。在高级威胁检测中，聚类法特别适合于未知威胁的检测，直接对非结构化数据的特征进行建模，在形成行为模型基线后，发现异常威胁行为。

7.6 国家级安全平台实施

国家级安全平台实施致力于提升国家级工业互联网安全综合管理和保障能力，加强国家与省/行业级安全平台的系统联动、数据共享、业务协作，形成国家整体安全综合保障能力。

第八章 安全技术视图

8.1 安全技术体系总览

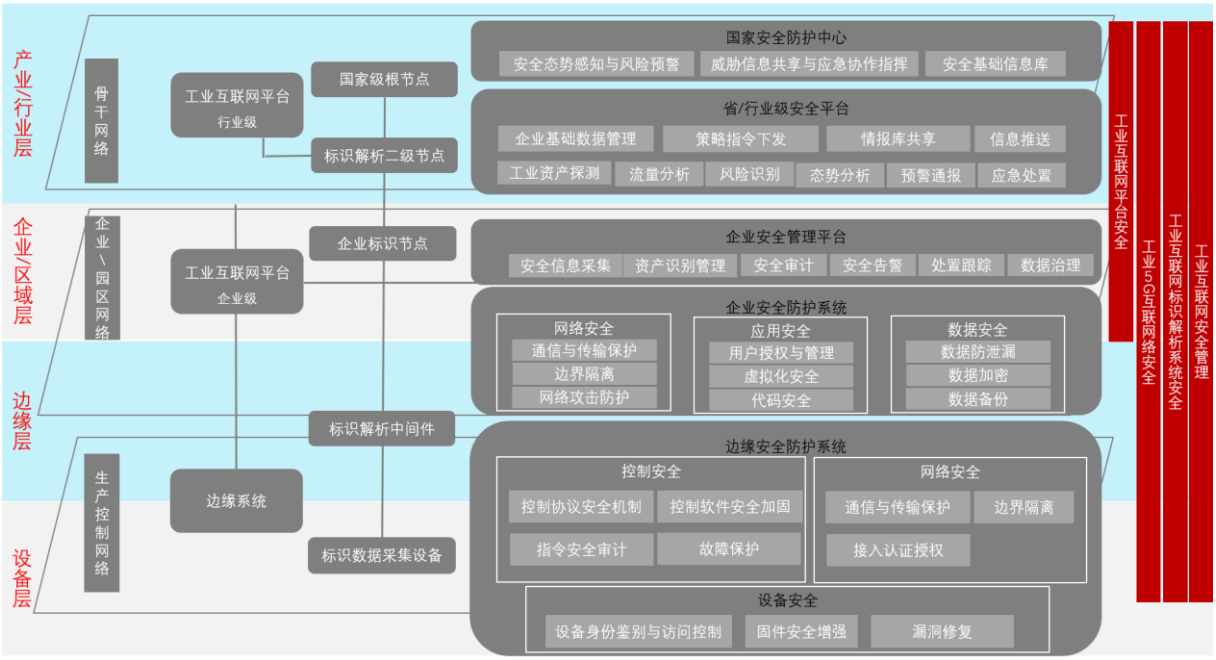

图 8-1 工业互联网安全技术体系

工业互联网安全技术体系是支撑功能架构实现、实施架构落地的整体技术结构。工业互联网安全所采用的技术包括信息安全技术、制造安全技术以及 IT 与 OT 融合技术，比如工业大数据、工业人工智能等。

表 8-1 工业互联网安全技术体系

层次	防护维度	技术手段	技术措施
边缘安全防护系统	设备安全	设备身份鉴别与访问控制	
		固件安全增强	
		漏洞修复	
	控制安全	控制协议安全机制	身份认证
			基于角色访问控制
			加密
		控制软件安全加固	

		指令安全审计	协议深度解析
			攻击异常检测
			无流量异常检测
			重要操作行为审计
			告警日志审计
		故障保护	合理可预见误操作
			恶意攻击操作
			智能设备对环境的抵抗或切断
			异常扰动或中断的检测与处理
	网络与标识安全	通信和传输保护	
		边界隔离	
		网络认证授权	
企业安全防护系统	网络安全	通信和传输保护	
		边界隔离	
		网络攻击防护	访问网络设备和标识解析节点做身份认证
			源地址限制
			访问失败审计
	平台与应用安全	用户授权与管理	租户资产隔离
			租户数据资产共享保护
		虚拟化安全	不同层次隔离
			不同用户隔离
			虚拟化加固
		代码安全（源代码审计）	
	数据安全	数据防泄漏	工业设备与工业互联网平台之间网络传输数据防泄漏
			工业互联网平台中虚机之间交互数据
			虚机与存储之间交互数据防泄漏
			主机或虚机与网络设备交互数据的防泄漏

			维护通道加密
		数据加密	分级加密存储数据
			按国家密码管理规定生成、使用和管理秘钥
			工业互联网平台不能解密客户数据
		数据备份	发生个人信息泄露，及时采取补救措施和告知用户并向主管部门报告
			签订数据备份策略服务协议
企业安全管理平台	保障企业内部安全管理有序进行	安全信息采集	
		资产识别管理	通过流量探针针对企业内网扫描，发现并对资产集中管理
		安全审计	通过记录和分析历史操作事件及数据，发现能够改进系统性能和系统安全的地方，防止有意或无意的人为错误，防范和发现网络犯罪活动
		安全告警	及时发现资产中的安全 威胁、实时掌握资产的安全态势
		安全处置跟踪	根据安全事件或安全资产溯源到相关责任人
		数据治理	对收集到的相关数据进行分析统计，为企业做出相关研判提供依据
	与省/行业级安全平台实现有效协同		
省/行业级安全平台	保障本省/行业平台的安全运行	工业资产探测	
		流量分析	
		风险识别	
		态势分析	
		预警通报	
		应急处置	
	与国家级安全平台和企业安全综合管理平台实现对接	企业基础数据管理功能	
		策略/指令下发	
		情报库共享	
		信息推送	

国家级安全平台	保障国家级安全平台有序运行	建立安全态势感知与风险预警系统	开展全国范围内的安全监测、态势分析、风险预警和 跨省协同工作，并与省/行业级安全平台对接
		建立威胁信息共享与应急协作指挥系统	实现对工业互联网威胁信息共享和应急协作指挥，具备综合研判、决策指挥和过程跟踪 的能力，支持工业互联网安全风险上报、预警发布、事件响应等
		建立安全基础信息库	依托现有基础进行资源整合，建立安全基础信息库，具体包括工业互联网安全漏洞库、指纹库、恶意代码库等基础资源库
	与省/行业级安全平台的系统联动、数据 共享、业务协作		

8.2 通用安全技术

图 8-2 通用安全技术视图

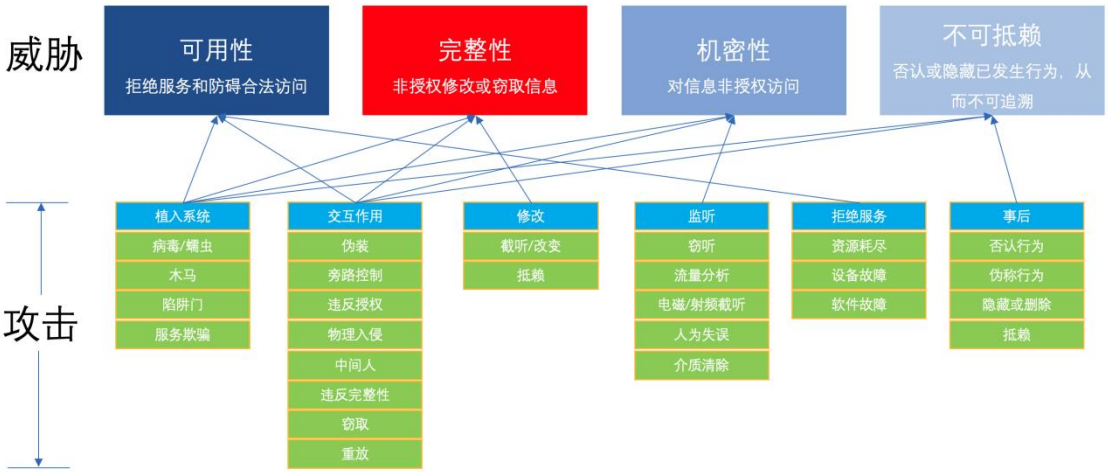

图 8-3 通用安全技术威胁和攻击视图

加密是在 IT 系统中广泛使用的技术，例如，数字签名是一种非对称密钥加密技术，旨在确保数据的作者身份、完整性和不可否认性。然而，数字签名的正确实现取决于公钥基础设施（PKI）的存在、基于标准的安全生成、分发和维护密钥对以及标准化和最新的签名方案。

完整性技术旨在实现系统完整性要求的技术和过程。完整性要求可分为以下几类：

（1） 端点的完整性

（2） 通信的完整性

（3） 管理和监测业务的完整性

（4） 整个系统的整体架构完整性

需要注意的是一项技术或过程的正确实现可能取决于另一项技术或过程的正确实现。例如，通信的完整性在一定程度上取决于诸如 MAC 和数字签名等加密技术的正确实现和使用，而这些技术又取决于密钥的正确生成、分发和管理。

可用性技术旨在实现可用性需求的技术和过程。值得注意的例子包括用于系统体系结构可用性、减轻或防止拒绝服务攻击的技术。这些技术的成功部署取决于体系结构威胁建模。

保密性技术旨在实现端点、通信和连接以及管理和监视操作的保密性要求的技术和过程。整个工业互联网系统的保密性要求也应在架构上进行评估。例如，应使用访问控制技术来实施最小特权原则，从而减少内部人员可能违反的影响。这需要从体系结构威胁建模派生的策略。

访问控制技术也是常用技术，下表列出了访问控制相关技术与过程：

表 8-2 访问控制相关技术与过程表

访问控制		
终端访问控制	端点内的限制和信息流保护	沙箱、以数据为中心的细粒度访问控制、内核隔离、可信计算
通信访问控制	通信加密	不同层采用不同协议、强制断连
	信息流控制	网络分区、网关过滤、防火墙、单向网闸
运维管理访问控制		
架构访问控制	数据整个生命周期实施访问控制	
	关键系统特性访问控制	架构访问控制评估
	内部和外部攻击对系统访问控制的影响	最小权限控制原则

8.3 工业端点安全

端点覆盖了工业互联网设备层、边缘层、企业层和产业层整个范围，包括简单的传感器、可编程逻辑控制器（PLC）和具有重要计算能力的大型云服务器。端点可以位于专用硬件或共享或虚拟化硬件上。端点安全包括如图 8-4 所示的安全功能。

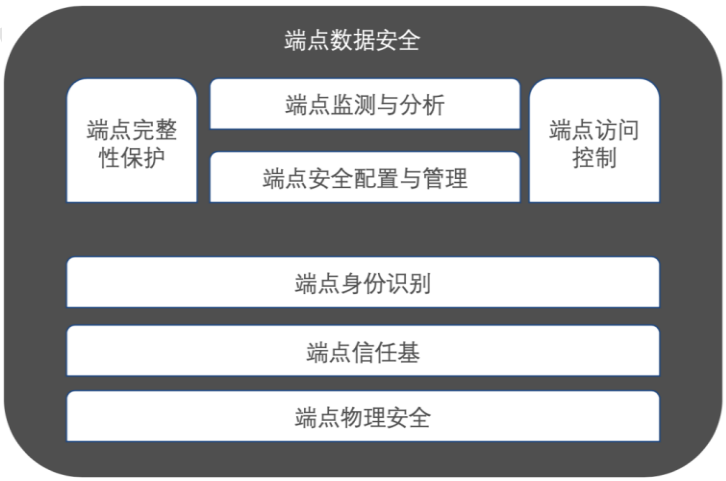

图 8-4 工业端点安全

端点上的安全威胁和漏洞

终点有许多潜在的易受恶意或无意错误影响的漏洞。图 8-5 显示了广泛的解决方案堆栈，从裸机应用程序（左侧）到虚拟机上运行的来宾操作系统（右侧），虚拟机管理程序将应用程序隔离在各自的容器中。每个配置都有其优缺点，必须针对每个应用程序进行评估。例如，裸机应用程序通常实现的安全控制较少，但运行在资源受限的硬件上。另一方面，基于 Hypervisor 的安全解决方案需要更多的处理能力，但可以将虚机专用于安全防护。

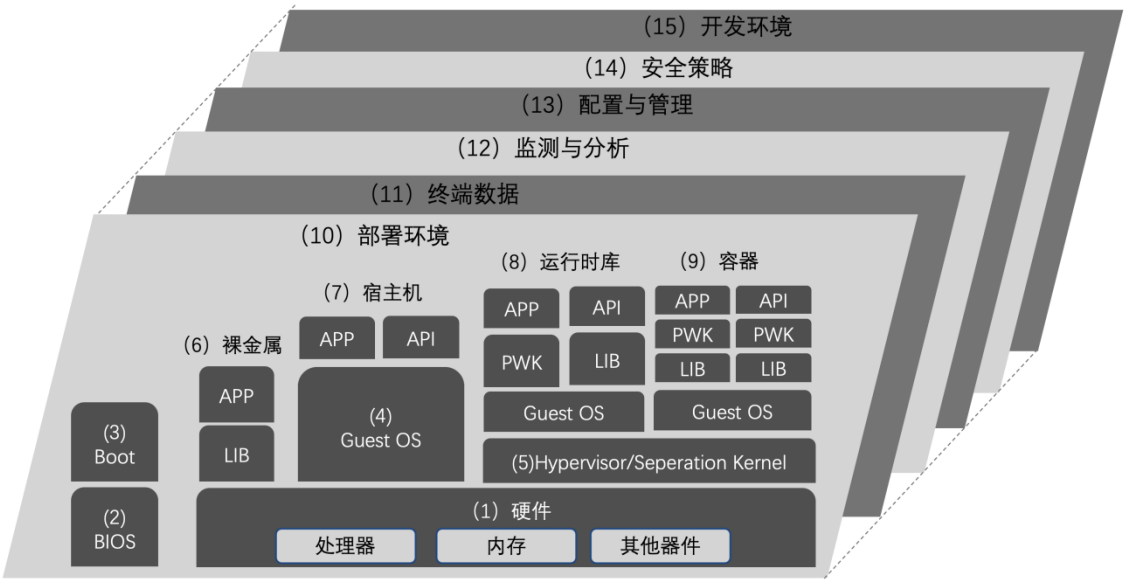

图 8-5 端点安全解决方案堆栈图

（1）硬件组件和配置的更改

在整个端点生命周期中，必须确保硬件完整性，以阻止对硬件组件的不受控制的更改。端点必须能够保护自己免受未经授权的访问和对关键资源（如内存、处理周期和特权处理模式）的独占。

（2）+（3）拦截或覆盖系统引导过程

可以通过修改硬件平台固件和操作系统（如 BIOS）之间的固件接口来更改端点引导过程。对引导加载程序的更改是另一个威胁，因为更改可能会启动未经授权或不安全的操作系统版本，从而损害端点的完整性。此级别的攻击还可能影响端点的正常或安全引导过程、对所有硬件资源的识别以及为保护其他组件建立可靠的信任根。

（4）+（5）对来宾操作系统、管理程序和分离内核的损害

对这些层的攻击可以改变系统的行为，允许信息流绕过安全控制，并使攻击者能够获得对端点硬件和软件资源的特权访问。一旦获得对该层的访问权限，攻击者将有机会对这些层的攻

击可以改变系统的行为，允许信息流绕过安全控制，并使攻击者能够获得对端点硬件和软件资源的特权访问。一旦获得对该层的访问权限，攻击者将有机会影响整个软件堆栈。

（6）+（7）+（8）+（9）非法更改应用程序或 API

端点应用程序通常是恶意软件试图渗透和破坏的目标。恶意应用程序的执行或应用程序 API 的重写会对端点的可信度产生不利影响。公开的 API 应受到保护，以防拒绝服务攻击，因为来自未经授权的用户的连续访问可能会限制对公开功能的响应和访问。

（10）部署环境的漏洞

错误和潜在恶意代码可能作为部署的一部分渗透到端点，例如，不正确或恶意的安装脚本、截获的通信或未经授权替换更新服务器上的软件包。在复杂的端点部署中尽可能减少端点配置对于减少部署过程中的漏洞非常重要。

（11）对端点数据的错误或蓄意修改

从低级固件到软件堆栈的整个端点的数据代表了一个关键的漏洞区域。这些漏洞包括未经授权访问关键任务或专用数据。攻击者可能通过注入错误数据对系统的行为产生不利影响。拒绝服务对数据访问的攻击可能会妨碍端点的及时和准确执行功能导致代价高昂的结果。

（12）违反监控和分析措施

攻击者可修改监视数据，使其看起来像没有发生特定事件一样。修改安全日志和监视数据可能会导致未检测到的漏洞或受损状态。

（13）配置和管理中的漏洞

配置和管理的漏洞可能是由于对配置管理系统的访问控制不当、在系统中插入未经授权的更改或更新有效载荷损坏造成的。应对端点的更新进行规划和管理，以限制不同操作配置的数量以减少碎片化配置。

（14）安全政策不受控制的变化

安全政策的修改可对系统及其端点构成严重威胁。

（15）开发环境中的漏洞

在软件开发生命周期中引入漏洞会使系统易受攻击。这些脆弱点可能在代码的架构、设计或编写过程中引入。使用易受攻击或恶意的库或不受信任的开发框架可能会导致它们包含在系统运行的代码中。

保护端点的架构考虑

在端点上实现安全性取决于它们的计算和通信能力。在边缘，端点可能是具有较少计算能力和静态配置的资源受限设备。在云中，端点可能是具有非凡计算能力和动态配置的服务器。

端点安全体系结构应该是模块化的、可伸缩的，并且对 OT 系统没有干扰。跨不同端点的通用模块和一致接口简化了集成并增强了端到端的安全性。跨所有端点（如边缘、网络和云）的安全 API 促进了清晰的集成框架。安全隔离技术将能力和服务分开，同时减少了它们可能受到攻击的暴露面。

（1） 端点安全生命周期

端点的安全性与制造商有直接的关系。硬件在制造后很难更改，软件也直接取决于制造商是否愿意和有能力尽可能发现并纠正安全缺陷。

一旦制造商将端点交付给市场，系统集成商就承担了安全集成产品的重任。理想情况下，系统集成商为整个系统的端到端安全性设计一个框架。安全成熟度模型支持基于实现机制和架构设计、开发和维护过程的评估。

（2） 端点硬件与软件

与软件相比，在硬件中实现安全性有优点和缺点。专门的防篡改硬件提供了更高级别的信任，特别是对于加密密钥和操作。但这会增加硬件成本，同时在管理和更新方面都增加了复杂度。软件安全在 IT 和企业环境中一直占主导地位，但这些技术措施往往难以在 OT 环境下实施。

电池寿命是许多资源受限设备的一个问题。在大多数情况下，与软件相比，硬件辅助的安全性显著延长了的电池寿命。

通常，硬件实现是不可升级的，因此性能和电池寿命的提高可能会以安全功能的刚性和静态实现为代价。如果发现算法中存在漏洞，则更难对设备进行所需的更改。在硬件和软件上加强安全性，需要设计者综合权衡考虑。

硬件安全模块（HSM）为安全操作提供加固和隔离的硬件组件。常用的功能包括强抗篡改、密钥存储和密钥生成、强认证等生命周期管理。在升级过程中，还可以利用 HSM 来提供安全性。HSM 的一个常见实现是可信平台模块 TPM。

（3） 端点部署需要考虑安全保护

端点部署的时间很长，有时长达数十年，要考虑端点的安全保护。安全措施不能影响现有的生产过程，安全控制应与工业过程松散耦合，以最小化它们之间的相互依赖性。

快速有效地实现安全性的最常见技术是部署一个安全网关，该网关为其后面的设备提供安全防护。

使用网关通常比在环境中修改设备更快、更经济。网关可以相对快速地部署，以在所有设备上提供一致的安全级别，并统一管理设备。网关还可以消除设备管理方式的多样性。这使得安全性与设备的品牌、型号和制造商无关。网关提供网络级的安全性，但不能提供边缘设备的完整性和安全性，从而提供良好的安全控制和可见性。

端点物理安全

端点部署在各种环境中，具有不同的安全要求，比如免受盗窃、篡改、破坏或环境条件的不利影响。

物理访问控制广泛应用于工业系统中，以防止未经授权的用户与端点和通信设备进行物理接触。比如物理周边安全措施，如门和墙；使用访问控制技术（锁、生物识别技术、RFID 卡）阻止未经授权方的访问；通过对受保护资产的监视进行监控。

一些端点，如智能仪表和环境传感器，物理外壳可阻止未经授权的随意篡改，并保护系统组件免受恶劣天气条件和其他可能导致意外故障的危害。外壳应提供稳定的工作条件，通过提供受控电源、稳定的温度、防尘和其他可能对端点确定性产生不利影响的环境物质。应控制对为外围设备（如 USB）的物理访问，以防止未经授权附加外围设备。

端点应实现防篡改硬件组件或其他安全存储以防止密钥提取。

在高度控制和规范的环境中，端点的物理安全状态应作为端点监视和配置管理功能的一部分进行自动监视和控制。这种物理安全应该能够检测并报告对硬件的物理配置或集成的任何未经授权的访问或修改。这些端点可以公开接口，允许更高级别的系统物理安全服务轻松监视或接收有关端点安全状态的通知。

建立信任根

由硬件、软件、人员和组织过程组成的信任根（RoT）建立了对系统的信任。设备上的信任根决定了对属于该特定设备的凭据真实性的信任级别。信任根应该能够生成、管理和存储至少一个标识。

RoT 的强度决定了设备可获得的信任级别。理想情况下，RoT 应该被实现在硬件中，称为硬件信任根（HRoT）。HRoT 是比基于软件或固件的 RoT 更强大的安全控制。信任根必须是可证明的，这意味着它有一种机制来共享其完整性以及安全地提供给其他受信任系统的安全级别。

端点标识

端点标识被广泛的应用于安全控制，这些控制依赖于对标识的正确处理。例如，身份是资产管理、身份验证、授权和远程维护的基础。

实体是具有可识别的不同存在的项。例如，设备是一个实体。但有些设备包含多个端点，每个端点都是实体，每个端点包含多个组件，每个组件也是实体。

端点可以有一个或多个用于不同应用程序的标识。凭据用于验证终端点的标识。

端点访问控制

端点访问控制依赖于两个相关概念：身份验证和授权。

实体有两种形式：人实体和非人实体。两种类型的实体都必须提供凭据来声明其身份。凭据可以用于各种目的：身份验证、标识和授权。

（1） 端点身份验证

在可能的情况下，相互身份验证优先于单向身份验证实现，以防止模拟未经身份验证的端点。在可能的情况下，建议对关键端点进行多因素身份验证。

（2） 端点通信授权

端点之间的所有通信不仅必须经过身份验证，而且还必须经过授权。应该评估工业互联网环境中的每个连接尝试，以确定它是否符合端点或通信策略。任何此类违反都必须生成事件通知，并可能导致阻止网络连接尝试。

端点完整性保护

测量设备引导过程可以验证其完整性，因此可以判断设备在已知良好状态下通电。鉴于设备在 OT 环境中可能不会长时间重新启动，因此还应实现运行时的静态和动态完整性保证。必须在信任根中适当地保护标识，以保持其完整性并避免标识欺骗，并且必须监视和维护数据完整性，以建立对数据的信任，包括静止数据和动态数据。

（1） 引导过程完整性

启动过程初始化主要硬件组件，并启动操作系统。必须在启动环境中建立信任，才声明对任何其他软件或可执行程序的信任。因此，启动的环境必须经过验证，并确定处于可信的状态。

通过测量引导过程，可以检测主机操作系统和软件的操作，从而检测到设备行为中的恶意更改。它可以在启动时检测 Rootkit、病毒和蠕虫。

Trusted boot 和 Measured boot 都是指引导序列中的每个实体在执行之前测量执行链中

的下一个实体的过程。它在引导序列期间创建一个信任链，在引导过程中测量每个元素，然后执行（如果处于适当的状态）。这些度量可以被远程验证，稍后用于评估端点上的信任。

主机处理器提供的引导进程保护可以通过硬件来增强。设备 CPU 的供应商在他们的处理器中提供对启动过程保护的支持。

启动过程保护的一个重要问题是度量的管理（完整性度量）。如果需要在现场更新端点，则在其引导过程中为软件和固件批准的完整性度量也需要以安全的方式更新。

（2） 运行时完整性

在启动进程完整性得到验证之后，操作系统正在运行，应用程序可以执行。运行时完整性控制监视器，理想情况下，在引导过程之外强制端点的完整性。

黑名单控件试图识别包含恶意代码的文件。在资源受限的端点上提供一个完整的恶意指示器黑名单并保持足够小的文件大小是一项挑战。此外，新的威胁不断被发现，因此必须更新这些定义。未知漏洞（“零日漏洞”）在未被检测到的情况下被利用的风险一直存在。

内存区域保护控制内存访问权限，从而创建阻止未经授权访问的 TEE。保护可以在硬件、软件、操作系统、分离内核或固件中实现。通常在引导过程中分配内存区域。这在小型、简单、资源受限的设备中尤其有效。

动态完整性控制包括主机入侵检测（HID）或主机入侵保护（HIP）或运行时进程完整性认证控制等应用程序。HIP 监测和分析端点以及网络流量，寻找触发警报的异常活动或已知特征。HIPs 还可以监视应用程序对文件系统上受保护资源、受保护 RAM 和特权目录的访问。

虽然没有确定的最佳方法来实现设备完整性解决方案，但是应该在设备的约束范围内尽可能多地实现运行时完整性。

端点数据保护

保护端点中的数据涉及静态数据和动态数据。动态数据的保护策略在边缘、云端和通信中各不相同。密码学加强了数据的机密性并确保了数据的完整性。它可用于所有数据，仅用于敏感部分或整个存储介质。在实践中，可以同时应用多种数据保护技术，从而提供对不同类型攻击的保护。

（1） 数据保密

数据保密是指确保信息不泄露给未经授权的各方。为了实现这一点，密码学使未经授权的实体无法理解数据，因为这些实体没有用于解密数据的正确密钥。

数据防泄漏（DLP）通常用于管理数据机密性。DLP 控制数据（如文档、记录、电子邮件或任何其他敏感数据）的使用，以检测和防止数据泄露。DLP 可以是基于端点的，也可以是基于网络的。基于端点的 DLP 控件尝试在端点的内部或外部访问或移动数据。在内部，端点 DLP 控制并防止通过物理设备总线访问数据。在外部，端点 DLP 控制和防止通信，包括在数据通过网络适配器之前的通信。基于网络的 DLP 仅依赖于在端点之间通信时识别机密或敏感信息。两者都试图识别违反数据使用策略的行为，但都有不同的实现。

（2） 数据完整性

数据完整性确保检测到数据被更改。传统的 OT 数据完整性技术（如 CRC 校验）提高了系统的可靠性和恢复能力，但由于缺乏加密强度，对某些恶意更改无效。较新的技术，如数字签名，为完整性度量提供了更大的信任。

通常，存储在端点上的数据包括两种类型：可执行数据（例如二进制代码和解释脚本）和非可执行数据（例如原始数据、配置文件、日志文件）。

非可执行数据由可执行数据（代码）操作。可执行数据的完整性由运行时完整性技术保护。

在操作数据时，必须监视正在使用的非可执行数据的完整性。动态数据的完整性通过以下方式得到加强：

① 适当的编码技术（如使用适当的编程语言、实现缓冲区溢出保护、严格检查正确的输入参数以防止注入攻击）；

② 运行时完整性技术，监控内存访问，以检测和防止内存攻击。

数字签名是一种常用的数据完整性检测技术。理想情况下，签名密钥保存在受保护的存储器（如 HRoT）中，签名操作在 TEE（如 TPM）中执行。

应用数字签名比散列提供更强的完整性。此外，由于任何一方都可以验证数据，所以通用安全操作（如软件和固件更新）可以在应用更新之前验证更新的完整性。此外，还可以验证端点上的配置文件和日志文件，以确保它们在将来任何时候的完整性。

端点监测和分析

监测机制也应受到保护。端点监测涉及到检测设备的可能篡改或损坏。端点安全状态的监视可以在端点内部执行，也可以在端点外部执行。对计算能力比较弱的边缘设备的监测很可能是从操作域中的另一个端点执行的。

端点配置和管理

端点必须为端点组件提供安全且受控制的更改，尽管在某些罕见的情况下不需要安全性。应对所有更新和更改进行签名，对其有效负载进行加密，并记录操作，以便随后对端点进行审核和恢复。这些服务应以非侵入式方式提供给操作功能，并与系统级配置管理和控制具有单独的逻辑连接。

端点保护加密技术

终结点必须始终使用标准加密算法。这些算法应该使用安全的编码实践来实现，并且尽可能使用定期更新和维护的库。应避免在没有公开评估的情况下创建加密算法。

此外，密钥必须是随机的、不可预测的，并且具有足够的长度，以防止对可用密钥空间进行暴力或彻底搜索。两类随机数发生器（RNG）是常用的：确定性和非确定性。确定性 RNG（也称为伪随机数生成器）使用一个称为 seed 的秘密起始值来初始化生成算法，而非确定性 RNG 依赖于一些不可预知的不易控制的物理源。RNG 应该由设备的硬件提供，但在资源受限的设备中这可能是一个挑战。

特定密钥对合法实体有效使用的时间长度称为加密周期（NIST-KEYM）。当密钥被泄露时，必须有一个密钥撤销过程来通知密钥在其加密期到期之前是无效的。不幸的是，与更改密钥相关联的过程可能很复杂，因此建议使用密钥管理系统来自动化密钥管理中的各个步骤。

并非所有终结点都需要加密控制。在某些情况下，数据可能是公开的，不需要任何保密控制。在其他情况下，冗余传感器可能会报告相同的测量结果；因此可以检测到对任何传感器数据的篡改，从而不需要加密完整性控制。

嵌入式设计人员可以卸载计算资源受限设备中的部分或全部加密操作，以保护微控制器单元（MCU）。最常见的动机是希望将加密凭据保存在安全的环境中，同时提高性能并减轻主处理器的负担。对安全随机数生成的需求也是一个因素。更安全的 MCU 具有高质量的随机生成器模块、构建有应对物理攻击的密码引擎或在制造时注入的强大、唯一的公钥/私钥对。

端点保护隔离技术

隔离是指用于保护系统组件不受不必要影响的技术，其中端点的元素不能受端点的其他元素影响，从而保护其功能不受故障和恶意活动的影响。

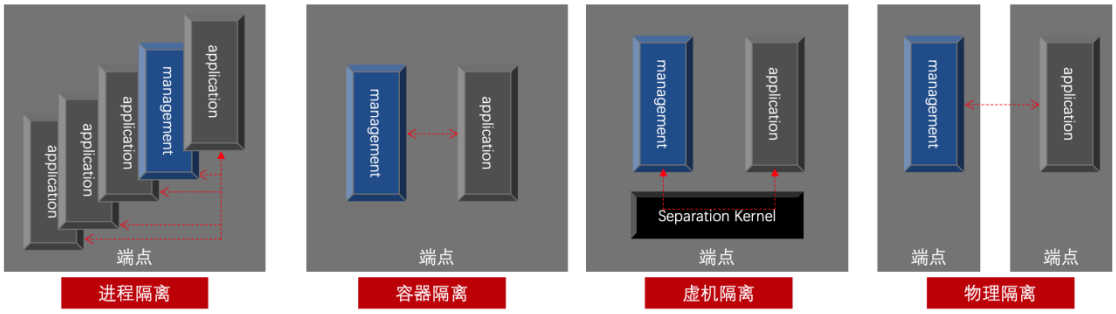

图 8-6 端点保护的隔离技术

（1） 进程隔离

进程隔离模型依赖于操作系统在进程级别将业务或操作组件与安全组件隔离。

进程隔离是当今业界主要的安全部署模型。但是，损害操作系统中的任何组件，包括应用程序和库，会破坏设备的完整性，并可能形成进一步攻击的立足点。

进程隔离技术通常包括安全代理、执行安全操作的软件库、软件密钥存储以及依赖于操作系统安全性强制的任何目录和文件访问控制列表。

（2） 容器隔离

容器隔离模型实现硬件或软件强制隔离边界。软件容器依赖于操作系统来实施资源隔离边界。

软件容器通常有如下实现方式：

① 操作系统管理的容器，如 Android（Trusty TEE）或 Linux 容器，如 LXC 和 Docker；

② 安全内存映射，为安全性提供适当的入口/出口位置，可实现到非常小的传感器类型设备；

③ 网络接口控制器，直接在网络接口的硬件上嵌入策略和实施，以便只有来自安全策略的预定义源/目标、端口和协议组合集才能与端点通信。所有其他通信尝试都会导致失败。

硬件容器通过在同一芯片或同一块主板上启用单独的计算引擎来分离安全实现。这将创建一个安全协处理器，该协处理器实现与主处理器的计算引擎分离的某种级别的安全功能。

硬件容器通常有如下实现方式：

① TPM：TPM 是一个受信任的执行环境（硬件信任根），它提供凭据的安全存储和加密操作的受保护执行。它与主 CPU 隔离，并作为离散芯片、安全协处理器或固件实现；

② 安全协处理器：在独立芯片上的受信任执行环境（包括硬件信任根）中建立非 CPU 安全存在，使许多安全功能得以实现，包括所有 TPM 类型的操作，还包括附加的完整性控制、通信安全、事件监视，安全分析和其他安全相关操作。这种方法的关键是将安全元素部署在物理上独立的芯片上。

（3） 虚拟隔离

虚拟隔离模型有时称为 Hypervisor 隔离，它使用 Hypervisor 在设备上运行的每个虚拟实例之间实现隔离。因此，Hypervisor 上运行的一个实例可以是充当设备上 TEE 的安全实例。虚拟实例 TEE 可以存储机密信息，例如身份材料，并且可以实现安全控制；例如相互认证、连接授权、加密功能、防火墙、深包检查、完整性控制和远程引导认证功能。设备引导过程通常会测量虚拟机监控程序的完整性，然后虚拟机监控程序在启动每个虚拟实例之前对其进行测量，从而将信任链扩展到虚拟 TEE 中，以便在引导后立即确保完整性。启动后，运行时完整性控件必须确保虚拟 TEE 完整性保持不变。

虚拟 TEE 的优点之一是在同一物理硬件上整合多个平台。这遵循云模型，用于将多个物理服务器整合到单个管理程序上，以从规模经济中获益。例如，这使得可编程逻辑控制器（PLC）逻辑和 Windows 人机界面（HMI）能够在 IIoT 环境中的同一物理设备上组合。

虚拟隔离实现了推动云应用增长的规模经济。在边缘，虚拟化允许 OT 组件在不改变其现有操作系统的情况下运行，同时允许安全功能在其自己的操作系统中独立运行。由于安全操作系统与 OT 操作系统在同一物理设备上，它可以在 OT 操作环境下提供嵌入式身份、安全引导认证和通信拦截模式等多种控制。

分离核是虚拟隔离的一种特殊形式。它们提供了强大的隔离，覆盖了底层硬件平台提供的所有资源（处理器时间、内存和 I/O 设备）。除了将组件彼此隔离之外，它们还根据安全策略启用组件和设备之间的通信控制。

与单片系统管理程序内核相比，分离内核没有实现许多通常与操作系统相关联的服务，例如设备驱动程序、文件系统和网络堆栈。分离内核的存在提供了组件之间的分离，并支持组件之间的受控通信。通过故意将内核的功能限制为隔离和简单的 IPC 原语，分离内核大大减少了攻击面和实现复杂性。

（4） 物理隔离

物理隔离将安全性转移到完全独立的设备上。独立的设备（如网关）提供安全性。

资源受限的设备安全

资源受限的设备与功能更强大的设备具有相同的安全要求，包括运行时保护、启动时保护、通信身份验证、配置管理和对更大分析系统的贡献。

资源受限的设备必须能够执行加密操作。较新的设备能够使用硬件加速器、协处理器和嵌入式加速器执行加密操作。这些通常是通过片上系统（SoC）设计集成的，其中单个集成电路不仅集成了 CPU，还集成了网络控制器和其他功能。FPGA 是另一个流行的 SoC 解决方案。

尽管更快的芯片和算法使得在新设备上构建安全性变得更加容易，但许多制造商都背负着几十年前没有这种能力的设备。对于这些系统，制造商要么必须更新固件以支持支持高效软件加密操作和协议（如基于 ID 的加密）的新软件，要么必须在网关设备中实现。

不幸的是，许多工业协议还不支持足够的身份验证，但是不安全的协议可以通过传输层安全（TLS）和其他较低层协议来提供所需的安全属性，如身份验证。或者，个别命令、消息和数据报有时在更高的数据对象层进行身份验证，而无需信任底层协议。

配置管理可以安全地完成，设备可以安全地为更广泛的分析系统提供安全遥测，从而可以对设备的遥测进行身份验证。运行时安全性可以在设备中提供，也可以在可信网关中提供。

其他限制包括无线限制、电池消耗、通信的间歇性可用性和对维护窗口的限制，从而减少更新的频率。这迫使运行时安全性基于白名单而不是黑名单，并增加了对第三方安全性的依赖。

8.4 工业控制安全

工业控制安全主要有四大技术：工业设备指纹识别、工业漏洞库、工业入侵检测、工业协议指令审计。

PROFIBUS 协议解析与指令审计

PROFIBUS 是一种典型的程序自动化协议，且在世界的使用范围较广，具有通用性。本章节以 PROFIBUS DP 为例，介绍程序自动化协议的通讯的基本原理。

PROFIBUS 是一个用在自动化技术的现场总线标准，在 1987 年由德国西门子公司等十四家公司及五个研究机构所推动，PROFIBUS 是程序总线网络（PROcess FIeld BUS）的简称。

PROFIBUS DP（分布式外设，Decentralized Peripherals）用在工厂自动化的应用中，

可以由中央控制器控制许多的传感器及执行器，也可以利用标准或选用的诊断机能得知各模块的状态。

（1） PROFIBUS 通信协议（OSI 模型）

表 8-3OSI 模型与 PROFIBUS 对应关系

OSI 模型	PROFIBUS				
7	应用层	DPV0	DPV1	DPV2	网络管理
6	表示层	--			
5	会话层				
4	传播层				
3	网络层				
2	数据链路层	FDL			
1	物理层	EIA-485	光纤	MBP*	

MBP 为曼彻斯特总线电力传输（Manchester Bus Powered）的缩写。

（2） 应用层

为了有效利用 PROFIBUS DP 的机能，PROFIBUS DP 定义了几种不同的服务档次：

DP-V0：循环式的数据交换，诊断机能。

DP-V1：循环式及非循环式的数据交换，警告处理。

DP-V2：时钟同步数据模式，从机和从机之间的数据广播。

（3） 数据链路层

数据链路层 FDL（总线数据链路层）混合了一般主站（Master）一从站（Slave）之间的通信及令牌传递的消息。在 PROFIBUS 网络中，控制器或控制系统为主站，感测器及致动器为从站。

发送的消息不止一种，依其起始字符（Start Delimiter, SD）可以识别是哪一种消息：

无数据：SD1 = 0x10

SD1	DA	SA	FC	FCS	ED

变动长度数据：SD2 = 0x68

SD2	LE	LEr	SD2	DA	SA	FC	DSAP	SSAP	PDU	FCS	ED

固定长度数据：SD3 = 0xA2

SD3	DA	SA	FC	PDU	FCS	ED

令牌（Token）：SD4 = 0xDC

SD4	DA	SA	ED

简单的收到告知（acknowledgement）：SC = 0xE5

SC

SD：起始字符

LE：协议数据单位（Protocol Data Unit，PDU）及 DA、SA、FC、DSAP 及 SSAP 所有数据的长度

LEr：重复 LE 的内容（因 PROFIBUS 的汉明距离 HD=4，不在 FCS 检查码范围内的数据需重复一次，因此需重复 LE 内容）

FC：功能码

DA：目的设备地址

SA：来源设备地址

DSAP：目的设备的服务点（SAP）

SSAP：来源设备的服务点

表 8-4SAP 数值与服务对照表

SAP（十进制）	服务
默认值 0	循环数据交换（Write_Read_Data）
54	主站至主站服务点（M-M Communication）
55	更改从站地址（Set_Slave_Add）
56	读取输入（Rd_Inp）
57	读取输出（Rd_Outp）
58	给 DP 从站的控制命令（Global_Control）
59	读取配置（Configuration）数据（Get_Cfg）
60	读取诊断数据（Slave_Diagnosis）
61	写入首选项数据（Set_Prm）
62	检查配置数据（Chk_Cfg）

除了 SAP55 之外的其他服务点都是必备的，若设备中没有非易失性存储器，可以不支持更改从站地址的 SAP55 服务。

PDU：协议数据单元（Protocol Data Unit）。

FCS：框架检查码，是直接将消息中的字节相加而得，包括 PDU、DA、SA、FC、DSAP 及 SSAP，不考虑溢出。

ED：结束字符，为 0x16。

发送字节时使用异步的发送模式，奇偶校验位为偶校验位，启始比特及停止比特均为 1 个。当发送数据时在字节的停止比特跟下一字节的启始比特之间不能有停顿。主站在检测网络上至少 33 比特没有数据（为逻辑状态 1）时，会提交一条新的消息。

（4） 传输层

若依据 EIA-485 规范（旧称“RS-485”或“RS485”）的电气传输方式，会使用阻抗 150 欧姆的双绞线，比特率范围可以从 9.6 Kbit/s 到 12 Mbit/s。两台中继器之间的网络线长也有限制，随比特率的不同，上限从 100 米到 1200 米。

OPC 协议解析与指令审计

OPC（OLE for Process Control），用于过程控制的 OLE（Object Linking and Embedded，对象的连接和嵌入），是一个工业标准，管理这个标准的国际组织是 OPC 基金会，OPC 基金会现有会员已超过 220 家。遍布全球，包括世界上所有主要的自动化控制系统、仪器仪表及过程控制系统的公司。基于微软的 OLE（现在的 Active X）、COM（部件对象模型）和 DCOM（分布式部件对象模型）技术。OPC 包括一整套接口、属性和方法的标准集，用于过程控制和制造业自动化系统。

OPC 协议有两个大类，一种是基于微软 COM/DCOM 技术的“Classic”，另一种是基于 Web service 的 OPC UA。前者在 DCOM 协议之上，诞生较早，已广泛应用在各种工业控制系统现场，成为工业自动化领域的事实标准。后者与前者比出生较晚，但在设计时考虑了安全因素，有了加密机制，不过目前应用范围较小。本章节着重介绍 OPC Classic。

与大多数应用层协议不同，OPC 的基础协议 DCOM 协议使用动态端口机制，在真正建立数据连接之前通讯双方还需要协商需要使用的端口。

OPC 客户端使用 51308 作为源端口首先向 OPC 服务器的 135 端口发起连接，连接成功后再经过 OPC 服务器分配新端口 50207，并通过接口 ISystemActivator 的方法 RemoteCreateInstance 的应答报文返回给客户端，之后客户端使用 51309 作为源端口向服务器的 50207 端口发起新的连接用来后面的真正数据的传输，如图 8-7 所示：

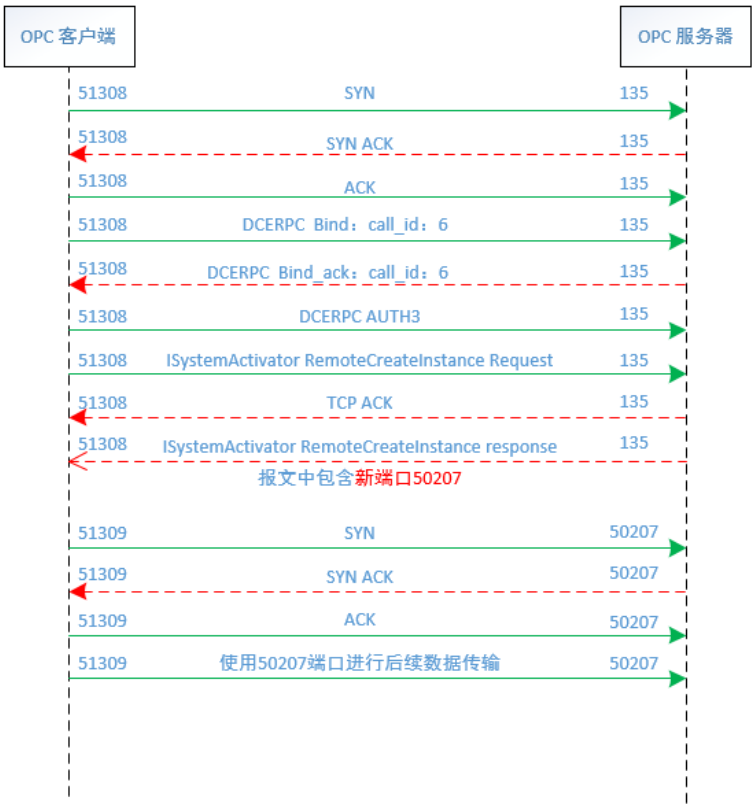

图 8-7 OPC 协议交互过程图

Wireshark 抓取的报文图如下：

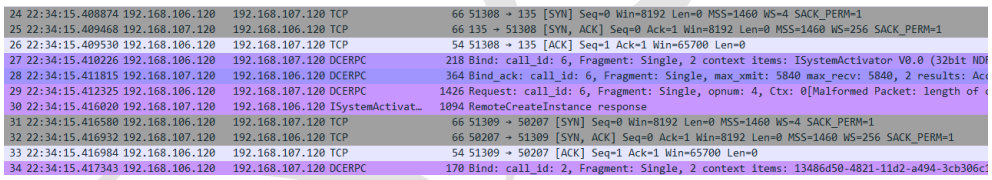

图 8-8 Wireshark 抓取报文图

接口 ISystemActivator 的方法 RemoteCreateInstance 的应答报文中包含 OPC DA 的动态端口，如图 8-9 所示：

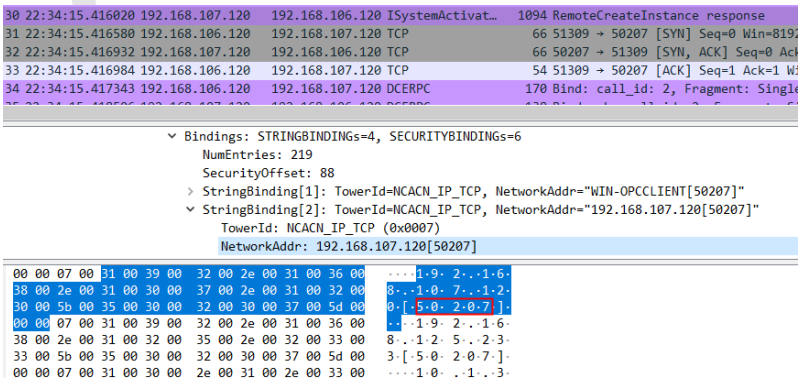

图 8-9 展开 Wireshark 抓取报文图

BACnet 协议解析与指令审计

BACnet 是用于智能建筑的通信协议，是国际标准化组织（ISO）、美国国家标准协会（ANSI）及美国采暖、制冷与空调工程师学会（ASHRAE）定义的通信协议。BACnet 针对智能建筑及控制系统的应用所设计的通信，可用在暖通空调系统（HVAC，包括暖气、通风、空气调节），也可以用在照明控制、门禁系统、火警侦测系统及其相关的设备。优点在于能降低维护系统所需成本并且安装比一般工业通信协议更为简易，而且提供有五种业界常用的标准协议，此可防止设备供应商及系统业者的垄断，也因此未来系统扩展性与兼容性大为增加。

（1） BACnet 协议模型

① 所有的网络设备，除基于 MS/TP 协议的以外，都是完全对等的（peer to peer）；

② 每个设备都是一个“对象”的实体，每个对象用其“属性”描述，并提供了在网络中识别和访问设备的方法；设备相互通信是通过读/写某些设备对象的属性，以及利用协议提供的“服务”完成；

③ 设备的完善性（Sophistication），即其实现服务请求或理解对象类型种类的能力，由设备的“一致性类别”（Conformance Class）所反映。

（2） BACnet 的体系结构

BACnet 与 OSI 协议的层次对应关系如图 8-10 所示：

<table>
<tr><th colspan="4">BACnet 的协议层次</th><th>对应的
OSI 层次</th></tr>
<tr><td colspan="4">BACnet 应用层</td><td>应用层</td></tr>
<tr><td colspan="4">BACnet 网络层</td><td>网络层</td></tr>
<tr><td colspan="2">ISO 8802-2
(IEEE 802.2)类型 1</td><td>MS/TP
(主从/令牌传递)</td><td>PTP
(点到点协议)</td><td rowspan="2">数据
链路层</td></tr>
<tr><td>ISO 8802-3
(IEEE 802.3)</td><td>ARCNET</td><td>EIA-485
(RS485)</td><td>EIA-232
(RS232)</td><td>LonTalk</td><td>物理层</td></tr>
</table>

图 8-10 BACnet 与 OSI 协议层次对应关系

BACnet 建立在包含四个层次的简化分层体系结构上，这四层相当于 OSI 模型中的物理层、数据链路层、网络层和应用层。

BACnet 标准定义了自己的应用层和简单的网络层，对于其数据链路层和物理层，提供了五种选择方案：

第一种选择是 ISO 8802-2 类型 1 定义的逻辑链路控制（LLC）协议，加上 ISO 8802-3 介质访问控制（MAC）协议和物理层协议。ISO 8802-2 类型 1 提供了无连接（Connectionless）不确认（Unacknowledged）的服务，ISO 8802-3 则是著名的以太网协议的国际标准。

第二种选择是 ISO 8802-2 类型 1 定义的逻辑链路控制（LLC）协议，加上 ARCNET（ATA/ANSI878.1）。

第三种选择是主从/令牌传递（MS/TP）协议加上 EIA-485 协议。MS/TP 协议是专门针对楼宇自动控制设备设计的，同 ISO 8802-2 类型 1 一样，它通过控制 EIA-485 的物理层，向网络层提供接口。

第四种选择是点对点（PTP）协议加上 EIA-232 协议，为拨号串行异步通信提供了通信机制。

第五种选择是 LonTalk 协议。

（3） BACnet 的协议栈和数据流

由应用层服务原语产生的应用层协议数据单元（APDU），构成了网络层服务原语的数据部分，并通过网络层服务访问点下传到网络层。

同样，这个请求将进一步下传到本地设备协议栈的以下各层。

服务原语：用于描述服务用户和服务提供者之间交互作用的、抽象的、与具体无关的表现方式。服务原语只有 4 种类型：

① 请求（Request）用户实体要求服务做某项工作

源（N+1）实体—>源（N）实体

② 指示（Indication）用户实体被告知某事件发生

目的（N）实体—>目的（N+1）实体

③ 响应（Response）用户实体表示对某事件的响应

目的（N+1）实体—>目的（N）实体

④ 确认（Confirm）用户实体收到关于它的请求的答复

源（N）实体—>源（N+1）实体

（4） BACnet 应用层

BACnet 应用层主要有两个功能：

① 定义楼宇自控设备的信息模型——BACnet 对象模型

② 定义面向应用的通信服务

（5） BACnet 应用进程模型

BACnet 应用进程模型如图 8-11 所示：

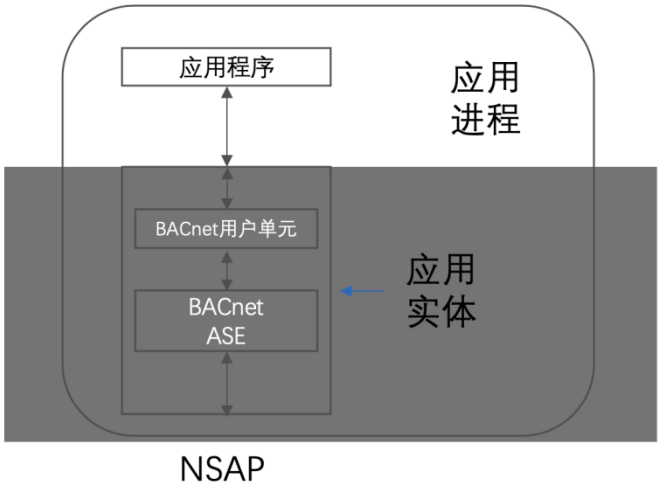

图 8-11 BACnet 应用进程模型

一个应用进程包括：应用程序和应用实体，应用实体位于应用层内，属于通信协议的部分，应用程序不属于协议部分。应用程序和应用实体之间通过 API 进行通信。

应用层有四种原语，分别为：请求（Request）、指示（Indication）、响应（Response）和证实（Confirm）。

（6） BACnet 对象模型

BACnet 网络协议使用面向对象技术，通过封装在 APDU 内的对象数据进行通讯。BACnet 的 28 个对象与应用实例对照表如表 8-5 所示：

表 8-5 BACnet 对象与实例对照表

序号	对象名称	应用实例
01	Accumulator	累加器
02	Analog Input	模拟输入对象
03	Analog Output	模拟输出对象
04	Analog Value	模拟值对象
05	Averaging	平均器
06	Binary Input	二进制输入对象
07	Binary Output	二进制输出对象

08	Binary Value	二进制值对象
09	Calendar	日期表对象
10	Command	命令对象
11	Device	设备对象
12	Event Enrollment	事件登录对象
13	Event Log	事件日志对象
14	File	文件对象
15	Global Group	全局组对象
16	Group	组对象
17	Life Safety Point	生命安全监测点的信息检测
18	Life Safety Zone	生面安全区域的信息检测
19	Loop	控制环对象
20	Multi-State Input	多态输入对象
21	Multi-State Output	多态输出对象
22	Multi-State Value	多态值对象
23	Notification Class	通告类对象
24	Program	程序对象
25	Pulse Converter	脉冲转换器
26	Schedule	时间安排对象
27	Trend Log	趋势记录对象
28	Trend Log Multiple	多趋势记录对象

（7） BACnet 服务

BACnet 具有 35 种服务，服务是操作对象的方法。这 35 种服务分为 6 类，分别为：报警与事件服务、文件访问服务、对象访问服务、远程设备管理服务、虚拟终端服务和网络安全服务。其中，对象服务访问包括：创建对象服务、删除对象服务、读属性服务、条件读属性服务、读多个属性服务、写属性服务、写多个属性服务。远程设备管理服务包括：设备通信控制服务、有证实专有传输服务、无证实专有传输服务、重新初始化设备服务、有证实文本报文服务、无证实文本报文服务、时间同步服务。

IEC104 协议解析与指令审计

IEC104 规约由国际电工委员会制定。IEC104 规约是把 IEC101 的应用服务数据单元(ASDU)用网络规约 TCP/IP 进行传输的标准，该标准为远动信息的网络传输提供了通信规约依据。采用 104 规约组合 101 规约的 ASDU 的方式后，可很好的保证规约的标准化和通信的可靠性。

（1） 应用规约数据单元基本结构

应用规约数据单元：APDU（Application Protocal Data Dnit）；

应用规约控制信息：APCI（Application Protocal Control Information）；

应用服务数据单元：ASDU（Application Protocal Control Unit）；

APDU=APCI + ASDU。

① 应用规约数据单元 APDU

定义了启动字符、应用服务数据单元的长度规范、可传输一个完整的应用规约数据单，格式见表 8-6。

- 启动字符：68H（一个字节）；
- 长度规范：报文最大长度 255 字节，应用规约数据单元的最大长度为 253 字节，控制域的长度是 4 字节，应用服务数据单元的最大长度为 249 字节；
- 控制域：控制域定义抗报文丢失和重复传送的控制信息、报文传输的启动和停止、传输连接的监视。控制域的这些类型被用于完成计数的信息传输的（I 格式）、计数的监视功能（S 格式）和不计数控制功能（U 格式）；
- 应用服务数据单元。

表 8-6 APDU 基本结构

启动 68H **应用规约数据单元的长度（APDU）** **控制域 八位位组 1** **控制域 八位位组 2** **控制域 八位位组 3** **控制域 八位位组 4**	**应用规约控制信息 APCI** **启动一个字节** **长度一个字节** **四个控制域八位位组**
IEC60870-5-104 的应用服务数据单元	应用服务数据单元 ASDU 最大帧长为 249

② 应用规约控制信息 APCI

控制域定义抗报文丢失和重复传送的控制信息、报文传输的启动和停止、传输连接的监视。控制域的这些类型被用于完成计数的信息传输的（I 格式）、计数的监视功能（S 格式）和不计数的控制功能（U 格式），以上格式分别见表 8-7、表 8-8 和表 8-9。

表 8-7 信息传输格式类型（I 格式）的控制域

发送序号 N（S）	**LSB**	**0**
MSB 发送序号 N（S）		
接收序号 N（R）	**LSB**	0
MSB 接收序号 N（R）		

表 8-8 计数的监视功能类型（S 格式）的控制域

0	0	1
0		
接收序号 N（R） LSB		0
MSB 接收序号 N（R）		

表 8-9 不计数的控制功能（U 格式）类型的控制域

TESTFR		STOPDT		STARTDT		1	1
CON	ACT	CON	ACT	CON	ACT		
0							
0							0
0							

③ 应用服务数据单元 ASDU

应用服务数据单元 ASDU 由数据单元标识符和一个或多个信息对象所组成。数据单元标识符在所有应用服务数据单元中常有相同的结构，一个应用服务数据单元中的信息对象常有相同的结构和类型，它们由类型标识域所定义。

数据单元标识符的结构如表 8-10 所示：

表 8-10 数据单元标识符

报文类型标识	一个字节
可变结构限定词	一个字节
传送原因	两个字节
公共地址	两个字节
信息体地址	三个字节
信息体元素	N
……	……
……	……

报文类型标识的结构如表 8-11 所示：

表 8-11 报文类型标识

报文类型标识	描述	标识符
1	单点信息（遥信）	M_SP_NA_1
3	双点信息（遥信）	M_DP_NA_1
9	测量值，规一化值（遥测）	M_ME_NA_1
13	测量值， 标度化值（遥测）	M_ME_NB_1
30	带时标的单点信息（soe 信息）	M_SP_TB_1
31	带时标的双点信息（soe 信息）	M_DP_TB_1

100	总召唤命令	C_IC_NA_1

（2） 规约的过程描述

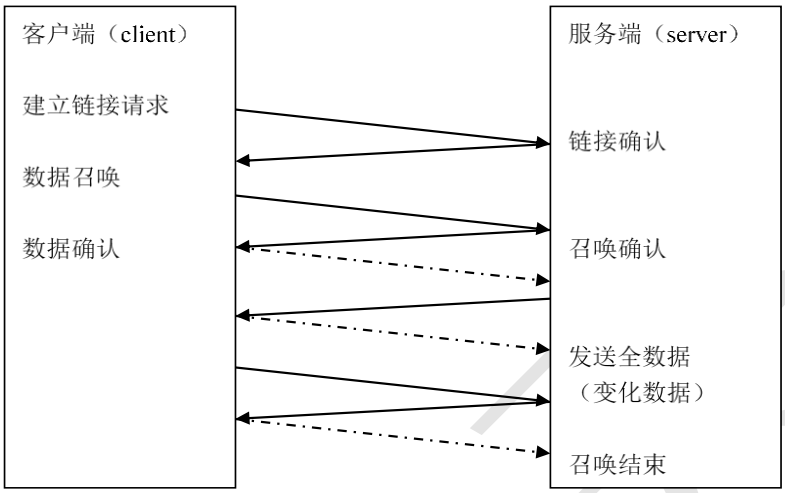

图 8-12 规约过程描述

DLT645-2007 协议解析与指令审计

智能电表的协议有多种，以 DLT645-2007 电能表通讯协议为例，介绍智能电表的通讯协议。

（1） 帧格式

DL/T645-2007 协议的帧格式如表 8-12 所示：

表 8-12 报文类型标识

说明	代码	
帧起始符	68H	
地址域	A0	
	A1	
	A2	
	A3	
	A4	
	A5	
帧起始符	68H	
控制码	C	
数据域长度	L	
数据域	DATA	
校验码	CS	
结束符	16H	

① 帧起始符

标识一帧信息的开始，其值为 0x68H = 01101000B。

② 地址域 A0-A5

地址域由 6 个字节构成，每字节 2 位 BCD 码，地址长度为 12 位十进制数。每块表具有唯一的通信地址，且与物理层信道无关。当使用的地址码长度不足 6 字节时，高位用“0”补足。通信地址 999999999999H 为广播地址，只针对特殊命令有效，如广播校时和广播冻结等。广播命令不要求从站应答。地址域支持缩位寻址，即从若干低位起，剩余高位补 AAH 作为通配符进行读表操作，从站应答帧的地址域返回实际通信地址。地址域传输时低字节在前，高字节在后。

③ 控制码

控制码的格式如图 8-13 所示：

图 8-13 控制码格式

④ 数据域长度 L

L 为数据域的字节数。读数据时 L≤200，写数据时 L≤50，L=0 时无数据域。

⑤ 数据域 DATA

数据域包括数据标识、密码、操作都代码、数据、帧序号等，其结构随控制码的功能而改变。传输时发送方按字节进行加 33H 处理，接收方按字节进行减 33H 处理。

⑥ 校验码 CS

从第一个帧起始符开始到校验码之前的自有各字节的模 256 的和，即各字节二进制算术

和，不计超过 256 的溢出值。

⑦ 结束符 16H

标识一帧信息的结束，其值为 16H = 00010110B。

（2） 读数据

① 主站请求帧

- 功能：请求读电能表数据；
- 控制码：C=11H；
- 数据域长度：L=04H+m（数据长度）；
- 帧格式 1（m=0）：

图 8-14 主站请求帧结构 （m=0）

- 帧格式 2（m=1，读给定块数的负荷记录）：

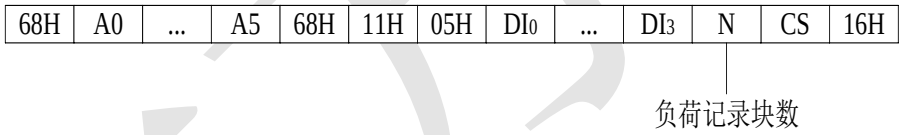

图 8-15 主站请求帧结构（m=1）

- 帧格式 3（m=6，读给定时间、块数的负荷记录）：

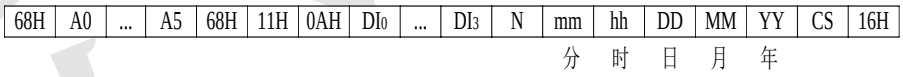

图 8-16 主站请求帧结构（m=6）

② 从站正常应答

- 控制码：C=91H 无后续数据帧；C=B1H 有后续数据帧；
- 数据域长度：L=04H+m（数据长度）；
- 无后续数据帧格式：

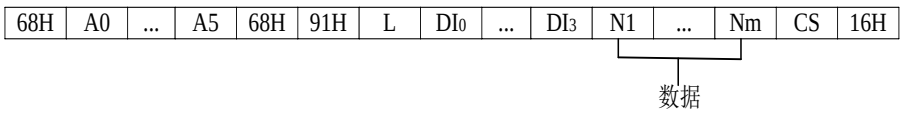

图 8-17 从站正常应答帧结构（C=91H）

- 有后续数据帧格式：

68H	A0	...	A5	68H	B1H	L	DI_0	...	DI_3	N1	...	Nm	CS	16H

图 8-18 从站正常应答帧结构（C=B1H）

如果没有满足条件的负荷记录，从站按正常应答帧格式返回（数据域只有数据标识，数据域长度为 4）。

③ 从站异常应答帧

- 控制码：C=D1H；
- 数据域长度 L=01H；
- 帧格式：

68H	A0	...	A5	68H	D1H	01H	ERR	CS	16H

错误信息字

图 8-19 从站异常应答帧结构（C=D1H）

CAN 协议解析与指令审计

本章以 CAN 协议为例，介绍车用通讯网络协议。控制器局域网总线（Controller Area Network，CAN）是一种用于实时应用的串行通讯协议总线，它可以使用双绞线来传输信号，是世界上应用最广泛的现场总线之一。CAN 协议用于汽车中各种不同元件之间的通信，以此取代昂贵而笨重的配电线束。该协议的健壮性使其用途延伸到其他自动化和工业应用。CAN 协议的特性包括完整性的串行数据通讯、提供实时支持、传输速率高达 1Mb/s、同时具有 11 位的寻址以及检错能力。

CAN 总线网络主要挂在 CAN_H 和 CAN_L，各个节点通过这两条线实现信号的串行差分传输，为了避免信号的反射和干扰，还需要在 CAN_H 和 CAN_L 之间接上 120 欧姆的终端电阻。

（1） 信号表示

CAN 总线采用不归零码位填充技术，也就是说 CAN 总线上的信号有两种不同的信号状态，分别是显性的（Dominant）逻辑 0 和隐形的（recessive）逻辑 1，信号每一次传输完后不需要返回到逻辑 0（显性）的电平。

位填充规则：发送器只要检测到位流里有 5 个连续相同值的位，便自动在位流里插入补充位。

（2） 通讯速率与通讯距离

CAN 总线上任意两个节点的最大传输距离与其位速率有关，如表 8-13 所示：

表 8-13 CAN 总线速率与最大通信距离关系

位速率/kbps	1000	500	250	125	100	50	20	10	5
最大距离/m	40	130	270	530	620	1300	3300	6700	10000

（3） 总线协议层次结构

① 物理层

在物理层中定义实际信号的传输方法，包括位的编码和解码、位的定时和同步等内容，作用是定义不同节点之间根据电气属性如何进行位的实际传输。

在物理连接上，CAN 总线结构提供两个引脚 CANH 和 CANL，总线通过 CANH 和 CANL 之间的差分电压完成信号的位传输。

在不同系统中，CAN 总线的位速率不同；在系统中，CAN 总线的位速率是唯一的，并且是固定的，这需要对总线中的每个节点配置统一的参数。

② 传输层

传输层是 CAN 总线协议的核心。传输层负责把接收到的报文提供给对象层，以及接收来自对象层的报文。传输层负责位的定时及同步、报文分帧、仲裁、应答、错误检测和标定、故障界定。

③ 对象层

在对象层中可以为远程数据请求以及数据传输提供服务，确定由实际要使用的传输层接收哪一个报文，并且为恢复管理和过载通知提供手段。

（4） **CAN 总线报文结构**

① 数据帧

大多数情况下使用的报文结构。

从标识符长度上，又可以把数据帧分为标准帧（11 位标识符）和扩展帧（29 位标识符）。

数据帧由 7 个不同的位场组成：帧起始、仲裁场、控制场、数据场、CRC 场、应答场、帧结束。其中数据场的长度为 0~8 个字节。标识符位于仲裁场中，报文接收节点通过标识符进行报文滤波。

② 远程帧

用来向某一个节点请求数据。

由总线上的节点发出，用于请求其他节点发送具有同一标识符的数据帧。当某个节点需要数据时，可以发送远程帧请求另一节点发送相应数据帧。与数据帧相比，远程帧没有数据场。

③ 错误帧

任何单元，一旦检测到总线错误就发出错误帧。

④ 过载帧

用于先行和后续的数据帧或者远程帧之间提供附加延时，保证接收端能够来得及处理前面收到的数据，包括过载标志和过载界定符。

Modbus 协议解析与指令审计

Modbus 是 OSI 模型第 7 层上的应用层报文传输协议，它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信。

自从 1979 年出现工业串行链路的事实标准以来，Modbus 使成千上万的自动化设备能够通信。目前，继续增加对简单而雅观的 Modbus 结构支持。互联网组织能够使 TCP/IP 栈上的保留系统端口 502 访问 Modbus。

Modbus 是一个请求/应答协议，并且提供功能码规定的服务。Modbus 功能码是 Modbus 请求/应答 PDU 的元素。Modbus 事务处理框架内使用的功能码，如图 8-20 所示：

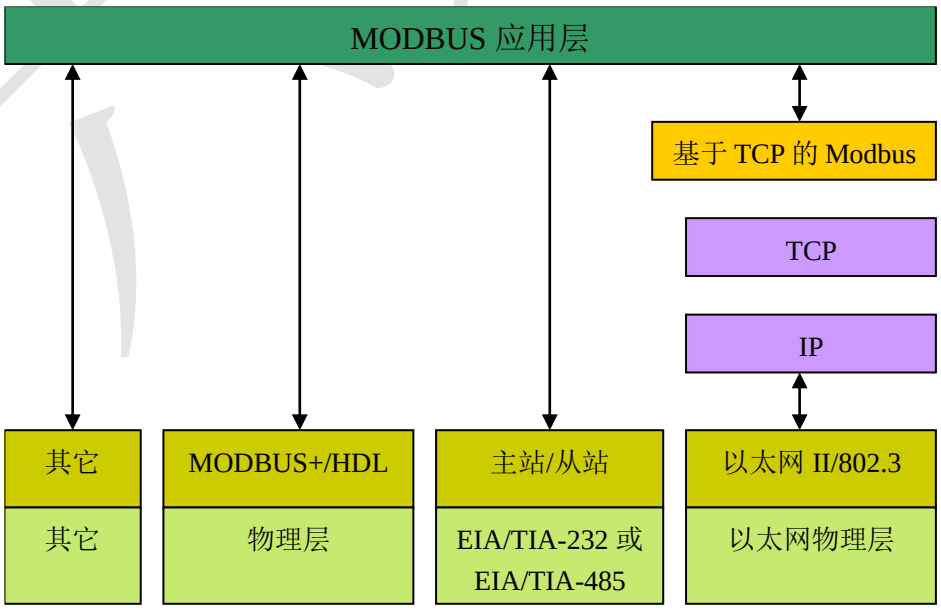

图 8-20 Modbus 通信栈

（1） Modbus 网络体系结构

Modbus 协议允许在各种网络体系结构内进行简单通信，体系结构如图 8-21 所示：

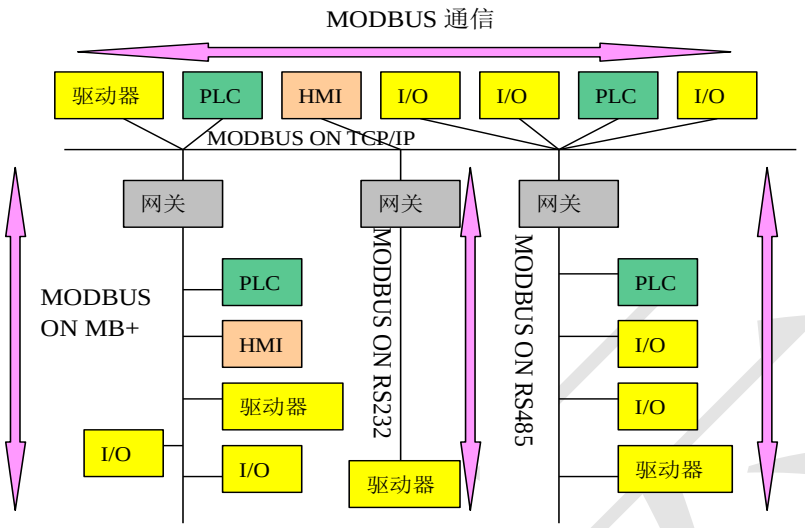

图 8-21Modbus 网络体系结构的实例

每种设备（PLC、HMI、控制面板、驱动程序、动作控制、输入/输出设备）都能使用 Modbus 协议来启动远程操作。在基于串行链路和以太 TCP/IP 网络的 Modbus 上可以进行相同通信。一些网关允许在几种使用 Modbus 协议的总线或网络之间进行通信。

（2） Modbus 事务处理

当服务器对客户机响应时，它使用功能码域来指示正常（无差错）响应或者出现某种差错（称为异常响应）。对于一个正常响应来说，服务器仅对原始功能码响应，如图 8-22 所示：

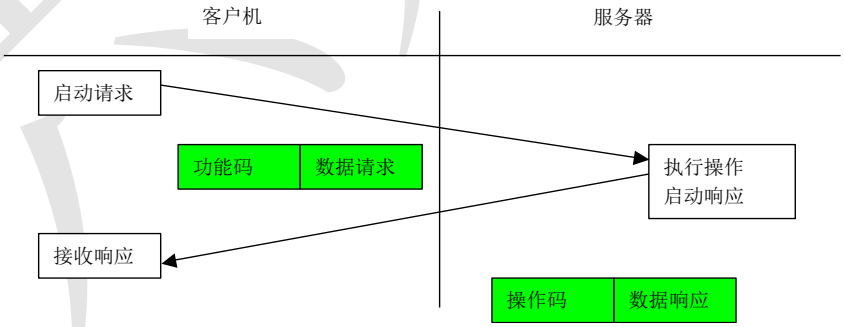

图 8-22 Modbus 事务处理（无差错）

对于异常响应，服务器返回一个与原始功能码等同的码，设置该原始功能码的最高有效位为逻辑 1，如图 8-23 所示：

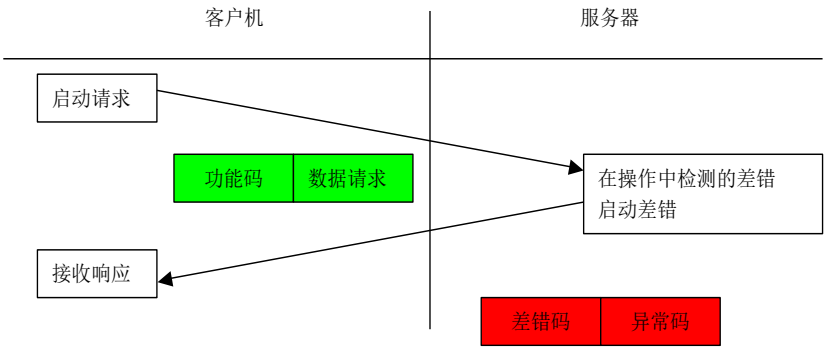

图 8-23Modbus 事务处理（异常响应）

（3） 公共功能码定义

公共功能码定义如表 8-14 所示：

表 8-14 公共功能码定义

功能	访问类型	内存类型	功能码说明	功能码		（十六进制）
				码	子码	
数据访问	比特访问	物理离散量输入	读输入离散量	02		0x02
		内部比特	读线圈	01		0x01
		或	写单个线圈	05		0x05
		物理线圈	写多个线圈	15		0x0F
	16 比特访问	输入存储器	读输入寄存器	04		0x04
			读多个寄存器	03		0x03
		内部存储器	写单个寄存器	06		0x06
		或	写多个寄存器	16		0x10
		物理输出存储器	读/写多个寄存器	23		0x17
			屏蔽写寄存器	22		0x16
	文件记录访问		读文件记录	20	6	0x14
			写文件记录	21	6	0x15
封装接口			读设备识别码	43	14	0x2B

常用功能码：

- 01（0x01）读线圈
- 02（0x02）读离散量输入
- 03（0x03）读保持寄存器
- 04（0x04）读输入寄存器
- 05（0x05）写单个线圈

- 06（0x06）写单个寄存器
- 15（0x0F）写多个线圈
- 16（0x10）写多个寄存器
- 43（0x2B）读设备识别码

（4） Modbus-Tcp 请求报文

Modbus-TCP 请求报文如表 8-15 所示：

表 8-15 Modbus-TCP 请求数据

Modbus-TCP 请求数据： 0080f4e1aaee1c3947c109f10800450000345ca6400080060000c0a8017bc0a8010ae97501f6c7c81b08e91000215018fad083fc0000 72 13 00 00 00 06 01 03 00 04 00 04				
	示例	长度	说明	备注
Map **报文头**	0x72	1	事务处理标识符 Hi	客户机发起，服务器复制，用于事务处理配对
	0x13	1	事务处理标识符 Lo	
	0x0000	2	协议标识符号	客户机发起，服务器复制 Modbus 协议 = 0.
	0x0006	2	长度	从本字节下一个到最后
	0x01	1	单元标识符	客户机发起，服务器复制串口链路或其他总线上远程终端标识
功能码	0x03	1	功能码，读寄存器	参考标准 Modbus 协议
数据	0x0004	2	起始地址	
	0x0004	2	寄存器数量	
校验				

（5） Modbus-Tcp 响应报文

Modbus-TCP 响应报文如表 8-16 所示：

表 8-16Modbus-TCP 响应数据

Modbus-TCP 响应数据： 1c3947c109f10080f4e1aaee080045000039d5360000400621b3c0a8010ac0a8017b01f6e975e9100021c7c81b1450 1820006b490000 72 13 00 00 00 0b 01 03 08 00 00 00 0a 00 64 00 00				
	示例	长度	说明	备注
Map 报文头	0x72	1	事务处理标识符 Hi	客户机发起，服务器复制，用于事务处理配对
	0x13	1	事务处理标识符 Lo	
	0x0000	2	协议标识符号	客户机发起，服务器复制 Modbus 协议 = 0.
	0x000b	2	长度	从本字节下一个到最后
	0x01	1	单元标识符	客户机发起，服务器复制串口链路或其他总线上远程终端标识
功能码	0x03	1	功能码，读寄存器	参考标准 Modbus 协议
数据	0x 08	1	字节个数	
	0x----		数据每 2 个字节代表 1 个数据	
校验				

（6） Modbus 数据分析

PC 机向 PLC 使用功能码 06 向寄存器 03 写入 0X15，当写入成功后，PLC 向 PC 机响应数据。具体的抓包分析如图 8-24 所示：

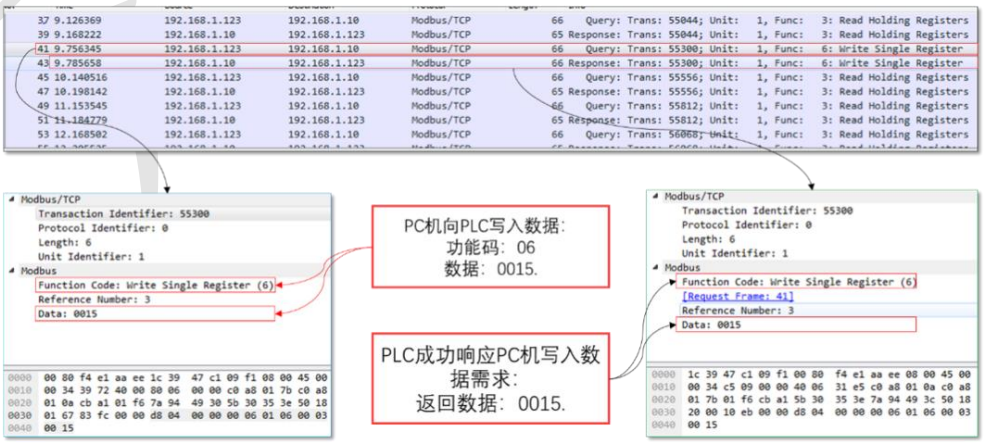

图 8-24 Modbus 数据抓包分析

8.5 工业网络安全

工业互联网网络体系由网络互联、数据互通和标识解析三部分组成。网络互联实现要素之间的数据传输；数据互通实现要素之间传输信息的相互理解；标识解析实现要素的标记、管理和定位。

（1） 网络互联

网络互联呈现出融合、开放、灵活三大趋势。

① 网络架构将逐步融合（IT 与 OT 融合）

一是网络结构扁平化，工厂内网络的车间级和现场级将逐步融合（尤其在流程行业），IT 网络与 OT 网络逐步融合。

二是高实时控制信息与非实时过程数据共网传输，新业务对数据的需求促使控制信息和过程数据的传输并重。

三是有线与无线的协同，以 5G 为代表的无线网络将更为广泛的应用与工厂内，实现生产全流程、无死角的网络覆盖。

② 网络更加开放（TSN）

一是技术开放，以时间敏感网络（TSN）为代表的新型网络技术将打破传统工业网络众多制式间的技术壁垒，实现网络各层协议间的解耦合，推动工业互联网网络技术的开放。

二是数据开放，工业互联网业务对数据的强烈需求，促使传统工业控制闭环中沉没或消失的数据开放出来，而生产全流程的数据将由更标准化的语法和数据模型开放给上层应用使用。

③ 网络控制和网络管理将更为灵活友好（SDN）

一是网络形态的灵活。未来工厂内网将能够根据智能化生产、个性化定制等业务灵活调整形态，快速构建出生产环境，工厂外网将能够为不同行业、企业提供定制化的网络切片，实现行业、企业的自治管理控制。

二是网络管理的友好。随着网络在产研供销中发挥日益重要的作用，网络管理将变得复杂，软件定义技术应用将提供网络系统的可呈现度，网络管理界面将更为友好。

三是网络的服务将更为精细。工厂内网将针对控制、监测等不同性能需求，提供不同的网络通道；工厂外网将针对海量设备广覆盖、企业上网、业务系统上云、公有云与私有云互通

等不同场景，提供细分服务。

（2） 数据互通

数据互通，旨在实现数据和信息在各要素间、各系统间的无缝传递，使得异构系统在数据层面能相互“理解”，从而实现数据互操作与信息集成。数据互通使得异构系统在数据层面能相互“理解”，从而实现数据互操作与信息集成。

（3） 标识解析

标识数据采集，主要定义了标识数据的采集和处理手段，包含标识读写和数据传输两个功能，负责标识的识读和数据预处理。标签管理主要定义了标识的载体形式和标识编码的存储形式，负责完成载体数据信息的存储、管理和控制，针对不同行业、企业需要，提供符合要求的标识编码形式。标识注册是在信息系统中创建对象的标识注册数据，包括标识责任主体信息、解析服务寻址信息、对象应用数据信息等，并存储、管理、维护该注册数据。

标识解析能够根据标识编码查询目标对象网络位置或者相关信息的系统装置，对机器和物品进行唯一性的定位和信息查询，是实现全球供应链系统和企业生产系统的精准对接、产品全生命周期管理和智能化服务的前提和基础。标识数据处理定义了对采集后的数据进行清洗、存储、检索、加工、变换和传输的过程，根据不同业务场景，依托数据模型来实现不同的数据处理过程。标识数据建模构建特定领域应用的标识数据服务模型，建立标识应用数据字典、知识图谱等，基于统一标识建立对象在不同信息系统之间的关联关系，提供对象信息服务。

标识解析系统发展趋势，一是基于标识解析的数据服务成为工业互联网应用的核心，闭环的私有标识及解析系统逐步向开环的公共标识及解析系统演进。二是工业互联网标识解析安全机制成为工业互联网应用的基础，发展安全高效的标识解析服务成为共识。

通信和连接保护

通信和连接性保护提供端点到网络的连接的物理安全性，保护网络中的信息流，以及端点之间通信的加密保护。在下图中，这两个功能由跨顶层四个构建块的区域支持：网络配置和管理、网络监视和分析、通信端点保护和连接的物理安全。

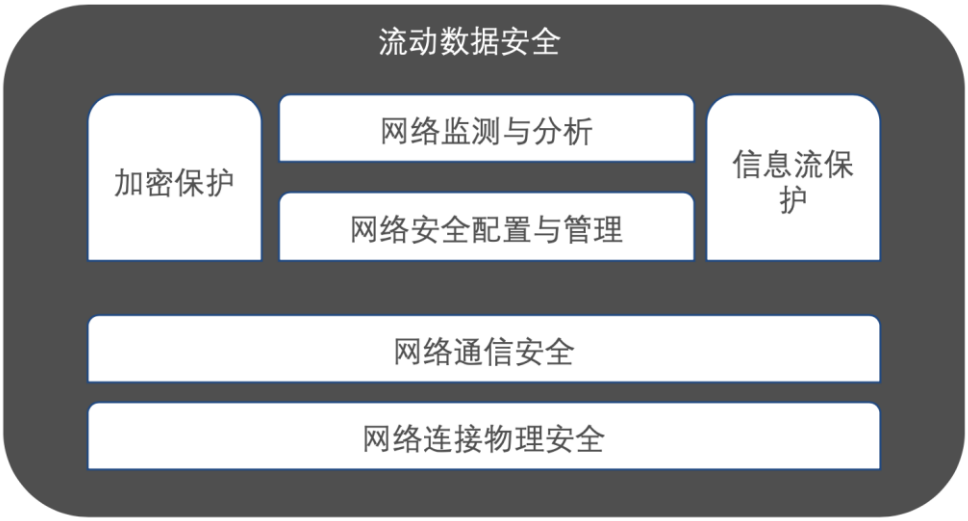

图 8-25 流动数据安全

网络连接物理安全确保网络物理连接层（电缆、无线电）受到保护。加密保护使用加密技术来保护通信方的真实性以及交换数据和元数据的完整性和机密性。

信息流保护通过使用网络分割和周界保护技术隔离网络流，确保只有允许的类型的消息和内容才能到达敏感系统和网络。

网络配置和管理控制对所有网络元素的更新，并为通信提供安全策略和配置的实施，包括网络分段、加密保护的通信设置以及网关和防火墙的配置。

网络监测与分析收集网络数据进行分析，包括入侵检测、网络访问控制、深度包检测和网络日志分析。动态数据保护提供控制，以保持其数据的完整性、机密性和可用性。

不同的信息交换模式具有不同的安全需求。工业系统中广泛使用的模式包括请求-响应模式和发布-订阅模式。

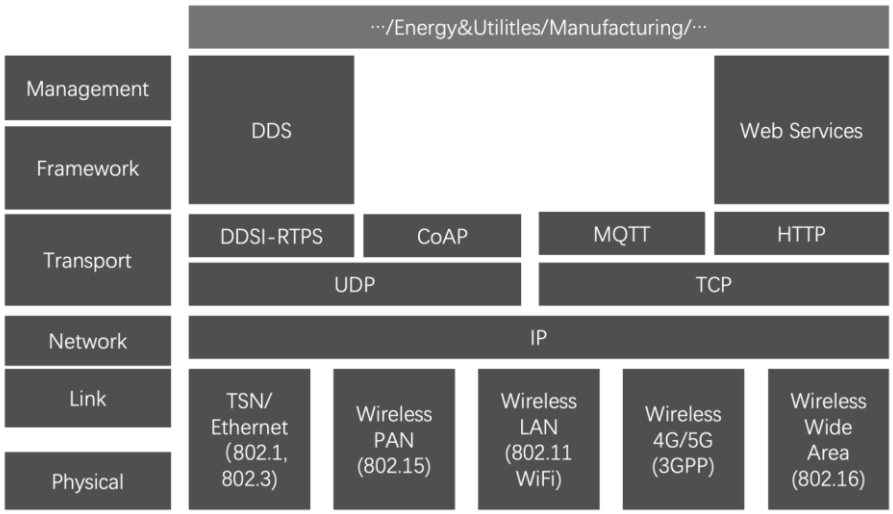

图 8-26 工业通信和连接标准示例图

请求-响应模式可以在堆栈的任何层使用。使用此模式的协议包括 Java 远程方法调用（Java RMI）、Web 服务/SOAP、远程过程调用数据分发服务（RPC over DDS）、开放平台通信（OPC）、全局平台安全通道协议和 Modbus。它们对安全性的支持各不相同；例如，Modbus 不能抑制广播消息，不提供消息校验和，并且缺乏对身份验证和加密的支持。

发布-订阅通信模式的主要威胁类型是未经授权的订阅、未经授权的发布、篡改和重播以及对交换数据的未经授权的访问。这种模式的某些实现（例如，经典的 MQTT 和 AMQP）依赖于中间消息代理存储和转发消息，但是消息代理可能是单点故障。另一种方法是无代理的对等实现，如 DDS 标准。

与互联网时代 TCP/IP、HTTP 一统天下的局面不同，物联网的通信环境有 Ethernet、Wi-Fi、RFID、NFC（近距离无线通信）、Zigbee、6LoWPAN（IPV6 低速无线版本），Bluetooth、GSM、GPRS、GPS、3G、4G 等网络，而每一种通信应用协议都有一定适用范围。AMQP、JMS、REST/HTTP 都是工作在以太网，COAP 协议是专门为资源受限设备开发的协议，而 DDS 和 MQTT 的兼容性则强很多。

（1） REST（松耦合服务调用）

REST 即表述性状态传递（Representational State Transfer, REST）是 Roy Fielding 博士在 2000 年他的博士论文中提出来的一种软件架构风格。它是一种针对网络应用的设计和开发方式，可以降低开发的复杂性，提高系统的可伸缩性。

而 REST 被应用于物联网主要是基于 HTTP web 服务的转化，因为 REST 模式的 Web 服务与复杂的 SOAP 和 XML-RPC 对比来讲明显的更加简洁，越来越多的 web 服务开始采用 REST 风格设计和实现。

REST 其实是互联网中服务调用 API 封装风格，物联网中数据采集到物联网应用系统中，在物联网应用系统中，可以通过开放 REST API 的方式，把数据服务开放出去，被互联网中其他应用所调用，所以它非常利于服务平台与物联终端的独立开发，但它的通讯数据量与 API 内容密切相关，且是一种无状态通信，对安全机制需要重新设计。

（2） CoAP 协议

由于物联网中的很多设备都是资源受限型的，即只有少量的内存空间和有限的计算能力，所以传统的 HTTP 协议应用在物联网上就显得过于庞大而不适用。IETF 的 CoRE 工作组提出了一种基于 REST 架构的 CoAP 协议。

CoAP 是一种应用层协议，它运行于 UDP 协议之上而不是像 HTTP 那样运行于 TCP 之上。CoAP 协议非常的小巧，最小的数据包仅为 4 字节。

CoAP 并不能替代 HTTP 协议，但是对于那些小设备（256KB Flash 32KBRAM 20MHz 主频）而言 CoAP 的确是一个好的解决方案。

CoAP 采用和 HTTP 协议相同的请求响应工作模式。CoAP 协议共有 4 中不同的消息类型：

① CON——需要被确认的请求，如果 CON 请求被发送，那么对方必须做出响应；

② NON——不需要被确认的请求，如果 NON 请求被发送，那么对方不必做出回应；

③ ACK——应答消息，如果接受到 CON 消息的响应；

④ RST——复位消息，当接收者接受到的消息包含一个错误，接受者解析消息或者不再关心发送者发送的内容，那么复位消息将会被发送。

（3） MQTT 协议（低带宽）

MQTT（Message Queuing Telemetry Transport，消息队列遥测传输协议），是一种基于发布/订阅（publish/subscribe）模式的“轻量级”通讯协议，该协议构建于 TCP/IP 协议上，由 IBM 在 1999 年发布。MQTT 最大优点在于，可以以极少的代码和有限的带宽，为连接远程设备提供实时可靠的消息服务。做为一种低开销、低带宽占用的即时通讯协议，使其在物联网、小型设备、移动应用等方面有较广泛的应用。

MQTT 协议运行在 TCP/IP 或其他网络协议，提供有序、无损、双向连接。其特点包括：

① 使用的发布/订阅消息模式，它提供了一对多消息分发，以实现与应用程序的解耦；

② 对负载内容屏蔽的消息传输机制；

③ 对传输消息有三种服务质量（QoS）：

- 最多一次，这一级别会发生消息丢失或重复，消息发布依赖于底层 TCP/IP 网络，即：<=1；
- 至多一次，这一级别会确保消息到达，但消息可能会重复，即：>=1；
- 只有一次，确保消息只有一次到达，即：=1。在一些要求比较严格的计费系统中，可以使用此级别；

④ 数据传输和协议交换的最小化（协议头部只有 2 字节），以减少网络流量；

⑤ 通知机制，异常中断时通知传输双方。

实现 MQTT 协议需要：客户端和服务器端，MQTT 协议中有三种身份：发布者（Publish）、代理（Broker 服务器）、订阅者（Subscribe）。其中，消息的发布者和订阅者都是客户端，消息代理是服务器，消息发布者可以同时是订阅者。

MQTT 传输的消息分为：主题（Topic）和负载（Payload）两部分

- Topic，可以理解为消息的类型，订阅者订阅（Subscribe）后，就会收到该主题的消息内容（payload）
- Payload，可以理解为消息的内容，是指订阅者具体要使用的内容

MQTT 协议一般适用于设备数据采集到端（Device->Server，Device->Gateway），集中星型网络架构（hub-and-spoke），不适用设备与设备之间通信，设备控制能力弱，另外实时性较差，一般都在秒级。

（4） DDS 协议（高可靠性、实时）

数据分发服务 DDS（Data Distribution Service）是对象管理组织（OMG）在 HLA 及 CORBA 等标准的基础上制定的新一代分布式实时通信中间件技术规范，DDS 采用发布/订阅体系架构，强调以数据为中心，提供丰富的 QoS 服务质量策略，能保障数据进行实时、高效、灵活地分发，可满足各种分布式实时通信应用需求。DDS 信息分发中间件是一种轻便的、能够提供实时信息传送的中间件技术。

DDS 很好地支持设备之间的数据分发和设备控制，设备和云端的数据传输，同时 DDS 的数据分发的实时效率非常高，能做到秒级内同时分发百万条消息到众多设备。DDS 在服务质量（QoS）上提供非常多的保障途径，这也是它适用于国防军事、工业控制这些高可靠性、可安全性应用领域的原因。但这些应用都工作在有线网络下，在无线网络，特别是资源受限的情况下，没有见到过实施案例。

（5） AMQP 协议（互操作性）

AMQP，即 Advanced Message Queuing Protocol，一个提供统一消息服务的应用层标准高级消息队列协议，是应用层协议的一个开放标准，为面向消息的中间件设计。基于此协议的客户端与消息中间件可传递消息，并不受客户端/中间件不同产品，不同的开发语言等条件的限制。Erlang 中的实现有 RabbitMQ 等。

AMQP 协议是一个二进制协议，拥有一些现代特点：多信道、协商式、异步、安全、跨平

台、中立、高效。AMQP 通常被划分为三层：

① 模型层定义了一套命令（按功能分类），客户端应用可以利用这些命令来实现它的业务功能。

② 会话层负责将命令从客户端应用传递给服务器，再将服务器的应答传递给客户端应用，会话层为这个传递过程提供可靠性、同步机制和错误处理。

③ 传输层提供帧处理、信道复用、错误检测和数据表示。

实现者可以将传输层替换成任意传输协议，只要不改变 AMQP 协议中与客户端应用程序相关的功能。实现者还可以使用其他高层协议中的会话层。

AMQP 协议最早应用于金融系统之间的交易消息传递，在物联网应用中，主要适用于移动手持设备与后台数据中心的通信和分析。

（6） XMPP 协议（即时通信）

XMPP 是一种基于标准通用标记语言的子集 XML 的协议，它继承了在 XML 环境中灵活的发展性。因此，基于 XMPP 的应用具有超强的可扩展性。经过扩展以后的 XMPP 可以通过发送扩展的信息来处理用户的需求，以及在 XMP 的顶端建立如内容发布系统和基于地址的服务等应用程序。而且，XMPP 包含了针对服务器端的软件协议，使之能与另一个进行通话，这使得开发者更容易建立客户应用程序或给一个配好系统添加功能。

XMPP 协议是自由、开放、公开的，并且易于了解。而且在客户端、服务器、组件、源码库等方面，都已经各自有多种实现。但随着通常超过 70%的 XMPP 协议的服务器的数据流量的存在和近 60%的被重复转发，XMPP 协议目前拥有一个大型架空中存在的数据提供给多个收件人。适用于即时通信的应用程序，还能用在网络管理、内容供稿、协同工具、档案共享、游戏、远端系统监控等。

网络数据隔离

通常有三种基本的网络通信通道：数据、控制和管理。每个通道都应与其他通道隔离，并分别进行管理和监视。

数据通道有时称为操作监视通道，用于报告操作信息和端点的状态。控制通道用于改变工业过程的行为，并改变端点的状态。管理通道承载管理通信，如计算机配置文件、安全策略、端点配置更改和访问控制设置。

使用单独的通信信道可以降低管理和监视每种通信的成本和复杂性。在给定的端点上，每种类型的通道随时都可能有多个活动实例。可以为每个通道定义单独的安全控制。其中包括技术保密控制，如加密、网络分段和通信授权，以及完整性控制，如消息签名。

网络分区

工业安全标准，如 ISA/IEC 62443-1-1、ISA/IEC 62443-3-3、ANSSI、NIST 800-821 和其他标准，都建议将网络分成若区域，每个网络区域包含若干资产。

网络分区可以是细粒度的，也可以是粗粒度的。分割的候选对象包括公共网络、商业网络、操作网络、工厂范围的网络、控制网络、设备网络、保护网络和安全网络。细粒度分割通常更好，但维护成本通常更高。

网关和过滤

网关可以在没有附加控制的情况下在网络区域之间转换和转发信息，例如，协议转换网关可以将传统的、不安全的通信协议转换为现代的、加密的协议。网关还可以通过多种方式过滤信息流，例如，防火墙仅转发符合特定规则的消息，单向网关在物理上能够仅在一个方向上传输信息，并阻止在另一个方向上的所有通信。

网关可以对重要的应用程序功能进行编码。例如，拥有双网卡的历史服务器可以看作是一个双向信息网关，具有显著的持久性和分析功能。历史服务器使用设备通信协议通过一个网络接口从 OT 网络收集数据，并使用客户机/服务器协议通过第二个网络接口将数据发布到 IT 网络。再比如数据分发服务（DDS）网关通常在应用程序/中间件级别转换信息流，同时还支持安全持久性、安全的分布式日志记录和安全的数据转换。

“工业互联网参考体系结构”建议使用网关集成多种连接技术，例如保护传统端点和通信链路，同时在 IIoT 系统中实现棕地和绿地部署的互操作性，安全网关充当中介。应该使用类似的方法将对安全功能支持有限的遗留端点集成到现代 IIoT 系统中。

IIoT 网关对一个或多个遗留端点进行代理，并将遗留端点期望的遗留协议转换为新端点使用的现代互操作性协议。它可以防止传统的端点攻击面暴露在网络中。它还可以在支持每用户身份验证和基于角色的授权的 IIoT 系统和不支持这种授权的遗留系统之间进行中介。此外，IIoT 网关可以将信息规范化为几个选定的互操作性协议，这样应用程序就可以互操作，而不必支持所有这些协议。这样可以减少攻击面。

IIoT 网关和每个遗留端点之间的链接也可以使用对遗留协议透明的技术进行保护。例如，

在 LAN 中，VLAN 技术可用于分离传统网段上的设备，当这些设备需要与 IIoT 网关通信而不需要彼此通信时。在广域网中，易受攻击的传统通信协议可以通过在 IIoT/WAN 网络边界部署的防火墙中实现的 VPN 透明地隧道化。

单向网闸

单向网闸在 IEC 62443-1 和 NIST 800-821 标准都有定义，它在硬件物理级别上只允许信息在一个方向上流动。

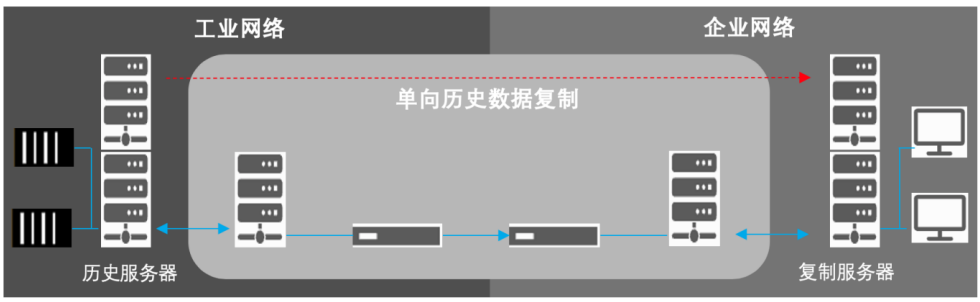

图 8-27 单向网闸信息复制示例图

上图展示了一个典型的单向网闸，部署在 IT 与 OT 边界，将工厂历史服务器的数据复制到公司数据库。传输（TX）代理向工厂历史服务器查询历史数据点，并通过单向硬件将其推送到公司 IT 网络。接收（RX）代理将历史数据存储在副本历史服务器。外部用户和应用程序查询副本历史服务器以访问历史数据。来自企业网络或企业历史服务器的任何攻击都不会影响单向受保护工厂网络的运行。

与防火墙不同，单向网闸通常不会将消息从源网络转发到目标网络，因为网关软件在每个网络上保持独立的通信连接。

网络访问控制

网络访问控制（NAC）将网络控制和网络安全控制结合起来，授予或限制对通信网络的逻辑访问。例如，用户将以太网电缆连接到交换机或路由器。电缆建立物理连接，交换机或路由器评估终端设备是否被授予对通信协议的逻辑访问权。如果未授予访问权限，物理链路将保持“死”状态以进行网络通信，连接的终端设备将保持锁定在网络之外。

一种著名的访问授权机制是 IEEE 802.1X1。根据每个设备的凭据（如身份证书）以及用户名和密码，允许或拒绝设备访问网络。IEEE 802.1X 允许网络运营商对可以在网络中通信的设备集保持强大的控制。

基于 IEEE 802.1X 认证方法的网络访问控制在许多现代以太网交换机和无线局域网接入

点上都是可用的。在以太网交换机中，802.1X 通常按端口执行。在无线局域网中，WLAN 接入点代替物理网络端口作为认证点。

请求访问网络的设备必须实现请求者。交换机、路由器或无线接入点实现认证对应方认证器。在某些情况下，网络设备可以实现认证器和请求功能。

请求者请求来自将访问请求转发到身份验证服务器以供审阅的身份验证程序的访问。认证后，交换机或无线接入点启用端口或无线连接，以进行除 IEEE 802.1X 认证帧以外的通信。认证服务器可以集成到设备本身中。

认证服务器也可以作为整个网络的集中资源，通过远程认证拨号用户服务（RADIUS）服务器实现。然后可以集中管理用户名和密码等访问凭据，所有网络设备都可以作为身份验证器进行访问。此外，用户特定的配置信息可以通过 RADIUS 发布，并通过 IEEE 802.1X 分配，例如特定 VLAN 的成员资格。

工业网络通信安全模型和策略

IIoT 系统中的各种系统组件可以由一个实体拥有和部署，但也可以由其他实体管理、维护或使用。例如，维修公司必须能够访问喷气发动机的控制和仪表以及监控通道，以便进行预测性维修。在某些情况下，该通道在设备运行时进行，且操作不得受到该通道的影响。一旦适当的安全策略到位，就可以使用诸如 SAML、OAuth、OpenID 等技术强制跨软件和硬件边界保护事务。

安全策略通常是使用安全模型正式或半正式捕获的。安全模型指定了主体和对象之间允许和禁止的关系，因此可以更具体地定义安全策略。例如，Linux 文件系统的安全模型指定哪些主体（即进程）可以对哪些对象（如文件）执行哪些操作（如读、写、执行）。IIoT 通信和 DDS 等连接协议也存在类似的安全模型。

通信和连接安全策略必须从全面的风险分析中得出。这些策略指定如何筛选和路由通信量、如何保护交换的数据和元数据以及应使用哪些访问控制规则。通信和连接策略可以用策略定义语言（即 XML 或 XACML）定义，并通过通信中间件和网络管理规则的组合来实施。应对这些政策进行明确的一致性测试和全面性评估。应使用从定义的策略派生的测试用例进行安全测试。

应以精细的粒度指定和实施安全策略。正确的策略必须以详细、一致和全面的方式定义，定义的策略必须通过安全测试强制执行，以提供此类强制执行的证据。

8.6 工业边缘系统安全

边缘层提供海量工业数据接入、转换、数据预处理和边缘分析应用等功能。包括：工业数据接入、协议解析、数据预处理、边缘智能分析、边缘应用部署与管理。

工业互联网边缘层面临的困难：

（1）数据采集，需要解决数据过少问题；

（2）协议转换，需要解决数据过杂问题；

（3）边缘智能，解决数据过多的问题。

根据 IDC 报告，40%的数据将在边缘侧进行存储，处理与分析，因为边缘侧业务数据存在下面三方面困难：

（1）不敢传：数据安全；

（2）不需传：本地化、实时性；

（3）不能传：时延、功耗、计算量、协议适配。

不是所有业务和数据都适合放在云上计算，一般在设备侧适合采用边缘计算，车间侧适合采用雾计算，企业侧或整个行业适合采用云计算。适合云计算的业务包括非实时和大数据业务、需要纵向和横向对比分析的业务、需要和业务系统集成的业务、需要全局优化的业务。

边缘计算是指在网络边缘处理数据，可以减少请求响应时间，延长电池寿命并减少网络带宽，同时确保数据安全性和私密性。边缘节点（包括智能设备，手机，平板电脑等）生成数据并将其上传到云中心，服务提供商也生成数据以上传到云中心。边缘节点向云中心发送请求，云中心将相关数据返回到边缘节点。如图 8-28 所示：

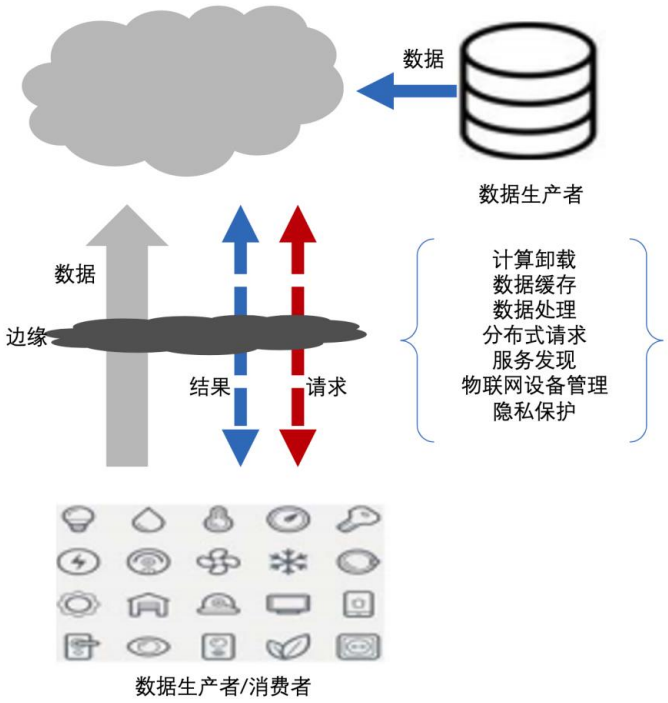

图 8-28 边缘计算

在数据上传过程中，别有用心的人很容易收集数据。为了确保数据的私密性，可以从以下几个方面入手：

（1） 在网络边缘处理用户数据，以便仅在本地存储，分析和处理数据；

（2） 为不同的应用程序设置权限，并限制对私有数据的访问；

（3） 边缘网络是一个高度动态的网络，需要有效的工具来保护网络中的数据传输。

8.7 工业互联网平台安全

工业互联网平台的目标是重构工业企业的传统 IT 架构，打通 IT 和 OT，一方面从 OT 和 IT 采集数据，实现设备数据与业务系统数据的汇聚集成，形成数据湖，基于统一数据开发 APP，消除数据孤岛；另一方面，基于数据建模和分析构建工业 APP，推动装备从“功能机”演进为“智能机”，构建起“状态感知-实时分析-科学决策-精准执行”的闭环智能。支撑工业互联网平台的三大特性：泛在物联、弹性供给、高效配置。

工业互联网平台包括 IaaS、PaaS 和 SaaS 三层。

图 8-29 工业互联网平台安全

平台 IaaS 层安全

（1） 边界安全

① 流量安全监控

云环境边界的流量监测与可视化可通过开发流量安全监控模块实现，流量安全监控模块是毫秒级的攻击监控产品。通过对工业互联网平台入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为，并与其他防护模块联动防护。同时，流量安全监控模块在整个工业互联网平台综合安全防护系统构建的纵深防御体系中，提供了丰富的信息输出与基础的数据支持。

② 抗 DDoS 流量清洗

DDoS 流量清洗模块为工业互联网平台用户提供基于云计算架构设计和海量 DDoS 攻击防御。该模块应基于云计算的环境设计，具有高度的扩展性和可移植性，可以有效的应用于工业互联网平台企业通过不同框架搭建的云计算环境中，提供经过强大的抗 DDoS 能力，如图 8-30 所示。

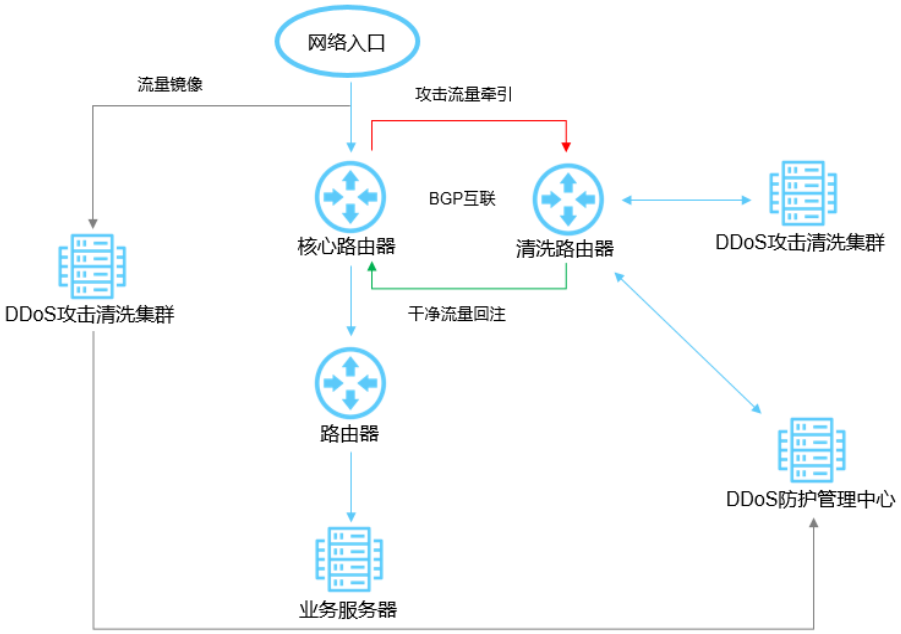

图 8-30 针对 DDoS 防护的流量调度示意

③ 云边界安全网关

安全接入网关是工业互联网平台与边缘计算节点进行安全通信的网关型服务设备，该网关用于与物联网接入安全网关、工业控制系统安全接入网关进行安全的通信，并对攻击请求进行抵御。此外，安全接入网关对通过企业办公网及互联网访问工业互联网平台的用户进行身份鉴别，并对访问过程提供完整性和机密性保护。

访问请求在经过抗 DDoS，接入认证等功能处理后，才会转发至内网。即将转发至内网的流量都是经过授权的用户发送的非暴力攻击请求，针对这一部分内容，应采用并行计算安全引擎对流量进行内容层过滤，排查其中是否存在基于已知漏洞、恶意代码发起的攻击尝试，对风险行为进行阻断。

为实现高性能的攻击行为识别与过滤，安全过滤应采用并行处理架构，其逻辑结构如图 8-31 所示，把最耗费 CPU 资源的网络数据处理放在数据平面，由多个 CPU 并行处理。

图 8-31 一体化引擎安全防护架构图

（2） 云网络安全

① 访问控制

工业互联网平台的云端业务系统都需要进行分区、分安全域进行管理，支持针对云内所有虚拟机基于地址、端口号或业务应用类型进行逻辑安全域的划分，支持在任意安全域之间部署访问控制策略，根据安全防护级别配置默认防护动作，同时，访问控制规则需支持多条并可依据优先级进行顺序调整。

云网络微隔离防护系统支持基于 IP 地址、应用类型和业务系统等多个维度划分逻辑安全域，支持基于安全域甚至虚拟机粒度进行微隔离访问控制。

② 入侵防范

为应对基于漏洞的入侵行为，工业互联网平台的业务系统需具备入侵防范的能力，能够针对云内任意虚拟机的东西向流量和南北向流量进行入侵检测和安全防护，该入侵防范系统需内置工业入侵特征库，能够识别出工业控制协议，能够针对工业控制系统的入侵和攻击行为进行有效防护。

云网络微隔离防护系统能够实时针对所有进出虚拟机的业务流量进行异常威胁检测，因此，无论是来自于外部的入侵行为，还是来自于内部的入侵行为，安全组件都能够及时的发现并阻断告警，避免因内外部恶意入侵导致对工业互联网平台的运营威胁。

③ 病毒防护

网络病毒无论对物理主机还是虚拟主机造成的影响都是极大的，轻则耗尽系统资源，导致

业务无法正常运营；重则窃取或加密核心数据，导致经济损失或服务中断。而网络访问正是导致虚拟机中毒的一个重要路径，因此部署云网络层的防病毒产品是极其必要的，一方面可以有效遏制病毒通过网络路径感染虚拟机，另一方面也可以防止单台虚拟机中毒后导致的大面积内部横向扩散和感染，极大的降低感染病毒给数据中心带来的安全风险。

云网络微隔离防护系统的安全组件支持网络病毒防护引擎，能够实时基于虚拟机的网络流量进行病毒和恶意软件的检测，有效避免虚拟机通过邮件或者网络文件下载导致的主机中毒，同时，能够有效遏制已经感染病毒的虚拟机对内部其他虚拟机的横向污染，将病毒的影响范围降到最低。

④ 安全可视

作为工业互联网平台的运维管理人员，其需要能够实时且全面的了解整个平台内部的运营状况和安全态势，那么全面高效的可视化工具就尤为重要。

产品支持对云平台内所有虚拟资产绘制逻辑一致的 3D 网络拓扑，通过该拓扑，用户可以实时了解工业互联网平台的运营状态和安全态势，包括：虚拟机运行状态信息、虚拟机流量统计信息、实时访问应用情况、虚拟机受攻击情况和安全事件相关信息等。

（3） **云主机安全**

① 云主机系统安全加固

建议工业互联网平台采用安全的方式对云服务器实例上的操作系统进行访问和操作。例如，使用 SSH 公钥和私钥对，并妥善保存私钥（至少要求使用复杂密码，可在创建实例时设置）；采用更安全的 SSHv2 方式远程登录；采用 sudo 指令的方式实现临时提权等。

② 虚拟主机恶意代码防范

传统的病毒防护解决方案都是通过安装防病毒应用程序到主机的操作系统中。在整合服务器虚拟化后，要实现针对病毒的实时防护，同样需要在虚拟主机的操作系统中安装防病毒 Agent 程序，但是服务器虚拟化的目的是整合资源，最大化的发挥服务器资源的利用率，而传统的防病毒技术需要在每个虚拟主机中安装程序，例如：一台服务器虚拟 6 台主机，传统方法需要安装 6 套 Agent，并且在制定扫描任务就需要消耗虚拟主机的计算资源，这种方式并没有达到节约计算资源的效果，反而增加了计算资源的消耗，并且在病毒库更新是带来更多的网络资源消耗。

针对有代理方案的诸多弊端，本方案采用在每个物理主机上部署独立安全组件虚拟机的方式进行主机的病毒防护，实现主机层的恶意代码防范。

平台 PaaS 层安全

（1） 安全编码标准

安全编码标准是为了实现应用安全开发的具体规范，建议工业互联网平台企业根据平台自身特点、常见安全问题和行业最佳实践编制安全编码标准，指导应用开发人员根据严格遵守技术要求的进行系统和应用的开发工作。

（2） 自动化测试工具

自动化测试是把以人为驱动的测试行为转化为机器执行的一种过程。通常，在设计了测试用例并通过评审之后，由测试人员根据测试用例中描述的规程一步步执行测试，得到实际结果与期望结果的比较。通过研制自动化测试工具，可以对借助工业互联网平台开发的工业 APP 进行功能、业务逻辑、代码缺陷在内的各方面验证，从而从根本上提高平台发布服务的安全水平，降低对外保护的脆弱性，减少被攻击的可能。

在另一方面，工具的建成也将为工业企业自行开发 APP 或第三方利用 PAAS 平台开发 APP 提供极大的便利，提升平台企业的竞争力，是平台企业开展安全综合防护系统建设是具有极大附加价值的安全措施。

（3） API 安全网关

API 网关是一系列服务集合的访问入口。从面向对象的设计角度来看，它与外观模式类似，实现对所有服务的封装。

API 安全网关，针对 API 服务的安全保护需求，实现了 API 接口的统一代理、访问认证、数据加密、安全防护、应用审计等能力。从而实现对数据分析服务和微服务组件的安全防护。

API 安全网关是以零信任架构为基础，用于业务应用/应用前置和后台服务之间的安全 API 调用，是零信任的访问控制策略执行节点。

API 安全网关，基于 Netty NIO 的响应式架构（分布式缓存基于 Redis；数据库基于 Mysql，分布式配置基于 ZooKeeper），实现 API 配置缓存，运行时不依赖 DB，配置更新后自动通知各网关节点。支持自定义组件，动态加载，在不中断网关服务的情况下重新加载配置和运行组件；同时还具备 API 服务连续异常后自动熔断和自我恢复，访问异常、超时处理等功能。

API 安全网关核心运行过程不写磁盘 IO，避免磁盘 IO 性能影响网关吞吐量；Docker 容器

化支持，拆分网关、管理服务、第三方中间件依赖等镜像，便于灵活扩容。

API 网关工作架构如图 8-32 所示。

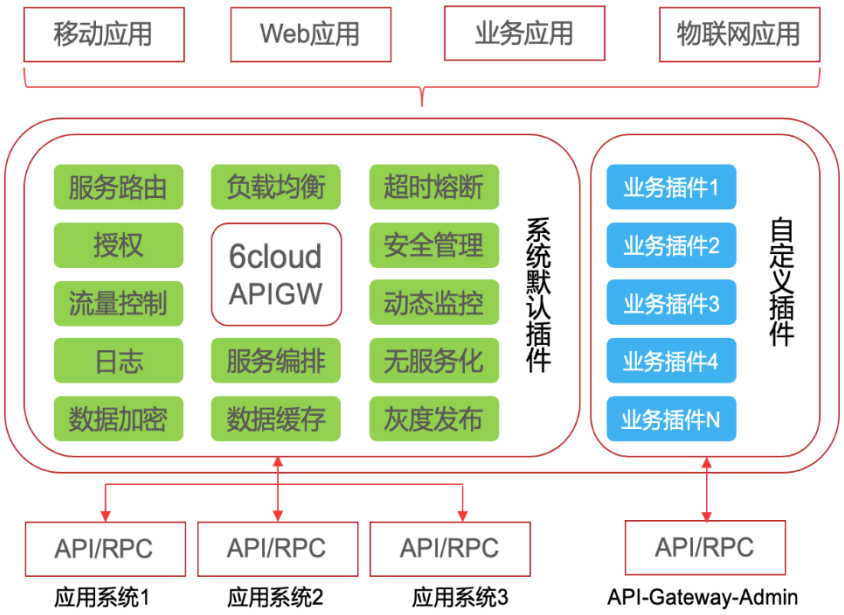

图 8-32 API 网关工作架构

① 多维度认证授权

网关提供多种认证模式，如：Token、IP 地址等，通过运营中心的身份管理中心作为认证数据源、认证策略控制台和自适应策略变更中心。只有通过认证的客户端才能进一步访问网关暴露的服务。认证通过后再检测客户端是否有权限访问指定的 API。

② 流量控制策略

支持配置 API 流量阈值，如：每秒、每分、每小时的请求次数限制，当流量超过阈值，新来的请求会被网关拦截，确保后端服务可以正常运行。客户可以根据需求选择集群或者单网关节点的流量控制。

③ 服务编排控制

对于 APP 或者前端 Web 应用，存在一个页面需要集成多个后端服务数据的情况，而其是远程连接，导致大部分的时间都消耗在建立连接上；为此可以通过管理中心将多个后端服务编排成一个新的服务，由网关将每个后端服务的数据聚合后再返回给客户端，提高页面的响应速度。

④ 传输加密

安全网关在代理 API 调用的过程中使用专业的 TLS 传输技术，确保 API 调用方与 API 服务器之间数据通信的安全性，并可通过约定的 APPID/APPKey 对传输数据进行加密，可有效防止中间人攻击。

⑤ API 监控告警

通过监控平台提供 API 调用过程的各种统计报表，便于运维人员提前规避风险；管理人员可以自定义各种报警规则，系统将自行监控并推送告警信息。

平台 SaaS 层安全

（1） 应用安全加固

为保障发布的 Web 应用的安全性，建议以镜像管理中心提供的安全镜像为基础进行应用部署，并以此为基础进行中间件及数据库的安全加固。

对于采用移动 APP 形式的工业 APP，应采用移动应用安全加固，对应用安装文件进行保护，防止对 APP 的逆向、调试，防止通过移动端对应用安全性造成破坏。

（2） Web 应用入侵防护

Web 应用防火墙（Web Application Firewall，WAF），基于云安全大数据能力实现，通过防御 SQL 注入、XSS 跨站脚本、常见 Web 服务器插件漏洞、木马上传、非授权核心资源访问等 OWASP 常见攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站的安全与可用性。

WAF 的主要功能是将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器，完成整个 Web 应用防护。

（3） 脆弱性扫描服务

为快速识别业务运行过程中，系统存在的漏洞，需要研制工业互联网平台中部署能够发现云平台、主机、Web 应用和数据库漏洞的漏洞扫描产品，及时更新系统最新的漏洞情况并报送安全态势感知平台，实现对资产和资产风险的可视化。

① Web 漏洞扫描功能

平台漏扫系统应具备强大的 Web 应用漏洞安全检测能力，全面支持 OWASP TOP 10 漏洞检测，比如 SQL 注入、跨站脚本攻击 XSS、网站挂马、网页木马、CGI 漏洞等。

系统应能够自动化解析 json、base64 数据并进行扫描。支持自定义 Cookie 进行深入检测。支持基于 basic、Cookie 等认证方式的 Web 扫描。还支持被动扫描，支持用户录入 URL，能够扫描一些常规页面爬取软件检测不到的 URL。方便用户及时发现 WEB 网站中存在的安全漏

洞，避免信息安全事件的发生。而且，系统需要具备领先的 Web 漏洞验证机制，能够对发现的 Web 漏洞进行验证，记录下扫描漏洞发现的测试数据包，用于取证。并对注入漏洞，自动识别数据库类型，获取 Instance Name（实例名称/数据库名称）和 Username（用户名称），使误报率大大降低。

② 数据库安全扫描功能

平台漏扫系统应具备专业的数据库安全扫描能力，支持主流云平台使用的各类数据库。

系统应具备的数据库漏洞知识库，覆盖权限绕过漏洞、SQL 注入漏洞、访问控制漏洞等。系统还应提供两种扫描方式：授权检测、非授权检测，帮助平台企业、用户可以根据不同的情景选择扫描检测方式，并选取相应的扫描策略实现对数据库的安全检测，检测完成后自动生成检测报告，报告包含检测出的漏洞详细描述和修复建议。方便用户及时发现数据库中存在的安全漏洞，保障用户的数据安全。而且，系统还应可以通过对数据库对象、二进制文件等进行对比，从而发现数据库中潜藏的木马。

③ APP 安全扫描功能

平台漏扫系统应支持对 Android 上的移动应用（APP）进行漏洞扫描，采用静态分析的方式，准确发现 APK 中存在的组件安全、配置安全、数据安全和恶意行为等安全风险。从而大幅提升移动 APP 的安全性，避免因 APP 漏洞造成业务损失。

④ 大数据漏洞扫描功能

平台漏扫系统应支持对主流大数据组件进行漏洞扫描和安全配置合规性检查，包括 Hadoop、Spark、Hbase、Solr、ES 等。能够生成统计分析报告，提供详细的漏洞描述和漏洞修复建议，从而增强大数据平台各组件安全的合规性。

数据安全防护

数据安全是贯穿各层次、业务全流程和生命周期的安全问题，安全综合防护系统为了确保数据层面的安全设计了全栈加密的基础服务接口，通信过程的加密服务和全生命周期的数据安全服务。

（1） 数据机密性保护

防止敏感数据泄密是工业互联网平台安全防护的核心目标，为了实现这一目标，应在数据的全生命周期中、提供全栈的加密保护能力，包括应用程序敏感数据加密、数据库加密、块存

储数据加密、对象存储系统加密、硬件加密模块、和网络数据传输加密。

（2） 数据完整性保护

工业互联网平台应在数据生产、传输和存储的全流程中对数据的完整性进行保护。对穿过工业互联网平台的数据交互，应通过云边界安全接入网关及 API 接入控制网关的加密通信过程实现数据传输过程中的完整性保护，同时在数据的使用过程中进行校验，通过数据校验位，散列算法等对远程传输的结果和本地计算结果进行比对，确保工业互联网平台提供和存储的数据是未被篡改的。

（3） 残留数据清除

对于曾经存储过用户数据的内存和磁盘，一旦释放和回收，其上的残留信息应自动进行零值覆盖，实现对残留数据的物理清除。

（4） 数据存储备份

针对关键信息的存储本分依靠多重技术实现：

① 镜像快照：通过云操作系统的镜像快照功能，保留某个时间点上的系统数据状态，用于数据备份，便于用户快速实现灾难恢复；

② 块存储技术：块存储支持在可用区内自动复制用户的数据，防止意外的硬件故障导致数据不可用，以保护用户的业务免于组件故障的威胁；

③ 分布式文件系统：通过使用三副本技术，将系统中的数据保存三份。如果其中一份副本丢失，系统会自动进行三副本的拷贝操作，始终保持拥有三份副本。同时，根据安全策略，三份副本不会存储在同一个物理存储介质上，保持存储的分离操作；

④ 云存储备份：基于虚拟机快照采用差分备份技术，用灾备存储资源对数据进行备份。

（5） 数据库审计

数据库审计模块是应对用户应用上云、云端数据安全面临挑战而规划的适用于工业互联网平台环境中数据库安全审计的产品。数据库审计系统将传统产品与云端相结合，在工业互联网平台环境中形成一套为数据库运维和安全管理人员提供安全、诊断与维护能力为一体的安全管理工具。

数据库审计系统计划实现对云端自建数据库、RDS 数据库访问的全面精确审计及 100%准确的应用用户关联审计，并具备风险状况、运行状况、性能状况、语句分布的实时监控能力。

数据库审计系统通过数据库化的界面语言、智能化的协议识别、可视化的运行状况呈现、可交互可下钻的风险追踪能力，完美实现快速部署、方便维护的云数据库审计。

8.8 工业应用安全

工业应用软件是对工业各类工业生产环节规律的代码化，支撑了绝大多数的生产制造过程。工业软件不但可以控制产品和装备运行，而且可以把产品和装备运行的状态实时展现出来，通过分析、优化，作用到产品、装备的运行，甚至是设计环节，实现迭代优化。

工业应用软件代表了信息物理系统的思维认识，是感知控制、信息传输、分析决策背后的世界观、价值观和方法论。

工业组态软件安全

随着工业信息化的发展，信息技术对工业领域的影响越来越深，传统信息安全领域的威胁正逐步向工业控制系统领域扩散，工业控制系统的安全问题日益突出。黑客们也已经将注意力从以往对网络服务器的攻击逐步转移到了对工业控制系统的攻击上。通过攻击工业控制系统不仅可对网络系统造成威胁，甚至可以破坏工业基础设施，危及人身安全及国家安全，因此工业控制系统安全已经受到广泛关注.组态软件作为工业控制系统软件功能的重要组成部分，其安全性将直接影响着整个工业控制系统的安全。

（1） 工业控制系统由哪些重要部分组成

工业控制系统由组态软件、智能仪表、IPC、PLC、远程数据采集模块等组成。它由智能仪表实现过程参量的控制，由 PLC 进行开关量的控制，由远程数据采集模块进行数据采集，采用工控组态软件由上位机工业控制机计算进行集中监控，具有成本低、可靠性高、实用性强及控制性能好等特点。

（2） 什么是组态软件

组态软件通常可以称为“组态式监控软件”。其中“组态”，其含义为“配置”、“设定”、“设置”，具体是指客户按照功能需要，选择各功能模块进行组合的方式来实现软件开发，而不需要重新编写开发程序代码。其中“监控”，其含义为“监视和控制”，具体是指通过计算机信号及网络通信协议对自动化设备的运行监视、管理和控制等操作。在过程控制与数据采集等工业控制领域有着广泛的应用。它提供了简单方便的图形开发环境，通常各种组态软件都包含

了丰富的图元（也可以自定义图元），能够通过简单灵活的图元拖拽，简单的类 C 语言的脚本编写来开发系统的图形化界面。

组态软件主要用在工业控制系统的系统监控层面上。现在主流的组态软件通常提供常用软件的接口，例如可以方便的与 OPC 服务器连接，与各种外部数据库连接，与 Web 服务器连接等。此外组态软件一般都预置了主流的硬件厂商的各种 I/O 设备的驱动程序。然而只要有应用就会有风险，组态软件面临的主要风险有：

① 高权限导致高风险；

② 校验不严格导致程序漏洞；

③ 软件联网导致远程攻击等。

在面对这些风险的同时，我们应该：

① 在软件开发环节防止软件漏洞的产生；

② 严格控制组态软件的运行权限；

③ 加强访问控制策略。

通过上述的安全措施，可在组态软件开发、实际生产部署、操作运维等方面提高工控系统整体安全，可在开发环节有效避免由于异常输入所导致的缓冲区溢出、命令注入等安全漏洞，在实际生产部署环节有效避免由于权限设置不当导致的攻击，在操作运维环节可有效避免由于管理策略缺失导致的身份冒用、越权操作等漏洞，使得整个系统的安全防护能力有所提升，避免出现木桶理论中的短板效应。

MES 安全

MES（Manufacturing Execution System），制作企业生产过程执行系统。该系统以控制系统的生产过程数据为基础，全面支撑企业的资产，经营等多项业务管理。控制系统网络不断开放的同时，带来安全问题日益严峻，各种安全问题如攻击和病毒、入侵等已经引起了高度重视。

MES 系统作为制作行业经营管理层与过程控制层之间的“桥梁”，在提高企业生产效率、改善产品质量、降低生产损耗等方面有重要作用。对于 MES 安全，应该注意以下几点：

（1） 有效安装防火墙等防护软件

用户在使用计算机网络过程中，必须重视防火墙的作用，对其进行有效的安装，这是互联

网安全性能的重要保障，作为一种信息安全的防护系统，防火墙也称为防护墙，其主要作用是在特定的规则下，限制不安全的数据传输，以此阻止黑客入侵，从而保护计算机内部的网络安全。

（2） 网络监控入侵检测技术

对局域网内的计算机进行监视和控制就是网络监控，通过监控的手段保护计算机网络的安全。入侵检测作为一种新兴的防范技术，它综合了众多的技术，例如专家系统入侵检测方法、神经网络入侵检测方法等。其主要通过获取安全日志、行为等信息来监控计算机，从而推断出计算机网络是否遭受到入侵和攻击，以此达到保护计算机网络安全的目的。

（3） 及时安装漏洞和补丁程序

计算机软件在设计时，都会存在漏洞和缺陷，这些地方就是黑客攻击计算机网络的重要突破口，除了开发商需要编写有效的补丁程序之外，计算机用户也要及时进行漏洞扫描和下载漏洞补丁。

（4） 安全域划分

通过合理的划分安全域可以保证安全需求的同时节省安全设备的投入，提高安全设备的效率。比如：一个公用网络系统内有多个系统，它们有着相同或者近似的安全保护需求，并且它们在运行时或数据交换时彼此信任，互相关联并可用相同的安全防护策略，那么把这些划分在一起统一进行安全部署。

（5） 系统安全通信及秘钥管理

面向 MES 系统的秘钥管理工具有一定的特殊性，这是由实际的运行需求限制决定的。协议需要至少满足三点：组播通信、协议的高效性、秘钥更新。可以参考使用 SCADA 中常出现的 KDC 和 ASKMA 协议来实现组群秘钥管理和安全组播。

工业应用开发安全

工业应用开发安全，指的是工业软件应用开发的安全。

（1） 应用系统架构安全设计要求，在应用系统设计阶段，应充分考虑该架构的安全性，主要体现在应用数据和用户会话的安全，还应当考虑应用系统自身体系架构内部的安全，以及与外系统接口的安全。针对某些特殊应用，还需考虑恢复、抗攻击等安全机制。

（2） 应用系统自身架构安全，自身结构中各组件之间通讯过程的安全机制。组件之间的通讯包括命令级的和数据级的，应充分考虑：传输命令和数据所采用的协议的安全性。应根据

组件之间通讯内容安全性要求程度的不同选择不同安全性要求的协议；考虑程序的模块之间的安全通讯机制；不应使用标准的服务端口或者常见病毒、蠕虫等使用的服务端口。认证与访问控制机制，应考虑：组件之间的信任机制、用户的身份认证机制、对于组件资源的访问控制机制。组件内重要文件和数据的安全防护机制：存在于组件内部的重要数据资源应当考虑其相应的安全防护机制，这些重要的数据资源包括：文件和数据存放是否加密及采用的加密方式。

（3） 应用系统与外系统接口的安全，应用系统与外系统的接口安全设计，主要应考虑以下几个要素：与外系统的之间通讯中的安全机制。应充分考虑：传输命令和数据所采用的协议的安全性。应根据系统之间通讯内容安全性要求程度的不同，选择不同安全性要求的协议；建议不使用默认的服务端口或者常见病毒、蠕虫等使用的服务端口。与外系统的认证与访问控制机制，应考虑：系统之间的信任机制，对于系统之间资源的访问控制机制。对外系统安全机制的符合性，应考虑：如果外系统采用的接口方式经评估认为是安全的，系统应当沿用其接口规范进行设计。

8.9 工业人工智能安全

随着工业互联网的发展，越来越多的机械设备进行了数字化、信息化、网络化改造，但安全防护建设速度落后于数字化信息化建设速度。工控设备体量大，种类多，维护复杂，更新周期长，传统的基于已知攻击特征和威胁情报的安全技术存在覆盖率低、准确性不高、滞后性强等弊端，已经难以抵御不断演变的高级威胁。

业界对于工业互联网安全的思维模式已经开始从传统的事件响应式向持续智能响应式转变，从已知威胁检测向未知威胁检测发展，利用人工智能技术和机器学习算法构建全面的预测、基础防护、响应和恢复能力。

利用人工智能技术提升网络安全能力

由于网络攻击是不断演变的，防御过程中经常需要面临先前未知类型的恶意软件，而人工智能则可凭借其强大的大规模运算能力脱颖而出，迅速排查筛选数百万次事件，以发现异常、风险和未知威胁的信号。人工智能技术在防御领域的这个天然优势，使其在发现和阻止黑客入侵工控设备、预防恶意软件和文件被执行、提高安全运营中心的运营效率、量化风险、网络流量异常检测、检测恶意应用这六大关键创新领域，得到了有效应用。

人工智能和机器学习算法与安全领域的融合，主要可分为有监督学习和无监督学习两大方向。监督学习，就是使用已经知道答案的数据或者是已经给定标签的数据给机器进行学习的一个过程。通俗的讲，监督学习就相当于针对已知的恶意代码行为进行学习，当我们学习完之后，也就知道类似的行为可能是恶意行为，通过这样的学习和调整自身，最终达到举一反三的效果。这种方法有诸多优点，但也有其局限性：模型的准确度完全依赖恶意样本。对于完全未知的、没有经过训练的 0day 攻击，监督学习也就无从获取经验。

与之相反，无监督学习，使用的数据是没有标记过的。即不知道输入数据对应的输出结果是什么。无监督学习善于寻找数据的模型和规律。异常检测是无监督学习算法中的一个重要方面，这种学习方法擅长发现数据集中间显著不同于其它数据的对象。异常检测具有广泛的应用，如电信和信用卡欺骗、贷款审批、消费者行为分析、气象预报、金融领域客户分类、网络入侵检测等。

美国国家网络空间安全保护系统 NCPS（National Cybersecurity Protection System，俗称“爱因斯坦计划”），是由美国国土安全部负责设计和运行的的保护美国联邦政府的网络空间基础设施安全的一套系统。DHS（美国国土安全部）在不断改进爱因斯坦计划的技术架构和部署架构。目前，爱因斯坦计划主要还是基于特征检测的，但目前正在进行基于非特征的检测试点，借助人工智能等技术对系统获取的数据进行快速的异常行为分析。并且通过这些试点，积累运维“非特征检测”和防护系统所需的人员技能、方法、技巧和流程。

人工智能技术本身的安全风险研究

人工智能技术有巨大的潜能改变人类命运，但同样可以被恶意攻击者利用，用以制作高级持续性威胁。即使是人工智能算法本身，也能被恶意攻击者影响，导致 AI 系统判断失准。在工业、医疗、交通、监控等关键领域，安全危害尤为巨大；如果 AI 系统被恶意攻击，轻则造成财产损失，重则威胁人身安全。

AI 安全风险不仅仅存在于理论分析，并且真实的存在于现今各种 AI 应用中。例如攻击者通过修改恶意文件绕开恶意文件检测或恶意流量检测等基于 AI 的检测工具；加入简单的噪音致使家中的语音控制系统成功调用恶意应用；刻意修改终端回传的数据或刻意与聊天机器人进行某些恶意对话，导致后端 AI 系统预测错误；在交通指示牌或其他车辆上贴上或涂上一些小标记，致使自动驾驶车辆的判断错误。

应对上述 AI 安全风险，AI 系统在设计上面临五大安全挑战：

（1） 软硬件的安全

在软件及硬件层面，包括应用、模型、平台和芯片，编码都可能存在漏洞或后门；攻击者能够利用这些漏洞或后门实施高级攻击。在 AI 模型层面上，攻击者同样可能在模型中植入后门并实施高级攻击；由于 AI 模型的不可解释性，在模型中植入的恶意后门难以被检测。

（2） 数据完整性

在数据层面，攻击者能够在训练阶段掺入恶意数据，影响 AI 模型推理能力；攻击者同样可以在判断阶段对要判断的样本加入少量噪音，刻意改变判断结果。

（3） 模型保密性

在模型参数层面，服务提供者往往只希望提供模型查询服务，而不希望曝露自己训练的模型；但通过多次查询，攻击者能够构建出一个相似的模型，进而获得模型的相关信息。

（4） 模型鲁棒性

训练模型时的样本往往覆盖性不足，使得模型鲁棒性不强；模型面对恶意样本时，无法给出正确的判断结果。

（5） 数据隐私

在用户提供训练数据的场景下，攻击者能够通过反复查询训练好的模型获得用户的隐私信息。

基于全流量的高级与未知威胁检测

（1） 基于全流量数据的必要性

震网事件将高级威胁攻击上升到国家战略层面的关键行业和敏感行业，已超出了一般黑客的手法范畴，其由国家层面主导研制并实施精确打击。从时间、技术、手段、目的、攻击行为等多方面来看，都是一次极不寻常的攻击。此类高级威胁的特殊性在于：

其一，传统的恶意代码追求影响范围的广泛性，而高级威胁攻击极富目的性；

其二，传统的攻击大都利用通用软件的漏洞，而高级威胁会针对行业专用软件，如工业控制系统漏洞；

其三，高级威胁会采用全新的 0 day 漏洞进行全方位攻击，而并非已知的漏洞，导致无法事先防御；

其四，通过社会工程学或恰当的疏漏渗透到内部专用网络中，从而使物理隔离的专用网络失效。

进一步从高级威胁的大数据特征来看，其相对于传统攻击特征有着巨大的差异：

其一，数据的价值密度变得更小、更分散，很难聚焦高价值的信息；

其二，用于分析的数据类型和数据格式多种多样，日志信息的行为、内容、结构各异；

其三，数据体量巨大、增长速度快，时间跨度长；

其四，多点攻击事件协同分析、关联，分布式的检测体系。

面对此类高级复杂的、持续的、目标针对性很强的攻击，传统的基于规则和特征匹配的安全产品无法进行有效防护，其只能根据已知攻击或木马病毒的特征进行匹配，无法适应高级威胁大数据的特点；而高级威胁攻击中往往会使用 0 day 或者 Nday 漏洞，此种未知的攻击方式无法被传统安全产品检测到。

另一方面，传统安全流量检测产品如防火墙、入侵检测设备、安全网关、WAF 防火墙等部署在边界，存在对应的流量检测盲区，容易被社会工程学等手段绕过。

图 8-33 总结了传统安全产品要面对的高级威胁攻击。

图 8-33 传统安全产品面对高级威胁攻击

近年来随着以云计算、大数据为代表的新技术的涌现，单位计算和存储的成本越来越低，这使得采用更大的样本空间、更智能的分析算法降低异常检测的误报率和漏报率成为可能，从而使得异常检测技术真正在安全产品中得到实际应用，并最终促成了全流量存储分析产品的产生。其技术原理和实现方式都与传统安全产品有显著的区别。

与传统的以特征匹配为基础的实时检测产品相比，全流量存储分析产品的最大特点是对原始流量的全量抓取、分析和存储，以及采用以异常检测为主的判断机制。有了原始流量的印证，就能够将当前检测到的攻击行为与历史流量进行关联，实现完整的攻击溯源和取证分析；有了异常检测方法，就能够通过对各类正常网络行为建模，实现对未知攻击行为的检测。全流量存储分析产品的出现，弥补了传统检测技术在应对高级威胁检测方面的不足。

（2） 基于全流量数据的检测方式

全流量存储分析产品是当前信息安全领域最为关注的两项前沿技术，即大数据分析技术和 APT 检测技术的融合。借助全流量存储分析，安全分析人员可以对已经发生的攻击行为进行多角度、全方位、可反复回溯的深度检测，从而更容易检测出潜在的入侵行为。

全流量数据并非全网、全数据量，而是对所需保护对象的全流量采集和长期数据存储，利用大数据技术从海量的网络流量中进行数据挖掘，恶意事件的关联分析和规则挖掘，根据已发现的特征或知识对未知的高级威胁攻击进行判定、预测和泛化，对高级威胁的动态性、大规模、复杂性进行自动管理和优化。

其一，流量存储及元数据提取。全流量数据检测设备一般通过旁路镜像采集并存储网络流量。全流量采集设备往往具备多个流量探针，分布在网络各处，采集多点的网络流量来进行分析取证；避免了边界防御设备只能采集边界流量的局限性，全面监测高级威胁每个攻击阶段。通过网络协议实时解码、元数据提取，建立完整的日志、协议、数据包全字段索引，以便于快速提取多维度的网络元数据进行异常行为建模，为后续异常数据挖掘、分析、取证建立扎实的基础。流量数据经过预处理和元数据提取，形成结构化的数据存放于数据库中。

其二，数据挖掘与异常行为检测。高级威胁相较于传统威胁，其数据价值密度更为分散，如何在海量数据中寻找高级威胁的蛛丝马迹，发现区别于正常行为的异常动作，是全流量高级检测产品的价值所在。

数据挖掘第一步在于数据预处理，包括从网络中直接获取的实时网络流，进行会话还原，消除因网络条件造成的乱序、重传、延迟等对后续分析的干扰进行应用协议识别；从非结构化的数据流中抽取结构化的元数据信息，以便后续的各类统计和关联分析。第二步在于元数据的提取，包含原始报文的具体内容，如：开始时间、结束时间、源地址、目的地址、源端口、目的端口、协议类型、应用类型、上行流量、下行流量、数据包分布状况等。第三步在于针对不同种类的高级威胁进行特征提取，抽取元数据，根据检测需求组合成相应的检测特征。

异常行为检测的方法是通过建立行为模型基线，可基于历史数据建立各类正常网络连接的行为模型，并通过偏离程度进行异常行为检测。

其三，异常行为的威胁甄别。针对异常行为的判定目前非常依赖于安全专家的人工分析，而威胁甄别的目的在于自动或者半自动的辅助判定异常行为的类别，其主要方式包括事件关联分析及威胁情报联动。

关联分析是基于一段时间内的多条事件，按照一定的规则进行综合分析，从整个网络的角

度来识别出安全问题或潜在的威胁行为，并产生对应的异常或威胁事件。自动化的关联分析一般由预设的关联规则来进行自动关联，如异常行为与告警日志的关联；半自动化的关联分析，可将异常行为在时间维度和空间维度上相近或重合的关联行为进行整合，并进行可视化呈现，从海量的数据中将各类异常关联展示，辅助安全专家进行分析。

威胁情报联动可用于异常行为的溯源和甄别。威胁情报是一种基于证据的知识，包括了情境、机制、指标、影响和操作建议。威胁情报描述了现存的、或者是即将出现针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。作为大数据时代的安全技术，威胁情报提供了异常行为的溯源和历史信息，极大的改变了攻守双方的认知处境，使得异常行为可归类、可追踪、可溯源。

其四，攻击线索追踪与回溯。利用大数据技术作为基础，能实现对全流量采集数据的查看和回溯。可由元数据构建大数据存储及检索索引，后续安全分析提供底层技术支撑特征提取分析中，只需操作元数据表，在需要分析原始报文时，通过查询元数据表索引，即可快速定位到相关报文。同时可通过高效的数据检索，进行海量数据的快速回溯分析，分类查看及调用任意时间段的数据，并从不同维度、不同时间区间，提供 L2-L7 层网络协议统计、会话日志、元数据日志，从而进行数据逐层挖掘和关联检索。

通常一次完整的攻击链可以分为探测扫描、渗透攻击、攻陷入侵、安装工具和恶意行为五个阶段，如图 8-34 所示。

第一，探测扫描阶段。包括了攻击者在攻击前的对目标的扫描，包括网络扫描、系统扫描、端口、漏洞扫描等，扫描行为是攻击入侵的前期准备阶段，通过信息收集、掌握目标机器的系统、漏洞信息，对进一步进行入侵攻击有事半功倍的效果。

第二，渗透攻击阶段。该阶段是已经对目标机器做了扫描，或是直接对目标机器进行攻击，包括利用栈堆方面的漏洞，利用 Web 系统平台方面的漏洞，逻辑配置错误方面的漏洞，内存破坏方面的漏洞等，对目标主机发起攻击。

第三，攻陷入侵阶段。该阶段表示了目标主机已经不黑客成功攻陷，接下来攻击者可以做他想做的事情，攻陷阶段的表现形式比如，FTP 登录成功，Telnet 猜测成功等。

第四，安装工具阶段。是指在攻击者成功进入目标主机后在目标主机中安装恶意软件，木马程序或是直接挂马等，通过这些恶意的工具实现与黑客的控制链接，下载其他恶意软件等。

第五，恶意行为阶段。即攻击者在目标主机安装完恶意软件后，恶意软件在目标主机产生

的恶意行为包括，控制链接，对主机进行恶意操作等。全流量数据使得安全设备有机会获取高级攻击在攻击链每阶段的取证报文，作为分析的依据。同时能够完整的呈现攻击的整个过程。

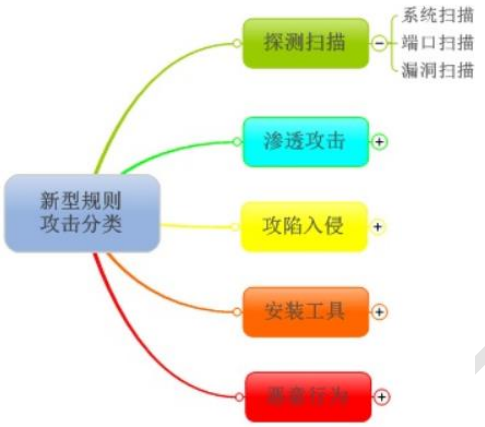

图 8-34 典型攻击链示意

第六，攻击防御联动。高级威胁由于其攻击的未知性和隐蔽性，其发现时间远远滞后于攻击时刻，导致其危害性巨大而很难防范。对此，Gartner 在 2015 年提出安全编排自动化与响应，即 SOAR（Security Orchestration， Automation and Response）。SOAR 是一系列技术的合集，它能够帮助企业和组织收集安全运维团队监控到的各种信息（包括各种安全系统产生的告警），并对这些信息进行事件分析和告警分诊。然后在标准工作流程的指引下，利用人机结合的方式帮助安全运维人员定义、排序和驱动标准化的事件响应活动。

SOAR 的三大核心技术能力分别是安全编排与自动化、安全事件响应平台、威胁情报平台。安全编排（Orchestration）是指将客户不同的系统或者一个系统内部不同组件的安全能力通过可编程接口（API）和人工检查点，按照一定的逻辑关系组合到一起，用以完成某个特定安全操作的过程。安全自动化（Automation）在这里特指自动化的编排过程，也就是一种特殊的编排。如果编排的过程完全都是依赖各个相关系统的 API 实现的，那么它就是可以自动化执行的。安全编排和自动化是 SOAR 的核心能力和基本能力。

安全事件响应包括告警管理、工单管理、案件管理等功能。告警管理的核心不仅是对告警安全事件的收集、展示和响应，更强调告警分诊和告警调查。只有通过告警分诊和告警调查才能提升告警的质量，减少告警的数量。工单管理适用于中大型的安全运维团队协同化、流程化地进行告警处置与响应，并且确保响应过程可记录、可度量、可考核。案件管理是现代安全事件响应管理的核心能力。案件管理帮助用户对一组相关的告警进行流程化、持续化的调查分析与响应处置，并不断积累该案件相关的痕迹物证（IOC）和攻击者的战技过程指标信息（TTP）。多个案件并行执行，从而持续化地对一系列安全事件进行追踪处置。

威胁情报平台（TIP）是 Gartner 在 2014 年定义的一个细分市场，通多对多源威胁情报的收集、关联、分类、共享和集成，以及与其它系统的整合协助用户实现攻击的阻断、检测和响应。通过威胁情报平台，高级威胁可以基于情报在全球范围内共享。

基于非结构化数据的高级与未知威胁挖掘

（1） 结构化数据与非结构化数据

结构化数据，简单来说就是数据库。也称作行数据，是由二维表结构来逻辑表达和实现的数据，严格地遵循数据格式与长度规范，主要通过关系型数据库进行存储和管理。

非结构化数据，是与结构化数据相对的，不适于由数据库二维表来表现，包括所有格式的办公文档、XML、HTML、各类报表、图片和音频、视频信息等。支持非结构化数据的数据库采用多值字段、定长字段和变长字段机制进行数据项的创建和管理，广泛应用于全文检索和各种多媒体信息处理领域。非结构化数据的占比见图 8-35。

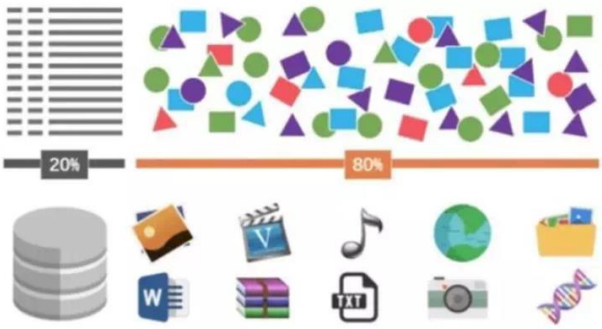

图 8-35 非结构化数据的占比图

针对传统威胁检测来说，其采用特征规则匹配的方式，基于流量进行特征提取，从结构化数据中获取威胁特征，并用于检测。而随着信息技术的发展，大量非结构化数据充斥在企业流量之中，如何基于非结构化数据进行威胁检测，成为当下新一代检测技术的研究热点。

（2） 非结构化数据处理技术

传统威胁检测的思路在于威胁特征的提取，即通过人工分析或机器分析，得到病毒文件的共性特征，针对结构化数据来说，此类共性特征较为容易提取。而针对非结构化数据来说，本质上也是从更多种类的数据中，发现异常特征或行为，进而进行威胁检测。

相对于结构化数据，非结构化数据具有以下特点：数据存储占比高、数据格式多样、结构不标准且复杂、信息量丰富、处理门槛高。当前行业公认：非结构化数据占数据总量的 80% 以上。结构化数据仅占到全部数据量的 20%，其余 80% 都是以文件形式存在的非结构化和半结构化数据，非结构化数据包含各种办公文档、图片、视频、音频、设计文档、日志文件、机

器数据等。

非结构化数据没有预定义的数据模型，因而不能用结构化的方式表达，对此，人们采用新技术，例如机器学习或深度学习的方式对非结构化数据进行特征提取和模型建立，来获取非结构化数据中的丰富信息。

非结构化数据处理技术是大数据处理技术中的难点，其挑战性问题在于语言表达的灵活性和多样性，具体的非结构化数据处理技术因数据类型各异，简单列举几种：包括 Web 页面信息内容提取；结构化处理（含文文本的词汇切分、词性分析、歧义处理等）；语义处理（含实体提取、词汇相关度、句子相关度、篇章相关度、句法分析等）；文本建模（含向量空间模型、主题模型等）；隐私保护（含社交网络的连接型数据处理、位置轨迹型数据处理等）。

非结构化数据的多样性导致不存在通用的非结构化数据处理技术，非结构化数据五花八门，有声音图像、文本网页、办公文档、设备日志等等；每类数据都有各自的计算处理手段，比如语音识别、图像比对、文本搜索、图结构计算等等，但是并不存在一种适用于所有非结构化数据的通用计算技术。语音识别的方法不能用于图像比对、文本搜索也不能用于图结构计算。

例如主题模型是处理非结构化数据的一种常用方法，从名字中就可以看出，该模型的主要功能就是从文本数据中提取潜在的主题信息。主题模型不同于其他的基于规则或字典的搜索方法，它是一种无监督学习的方法。主题可以由语料库中的共现词项所定义，一个好的主题模型的拟合结果应该如下所示——“health”、“doctor”、“patient”、“hospital”构成医疗保健主题，而“farm”、“crops”、“wheat”则构成农业主题。

主题模型的适用领域有：文档聚类、信息提取和特征选择。比如，纽约时报利用主题模型的结果来提升文章推荐引擎的功能。许多专家将主题模型应用到招聘领域中，利用主题模型来提取工作要求中的潜在信息，并用模型的拟合结果来匹配候选人。此外，主题模型还被用于处理大规模的非结构化数据，如邮件、顾客评论和用户社交数据。

（3） 非结构化数据的威胁检测方法

非结构化数据中包含的信息更为丰富，基于非结构化数据的威胁检测，其第一步就是进行非结构化数据的特征提取，需要根据检测威胁模型的特点，选取非结构化数据不同维度的信息并由特征工程提取出来，再采用机器学习或深度学习进行模型建立。机器学习是基于经验的学习，而非结构化数据中提取出的特征就是先验数据。常见的机器学习算法可分为监督学习和无

监督学习两大类。

监督学习通过已有的训练样本（即已知数据以及其对应的输出）来训练，从而得到一个最优模型，再利用这个模型将所有新的数据样本映射为相应的输出结果，对输出结果进行简单的判断从而实现分类的目的，那么这个最优模型也就具有了对未知数据进行分类的能力。其代表就是分类和回归。监督学习的典型例子就是决策树、神经网络。

神经网络作为目前最火热的机器学习算法，在高级威胁检测的多个场景下取得了良好效果。神经网络是一种运算模型，由大量的节点（或称神经元）之间相互联接构成。每个节点代表一种特定的输出函数，称为激励函数。每两个节点间的连接都代表一个对于通过该连接信号的加权值，称之为权重，相当于人工神经网络的记忆。网络的输出则依网络的连接方式，权重值和激励函数的不同而不同。而网络自身通常都是对自然界某种算法或者函数的逼近，也可能是对一种逻辑策略的表达。

人工神经网络模型主要考虑网络连接的拓扑结构、神经元的特征、学习规则等。目前，已有近 40 种神经网络模型，其中有反传网络、感知器、自组织映射、Hopfield 网络、波耳兹曼机、适应谐振理论等。神经网络具有自学习、联想功能以及高速寻找最优解的优势，其将非结构化数据中提取的特征进一步高维化和归一化，而不再是简单的结构化数据，因此相较于传统的检测方式在容错性、预测性和进化性上取得了长足的进步，是非结构化数据特征提取和检测的合适方法。神经网络能在先验数据的基础上，进行学习和预测，进而在面对高级威胁检测时，取得良好的检测效果。

无监督学习事先没有任何训练数据样本，需要直接对数据进行建模。通过循环和递减运算来减小误差，达到分类的目的。无监督学习的典型例子就是聚类。聚类是将物理或抽象对象的集合分成由类似的对象组成的多个类的过程。聚类分析算法主要有划分方法、层次方法、基于密度的方法、基于网格的方法和基于模型的方法。在高级威胁检测中，聚类法特别适合于未知威胁的检测，直接对非结构化数据的特征进行建模，在形成行为模型基线后，发现异常威胁行为。

8.10 工业大数据安全

安全监测与分析

安全监控聚合并存储运行工业物联网系统的各种类型的数据，从而能够分析过去的危害、当前的安全事件和预测未来的风险。安全分析工具通过适合高级仪表板显示的参数向组织提供有用的反馈。

当监视参数与组织的安全问题直接相关并且由利益相关者确定优先级时，它们是最有价值的。它们应该代表那些必须采取行动的人所理解的明确的可采取行动的条件。例如，一个参数可以报告成功响应其最新固件验证请求的电表部分，另一个参数可以指示其功率流已被实用程序远程控制禁用的最终用户站点部分。

监控涉及到攻击事件的模型以及安全和隐私策略。由三个阶段组成的事件模型包括潜在攻击者执行侦察以了解系统、正在进行的攻击和从攻击中恢复。应考虑与性能、规模和隐私相关的数据收集考虑因素，以及可能的分析类型和实施附加安全控制的各种可能措施。

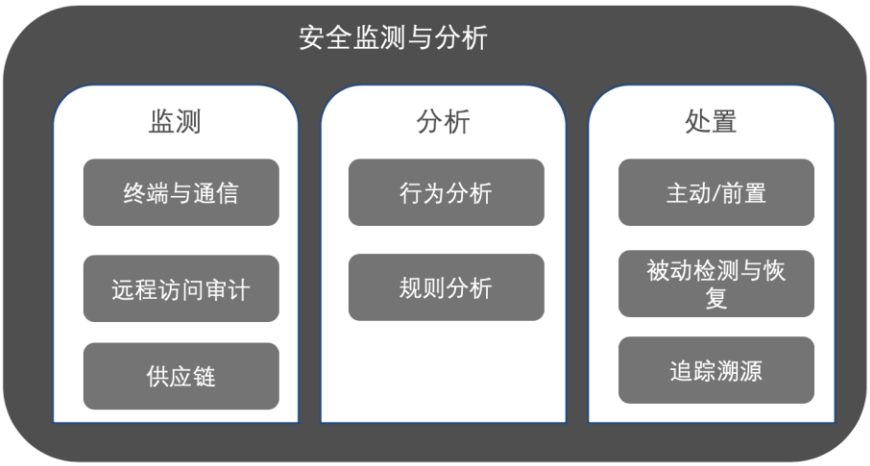

图 8-36 安全监控和分析视图

监控数据可以从端点和网络收集，并且应该安全地存储。在供应链过程的各个阶段，也可以从设备及其组件中收集数据，因为 IIoT 组件的制造是为了确保它们本身如预期的那样安全。可以执行不同类型的分析，以提供漏洞和攻击的指示。此分析允许主动实施安全控制以降低攻击的可能性，对正在进行的攻击作出反应，允许对以前的攻击进行法医分析，并学习和预测将来可能被利用的漏洞。

绿地系统可以在设计时考虑到监控，但是对于端点可能不支持监控功能的棕地实现，这可能会更加困难。

监控和分析也适用于供应链，这是一系列跨组织生产 IIoT 系统组件的过程。如果在供应链中发生攻击，它可能会对 IIoT 系统产生重大影响，使完整性验证变得重要。

监控和分析系统也必须安全。它必须防止机密和私人信息的泄露，以及可能导致后续攻击

的系统安全数据的泄露。它还必须防止攻击者向安全监视和分析系统中注入虚假数据，从而导致自我造成的拒绝服务攻击。

（1） 事件预防、检测、分析和响应

当安全分析产生可操作的结论，并将其纳入自动事件响应计划时，安全分析是最有价值的。自动反应的效果通常应该受到限制。例如，如果监视工具显示入侵者在网络上，则应仅隔离并关闭该网络段，以便在整个网络关闭导致对所有人的拒绝服务之前可以调查入侵。

① 事故发生前

在攻击之前，可能有迹象表明它很可能发生。攻击者在执行侦察以映射和了解系统及其漏洞时可能会留下痕迹。如果检测到这些轨迹，则有助于采取行动了解并减轻攻击。IIoT 系统应将安全事件的潜在指标及时传递给分析系统。

带有角色和职责的事件响应计划必须在事件发生前到位，并在指定时间段或根据需要进行测试和更新。在攻击过程中，可根据监测和分析信息以及事件响应计划采取以下行动：

- 可以在网络上检测到安全事件，并在分析表明可能发生攻击后用于发出警报；
- 在攻击传播之前，可从可疑端点访问的系统上更新安全策略，以增强其防御能力；
- 通知相关人员，更新仪表板、监视器和报告。

② 事故期间

在事故发生期间，需要有关系统中发生的更改的准确数据：

- 在安全事件期间，可从潜在受损设备访问或受其影响的系统上的安全策略可能会更新，以提供更高级别的防御；
- 这种被动安全响应可能包括修改安全控制配置、阻塞服务、关闭服务和恢复更改；
- 快速和增强的法医记录和安全日志可以加快事故调查和根本原因分析，并支持分析和操作流程的未来更新；
- 通知相关人员，更新仪表板、监视器和报告；
- 需要遵循事故响应计划中规定的政策和程序。

③ 事故发生后

事故发生后，系统应在安全、实用的情况下尽快恢复正常运行。衰减算法可以缓慢降低风险等级，使系统恢复到正常、稳定的状态，同时重置策略。

事故发生后的经验教训演习可以更新事故响应计划，以便对未来的事故进行更加有力和有效的预防。此外，应检查警报的报告仪表板，以确保检测到未来的事件。

图 8-37 安全监控时间线

（2） 安全监控和分析

① 安全监测的目的和种类

监测和分析系统支持三个目的。

法医监测和分析系统收集和储存安全数据，并提供给安全调查员，以确定哪些设备和数据受到妥协的影响，以及导致妥协的具体事件顺序。记录的网络流量有助于识别攻击从何而来，以及攻击可能已扩散到哪些计算机。

当前的监视和分析系统收集和分析数据，以确定正在进行的攻击、正在进行的安全策略冲突和当前受损的设备。失败的身份验证请求和篡改传感器警报可能表示正在进行攻击。

预测性监测和分析系统收集和分析数据，确定新的攻击即将发生的趋势，或 IIoT 系统已经改变的方式，可能使他们更容易受到未来的攻击。可能暗示新攻击的数据示例包括审计功能关闭的频率增加、系统配置更改和意外的用户帐户创建。这些可能表明系统已变得易受攻击，并且没有遵循适当的策略和过程。

② 安全分析系统的类型

传统上，安全分析往往是基于行为或规则的。这些系统也分别称为基于异常或基于特征的系统。基于行为/异常的系统首先学习“正常”操作的特征。一旦完成，当被跟踪的特征明显偏离正常操作时，系统会生成警报。基于异常的网络入侵检测系统和文件系统监控系统是行为分析的例子。安全关键型和可靠性关键型系统是行为分析的良好候选者，因为它们变化缓慢。

基于规则/签名的分析依赖于规则或签名库来识别可疑行为。当收到一组与规则匹配的安全值时，将引发警报。分析应该同时使用行为和基于规则的指标。行为指标检测那些仅凭规则

难以定义的事件。基于规则的指标检测那些显然从未打算发生的事件，分析人员很难从培训中学习。

规则和签名必须保持最新，这可能是一个挑战。如果不良行为被认为是好的，行为系统也可能要求管理层纠正或修改培训。

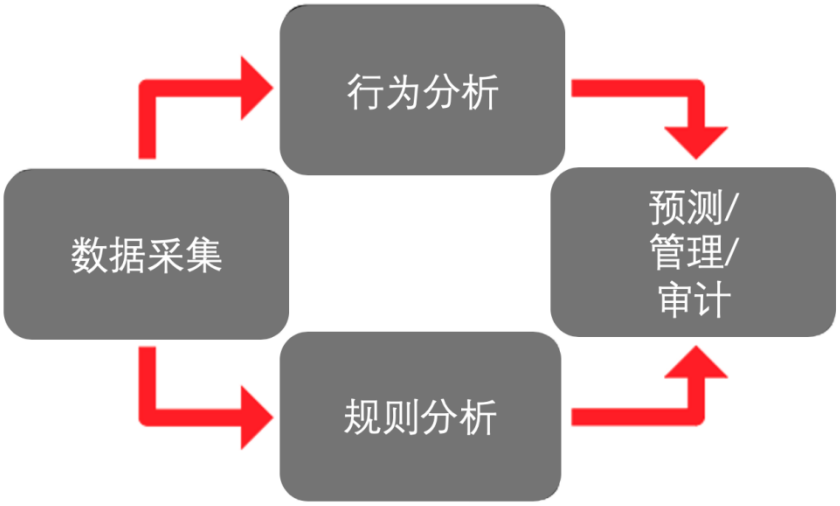

图 8-38 安全监控数据分析流视图

（3） 捕获和存储数据以进行分析

① 日志记录和事件监视

所有安全监视设计都必须考虑成功的入侵者可能会删除其活动的所有证据的风险。以安全和及时的方式将最重要的安全监控数据传输到外部监控系统可以降低这种风险。终结点必须基于本地终结点事件和通信事件记录数据。登录到网络日志系统还可以减轻入侵者干扰日志数据完整性的企图。

安全监视收集与安全相关的事件数据，然后对其进行聚合、关联和分析。它应该能够以通用和一致的方式监视和控制各种端点和通信。

操作监视和安全监视是有区别的。运行监控涉及确保冷却罐水位保持在一定高度、传感器温度不超过一定阈值、传送带上的速度保持恒定等事件。安全监视关注的是这样的事件，例如检测到从意外端点成功登录，然后是阻止的连接尝试或应用程序白名单冲突，这些事件一起表明潜在的攻击正在进行。

② 获取和监控安全数据

监控数据可以来自许多来源，特别是端点和网络。这些数据应安全地传达给监控和分析系统。

绿地端点应能够报告各种参数，并应支持报告哪些参数以及报告频率的配置。这种配置和报告应该安全地完成。性能也很重要，因此报告的数据量必须是所需的最小值，并且在事件期间可能会增加。一些数据可以存储在端点上，或者传输到安全存储服务。

可以监视的端点数据的示例包括：

- 时间和系统信息，包括时间戳、IP 地址、端口号、其他网络标识符、系统标识符、进程标识符和文件名；
- 描述导致事件的认证用户或事件影响或与之相关的系统用户的用户信息；
- 物理过程信息，描述数据所涉及的物理过程的各个方面，如物理设备名称、传感器类型、监测值名称或物理连接的设备寄存器名称或编号；
- 描述记录数据时 IIoT 设备所在位置的位置信息。

网络监控可以通过使用端口镜像将网络数据包从网络复制到监控设备的网络硬件来实现。这使得能够从各个方面分析网络分组通信，例如协议类型、源和目的地、定时和其他方面。这可用于检测协议堆栈中不同级别的攻击。

可监视的网络和主机信息包括：

- 完整的网络流量记录，包括一段时间内每个数据包中的每一位数据；
- 主机执行活动和审计记录，存储 CPU、进程或软件组件采取的每一个重要操作，如从物理进程读取值、控制进程的某些方面或访问敏感信息，如个人身份信息，或私人加密密钥；
- 网络统计，包括连接设置和故障事件、不同类型数据内容和通信连接的通信量统计；
- 来自安全分析系统的数据，也应视为安全数据，可用于分析引擎以进一步关联。

为了避免存储、传输和分析大量不必要数据的成本和困难，只应收集所需的最少数量的数据。最大限度地减少数据收集也降低了暴露数据的风险。

所有者/运营商不应在监控过程中收集敏感的最终用户数据。在无法避免的情况下，它们自己的过程和服务级别协议（SLA）应遵循隐私和安全规定，特别是当对数据的访问是间接的时，例如当网络包跟踪将用户数据作为有效负载的一部分包括时。应使用安全日志、监视存储和审核机制，例如远程存储日志。

（4） 安全数据保护

在收集、通信和存储用于监测和分析的敏感数据方面，存在着安全政策和法规方面的挑战。其中包括：

① 禁止对员工和其他授权用户进行某些类型的监控，或要求在监控用户之前通知用户或获得其许可的法规；

② 禁止跨地理边界传输个人可识别数据，或禁止在某些区域存储或分析此类数据的条例；

③ 敏感数据在静止状态时需要保护；

④ 敏感数据可能需要防止修改，例如将其写入一个只写，且只写一次的介质，并通过提供一种机制来比较设备日志数据和集中报告的数据。

（5） 监测的特殊考虑

除了监控的一般方面外，还应特别注意棕地系统、供应链系统以及与安全和隐私政策的关系。可能会对从不支持直接监视的旧式棕地端点收集的数据造成限制。如果可行，可以使用前端系统解决这个问题。供应链是一种特殊的监控案例，因为它需要监控 IIoT 组件的生产阶段，以确保其完整性。最后，数据监控应该符合隐私和安全策略。

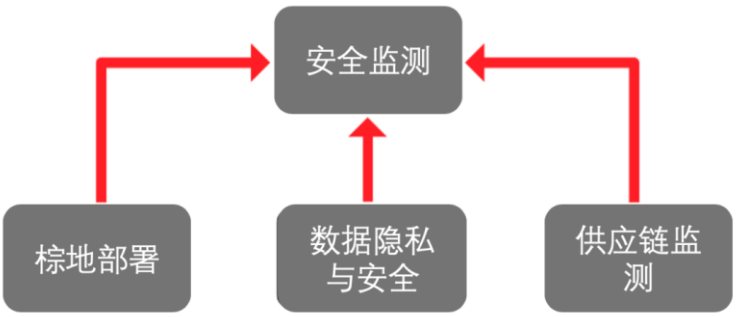

图 8-39 安全监控特殊考虑

① 安全模型和策略

当存在一个预期状态和交互的模型时，安全监视是有效的，允许检测到与该模型的偏差。例如，网络上预期的协议交互，包括它们的网络目的地。监视的数据应与预期的网络和端点行为（包括安全策略）一致。

② 供应链完整性监控

供应链是生产组成一个系统的组件、软件和部件的过程序列，跨越许多组织，包括供应商、供应商和多层外包。它是一个复杂的、全球分布的互联网络系统，逻辑上很长，具有地理上不同的路由。它包括组织、人员、过程、产品和服务以及支持系统开发生命周期的基础设施，包括研究和开发、设计、制造、获取、交付、集成、操作和处置组织的产品和服务。在 IIoT 系统中，应该对所有这些方面的可信度进行评估。

设备和系统在其生命周期中有不同的阶段。他们是：

- 设备（如仪表）模块制造/生产（硬件/软件）；
- 设备模块系统集成；
- 由所有者进行设备初始化/配置设置（配置）；
- 按实体/第三方在现场部署设备（激活）；
- 定期现场更新价格和服务信息；
- 固件升级和维护；
- 远程停用/重新激活（临时）；
- 终止（生命终止）。

为了检测和防止对供应链中产生的端点进行未经授权的更改，需要对硬件、软件和硬件子组件进行监控，以确保其完整性。由于供应链中的不同参与者对整个产品做出了贡献，因此不应在过程中发生意外的变化。

完整性验证可能依赖于信任的根、嵌入的标识符和数字签名，以及在整个构建过程中的监视和验证。真实的零件，完整的完整性验证能力，有助于确保在供应链过程中对监管链的完整性有信任。合并这些需求可以增强组织供应链流程的完整性，并降低供应链风险。

在集成阶段，当添加新模块时，完整性度量应该以加密安全的方式更新。所有配置设置、初始化参数和其他用户设置都应进行类似的更新。配置设置信息应使用安全硬件的受保护存储中设备的唯一密钥进行加密，该安全硬件具有防止攻击和篡改的对策。

如果没有适当的控制、监视和证明功能，供应链中有许多阶段的端点完整性无法得到保证，端点也不应受到信任。创建认证机制来评估设备在通过监管链阶段时的完整性，可以实现原本不存在的可信度量。

设备制造商必须确保整个供应链和生命周期的完整性，并提供测量其完整性的机制。然

后，服务提供商必须确保整个系统可以通过认证，一直到制造商的完整性测量。设备所有者/运营商应测量其环境中的所有端点和服务，以证明其在整个生命周期中的完整性。只有这样，一个系统才能值得信赖。

工业大数据平台安全

工业大数据也是一个全新的概念，从字面上理解，工业大数据是指在工业领域信息化应用中所产生的大数据。随着信息化与工业化的深度融合，信息技术渗透到了工业企业产业链的各个环节，条形码、二维码、RFID、工业传感器、工业自动控制系统、工业物联网、ERP、CAD/CAM/CAE/CAI 等技术在工业企业中得到广泛应用，尤其是互联网、移动互联网、物联网等新一代信息技术在工业领域的应用，工业企业也进入了互联网工业的新的发展阶段，工业企业所拥有的数据也日益丰富。工业企业中生产线处于高速运转，由工业设备所产生、采集和处理的数据量远大于企业中计算机和人工产生的数据，从数据类型看也多是非结构化数据，生产线的高速运转则对数据的实时性要求也更高。因此，工业大数据应用所面临的问题和挑战并不比互联网行业的大数据应用少，某些情况下甚至更为复杂。所以，工业大数据平台将带来工业企业创新和变革的新时代。

大数据的迅速发展，给工业带来了巨大价值，同时，安全问题已成为制约大数据平台建设部署及业务发展的重要阻碍。

（1） 工业大数据平台风险

① 工业设备大数据传输交换风险

大数据传输交换是整个工业大数据平台的入口，其安全性直接影响到平台的整体安全。

- 身份鉴权；
- 软件自身缺陷或者漏洞；
- 敏感数据泄露；
- 传输机制不健全；
- 缺乏对采集账号、人员、行为等一系列操作的审计手段，造成采集环节违规操作未及时发现并追责。

② 工业大数据存储管理安全风险

采集到大量的工业设备信息数据在计算处理之前，需要通过工业大数据平台中存储管理相关软件进行存储，数据存储安全是工业大数据平台安全的重要一环。

- 存储管理软件自身的安全配置不符合要求；
- HDFS、MPP 存储系统缺乏细粒度访问控制规范；
- 敏感数据未加密处理、容易引发数据泄露；
- 大量非结构化存储不统一，难以进行一致性安全管理；
- 在数据生命周期结束后，数据未被彻底删除。

③ 工业大数据计算框架安全风险

计算框架为一组抽象构件及构件实例间交互的方法，主要是通过计算得出结果向上层递交服务。

- 各节点认证机制不完善；
- 各节点间传输不安全；
- 设计不全面引发漏洞和权限，造成绕过认证或者数据泄露业务不可用等安全问题。

④ 工业大数据协调管理安全风险

- 软件运维风险；
- 日志审计、评估手段欠缺；
- 安全策略配置不当；
- 敏感数据沉淀；
- 逆向还原破解；
- 缺乏数据追溯手段。

（2） 工业大数据平台安全措施

面对上面的风险，工业大数据平台应该具备如下安全措施：

① 基础设施安全

对承载着大数据平台的云与虚拟化资源进行恶意防护，部署防火墙，进行入侵检测，完整性的监控和日志审计，实现跨（工业）物理、虚拟和云环境的一体化安全管理。

② 工业大数据接口安全防护

- 认证鉴权；
- 核心数据区域监控；
- 日志与审计。

③ 工业大数据存储安全防护

- 数据访问控制；
- 数据加密存储；
- 数据完整性；
- 数据备份和恢复；
- 数据残留与销毁。

④ 工业大数据处理安全防护

- 认证授权；
- 数据脱敏；
- 数据封装；
- 数据关联性隔离；
- 数据转移控制。

⑤ 工业大数据平台管理安全防护

平台管理是对分布式存储、处理和应用提供协调服务，主流的组件有 Zookeeper、Ambari、Oozie 等。

- 补丁管理；
- 元数据管理；
- 日志管理；
- 配置管理；
- 数据分类分级支撑管理。

工业态势感知

（1） 数据采集

我们对网络服务关键节点和网络检测设备的安全特征数据进行分析后发现，能不能采集到更多的数据，并从这些海量网络数据中抽取出影响安全态势的关键信息是基础。数据的采集处理对整个态势提取、分析和呈现有着重要的影响，如果不清、数据采集混乱，态势提取将无法实现。

工业态势感知就是“数据驱动安全”领域最好的应用，这也迫使我们（尤其是安全分析师）

必须成为数据的高手，不仅仅知道如何分析数据，更应该清楚如何采集所需的数据。数据采集通过软硬件技术的结合来产生和收集工业网络安全数据，其目的是为态势提取提供素材，为态势理解和预测打下数据基础。“巧妇难为无米之炊”，我们必须对数据的采集做到心中有数，知道哪些数据是必要且可用的、通过什么方式获取以及如何采集的、它们来自于哪里，同时也应当在采集这些数据时尽量不影响工业设备（终端）和网络的可用性。

① 制定数据采集计划

数据采集计划不能一蹴而就，它的制定也不是凭空想象出来的，而要遵循一定的方法和步骤，分阶段来实现。通常来说，至少涉及四个不同的阶段，即定义威胁、量化风险、识别源数据以及提炼有价值信息，如图 8-40 所示：

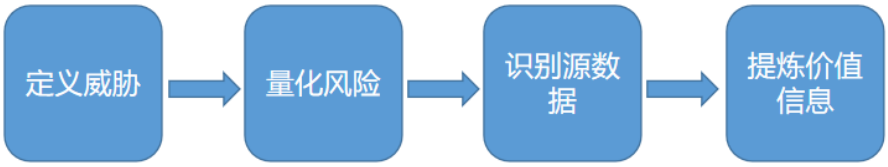

图 8-40 数据采集计划流程

- 定义威胁：这里的威胁并非来自竞争对手或者是行业竞争等，而是导致组织或个人数据的保密性、完整性和可用性受到负面影响的因素；
- 量化风险：也常被称为风险评估，即对组织信息资产所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性进行量化；
- 识别源数据：在确定了威胁和风险的基础上，接下来就是识别现实网络运行中主要的数据来源，为后续的态势提取提供数据基础；
- 提炼有价值信息：在识别出众多源数据后，我们需要单独检查每个源数据和认真分析源数据，提炼出真正有价值的信息，因为并非每种源数据都有采集的必要和意义。

② 主动式采集方式

- 通过 SNMP 采集数据；
- 通过 Telnet 采集数据；
- 通过 SSH 采集数据；
- 通过 WMI 采集数据；

- 通过多种文件传输协议采集数据；
  - FTP（File Transfer Protocol，文件传输协议）；
  - SFTP 的文件传输协议；
  - TFPT（Trivial File Transfer Protocol，简单文件传输协议）；
  - HTTP（Hyper Text Transfer Protocol，超文本传输协议）；
  - HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，安全套接字层超文本传输协议）；
- 利用 JDBC/ODBC 采集数据库信息；
- 通过代理和插件采集数据；
- 通过漏洞和端口扫描采集数据；
- 通过“蜜罐”和“蜜网”采集数据。

③ 被动式采集方式

- 通过有线和无线采集数据；
- 通过交换机、工业传感器采集数据；
- 通过 Syslog 采集数据；
- 通过 SNMP Trap 采集数据；
- 通过 NetFlow/IPFIX/sFlow 采集流数据；
- 通过 Web Service/MQ 采集数据；
- 通过 DPI（深度包检测）/DFI（深度流检测）采集和检测数据。

④ 数据采集工具

- 广为人知的图形化的，用来抓取、过滤和分析数据包的 Wireshark；
- 基于 UNIX 系统，较早出现的网络流量抓取、过滤和分析工具 TCPdump。

此外，还有基于的采集工具和系统——Flume 日志收集系统、Sqoop 数据抽取工具和 Kafka 分布式消息队列系统等，以及一些其他工具如 Tcpxtract、NetworkMiner、Softflowd、BASH 工具、ELSA、Nagios、Logstash、Fluentd 等。

（2） 态势认知

态势感知以安全大数据为基础，因此在数据来源方面，态势感知应该具备主动采集有效数据的能力，避免过度依赖外部威胁情报或第三方设备的数据。

它是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。

“态势感知是认知大量的时间和空间中的环境要素，理解它们的意义，并预测它们在不久将来的状态”，如图：

图 8-41 态势感知流程

态势认知包括：

① 攻击发现：如何从大量的日志、告警、事件、全量数据中发现攻击；

② 攻击确认：在确认攻击的来源、属性、目标等时发现证据数据不够；

③ 质量评估：单体信息素材质量评估：完整性、真实性、时效性；

④ 信息素材集合的质量评估：置信度（查全率、查准率、碎片率、错误关联率等）、纯度（不正确率、证据查全率）、费效比（优先级排序、攻击分值）、时效性（防护时间、检测时间、响应时间）、有效性（MoE）等。

（3） 态势理解

① 损害评估：对攻击或者活动在当下的影响评估，是基于事实的评估。这不但需要了解当前已知的攻击和活动，还要弄清楚这些行为对“我方”的意义，即影响了哪些资产或能力，以及这些资产或能力对我方的重要性。简单理解，损害评估就是对现实风险的理解和评估；

② 常用方法：“特征匹配”式假设推理（即所有条件都已知，且所得线索与过往经历的相似性程度较高），将资产、威胁、脆弱性做关联分析；

③ 行为分析：机器学习+人工；

④ 因果分析：溯源分析+取证分析。

（4） 态势预测

态势的预测是指根据当前状态对网络未来一段时间的发展趋势和历史信息进行预测，它是一个基本目标。由于随机性和不确定性，使得以此为基础的安全态势变化是一个复杂的非线性过程，采用传统预测模型方法已经逐渐不能满足需求，越来越多的研究正在朝智能预测方法发展，典型的如神经网络、支持向量机、遗传算法等智能预测方法。此类方法的优点是具有自学习能力，中短期预测精度较高，需要较少的人为参与。但是也存在一定的局限，如：

- 神经网络存在泛化、能力弱，易陷入局部极小值等问题；
- 支持向量机的算法性能易受惩罚参数、不敏感损失参数等关键参数的影响；
- 遗传算法的进化学习机制较为简单。

① 神经网络预测

神经网络预测是目前最常用的态势预测方法之一，它是一种工具，具有良好的拟合性、对目标样本的自学习和自记忆功能，还具有并行处理、高度容错和极强的逼近能力等特性，可以获取复杂非线性数据的特征模式。利用神经网络预测态势的原理为：首先以一些输入输出数据作为训练样本，通过网络的自学习能力调整权值，构建态势预测模型；然后运用模型，实现从输入状态到输出状态空间的非线性映射。神经网络具有非线性、很强的鲁棒性和容错性，善于联想、概括、类比和推广，而且局部的损伤不会影响整体结果。人工神经网络由大量神经元相互连接构成。一个典型的人工神经元模型由输入 X=（x1，x2，…，xn）、网络权值 W=（Wk1，Wk2，…，Wkn）、偏值 bk、求和单元Σ、激励函数 f、输出 ykt 组成。如图 8-42：

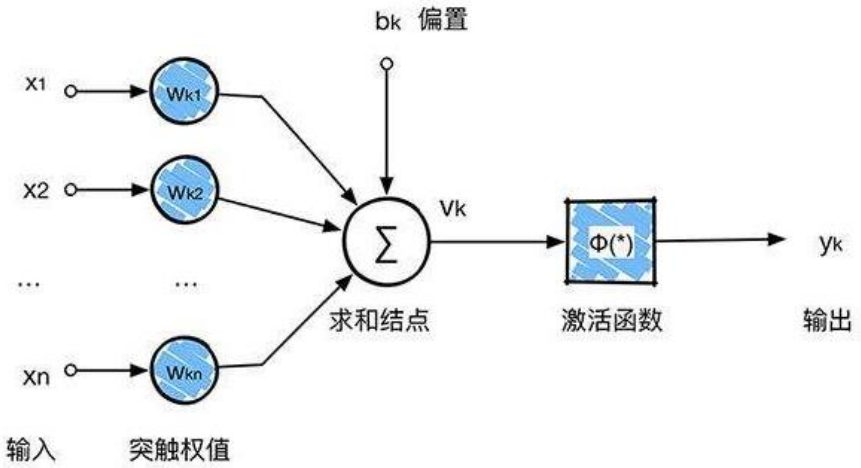

图 8-42 人工神经元模型

神经网络的学习规则可以粗略分为以下三类：

- 相关学习规则：这种规则只根据连接间的激活水平来改变权系数，常用于自联想网络，如 Hopfield 网络；
- 纠错学习规则：这种规则根据输出节点的外部反馈来改变权系数。它与梯度下降法等效，按局部改善最大的方向一步步进行优化，从而最终找到全局优化值。感知器学习就采用这种纠错学习规则；
- 无教师学习规则：它是一种对输入检测进行自适应的学习规则。网络的自组织学习算法即属于这一类。

神经网络的预测模型包括：

- 线性神经网络：线性神经网络由一个或多个线性神经元组成，是一种层次性前向网络，其传递为线性，学习为“最小均方（LMS）”。LMS 也就是最小二乘法算法，是通过调整线性神经网络的权重和阈值，使均方差最小。线性神经网络适用于对线性关系的数据进行预测；
- BP 神经网络：BP 神经网络全称为 Back-Propagation Neural Network，即反向传播网络，是指基于误差反向传播算法的多层前向神经网络，它是 D.E.Rumelhart 及其研究小组在 1986 年研究提出的，是目前应用最广泛的神经网络模型之一。典型的三层 BP 网络如图 8-43 所示：

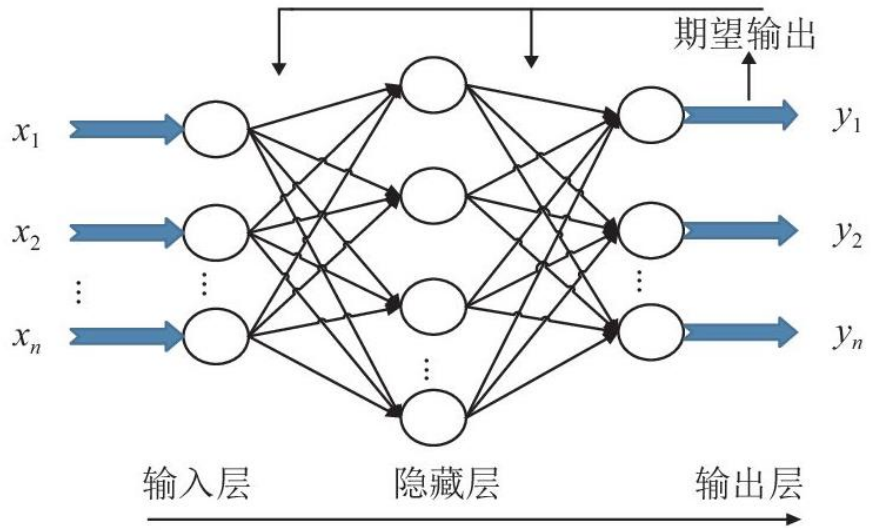

图 8-43 三层 BP 网络图

- Elaman 神经网络：是一种层次性反馈网络，一般分为四层：输入层、中间层（隐含层）、承接层和输出层，传递可以采用线性或非线性，各层连接类似于前向网络；

- Hopfield 神经网络：Hopfield 神经网络是由 J.Hopfield 于 1982 年提出的一种循环神经网络，它可用作连接存储器的互连网络。它从输出到输入是有反馈的连接，主要可分为离散型和连续型两种类型；
- Kohonen 神经网络：参照大脑对信号处理的特点，T.Kohonen 于 1981 年提出了一种神经网络模型，也就是自组织特征映射（SOM）模型。Kohonen 模型的思想在本质上是希望解决有关外界信息在人脑中自组织地形成概念的问题。对于一个系统来说，就是要解决一个系统在受外界信息作用时在内部自组织地形成对应表示形式的问题，这其中涉及神经网络的权系数调整。

② 支持向量机预测

支持向量机预测是一种基于统计学习理论的模式识别方法，专门研究小样本情况下的规律，它由 Vapnik 于 1995 年首次提出。其基本原理是通过一个非线性映射将输入空间向量映射到一个高维特征空间，并在此空间上进行线性回归，从而将低维特征空间的非线性回归问题转换为高维特征空间的线性回归问题来解决。与其他方法相比，支持向量机预测绝对误差小，保证了预测的正确趋势率，能准确预测态势。

它的主要特点：

- 它是专门针对有限样本情况的，其目标是得到现有信息下的最优解，而不仅仅是样本数趋于无穷大时的最优值；
- 它是结构风险最小化原则的具体实现，因此具有良好的推广能力；
- 其算法最终将转化为一个二次优化问题。从理论上说，得到的将是全局最优解，从而解决了神经网络中无法避免的局部最小化问题；
- 其将实际问题通过非线性变换转换到高维的特征空间，在高维空间中构造核来实现原空间中的非线性判别，使得学习机器有较好的推广能力，同时它巧妙地解决了维数问题，其复杂度与样本维数无关；
- 支持向量机存在唯一极值点。

③ 人工免疫预测

人工免疫就是研究、借鉴和利用生物免疫学原理、机制而发展起来的各种信息处理技术、计算技术及其在工程和科学中应用而产生的各种智能系统的统称，其研究涉及医学免疫学、科学、系统工程、模式识别、控制工程等学科，是典型的交叉学科。目前，人工免疫系统已发展

成为研究领域的重要分支。与上述智能方法相比，人工免疫系统具有全局优化、收敛速度快等优点。它继承了生物免疫系统的自学习、自适应、自组织和免疫记忆等优化学习机理，适合于解决态势预测问题，其拟合和预测结果都能较好地克服态势时间序列大幅度变化的影响。

④ 复合式攻击预测

复合式攻击行为已成为当下攻击的主流方式，且在未来相当长一段时期内有继续增长扩大的趋势，因此针对复合式攻击的识别与预测是领域研究面临的一个重要问题。相对于其他技术，复合式攻击预测方法的研究开展较晚，2005 年以后一批国内外学者对复合式攻击预测开始展开大量研究。总结起来，当前主流的复合式攻击预测方法主要包括以下四类：

- 基于攻击行为因果关系的复合式攻击预测方法；
- 基于贝叶斯博弈理论的复合式攻击预测方法；
- 基于 CTPN 的复合式攻击预测方法；
- 基于意图的复合式攻击预测方法。

此处只是简单的介绍了一下态势预测的四种方式，具体详细过程这里不过多阐述。态势预测除了机器学习还需要人工分析。

影响评估：影响评估与损害评估不同，它是一种情境推演，即当攻击或者活动继续开展，会造成怎样的影响，会不会和其他的攻击活动关联，会不会影响到其他的资产，以及如果我们采取了措施，会造成怎样的后果等等。这是一种基于观点的评估。简单理解，影响评估就是对潜在风险的理解和评估。

常用方法：除了采用“特征匹配”外，还需要做“情境构建”，通过分析和推断对方意图、时机、能力等对手信息，以及漏洞能否组合利用，或是是否存在未知漏洞等其他己方信息，探索其他潜在的假设，并持续进行态势跟踪，验证和推演构建的多个情境到底哪个是准确的。

序列分析：态势理解和态势预测实际上都是与时间强相关的，所以分类和序列分析两种方法通常会一起采用。

分类需要用到的训练集：基于时间序列分成 N 份数据，每份数据一般都需要一个“属性 k”和“参数 a”，用于构造算法函数，而这个“属性”的选择与态势感知的内容是相关的，比如要能够预测未来 1 个小时的风险趋势，那么这个属性就应该选择“风险评估值”；如果要预测未来 1 个小时内是否会发生 DDoS 攻击，则这个属性可能选择“DDoS 攻击告警次数”或“DDoS 攻击特征综合值”；如果要预测未来 1 个小时内是否会发生特定的某种 DDoS 攻击，则

这个属性可能会选择“特定 DDoS 攻击告警次数”或“特定 DDoS 攻击特征综合值”。

攻击特征如何表达？攻击特征综合值可以是多元特征的线性（甚至非线性）组合，比如 Synflood 攻击特征值=a1*攻击速率+a2*告警日志中出现 syn flood 关键字的频率+a3*。

（5） 响应处置

协同响应处置是态势感知能力落地的关键，也是我们选择态势感知产品或方案的重要指标。

三级响应机制：

① 一键阻断：自动阻断木马与黑客通信；

② 端点查杀：端点执行扫描、查杀等动作；

③ 高级人工服务：安全应急响应，解析网络威胁现状和威胁，并给出安全建设建议；

④ 应用态势感知，不管是为了提升检测发现威胁的能力，还是直观呈现安全现状及威胁，最终都是希望能够在安全事件过程中及时止损。而这就需要通过全局性的分析，发现威胁之后联调各安全设备进行协同响应处置。比如在攻击者发动攻击之前，协同防御设备进行策略调整，阻断其攻击；在已经潜入内部的攻击者造成破坏之前，立刻评估可能造成的损失范围和程度，并及时响应和处置。只有及时、高效的响应处置动作完成，才算真正解决了安全问题。然而根据态势感知、安全监测等模块获取的态势、趋势、攻击、威胁、风险、隐患、问题等情况，利用通告预警模块汇总、分析、研判，并及时将情况上报、通告、下达，进行预警及快速处置。可采用特定对象安全评估通告、定期综合通告、突发事件通告、专项通告等方式进行通告。

该模块还应包括通告机制成员单位、专家组、技术支持单位、信息支撑单位管理，信息通告刊物管理，网安部门通告机构、人员管理，通告规范、标准管理等内容。支持对通告机构、单位、人员等进行管理，支持通告预警策略的设置，包括通告预警生成策略、下发策略、考核策略等。通过关联和融合分析，计算网络整体安全值及风险值，依据态势监控指标体系，生成系统可直接展示的态势信息，然后建立数学模型进行预警分析，挖掘潜在安全威胁，根据预警指标生成预警信息。预警信息通用格式：预警名称、预警等级、发布时间、预警内容、防范措施等，参见图 8-44。

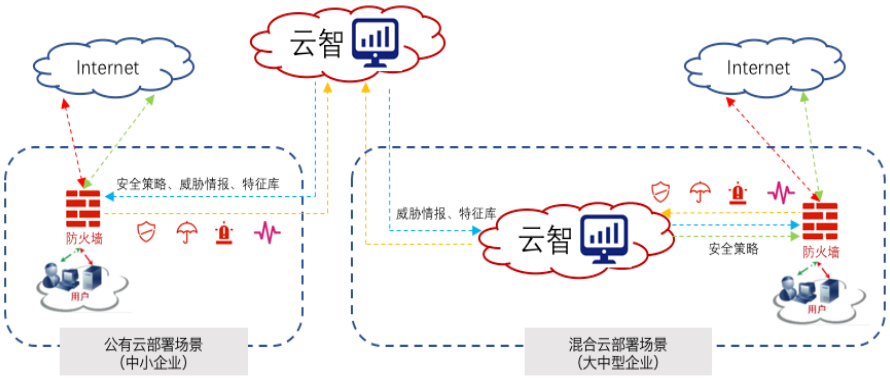

图 8-44 态势感知系统应用场景

8.11 工业 5G 安全

5G 有效提升工业互联网效率

（1） 5G 应用场景

根据 5G 高速，超低延迟和超大型连接的特点，存在三种应用场景：

① 增强型移动宽带 eMBB（Enhanced Mobile Broadband）：在现有移动宽带业务场景的基础上，增强了高流量的移动宽带服务，重点关注对宽带有高需求的服务，例如高清视频，虚拟现实 VR /增强现实 AR 等待，满足人们对数字生活的需求；

② 超高可靠和低延迟通信 uRLLC Ultra（Ultra Reliable and Low-Latency Communications），专注于对延迟极为敏感的服务，例如自动驾驶/辅助驾驶，远程控制等，以满足数字行业的需求；

③ 大规模机器类型通信 mMTC（Massive Machine Type Communications）：针对大型 IoT 服务，例如智慧城市，环境监控和智慧农业，以满足人们对数字社会的需求。

（2） 5G - 智能制造使能技术

5G 技术促进了无线网络从消费领域向工业领域的扩展，让该行业真正进入无线时代，实现了“工业 4.0”所需的“物理连接”和“灵活”生产，从而为人工智能提供了更清晰的显示神经网络，如图 8-45 所示。

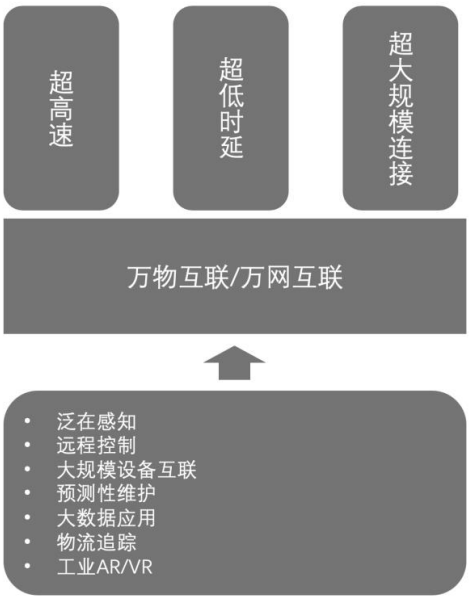

图 8-45 5G 智能制造使能技术

① 5G 使智能工厂向无线发展

- 工业应用场景：
  - 视频监控和操作维护等大量数据的传输，实时性可靠性要求不高；
  - 控制信息等少量数据传输：对数据传输的实时性、可靠性、安全性要求很高。
- 无线连接：
  - 无需布线，使工厂和生产线的建设更加方便，减少了很多维护工作并降低了成本；
  - 机器和设备的活动区域不受限制，这有助于在各种情况下顺利切换工作内容。
- 互联互通：
  - 5G D2D 通信可实现智能工厂中大型制造设备的互连；
  - 制造设备通过 5G 与基于云的工业软件互连，从而促进工厂结构的扁平化发展，并实现物流跟踪，远程运维，分布式设计和协作生产。

② 5G 网络下的工厂物联网络

图 8-46 5G 工厂物联网络

③ 5G 网络下的网络协同制造

图 8-47 5G 网络下的网络协同制造

④ 物联网与实时控制

5G 可以满足大规模低功耗嵌入式传感器的网络连接和数据传输，以及机器，设备和人员之间前所未有的交互和协调，并为工业自动化闭环控制应用（时间敏感的通信）提供了可能。通过 5G 网络连接。

⑤ 可视化生产

视频监视和机器视觉：可以通过基于 5G 的机器视觉分析来满足现代制造企业日益普及的需求，例如质量检查，操作和维护以及基于安全管理行为的监视，从而满足大量数据传输需求。

⑥ 人机协作

工业 AR：在智能制造过程中，可以通过诸如 AR 的技术来实现诸如人机协作，生产过程监控和生产任务划分指导之类的技术，例如：东部装配过程的指导以及业务 由远程专家支持，以提高生产活动的效率。此外，结合使用 5G 和工业 AR，可以培训员工提高技能。

⑦ 云化机器人

云化机器人：无线网络摆脱了电缆束缚，使机器人的移动应用成为可能，使工厂能够快速，经济高效地在不同类型的产品生产线之间切换生产；基于云的机器人通过 5G 连接到基于云的控制中心，通过大数据和人工智能对制造过程进行实时操作控制，并具有自组织和协作机器人来满足灵活的生产需求。

⑧ 车联网

通过 5G 等通信技术实现“人—车—路—云”一体化协同，促进与低延迟和高可靠性紧密相关的远程控制驾驶，编队驾驶和自动驾驶的应用，见图 8-48。

图 8-48 5G 车联网

⑨ 能源领域

5G 技术可以深度整合能源生产，传输，存储，消费和互联网，加速能源互联网的实现，并间接形成对各种能源设备的新要求。

- 发电领域：5G 可以满足实时数据收集和传输，远程调度和协调控制以及多个系统高速互连的功能；
- 输变电领域：5G 功率切片可满足智能电网的高可靠性和安全性要求，并提供智能服务，如传输和转换环境的实时监控和故障定位；
- 配电领域：基于 5G 网络，可以支持智能分布式配电自动化的实现，并实现全自动的故障处理过程。

5G 能源互联网如图 8-49 所示。

图 8-49 5G 能源互联网

⑩ 电子装备领域

随着 5G 布局的发展和替换的出现，对芯片，射频设备，终端天线，光学组件，传感器和面板灯的需求猛增，电子制造设备，测试设备，激光加工设备和模块设备已升级转型需求。

可以预见，5G 技术场景下，装备制造业向智能制造转型升级步伐将加快。

5G 提出的新安全需求

5G 提出的安全新需求来自下面三个方面，如图 8-50 所示：

（1） 5G 技术服务于万物互联的应用场景，其安全风险可能影响国家和多个社会领域；

（2） 多样化的终端形态与接入技术对安全提出了轻量化、低时延、高性能等全新的防护要求；

（3） 由于大量新 IT 技术的引入，对 CT 网络带来了新的安全威胁。

图 8-50 5G 新安全需求

5G 移动通信安全

（1） 5G 移动通信体系面临的安全风险

如图 8-51 所示，5G 移动通信体系面临的安全风险有：

① 用户侧/设备侧的安全风险：非法远程访问、恶意篡改、隐私泄露、DDoS 攻击利用；

② 用户侧/设备侧与基站之间的无线网络安全风险：无线漏洞、信令风暴、恶意流量；

③ 来自互联网、外部 DN、切片租户、MEC 针对 5G 核心网的安全风险 DDoS 攻击、设备漏洞、数据窃取；

④ 5G 核心网与 3G/4G 核心网络安全风险：互操作风险；

⑤ 不同运营商 5G 核心网络间安全风险：信令攻击、数据篡改；

⑥ 5G MEC 本身安全风险：虚拟化漏洞、内部风险（网管、4A 等）；

⑦ 5G 核心网本身安全风险：虚拟化漏洞、内部风险（网管、4A 等）。

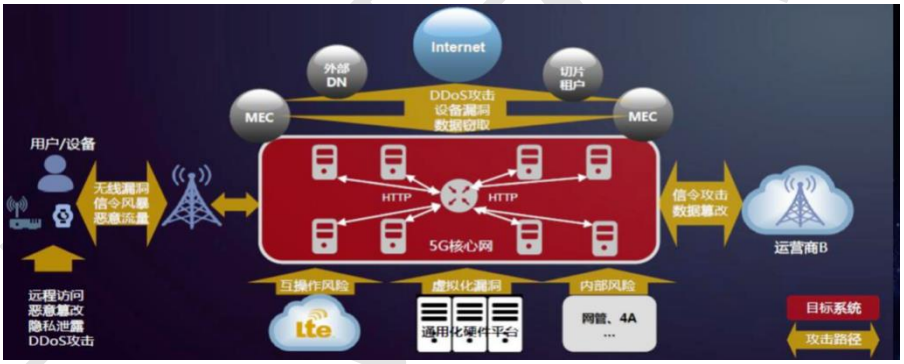

图 8-51 5G 移动通信体系面临的安全风险

（2） 5G 安全架构

从整体上来讲，5G 移动通信安全包括两个层面的安全：一个是无线网络通信安全，一个是业务安全，如图 8-52 所示。

图 8-52 5G 移动通信安全

如图 8-53 所示，网络安全随着移动通信的发展逐渐增强：

① 1G 无安全策略；

② 2G 简单安全策略（已证明可破解）；

③ 3G 全新安全架构，但仍然存在部分安全风险：没有实现有效数字签名，缺乏先进密码算法，非授权访问数据即服务；

④ 4G 安全性进一步提升，是目前为止已验证最安全的通信系统：用户 ID 加密，设备认证，实体认证，机密性，完整性；

⑤ 5G 安全架构需要重新设计。

图 8-53 移动通信安全发展

安全是对 5G 时代智能互联网的首位要求。3GPP R15&R16 对 5G 安全进行了全新的设计，相比于 4G 网络而言，5G 组网模式具有更好的机密性与完整性、接入认证、隐私保护、伪基站防护、网间安全和更好的用户安全隔离等特点。

（3） 5G 通信加密算法

5G 提供更好的机密性与完整性保护，主要体现在加密强度与加密算法方面：

① GSM：A5 加密算法，1989 年启动研究，1991 年首次部署，1992 年我国建设组网；1987 年发明，密钥长度为 64 比特；1999 年算法泄露，2016 年 3 块 GPU，9 秒破解了 A5 算法；

② 3G：采用 KASUMI 算法，1995 年发明，密钥长度为 128 比特，1998 年启动研究，2001 年首次部署，2009 年我国颁发牌照；2005 年，算法理论被破解，2010 年破解效率进一步提升；后期引入 SNOW 3G 算法；

③ 4G：采用 AES、SNOW 3G、ZUC 等加密算法；刚开始采用 AES 算法，密钥长度为 128 比特；2011 年 ZUC 成为标准算法；2011 年专用领域的商用量子计算机出现；

④ 5G：需要更长的密钥和更先进的加密算法，保障数据与信令传输安全；需要根据不同场景提供不同的加密方式，适应不同的通信需求：对称密钥长度到 256 比特的必要性，轻量级加密算法。

（4） 5G 隐私保护

如图 8-54 所示，5G 网络通过用户身份 SUPI 加密 IMSI 技术，改变 2/3/4G 网络中终端 UE 明文传输 IMSI 带来的安全威胁，防止伪基站获取用户的隐私数据（用户位置，会话监听等）。

注 1：国际移动用户识别码（International Mobile Subscriber Identity，IMSI），是用于区分蜂窝网络中不同用户的、在所有蜂窝网络中不重复的识别码。手机将 IMSI 存储于一个 64 比特的字段发送给网络。IMSI 可以用来在归属位置寄存器（Home Location Register，HLR）或拜访位置寄存器（Visitor Location Register，VLR）中查询用户的信息。为了避免被监听者识别并追踪特定的用户，大部分情形下手机和网络之间的通信会使用随机产生的临时移动用户识别码（Temporary Mobile Subscriber Identity，TMSI）代替 IMSI。

注 2：终端用户永久标识符（Subscription Permanent Identifier，SUPI），以确定用户的真实身份，并保护该用户在网络上传输的数据。

图 8-54 5G 隐私保护方案

（5） 5G 伪基站防护

5G 提供更好的伪基站防护：处于空闲状态的 UE，容易被伪基站通过虚假的广播信息唤醒到连接态，从而连接到伪基站进行数据通信；5G 网络 对空闲状态的 UE 设置了两类防御机制（事前防御、事后防护），保护处于空闲态 UE 的安全数据接入与唤醒。

① 事前防御：基站对广播信息签名，终端验证签名，从而可以判断出基站真伪；

② 事后防护：当终端恢复到连接状态后，上传空间态下终端接入的基站信息，核心网判断接入基站的真伪。

（6） 5G 网络间通信防护

如图 8-55 所示，5G 为保护互联互通信息的机密性和完整性在网络中新增了安全边界保护代理设备 SEPP，通过在运营商之间建立 TLS 安全传输通道，对传输的信息进行机密性和完整性保护，有效防止数据在传输过程中被篡改和窃听。

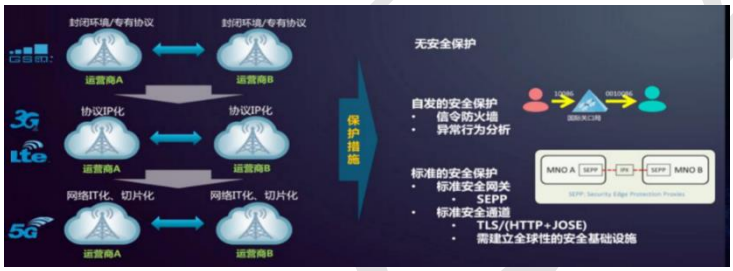

图 8-55 5G 网络间通信防护

（7） 5G 任性模型

5G 提供更细粒度的信任模型，如图 8-56 所示：在非漫游场景，相比于 4G 网络，基于 SBA 的核心网服务化架构以及 CU-DU 分离架构，为终端接入网络提供更细粒度的安全管控策略；同时在跨网络切换或者漫游过程中，提供基于 SEPP 传输技术，使能更强的网络边界保护。

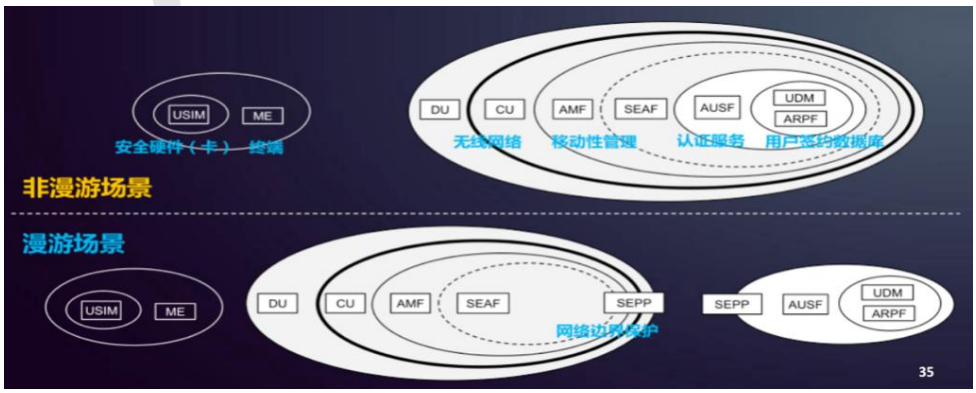

图 8-56 5G 任性模型

5G 垂直行业安全

从整个物联网的角度看垂直行业，其架构如图 8-57 所示：

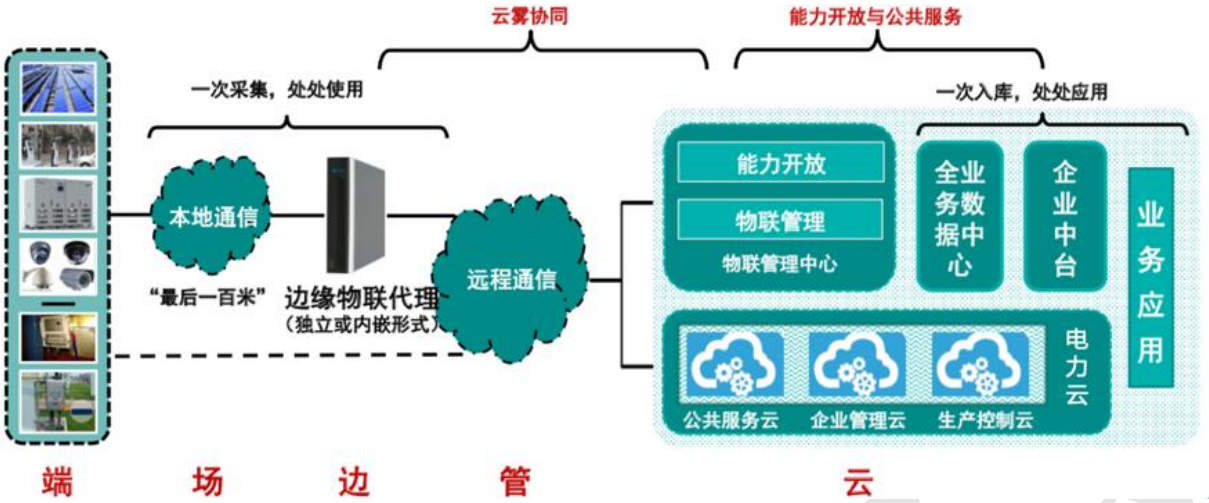

图 8-57 垂直行业典型架构

5G+智慧医疗，如图 8-58 所示：

图 8-58 5G+智慧医疗

5G+智慧教育，如图 8-59 所示：

图 8-59 5G+智慧教育

（1） 垂直行业安全需求

从整个物联网的角度看垂直行业安全需求，如图 8-60 所示：

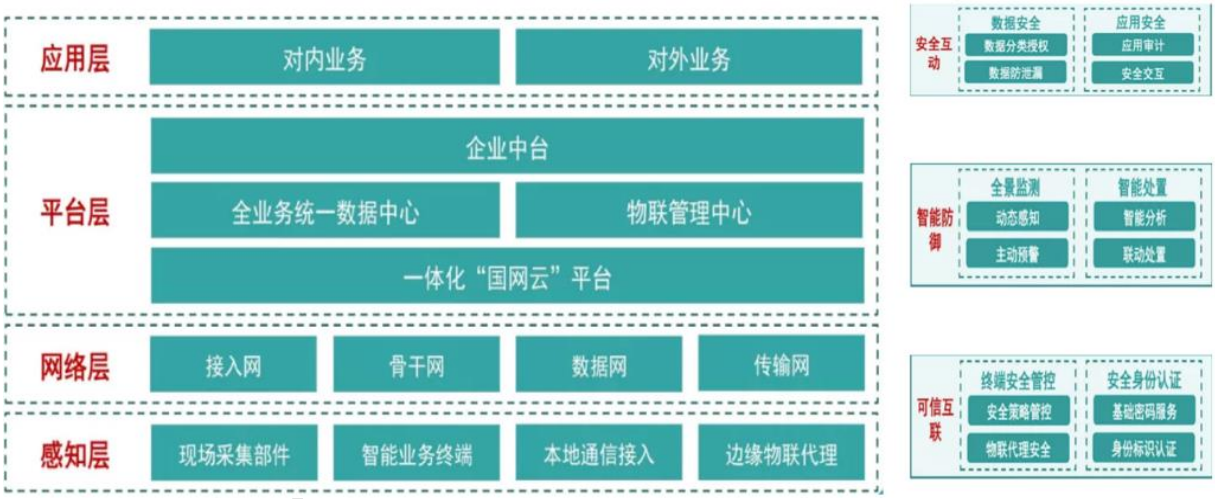

图 8-60 物联网垂直行业安全需求

① 感知层和网络层：可信互联=终端安全管控和安全身份认证。其中终端安全管控包括安全策略管控、物联代理安全；安全身份认证包括基础密码服务和身份标识认证；

② 平台层：智能防御=全景监测和智能处置。其中全景监测包括动态感知和主动预警；智能处置包括智能分析和联动处置；

③ 应用层：安全互动=应用安全和数据安全。其中数据安全包括数据分类授权和数据防泄露；应用安全包括应用审计和安全交互。

（2） 端场边安全需求

如图 8-61 所示，5G 垂直行业安全更多关注在端-场-边这三个部分：

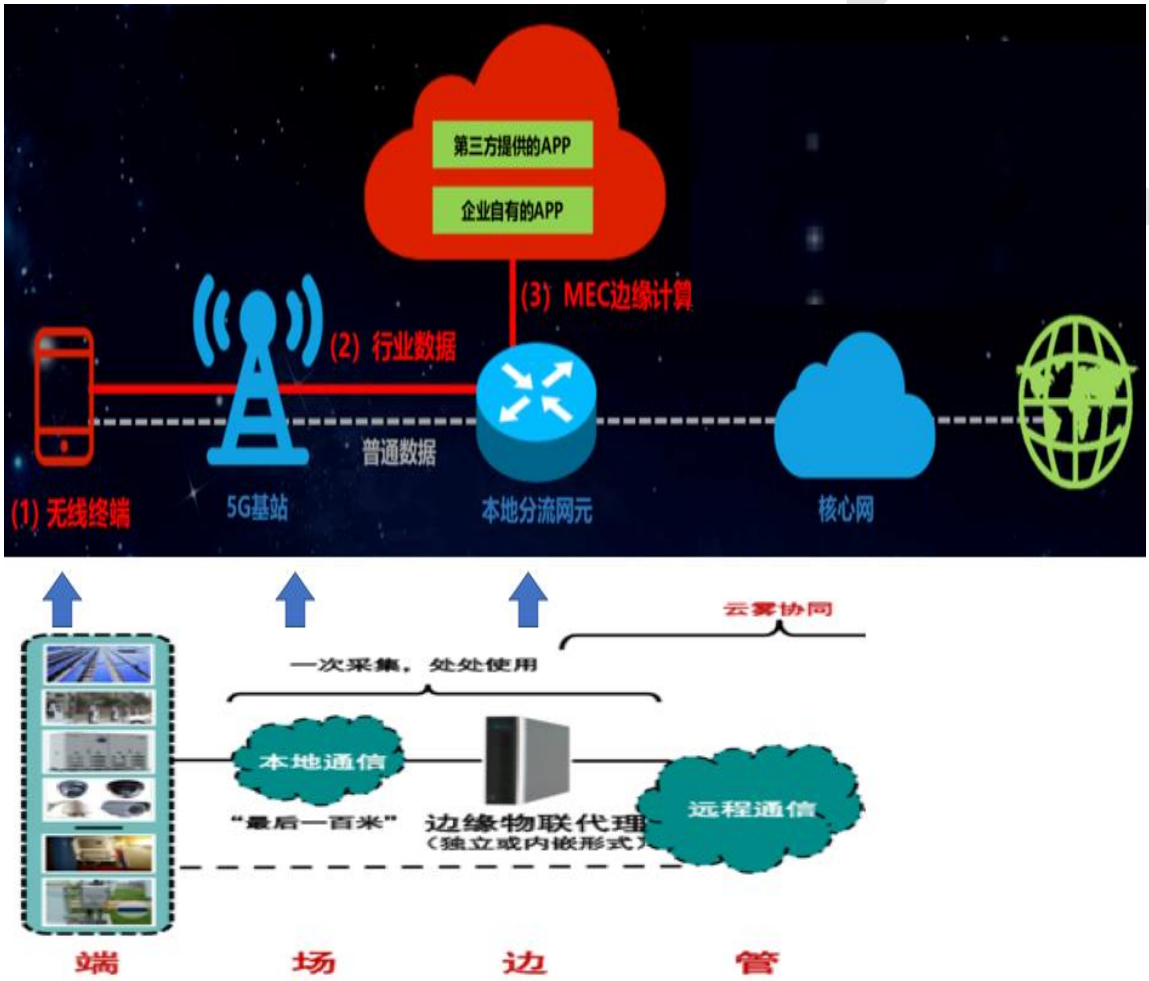

图 8-61 端-场-边安全需求

① 终端安全：

- 仅有指定的用户可以访问本地业务平台；
- 防止用户终端设备被随意冒用；
- 数据本地加密存储保护，确保不被窃取或破坏。

② 场安全：行业数据传输安全

- 行业数据不出企业控制区域，保障用户隐私安全；
- 行业数据与普通用户数据隔离，保障行业数据安全；
- 端到端数据加密技术，保障数据在全流程传输过程中保密；
- 重放攻击、频道抢占。

③ 边安全：MEC 边缘计算安全

- 防止非法应用通过 MEC，直接控制 UE 的行为；
- 防止外部网络通过 MEC 中间件，攻击整个移动网络；
- 防止非法应用和外部网络通过 MEC，推送不良信息；
- 有效隔离 APP，保障不同 APP 的安全防护隔离需求。

（3） 5G 终端安全

5G 终端安全主要涉及两个方面：安全的终端安全架构和多次认证接入技术。

安全的终端安全解决方案当前主要有：黑名单查杀、白名单模式、加固系统、隔离运行模式。

① 黑名单查杀

基于恶意名单匹配（Santa 的 MONITOR 模式），见图 8-62：

图 8-62 黑名单查杀

基于恶意特征匹配，见图 8-63：

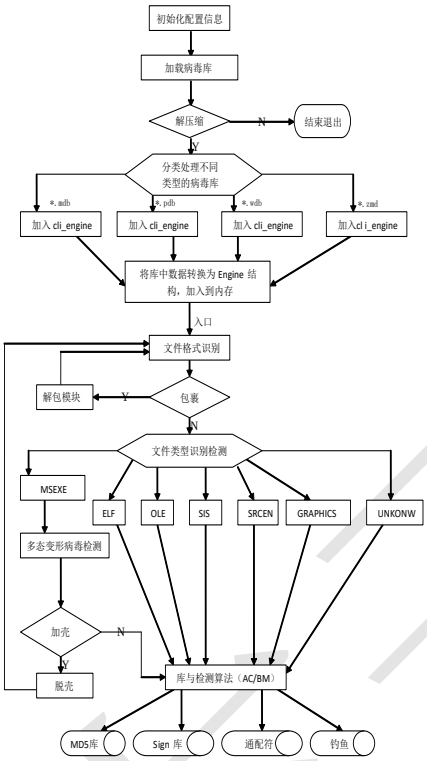

图 8-63 恶意特征匹配

② 白名单模式

基于信任名单匹配（Santa 的 LOCKDOWN 模式），见图 8-64：

图 8-64 白名单模式

构建白环境（可信环境）：

- 可信供应链：确保系统的全部构成部件的供应链是可信的，可按照 ISO 28000 系列国际标准的要求建立相应的可信安全供应链。注：ISO28000 是应运输和物流行业对共同安全管理标准的需求而发展并提出的，其最终目标是改进供应链的全面安全。作为新的管理体系规范，它首次为操作或依赖供应链中某一环节的组织提

供了框架。它能帮助行业各部门审核安全风险并实施控制和减轻风险的安排来管理供应链潜在的安全威胁和影响。它的管理方式与其他基本业务原则如质量、安全和客户满意度的管理方式相同。ISO28000:2007 与 ISO9001:2008（质量体系）及 ISO14001:2004（环境体系）是兼容的，其设计是为了帮助在一个组织内把质量体系、环境体系和供应链安全管理体系整合起来。该规范是以策划－实施－检查－行动（改进）为基础的管理体系，模仿了公认的 ISO14001 的标准。这意味着已经熟悉基于风险的方法的组织在分析供应链安全风险和威胁时可以运用相似的方法。ISO/PAS 28001《供应链安全管理体系－供应链安全的最佳实践规范－评估和计划》提供了实用的指导，以补充 ISO 28000 的规定要求，促使组织机构作出更好的风险管理决策。ISO/PAS 28004《供应链安全管理体系－ISO/PAS 28000 实施指南》，旨在协助标准使用者理解和实施 ISO 28000，从而获取更大的利益；

- 可信根：可信根是本质上可信的功能集，这些功能可以是硬件功能也可以是软件功能，主要用于执行鉴别，保护加密密钥，软件的测量或验证，探测及报告对程序或系统的未授权变更等。ISO/IEC 11889 系列国际标准对可信平台模块（TPM）的架构、结构、命令、算法和方法等进行了规定。注：可信计算涉及到“可信网络通信 TNC”、“可信平台模块 TPM”、“可信软件堆栈 TSS”；
- 可信操作系统：可信操作系统可提供安全的引导和操作环境，具有主体行为的可信性，客体内容的保密性、完整性和可信性，自身的完整性等特点。可信操作系统具备提供存贮器和文件保护，I/O 设备访问控制，用户鉴别，访问控制，能探测某些攻击等功能。不可信的操作系统极易导致恶意代码等攻击。ISO/IEC 15408 国际标准规定了安全操作环境的相关要求；
- 安全数据存储：除应对系统软件进行保护外，也还需对应用软件和存储在设备上的数据进行保护。安全数据存储的目的就是确保存储在设备上的数据只能由授权用户和进程进行访问，并提供相应机制以确保数据不能被感染、篡改或损坏；
- 安全通信：安全通信应提供安全的网络服务，便于设备或进程之间的安全通信。安全通信通过采用恰当的加密、身份识别、校验等措施，确保信息不被伪造、重放或损坏（如报文重复、丢失、插入、乱序、损坏、延迟等）。国际上主要的通信

组织都制定有相应的安全通信规约标准，如 CIP Safety Specification（CIP 安全通信规范）、IEC61784-3 等；

- 软件完整性：除采用可信操作系统外，也必须保护在设备上运行的应用软件免受篡改或感染；
- 安全设备管理：保护设备的组件也必须被安全管理。此外，也必须管理设备的安全生命周期，确保其身份识别、证书等在全部生命周期内的安全。同理，也须对保护设备的软件和配置进行安全管理。其中可信软件基（TSB）的动能架构如图 8-65 所示：

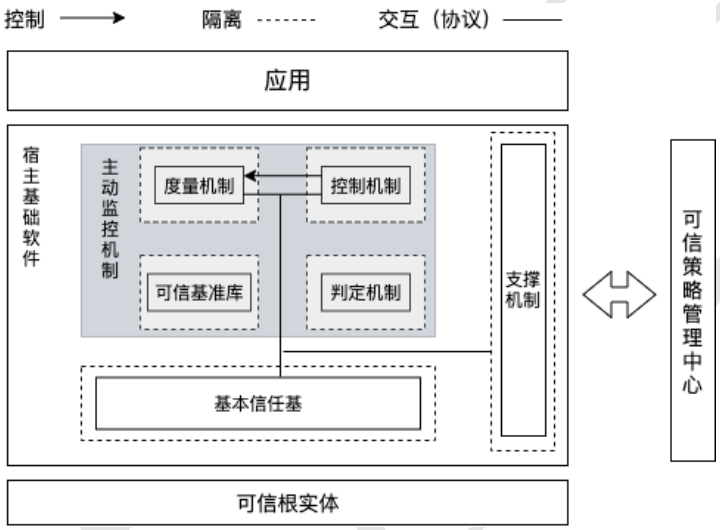

图 8-65 可信软件基（TSB）的动能架构

③ 加固系统

- 加强系统登录帐户和密码的安全；
- 取消远程协助和远程桌面连接；
- 禁用危险的系统服务；
- 关闭不常用的服务端口，比如 137、138、139 和 445 端口；
- 启动系统审核策略；
- 用户权利指派；
- 禁用系统默认共享。

④ 隔离运行模式

- 【沙箱】：如图 8-66 所示，将待分析的文件放入沙箱中，文件会模拟运行，并监控运行的所有行为，以达到动态分析的目的；

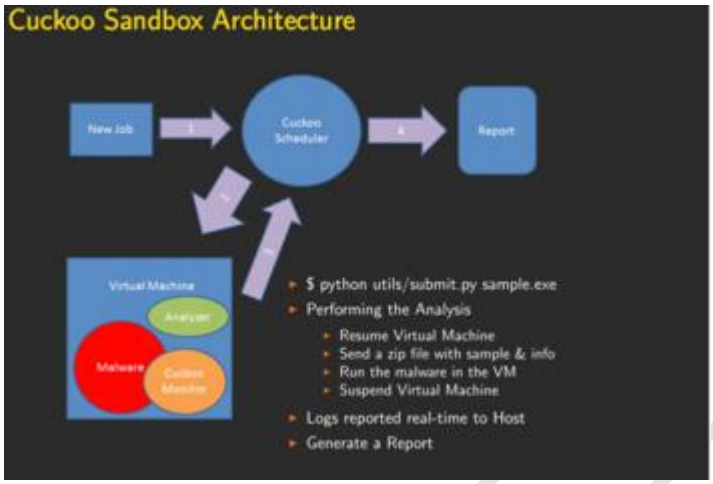

图 8-66 沙箱

- 【虚拟机】：如图 8-67 所示，每一个 Android 应用都运行在一个 Dalvik 虚拟机实例里，而每一个虚拟机实例都是一个独立的 Linux 进程空间；

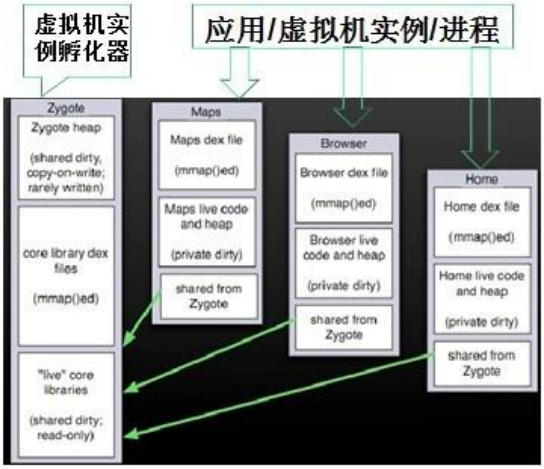

图 8-67 虚拟机

- 【容器】：如图 8-68 所示，容器为应用程序提供一个运行环境，外部的变化不影响容器内部了。

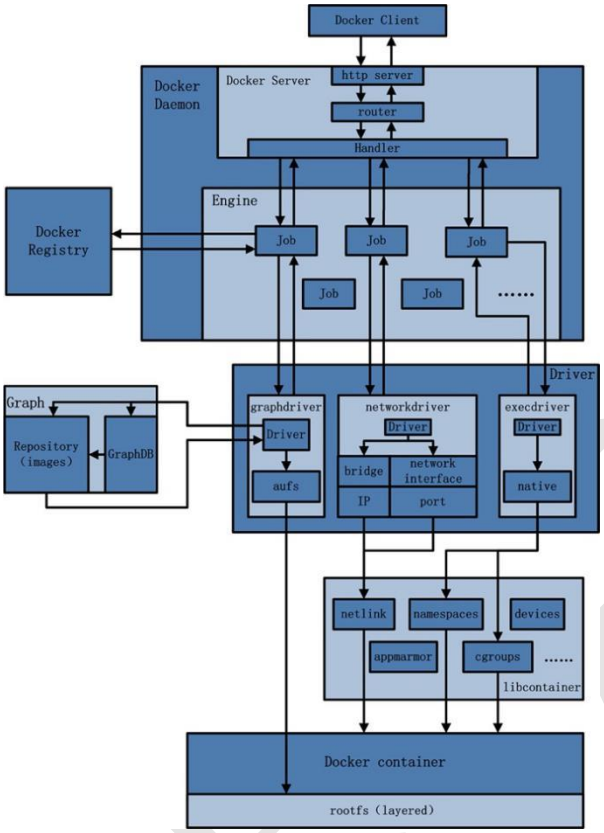

图 8-68 容器

运用上面的三大技术，通常会构建基于安全域的终端安全架构，如图 8-69 所示：

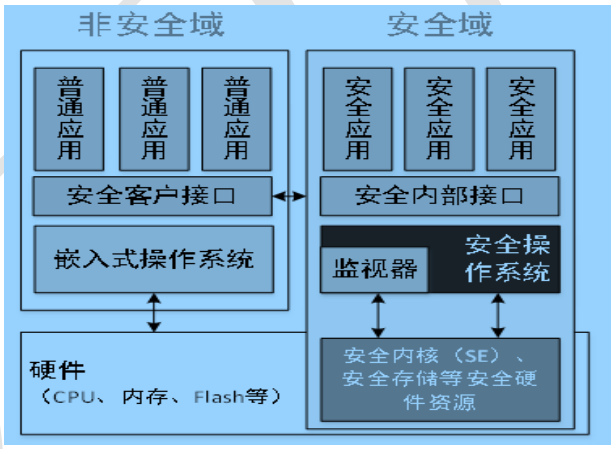

图 8-69 安全域终端安全架构

⑤ 5G 无线接入认证

如图 8-70 所示，5G 无线接入安全主要是接入认证安全，提供多次认证接入技术，在 5G 为垂直行业提供基于 AKA 的普适性安全机制以及切片内的认证与授权服务功能的基础上，提供额外的认证机制以保证用户接入的相对安全，具体流程见图 8-71。注：5G AKA（Authentication and Key Agreement）。

图 8-70 5G 无线接入认证

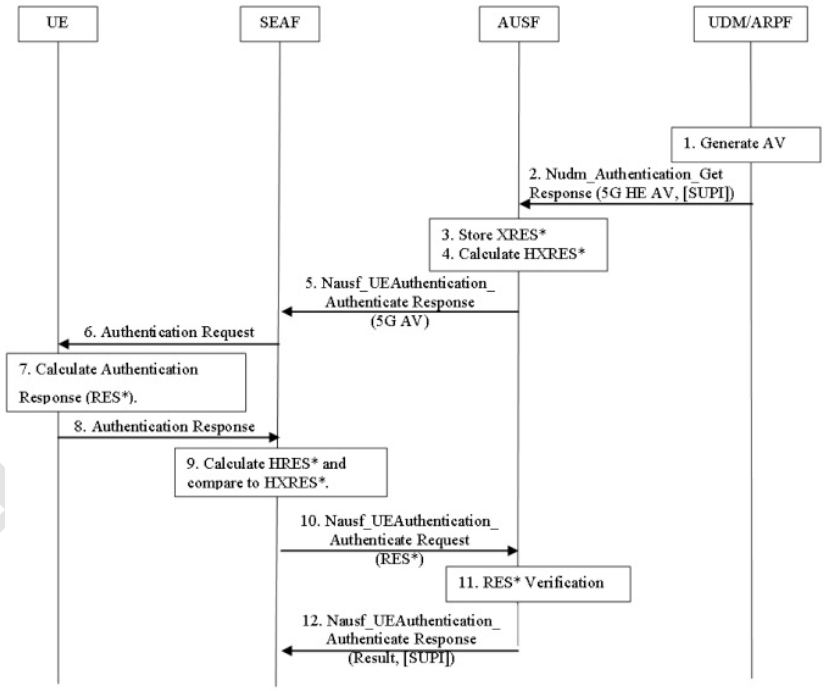

图 8-71 认证流程

⑥ 5G 网络切换三层隔离

借助 5G MEC 边缘技术使能行业数据不出企业区域，保障企业数据的传输安全与用户的隐私安全；同时结合 5G 网络切片的三级隔离机制，为客户提供定制化的、满足需求的安全方案（逻辑或物理隔离等），如图 8-72 所示。1 级隔离和 3 级隔离可以借助云网络微隔离零信任技术，比如六方云的云盾产品；2 级隔离可采用传统安全网关类产品如防火墙等。

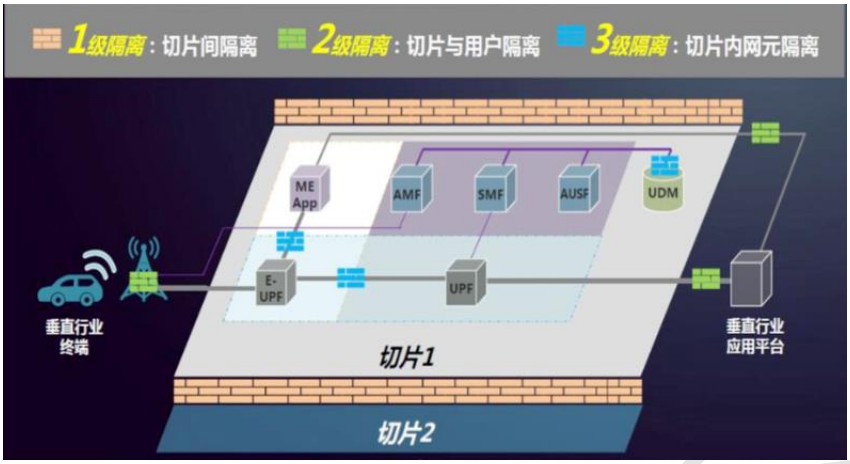

图 8-72 5G 网络切换三层隔离

⑦ 5G 垂直行业等保解决方案

以 5G 的安全技术为基础，联合行业终端安全/网络传输安全技术，以及基于 5G MEC 构建的安全态势感知/不良信息监测与管理等技术使能：

- 更灵活的业务接入；
- 更可控的数据与业务管理；
- 更安全的数据连接与传输。

构建面向行业的、满足国家等保要求的全流程安全防护方案，见图 8-73。

图 8-73 安全防护方案

终端与网络安全技术：5G 协议原生安全技术、行业终端安全防护技术、网络传输安全防护技术。

行业边缘计算安全态势感知技术：

- 行业数据不出企业；
- 提供全方位 MEC 安全防护技术，确保 MEC 与终端、MEC 与核心网之间的通信安全：APP 严选、研判、漏洞监测、二次加密；安全沙箱、脆弱性分析、通道加密等。

行业不良信息监测与管理技术：短信、网站、Email 等垃圾信息的监测、处置、上报等；黑白名单库、数据关联分析；异常访问分析与溯源；异常流量分析与研判。

5G 安全风险与影响及对策

5G 提供了前所未有的用户体验以及连接物联网的能力。它将成为构建万物互联的基础设施。5G 的广泛应用将加速数字经济的转型，促进新兴产业的发展，并给人类的生产和生活带来深刻的变化。还将对国家和社会公共安全，网络和信息安全，安全监管等方面产生重大影响。本文分析了其对安全性，现有安全威胁的影响，并从网络安全系统建设，安全立法和监督等方面提出了对策。

（1） 对国家与社会公共安全带来的安全风险及影响

5G 开启的万物互联时代将使 5G 网络成为社会和经济基础设施，并创造前所未有的规模的产业，承载与社会，经济和公众相关的重要信息，这可能对国家和地区产生影响社会公共安全。

① 攻击破坏关键基础设施，导致运行停滞或瘫痪。在万物互联时代，网络和信息系统已成为整个经济和社会的关键基础设施和神经中枢。5G 网络和能源系统，工业互联网以及其他重要的经济生产和社会管理系统受到攻击和破坏，导致服务中断或瘫痪可能造成重大的经济损失和社会影响；

② 入侵重要控制系统，侵扰社会秩序。通过入侵连接的设施和控制系统来扰乱公共秩序，例如，入侵车辆和管理设备及系统，例如智能交通管理系统，无人驾驶汽车，无人机，监控摄像头等，可能会扰乱交通秩序，甚至造成交通事故，威胁社会秩序和公共安全；

③ 大规模监控、窃取关乎国计民生的重要基础信息，危及产业、人员甚至国家安全。5G 渗透到社会各个领域将承载越来越重要的社会，经济和公共信息，例如有关水和电资源使用，交通、农业、地理、气象、卫生和其他经济与社会运营的数据以及国家基本数据。以及管理信息，例如执法和灾难应急响应。这些信息的泄漏以及基于大数据的分析和利用可能严重威胁中国的相关行业，人员和国家安全；

④ 篡改监测数据，引发公共安全事件。基于无处不在的 5G 网络功能，它使用各种传感器、摄像头和其他设备，可以实施大规模和大规模监控，收集环境条件、能源使用、交通动态、农业生产、医疗卫生、人员活动和其他信息。及时发现环境污染、森林火灾警报、自然灾害等。但是，如果上述监视数据被恶意篡改，将使收集的基本数据失真，无法及时反映状态变化。导致监测和应急机制不及时跟进可能会导致大规模的

安全事故，例如水污染、暴发等；

⑤ 散播恶意信息，扰乱社会秩序。利用 5G 网络在各个领域的渗透，大规模散布虚假和反动的信息，威胁到国家政治安全和社会稳定。

（2） 对网络与信息安全带来的安全风险及影响

5G 具有大带宽，海量连接和超低延迟等功能。基础架构使用软件定义的网络（SDN）/网络功能虚拟化（NFV），面向服务的体系结构以及其他基于云和基于 IT 的技术，并引入或增强了网络切片，移动边缘计算（MEC），小型基站，设备到设备（D2D）通信，服务功能开放以及其他技术和业务模型。安全风险以及新技术和新业务模型对网络和信息安全的影响，包括：

① 超大流量大大提升了基于流量检测、内容识别、加解密等技术的安全防护难度。5G 核心汇聚层可满足 200G / 400G * N 的超高带宽和低传输延迟要求，感知网络安全态势，防止恶意流量攻击，监视恶意程序和监视不良信息的能力，以及满足以下需求的能力：加密和解密传输的数据提出了很高的要求，这增加了安全保护的难度；

② 弱终端易成为受攻击对象。5G 万物互联，终端能力差异很大，弱终端由于资源、能力受限，难以采用全球用户身份模块（USIM）等强身份认证机制，终端自身安全防护能力也较弱，容易成为受攻击、受控对象；

③ 超大连接易引发全网或局部规模攻击。5G 支持 100 万个连接/公里。由于业务原因，网络抖动或黑客控制，突然的大规模访问或重新连接，可能会触发信令风暴或分布式拒绝服务（DDoS）攻击；大型终端同时发起流量攻击更有可能超过甚至击败网络防御功能；

④ 基础设施云化、IT 化进一步打破网络封闭状态。与传统网络不同，5G 全面引入了 SDN/NFV，MEC，网络切片等技术，并采用了面向服务的新架构来提出服务能力的开放，进一步打破了网络的封闭状态，模糊了安全边界，威胁和传播速度更快轻松的攻击和预防，全面的云化以及基础网络的 IT 带来了网络和信息安全保护方面的新挑战；

⑤ 边缘云、D2D 通信模式的引入绕过现有中心化的监测体系。5G 引入的边缘云和 D2D 通信改变了原始的网络架构和通信模式。其中，边缘云的分布式部署，计算能力和信息内容比集中管理面临更严重的内容安全风险。边缘云业务流量在本地分流，D2D 通信

流量没有通过核心网络，从而绕过了现有的集中式信息安全监控系统，因此很难对其进行有效的监控和管理；

⑥ 伪基站、身份泄漏问题得以解决，小基站安全性易受威胁。在 5G 时代，缓解了 2G 时代的伪基站问题以及延续到 3G 和 4G 的用户标识码（IMSI）身份泄漏，但是，为弥补宏基站高频覆盖问题，具有室内覆盖问题的各种类型的小型基站难以放置在专用计算机室中，物理安全性难以得到保证，并且它们需要通过公共网络传输回去。它们很容易受到攻击，并且会发起攻击来威胁网络和信息安全。具体而言，5G 各层面的安全威胁主要包括终端侧、空口、gNB 基站、传输、MEC、核心网、虚拟网络平台、管理运营支撑系统（MBOSS）及其管理、能力开放等安全域的多种安全威胁。

（3） 5G 的行业融合增加安全监管的难度

5G 与信息技术和各个行业的深度融合，数据量的爆炸性增长以及海量终端的连接，也将大大增加安全监管的难度。

① 海量数据与舆情监测。5G 网络功能的显着改善将促进海量数据的生成和视频内容的发展。不良视频内容的识别和海量数据的舆论分析将对安全监管构成挑战；

② 海量终端的溯源与取证。5G 支持大量的终端连接。大型终端的身份管理和认证过程不同于传统终端。需要新的身份验证方法，例如分布式身份验证，分层身份验证，（行业）用户身份验证或组身份验证，因此，海量源终端的可追溯性，证据收集，在线日志保留等都变得难以监控。

（4） 5G 安全对策建议

对于各种 5G 安全问题，需要采取必要的措施进行处理，建议从以下几个方面入手：

① 针对 5G 可能面临的安全形势及其重要性

- 加强保护水平，加强影响国民经济和民生的关键基础设施的安全水平保护要求；
- 增强整个网络的安全状况意识和协同保护功能。5G 网络将承载许多垂直行业应用。建议增强整个网络的安全意识和协作保护功能，包括各种垂直行业中的应用程序；
- 加强打击网络犯罪的斗争。在 5G 时代，对网络安全的危害程度正在增加，建议加强对网络犯罪的证据收集和打击；
- 自主研发和控制核心技术。5G 网络虚拟化和 IT，使用了大量的云技术，需要加强

对云技术，通用服务器，基本软件和芯片等核心技术和产品的开发和控制；

- 建立以自动监测为重点，结合传统方法的应急机制。在将基于 5G 的公共安全监控，应急通信等服务应用于相关领域的同时，加强监控设备和系统的安全检测和安全防护能力，并有效地将自动化监控机制与传统的监控方法相结合。容量不足时提供应急机制。

② 针对 5G 网络承载不同业务的安全需求及安全风险

- 用“三个同步原则”加强网络和信息的安全性。在建设阶段，同时规划，设计和建设 5G 网络和信息安全保障机制，以确保在线运营网络和服务的安全性；在运营阶段，同时实施了操作防御，监视，响应和预防的综合预防和控制系统，以满足安全保护和控制要求；
- 构建具有统一管理，智能防御和灵活性的 5G 安全系统。满足多路访问和不同场景的安全需求，并通过统一的安全管理，态势感知和协同防御能力建设，提供差异化的安全保护机制，实现安全威胁的智能协同防御；基于网络切片，安全功能的模块化组合通过根据需要灵活部署和协调安全功能，实现差异化的安全保护机制，以满足大带宽，大连接等不同场景的安全需求；通过轻量认证，分布式认证等，建立统一，可扩展的身份管理机制。满足物联网等各种终端安全需求的技术，实现用户身份的统一管理，标识和可追溯性；基于统一的中央平台和边缘计算功能，部署近源安全防御功能以形成分布式安全防御功能，以应对 5G 超大带宽，超大连接和 MEC 内容下沉带来的安全威胁；
- 为安全防御，监视，响应和预防实施集成的自适应预防和控制系统。 同时改善 5G 安全监控设备的建设，并支持恶意代码和内容安全等相关管理流程，以增强监控和发现能力；增强取证举报能力，启动联合防控机制，建立一键关闭功能，提高网络信息纠正能力。建立信息安全态势感知能力，建立信息安全监控预警系统，持续对安全威胁进行实时动态分析，自动适应网络和威胁环境的变化，不断优化安全防御机制；
- 建立协调一致的国防安全生态系统。通过安全能力和服务开放性的形式，通过跨网络和跨行业的合作，通过安全态势感知和安全协调能力的建设，为网络和垂直行业建立协作防御能力，共同提高对网络和网络的响应能力。

③ 针对 5G 安全监管的问题

有必要使用基于大数据的舆论监测分析技术，增强舆论监测能力。加强物联网行业用户的监管，保留物联网终端身份记录，提供终端安全事件监控，可追溯性和证据收集功能。同时，应对信息安全形势的变化，加强与信息安全相关的立法和监督。

- 有条件地使用电子记录，例如网络日志和网络记录作为法律证据。 在 5G 时代，个人活动记录在大量的网络记录中。对于大多数网络应用程序的实名背景，电子记录，尤其是不同应用程序之间的关联，具有很强的信誉。建议基于的实名认证，使用由电子记录（如在线日志，满足特定条件的应用程序记录）形成的证据链作为法律证据；
- 自动控制/远程控制设备的安全与责任立法。无人机，无人驾驶等自动控制，远程控制设备，可能发生干扰损失的安全事故，需要明确的设备使用的安全规格，发生事故时的责任界定；
- 识别由网络攻击行为的取证，入侵或不正确的网络服务造成的人身伤害和虚拟经济损失。网络服务提供商进行的网络攻击或不当服务不仅可能造成个人/客户虚拟网络收益的损失，而且还会涉及现实损失甚至人身伤害，网络攻击的取证，入侵以及由此产生的虚拟经济和实际识别 伤害和损失需要根据相关法律进行定义；
- 数据隐私问题。在不同系统中保留个人信息和网络活动记录可能成为大数据分析的个人隐私的重要信息。尽管获取孤立信息可能不会直接造成损失，但是在进行诸如关联分析之类的处理后，它可能会泄漏重要的个人隐私并成为网络欺诈甚至是有关实际犯罪的重要信息。建议加强对泄露私人信息的各个方面的打击，包括在线记录，网络活动记录等，以保护网络空间的安全。

8.12 工业安全管理

环境的变化以及新的漏洞和威胁的发现将需要更新策略、固件和软件，因此工业物联网系统的安全功能必须是可配置和可管理的，而不是静态定义的。此外，必须仔细控制、配置和管理部署的版本。

定期安全合规报告通常是强制性的，当然也是可取的。应定期分析网络和端点配置，以报

告与所有相关策略的偏差，并总结合规性姿势。

安全管理必须确定要管理的系统的安全目标。这些安全目标应确定用于确保信息机密性、端点和通信完整性以及管理所需系统功能可用性的技术。

安全运营管理与安全管理

操作管理是对系统及其端点的操作功能的配置，包括配置、操作系统设置、物理和逻辑网络设置以及操作过程的应用程序配置。

安全管理是对端点上的安全控件的管理，包括添加和删除安全控件、设置安全策略以及启用提取安全事件和日志。

操作管理应与安全管理分开，以便安全控制过程可以独立发展。

安全操作管理涉及保护操作管理过程和功能，以确保对系统操作元素（包括端点、通信、监控和管理系统）所做更改的完整性和机密性。

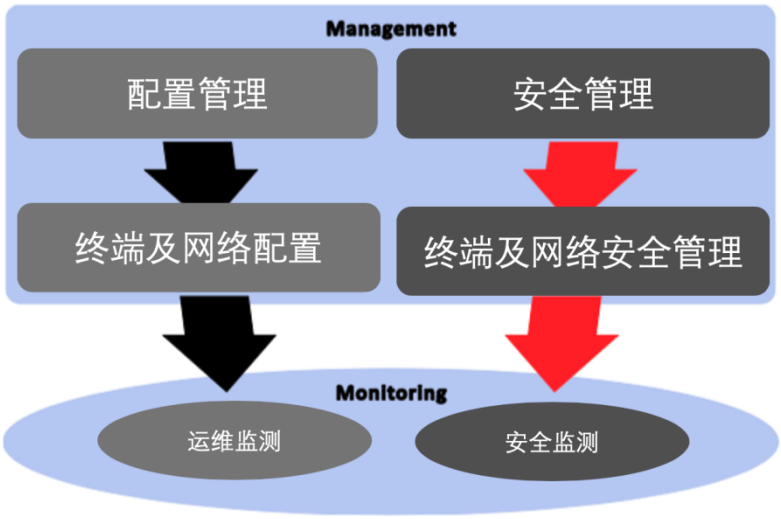

图 8-74 安全系统管理

两者都实现策略以配置端点上的设置，并且系统或安全性上的错误配置可能导致漏洞。端点、应用程序和数据的敏感特性要求在分离这些区域之间的关注点时特别小心，尽管它们之间的界限常常很模糊。

运营管理必须与运营监控互动。操作事件和安全事件也应该分开。安全监视使用来自端点和通信的安全事件来评估安全性并确定必须纠正的差距。操作管理和监视控制是特定于系统操作过程的，而不是安全管理和监视，安全管理和监视可以在不同的操作过程中是相同的。例如，凭据的设置、网络数据通道规则的定义和安全事件数据的目的地的标识都是跨各种操作过程所必需的，尽管实际设置可能因端点而异。

跨构成操作过程的所有端点的通用安全 API 将安全过程与操作过程隔离开来，而不依赖于 make、model 和端点的制造商。要实现这一点，端点需要三个与安全相关的 API。

明确定义这些公共 API 的互操作性标准将统一管理和监视基础设施的重要部分的实现。NIST SCAP 标准（用于定义脆弱性、测量和策略遵从性的可互操作内容自动化）和 IEC 62351 第 71 部分（用于电力行业的网络数据和安全管理）在一定程度上实现了这一目标，但迄今为止还没有发布标准，所以每一个管理和监控的实施都是不同的。

安全通信信道

通信信道包括数据信道和控制信道，其中管理作为控制信道的子信道。控制通道在数据通道上强制执行策略。

管理通道承载需要独立处理的几种类型的消息。例如，包含流向端点的策略的安全消息流应与流回聚合点的安全事件流分离，以强制分离策略管理和事件监视之间的关注点。

安全信道可分为安全配置信道和安全监视信道。安全配置通道包含策略定义。

分层通道如下图 8-75 所示。

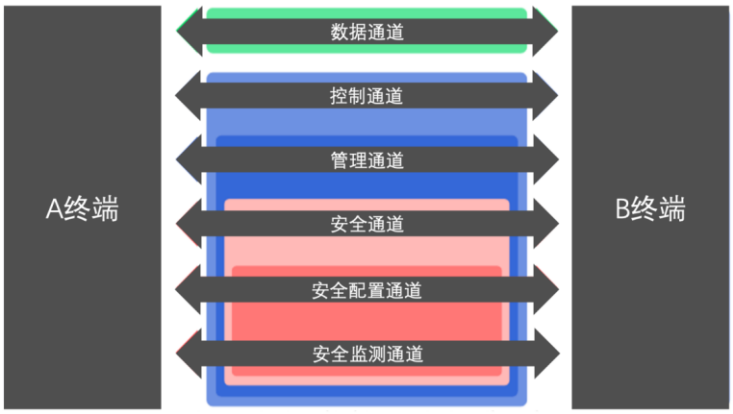

图 8-75 分层通道视图

安全运营管理

运营管理配置和控制 IIoT 系统及其组件，以实现组织的业务流程。系统的可信性取决于对所有系统元素的信任，以及对所有系统元素正确协同工作的保证。必须对整个系统进行安全管理，不得扰乱操作过程或降低系统的安全性或可靠性。

在操作管理中可能有安全考虑。在评估操作系统中的风险时，必须评估每个端点的关键性。安全管理系统必须比它管理的最关键的端点具有更高的关键性，因此需要遵守该级别端点所需的所有安全策略。不同的标准定义了确定系统临界性的不同机制。

运行管理系统中可能存在安全隐患。多个操作管理系统分别在特定的安全级别管理一组设备，因此不希望继承 OT 设备安全规则的设备自然被隔离。安全管理不受这种继承依赖性的影响；因此，最好将安全功能与安全功能隔离开来。

安全管理

系统的安全模型基于许多来源，从监管政策到行业标准、组织指令和个人经验。安全策略必须应用于可在组织内实施的安全模型，并应安排定期审查，以便在必要时对其进行更新。

（1） **安全策略管理**

安全策略是一个总括的术语；实际上有三种类型的策略。计算机策略包含一个数字文档，其中包含端点上技术安全控件的设置。组织策略记录环境的预期行为，包括技术和非技术行为（例如，防火墙不允许传入事件通信，或者每个房间都必须有灭火器）。监管政策通过区分好的行为和坏的行为来强制高水平的行为（州、国家或全球）。

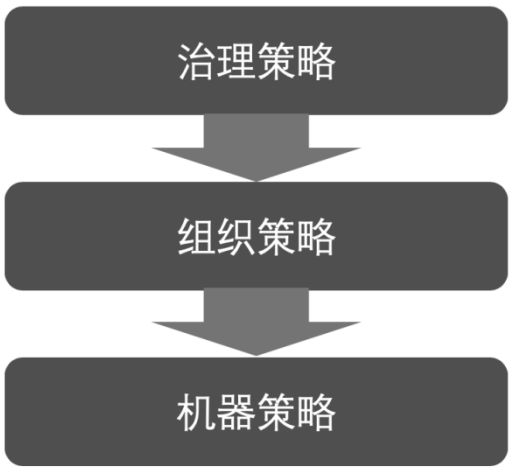

图 8-76 安全策略关系

安全策略描述系统安全元素的预期行为；安全监视描述环境中实际发生的事情。安全管理是一个迭代过程，它配置和更新系统以保持相同的安全级别。

安全管理平台能够为每个端点的安全控制、通信流以及软件和固件更新定义策略。该平台为事件监视和在适当时间发出警报提供了基础设施。分析提供情景和上下文感知，结果更新机器策略设置。自动化将策略推送到端点，并收集和分析来自端点的事件。

安全管理调整安全功能以应对条件的变化。用户界面和工作流应该足够简单，以便用户定义、更新和监视相应的安全状态。如果安全管理难以使用，人们将难以有效地应用安全，安全事件将更容易发生。

为了限制操作和安全问题之间交叉污染的风险，具有不同角色和职责的不同团队应各自拥有任何特定操作的最低访问级别。

安全管理平台应该平衡安全性和其他关键系统特性。

（2） 政策制定和定义

安全策略被分配给一个或一组端点。这项政策应该是综合性的。创建基线策略简化了对复杂 IIoT 系统中许多端点的应用。然后针对单个端点或端点组调整基线策略，从而消除每次重新生成整个策略的需要。提供一个一致的策略格式，并使端点能够解释策略，从而简化了识别安全漏洞的工作。

一个人必须能够理解基于监管或组织策略的安全性预期行为，并将其转换为计算机策略设置。至少有两个地方必须简化安全性以便于人们理解：策略定义和事件分析的结果。策略定义从定义 IIoT 环境中所需行为的人开始。然后将这些转换为存储在发送到终结点的计算机策略中的安全设置。事件分析从安全事件从端点发送到足够安全的位置进行分析开始。它可以触发警报并以仪表板、用户界面警报、电子邮件通知和报告的形式生成通知。

一个人必须能够根据机器策略最初定义组织安全策略。基于安全事件分析对安全策略应用适当的更新将创建一个反馈循环，通过该反馈循环，可以随着时间的推移维护（甚至增加）安全性。可能会自动执行此反馈循环。

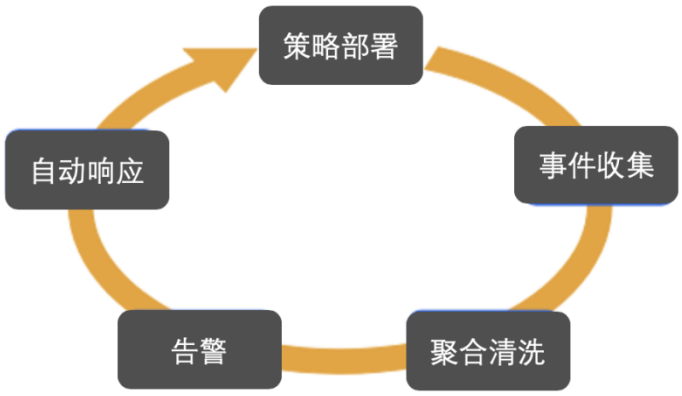

图 8-77 安全管理监控反馈循环

图 8-77 中的反馈循环从将机器策略推送到端点开始。端点基于机器策略设置收集事件，特别是违反安全策略的事件，并将事件发送出去进行安全分析。安全事件数据是相关的，当超过安全阈值时会触发警报，并执行自动响应以减轻安全事件。自动响应可以简单到在仪表板上设置警报或发送电子邮件，也可以复杂到发送新的机器策略更新以重新配置受影响的系统。反馈回路类似于监视器（事件收集）、分析（聚合/关联和报警）和行为（自动响应和策略部署）。

（3） **保单转让和交付**

在管理过程中，必须为每个端点定义安全策略。希望有一个粗粒度的机制来高效地跨多个端点定义此策略。管理过程必须是可伸缩的，并且要使人成为过程的一部分必须进行优化。

应该向人员公开适当的策略设置，以便她可以正确配置端点上的控件。为了简化策略管理，需要重用和自动化。

策略应同时推送到多个终结点。具有策略子元素的结构化策略允许跨多个不同策略重用元素。可以构建一个策略库，它将不同的策略子元素组合在不同的组合中，而不必为较小的更改重新定义策略。默认策略子元素通过管理与默认值的差异而不是重新定义整个策略，来简化定义策略。

终结点安全策略应可分配给终结点或一组终结点。这允许在原子级别管理端点，或与共享公共功能的其他端点一起管理端点，而无需分别为每个端点创建策略。

强烈建议使用自动机制将机器策略传递到端点。跟踪每个端点上的策略和子元素允许对策略管理过程进行更多的监督。自动化可扩展，并最大限度地减少人为错误的影响。

端点配置和管理

一旦在终结点上设置了计算机策略，则必须激活和实施在策略编写期间配置并传递到终结点的策略设置。这包括解析策略并为每个受影响的安全控件提供适当的策略子元素。

每个控件都应该接收与其相关的策略子元素，能够理解配置并对其执行操作。管理平台不需要洞察控件的配置；它只公开 UI 控件并存储结果。策略传递步骤也不需要洞察控件的配置；它们只确保策略以适当的完整性和机密性传递到正确的端点。只有端点上的控件本身需要了解保存在管理控制台上的配置设置。

要实现新的安全控制，只需要构建两个组件：一个是由人配置的策略元素，另一个是驻留在端点上并将计算机策略子元素转换为适当设置的安全控制解析器。

将策略应用于终结点后，应将策略冲突导致的任何事件从终结点传出。

为了编写和交付策略，以及在提取事件期间，必须小心保护有关策略和事件的元数据。必须严格执行对它们的访问控制，否则最好的安全实现将容易受到损害。来自任何数据监视的安全元数据都需要定义如何处理以及谁拥有和访问它的策略。收集的某些安全数据可能会涉及隐私。

随着软件数量和复杂性的增加，缺陷的数量也随之增加，其中一些缺陷将成为可利用的漏

洞。其他可能会导致不可预测的系统故障、定时问题、系统性能降低、可靠性或其他未知问题。一旦发现，这些缺陷往往可以通过修补来修复。如果实施了无线更新，则应首先解决影响无线进程完整性的网络相关漏洞。

IEC TR 62443-2-3:2015《IACS 环境中的补丁管理》定义了相关术语，规定了资产所有者和产品供应商的补丁需求，并定义了补丁信息交换的模式。它还为在操作系统中鉴定、验证和部署软件修补程序提供指导。

有时无法更新终结点。例如，如果一个端点太重要而无法继续操作，则可能导致任何修改。在重新进行必要的安全评估之前，某些更新可能会使认证或标准符合性失效。

多种方法为端点提供软件和固件更新。有些端点需要直接物理访问设备来更新它（即，通过连接串行电缆或 USB 驱动器）。另一些则允许用户从远程位置下载更新，并通过命令行或代理命令在本地安装更新。显然，自动升级对管理员来说更容易，更容易验证以确保更新及其来源的完整性，更容易被应用，也更容易验证它们是否被应用。因此，它们比在每个设备上需要物理干预的更新方法更高效，成本更低。

软件和固件更新增加了安全性、安全性、可靠性或功能特性，特别是在棕地场景中。具有很强安全性和可用性要求的系统通常在更新所有端点之前使用暂存区域来测试更新。如果对它们的工作没有信心，软件更新将被忽略，因为操作风险太大。

端点的安全更新可以使用软件来实现，也可以使用软件和硬件的组合来实现，硬件功能增加了额外的保护、完整性和信任层。强烈建议使用硬件容器，如 HSM、TPM 或其他 TEE。升级中使用的密钥可以由第三方证书颁发机构管理，并根据需要进行更新。用于安全更新固件或软件的相同机制也可用于更新系统配置并确保软件来自预期的源。

网关可以简化更新过程。如果网关位于同一供应商的多个端点前面，则可以从供应商更新存储库安全下载和验证软件更新。网关应包括足够的安全功能，以验证更新存储库服务器和软件更新的源，通过加密通道或通过下载加密的更新，然后验证下载的更新的完整性，安全地下载更新。然后，网关可以充当网关后面的端点的更新服务器，直接向端点提供经验证的更新，从而最小化更新过程的攻击面。

制造商可能会尝试在客户的设备上执行自动软件和固件更新，但这是有风险的。如果更新失败，设备可能无法操作或以未知和不可预测的方式运行。更糟糕的是，对手可能会征用该设备作为攻击其他设备的平台。

无论更新的检索方法如何，都必须始终确保更新的完整性。数字签名支持更新文件的验证，并提供比散列更强的安全性。

通信配置和管理

与端点安全强制一样，必须对网络通信进行安全管理和控制。该策略可应用于通信端点或它们之间的中间通信设备。在中间设备上实施网络安全策略的缓解控制可以包括防火墙和包过滤器、路由器、入侵检测系统（IDS）、入侵预防系统（IPS）、网络访问控制以及其他安全控制和设备。

在管理 IIoT 通信的安全性方面，网络访问控制起到很重要的作用。NAC 是一种管理控件，可防止端点进入网络。它依赖于监控流量的网络安全控制的信息。通过集成安全管理系统和安全监控系统，NAC 功能可以检测 IIoT 网段上未经授权的端点并强制断开它们。网关、防火墙、路由器和主动网络监视和控制设备允许强制断开未经授权的端点。

身份管理

身份管理包括管理特定身份域中已知的身份属性的生命周期和值、类型和可选元数据所涉及的过程和策略，该域是实体可以使用一组属性进行标识的环境。身份管理是端点安全中的主要功能之一，是身份验证和授权的基础。

现在已经有身份管理的标准和建议。ISO/IEC 291151 中的“实体认证保证框架”（EAAF）是描述凭证和认证实体生命周期的认证标准。NIST 800-57《密钥管理建议》2 对凭证和身份材料的管理采用了类似的方法。此外，“身份生态系统的功能模型表示”3 是一个身份解决方案模型，包括各种组件和交互。

如果未正确实现和遵守凭据管理过程，则端点身份验证的结果可能无法产生所需的信任级别。

将工业系统透视图应用于现有的身份管理建议会产生生命周期过程的变体。对人类实体的身份的处理与现有的 IT 模型没有太大的区别，因此这里的重点是非个人实体。管理生命周期包括三个阶段：注册、凭证管理和实体认证。

注册阶段确保适当的实体接收适当的身份材料。这需要组件制造商的参与，以在制造、采购、交付和调试期间建立信任。在这些步骤中，实体可能多次更改所有权，因此应保留跟踪监管链的审计跟踪。

组件的身份和完整性应该在注册阶段结束时在凭证管理阶段之前进行验证。仅在软件中

很难证明硬件组件的信任；强烈建议提供硬件支持。

凭证管理阶段是实现对所有者/操作员组织环境的配置的阶段。此过程包括生成凭据，或在终结点上启用凭据生成功能。应保留跟踪将标识材料提供给实体以及存储方式和其他安全实现属性的审核跟踪。应验证相关实体（如设备和端点）的完整性，以及它们的动态数据和静止数据，以确保凭证管理阶段是正确的。

实体认证阶段是在设备和端点实体的日常操作期间发生实际认证和授权过程的阶段。跟踪身份验证和授权尝试及结果的审核跟踪将根据策略在组织定义的时间段内保留。

（1） **报名阶段**

注册阶段为在实体中建立信任提供了基础。在颁发凭据之前，必须有一种机制来确保它是正确的实体（手动或自动）。为了扩大规模，建议采用自动化方法。

注册阶段有三个步骤：启动、实体验证和注册。Initiation 声明希望将实体置于管理之下，并为其提供身份和凭据。验证包括证明实体是要为其创建和发布身份的实体。注册（见图 7-83）意味着实体已经准备好创建和传递凭证，或者让实体自己生成凭证。始终验证已注册的标识是否绑定到为实体生成的凭据。

注册启动步骤要求在颁发所有者/操作员凭据之前，有某种方法可以在注册阶段跟踪实体。实体应具有制造商标识符，理想情况下是背书密钥和证书，由制造商分配和管理，并嵌入在制造过程中。制造商标识符允许组件生成器验证实体并建立对其真实性和完整性的信任。

实体验证扩展了注册过程，以断言接收凭据的实体是合格的，并且具有用于在注册阶段跟踪的制造商标识符。这种方法鼓励组件构建器和系统构建器在端点实体上公开 api，以访问各种标识符和服务来验证它们。

在注册步骤中，现在由组件生成器或系统生成器验证的实体存在于组织的资产跟踪系统中，可供配置。要启用安全注册过程，制造商应公开一项服务，将设备与新所有者关联，使实体能够在初次开机时进行联系和验证，提交制造商标识符，并在制造商标识符和凭据之间提供加密绑定。此过程应可重复，以便将来更改所有权。

由于多种原因，一个端点上可能存在多个标识符。一个原因是端点由多个实体管理，正如预测性维护场景一样。每个组件生成器嵌入一个标识符，但某些终结点可能包含多个子组件，每个子组件都有自己的标识符，从而导致在所有者/操作员启动注册阶段以发出自己的标识符之前，多个标识符与终结点实体相关联。系统构建器也可以在系统组装期间添加标识符。这些

标识符都具有独立于所有者/操作员标识符的生命周期。

在注册阶段，应该创建一个审计跟踪来跟踪执行的步骤。审核数据应保留一段策略定义的时间。审计跟踪数据的完整性应得到保证和证明，并视为机密。

（2） **凭证管理阶段**

在注册阶段之后，凭证管理阶段包括若干步骤，分为两类（见图 7-83）。第一类包括生成凭证、将凭证绑定到实体并将凭证颁发给应向其颁发凭证的实体所需的步骤。第二类包括用于存储凭证、结束使用寿命以及延长凭证使用寿命的步骤。

凭证管理的第一类步骤将实体带入凭证已就位并准备好使用的状态。凭证生成包括创建凭证本身或启用或指示实体创建凭证所需的任何步骤。然后，在凭证绑定期间，凭证或创建凭证的方法与分配给实体的标识相关联。最后，在凭证颁发期间，凭证或创建凭证的方法或指令使用安全的可审核流程传递给实体。具体过程取决于环境的组织策略。

例如，当 HRoT（如 TPM）就位时，不应在外部生成密钥对凭据并将其传递给实体。相反，它应该在 HRoT 内部创建，并且只在外部报告公钥以进行绑定。

凭证管理的第二类步骤处理凭证的正常日常使用及其生命周期内的边缘条件。凭据存储必须实现到基于特定终结点的授权级别的组织策略所需的级别。所需的授权级别越高，凭据存储要求就越严格。应在通信策略中强制实施授权级别，以便不允许没有足够强凭据存储的终结点连接到该终结点。

实体应分类为关键性类别。每个关键级别都应与一个身份验证级别相关联，该级别定义了要放置在成功身份验证中的信任级别。身份验证级别还定义了必须采取哪些控制措施以将虚假证明或模拟的风险降至最低。例如，在非常低的临界状态下端点，可以接受使用明文凭证使用 IP 地址或 MAC 地址作为标识进行身份验证。但对于稍微重要的实体，可能需要多因素身份验证来防止对存储和传输凭据的攻击。在更高和最高的关键性实体中，身份验证应该受到加密保护，并且应该使用防篡改硬件来存储静止和使用中的所有机密和凭据。

凭据存储必须在具有高严重性级别的某些终结点上满足严格的条件。可能存在组织策略要求，具有强身份验证和凭据存储的高度关键实体可能不信任具有不充分身份验证和凭据保护的实体。

在凭据生命周期结束时，必须从服务中适当删除凭据。当识别出要挂起的凭据时，将暂时阻止其用于身份验证。这适用于怀疑系统中存在潜在危害的任何凭证或生成过程。如果凭据或

生成过程可能会发生泄漏，则必须吊销凭据。

在 IIoT 系统中撤销凭证的其他原因是凭证过期或作为密钥轮换过程的一部分。在这两种情况下，新的凭据都已替换被吊销的凭据。

为了限制凭据泄露的风险，应按照组织的凭据轮换策略中的定义，以特定的频率替换凭据。在某些情况下，如果符合凭证轮换策略，则可以更新凭证，而不是替换凭证，以延长其使用寿命。

为了进行审核，必须跟踪所有凭据管理操作。审核数据应保留一段由组织数据保留策略定义的时间。审计跟踪数据的完整性应得到保证和证明，并视为机密。

（3） 实体认证阶段

实体身份验证在远程终结点的标识中建立信任级别。成功的授权基于成功的身份验证，导致授予资源权限。必须制定适当的身份验证和授权策略，以根据远程实体的身份控制对资源的访问。

出于审核目的，必须跟踪所有身份验证和授权操作。审核数据应保留一段由组织数据保留策略定义的时间。审计跟踪数据的完整性应得到保证和证明，并视为机密。

必须通过跟踪 OT 流程的员工和承包商，在整个系统中建立责任制。当个人信息被追踪时，隐私问题就会出现。员工识别码可以减少这些担忧，因此责任感将胜过隐私。但是，在跟踪客户、合作伙伴和其他数据时，必须注意保护 PII 和其他个人敏感数据。

可以同时具有强身份验证和强隐私性。例如，存在限制身份公开的身份验证方案。它们通过匿名凭据和组签名提供匿名加密身份证明。

安全模型变更控制

在端点的生命周期中会发生许多生命周期转换。例如，实现端点的实体注册和凭据管理阶段。类似地，每个端点的安全模型必须根据其生命周期状态进行更改。

调试为端点提供临时标识和策略，该策略将端点锁定为仅与配置服务器通信。理想情况下，组件生成器、系统生成器或两者都应调试端点。

设置将信任根中的标识替换为组织的标识，颁发凭据，并设置新策略以使终结点正常使用。

端点设置配置所需的安全控制，包括将标识材料部署到信任的根中、设置初始策略设置以及启动为其设计端点的业务流程。在某些情况下，端点可能需要设置在指定网络（物理或虚拟）

上进行，以确保在与 OT 设备通信之前完成入职流程。端点可以按计划（可能用于密钥轮换）或根据需要重新配置。

在正常使用期间，端点应用最佳端点安全策略。基于安全事件，终结点可能会过渡到警报状态，该状态将安全控制收紧到最低操作功能，或者在稍后的更新状态中重置终结点。在恢复正常使用之前，可能需要重新设置。

终结点停用终止终结点的有用生命周期，并将其转换为生命周期结束状态。已停用的终结点可以重用，因此它必须能够为其他目的重新启用和重新配置。应在整个安全生命周期中考虑端点可用性。

配置和管理数据保护

安全管理保持安全性随时间的一致性，并且不得干扰操作过程。

安全元数据，如连接状态和特征（加密或验证），以及设备上的安全控制状态，应收集并与操作管理系统共享，以便跟踪。安全元数据应与操作应用程序数据在单独的通信通道上发送。

在某些情况下，安全管理数据应在单独的物理网络适配器上发送，例如可能在网关设备或具有多个物理适配器的较大设备上找到的内容。在其他情况下，如果设备只有一个物理网络适配器，则应在逻辑上分离安全管理数据（即，在其自身的 VLAN 上）。

安全数据应符合特定网络的要求。例如，如果网络受到操作技术数据的带宽限制，则安全元数据可能需要通过连接来限制带宽，或者可以在网络负载较低时每隔一段时间以突发方式发送。需要控制管理服务器元数据更新的频率、吞吐量、容量和持续时间。

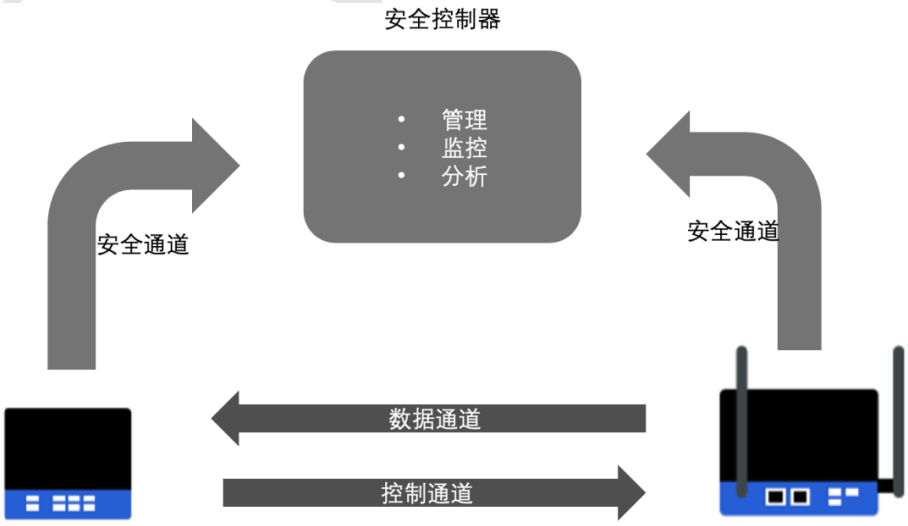

图 8-78 管理数据流

在系统设计中应考虑到隐私，以保护敏感数据，使其匿名化，并控制数据的保留期和存储位置，确保其被正确删除。

应记录隐私敏感数据，以确保对其有足够的认识。它应该根据管理访问权限和同意/撤销以及与第三方共享的策略进行管理。

需要对数据的所有权进行仔细的管理，以确保安全数据不被意外修改。访问控制必须在端点上实施，例如在设备上的配置或管理服务器的数据库中，以及在端点之间的通信中。

变更管理安全模型和策略

监管政策、行业标准和新指令的变化应引发对安全模型的审查。任何更新都会影响组织策略层次结构。例如，当管理策略加强网络访问控制时，这些更改必须通过设置某些网络的访问权限以匹配管理策略中的指令，反映在组织策略中。组织安全策略的更改同样需要调整计算机策略以进行安全控制设置、配置和安全控制。

必须仔细控制所有策略更新，并使用审核跟踪进行跟踪。

第九章 安全标准

9.1 工业安全国际标准

许多准则、标准和条例都与工业互联网有关，比如需要控制对金融系统的访问（萨班斯-奥克斯利法案）、保护信用卡信息（PCI DSS 标准）、保护关键基础设施（例如 NERC CIP、ANSSI 关键基础设施标准）、具有 ISA 99 的网络安全、IEEE PC37.240、安全完整性等级（SIL）、关键基础设施保护（CIP）、关键基础设施安全（CIS）等。

工业安全相关标准和条例

国际电工委员会（IEC）发布了 IEC 624435 工业自动化和控制系统安全系列标准。该系列广泛涵盖了制造和控制系统电子安全的概念，涵盖了不同行业的不同类型的系统、设施和工厂。

目前，IEC 62443 标准系列由四部分组成：

第一部分，阐述标准化术语，旨在提供由其他部分引用的一致的模型、参考和度量。

第二部分，创建有效工业自动化和控制系统（IACS）安全程序的政策和程序。

第三部分，包括网络安全技术、设计方法、评估方法、安全要求和保证级别。

第四部分，讨论 IACS 的安全开发生命周期和安全组件开发的要求。例如，IEC 62443-2-4“IACS 服务提供商的安全计划要求”标准化了集成和维护活动的安全功能，允许资产所有者选择最适合其站点的功能。62443-2-4、62443-3-1 和 62443-3-3 定义了基于攻击者强度的安全级别区分，这对系统设计很有价值。

美国国家标准与技术研究所（NIST）发布了 NIST SP 800-82“第 2 版”，它为提高工业控制系统（ICS）的安全性提供了指导，包括监控和数据采集（SCAD）系统、分布式控制系统（DCS）和其他控制系统配置，如可编程逻辑控制器（PLC），还考虑了性能、可靠性和安全要求。

NISTIR 7628，《智能电网网络安全指南》（第 1 卷，共 7 卷）解决整个电力智能电网安全问题的建议，NIST 与智能电网互操作性小组网络安全委员会共同编制了本指南。

北美电力可靠性公司（NERC）发布的 NERC CIP 标准，旨在通过定义关键基础设施保护（CIP）的可审核要求来提高电力行业的安全性和可靠性。NERC CIP 提供的安全指南主要针对发电和输电设施中使用的自动化系统，NERC CIP 适用于美国、加拿大和墨西哥部分地区的公用事业。

IEEE 1686《智能电子设备网络安全能力标准》定义了智能电子设备（IEDs）中要提供的功能和特性，本标准涉及 IED 的访问、操作、配置、固件修订和数据检索。

安全能力评估

网络安全能力成熟度模型（C2M2）及其垂直行业网络安全能力成熟度模型，比如能源和油气子部门分别对应 ES-C2M2 和 ONG-C2M2。

网络安全能力成熟度模型（C2M2）评估本组织及其产品的安全态势的现状，建立安全目标，说明当前状态、现有风险和业务战略以及确定当前状态和目标之间的差距的优先次序，并确定解决这些差距所需的安全活动。

该模型提出了一个整体的方法来确保工业互联网系统及其组件在其整个生命周期中的安全，从早期设计到实现、部署、维护和退役。它包括对特定安全技术的评估以及使用这些技术的管理和商业环境。

C2M2 模型包含 10 个安全活动域：

（1） 风险管理涉及风险管理计划的建立、运行和维护，以识别、分析和解决与组织、业

务单位、子公司、相关基础设施和利益相关者相关的安全风险；

（2） 资产、变更和配置管理目标 IT 和 OT 资产的管理，包括硬件、软件和集成子系统；

（3） 身份和访问管理的目标是为可能被授予访问组织资产的实体创建和管理身份。凭据可以包括个人访问、共享角色（例如，操作员）、设备或网络区域内或跨网络区域的分布式服务；

（4） 威胁和脆弱性管理的目标是建立和维护计划、程序和技术，以检测、识别、分析、管理和应对安全威胁和脆弱性；

（5） 态势感知是对相关环境的理解。建立和维护收集、分析、警报、呈现和使用操作和安全信息的活动和技术，有助于形成一个整体的操作图景。这包括来自其他 C2M2 域的状态摘要；

（6） 信息共享和通信建立并维持与内部和外部实体的关系，以收集和提供安全信息，包括威胁和脆弱性，以减少风险和提高业务弹性；

（7） 事件和事件响应、连续性行动建立并维护计划、程序和技术，以检测、分析和响应安全事件，并在整个安全事件期间维持行动；

（8） 供应链和外部依赖关系管理建立和维护控制，以管理与依赖外部实体的服务和资产相关的安全风险，包括第三方组件和服务提供商以及开源组件包含；

（9） 劳动力管理创造了一种安全文化，并确保所有人员的持续适用性和能力；

（10） 安全计划管理的目标是建立和维护一个安全计划，该计划提供治理、战略规划和赞助，以使安全目标与组织战略目标相一致，并使其关键基础设施面临风险。

使用该框架的建议方法是评估、确定和分析能力方面的差距，确定需要解决的差距的优先次序，制定解决差距的计划，并实施解决这些差距的计划。随着业务目标和风险环境的不断变化，应重复此过程。

NIST 框架侧重于关键基础设施。CERT 弹性管理模型（CERT-RMM）侧重于操作弹性管理。成熟度安全模型（BSIMM）侧重于安全软件开发。

安全产品测评标准

信息技术安全评估通用标准（Common Criteria for Information Technology Security Evaluation，简称 CC）是用于评估 IT 产品（包括安全集成电路、操作系统和应用软件）安全能力的国际标准（ISO/IEC 154083）。CC 用于评估产品满足安全需求的能力，使用两个关键概

念：评估保证级别和保护配置文件。

评估保证水平 EAL 范围从 EAL1 到 EAL7。例如，功能测试足以满足 EAL1 的要求，但要实现 EAL7，则需要进行彻底的测试以及正式验证的设计。

隐私标准、框架和条例

国际标准化组织（ISO）一直在制定一套有关隐私和个人身份信息保护的标准。

ISO/IEC 29100，“隐私框架”提供了一个指南，其中规定了一个通用的隐私术语，定义了处理 PII 的参与者和角色，描述了隐私保护注意事项，并包括对信息技术的已知隐私原则的引用。

ISO/IEC 29101，“隐私体系结构框架”规定了信息和通信系统处理 PII 的关注点，列出了实现此类系统的组件，并提供了将这些组件置于上下文中的体系结构视图。

ISO/IEC 29190，“隐私能力评估模型”为组织评估其管理隐私相关过程的能力提供了高级指导。

ISO/IEC 27018，“作为 PII 处理器的公共云中个人识别信息（PII）保护实施规范”确立了根据 ISO/IEC 29100 中描述的原则实施保护 PII 措施的公认控制目标、控制和指南。

ISO/IEC 29134，“隐私影响评估-指南”提出了一种对隐私影响进行评估的方法。

NISTIR 8062，《联邦信息系统隐私风险管理》描述了一个以隐私工程目标和隐私风险模型为重点的隐私风险管理框架。

工业协议规范

对象管理组管理数据分发服务（DDS）的开放规范，包括“DDS 安全规范”。有关规范、用户以及与其他技术的比较的更多信息，请访问 OMG 网站。

OPC 基金会维护 OPC 协议的开放规范。有关 OPC Classic、OPC UA 和 OPC.NET 的信息可以在 OPC 网站上找到。

DNP 用户组维护分布式网络协议（DNP3）。技术信息、一致性测试和一致性产品列表可在 DNP 网站上找到。

Modbus 组织管理 Modbus 协议的开发和使用。关于 Modbus 协议的信息，以及基于 Modbus 的工业系统开发和测试的技术资源，可以在 Modbus 网站上找到。

PROFIBUS 和 PROFINET International 管理 PROFIBUS 和 PROFINET 工业协议。协议规范、技术文件和软件工具可在 PROFIBUS 网站上找到。

MQTT 和 AMQP 都是 OASIS 标准，以及 XMPP.8 通用协议定义和标准，如 HTTP9 由 IETF 维护。

9.2 工业安全国家标准

2019 年 3 月 8 日，工业和信息化部与国家标准化管理委员会联合发布《工业互联网综合标准化体系建设指南》，该指南第三章明确提出工业互联网标准体系框架，框架对安全标准进行了系统的描述。

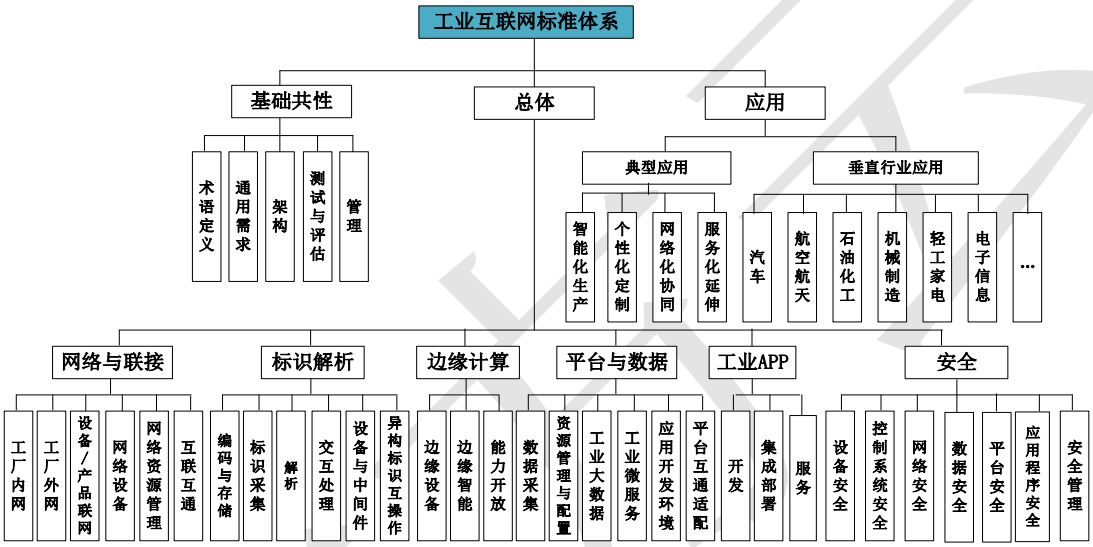

图 9-1 工业互联网标准体系

2019 年 5 月 13 日，《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测评要求》（GB/T28448-2019）等标准正式发布，等保 2.0 时代正式来临。

关于工业互联网安全的两个顶层文件：《国务院关于深化制造业与互联网融合发展的指导意见》和《深化“互联网+先进制造业”发展工业互联网的指导意见》。

工信部先后发布了安全相关指南：《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》 、《工业控制系统信息安全行动计划（2018-2020 年）》。

当前已经发布的工业信息安全相关国家标准：

- 《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 37962-2019）
- 《信息安全技术 工业控制系统安全检查指南》（GB/T 37980-2019）

- 《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》（GB/T 37934-2019）
- 《信息安全技术 工业控制系统专用防火墙技术要求》（GB/T 37933-2019）
- 《信息安全技术 工业控制系统网络审计产品安全技术要求》（GB/T 37941-2019）
- 《信息安全技术 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）
- 《信息安全技术 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）
- 《信息安全技术 工业控制系统安全管理基本要求》（GB/T 36323-2018）
- 《信息安全技术 工业控制系统信息安全分级规范》（GB/T 36324-2018）
- 《信息安全技术 工业控制系统风险评估实施指南》（GB/T 36466-2018）
- 《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 36470-2018）
- 《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）
- 《工业通信网络 网络和系统安全 系统安全要求和安全等级》（GB/T 35673-2017）
- 《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/T 33009.1-2016）
- 《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/T 33009.2-2016）
- 《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/T 33009.3-2016）
- 《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》（GB/T 33009.4-2016）

9.3 云计算安全国际标准

ISO/IEC 270172 标准对云计算的信息安全要素提供了指导。它协助实施特定于云的信息安全控制，补充了 ISO 27000 系列标准中的指导，包括关于云计算隐私方面的 ISO/IEC 27018、

关于业务连续性的 ISO/IEC 27031 和关于关系管理的 ISO/IEC 27036-4，以及所有其他 ISO 27nnn 标准。

NIST 发布了以下云计算标准：NIST SP 800-146，“云计算概要和建议”，NIST SP 500-291，“云计算标准路线图”，NIST SP 800-144，“公共云计算安全和隐私指南”，NIST SP 500-292，“云计算参考体系结构”和 NIST 标普 500-293，《美国云计算技术路线图》。

欧盟网络和信息安全局（ENISA）已经发布了一个可审计的标准，名为“云计算：信息安全的好处、风险和建议”，许多云提供商都通过了该标准的认证。

“云计算安全考虑”由澳大利亚信号管理局提供风险分析和测量，在评估云作为潜在解决方案时，云 SaaS 客户将考虑这些风险。

云安全联盟发布了许多指导原则，包括：

（1）“云计算 3.0 版中关键关注领域的安全指南”，其中包含针对云计算客户和提供商的实用的、当前的指导和建议；

（2）“云应用程序安全开发实践”提供了与云 SaaS 相关的实用指导，例如多租户和数据加密的安全设计建议，以及保护 API 的安全实现建议；

（3）“云控制矩阵版本 3.0”，是一个可审核的标准，映射到一个大型其他标准集，包括 COBIT、ISO/IEC 27001:2005、NIST SP 800-53、FedRAMP、PCI DSS、HIPAA/HITECH、NERC CIP2。云控制矩阵提供了指导云供应商和帮助潜在客户评估云供应商总体安全风险的基本安全原则。云提供商通过完成对云控制矩阵的评估，为其安全控制的设计和管理提供透明度。

智能电网互操作性小组（SGIP）编制了一份关于智能电网开发和部署的标准和实践概要。

使用 TCG 标准保护工业控制系统的具体指导包括在这些文件中：“TCG ICS 安全建筑师指南”、“TCG IoT 安全建筑师指南”和“TCG IoT 安全指南”。这些文件介绍了工业控制系统安全的方法，解决通信安全、系统完整性、固件更新、检测和从复杂攻击中恢复的问题。

SAE 标准的目标是整个移动工程行业产品和服务的安全、质量和有效性。SAE 数据库中的 10000 多个标准现在包括历史标准，可在 SAE 网站上访问。

9.4 云计算安全国家标准

国内已经发布的云计算安全相关标准有（截止 2020 年 5 月）：

- 《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249-2019）
- 《信息安全技术 云计算服务运行监管框架》（GB/T 37972-2019）
- 《信息安全技术 云计算安全参考架构》（GB/T 35279-2017）
- 《信息安全技术 云计算服务安全能力评估方法》（GB/T 34942-2017）
- 《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）
- 《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）
- 《基于云计算的电子政务公共平台安全规范 第1部分：总体要求》（GB/T 34080.1-2017）
- 《基于云计算的电子政务公共平台安全规范 第 2 部分：信息资源安全》（GB/T 34080.2-2017）

第十章 垂直行业应用实践

10.1 钢铁行业：让集团多工厂安全的网络互联以满足个性化制造

背景与目标

钢铁制造装备的大型化是高效率、低成本的基础，目前尚无颠覆性的制造工艺创新以改变现状，通过提升制造管理的柔性来适应日益快速变化的用户需求，就显得极为迫切。用户需求个性化的特征是用户对产品和服务的质量标准、性能 外形、速度的差异化要求，追求亲自参与产品全生命周期过程的用户体验；而对钢铁制造企业而言，则主要体现在钢铁产品多品种、小批量、短工期、交货的灵活性。

实现钢铁产品的个性化制造，解决方案就归结为“以大规模、标准化制造 的成本来满足多品种、小批量的需求”，在现有工艺装备不发生重大创新的前提下，生产组织呈现出足够的柔性和灵活性；换言之，有必要找到一种方式和手段，能够在“钢铁制造大规模、标准化”固有本质和“小批量、多品种”的新特征之间找到一种平衡，从而既满足用户的需求，又使得制造企业可以获利，在价值链上公平地共享价值。

工业互联网是一个有效的解决方案：整个集团的所有生产系统和应用系统通过互联网连接起来，打通横向上下游供应链信息，纵向 0 层到 4 层的生产数据，实现钢铁供应链上下游

协同，促进最终用户企业与钢企业生产直接对接，转变传统的以产定销的模式为以销定产，实现即时生产，提高钢铁产业链的整体协同制造效率。

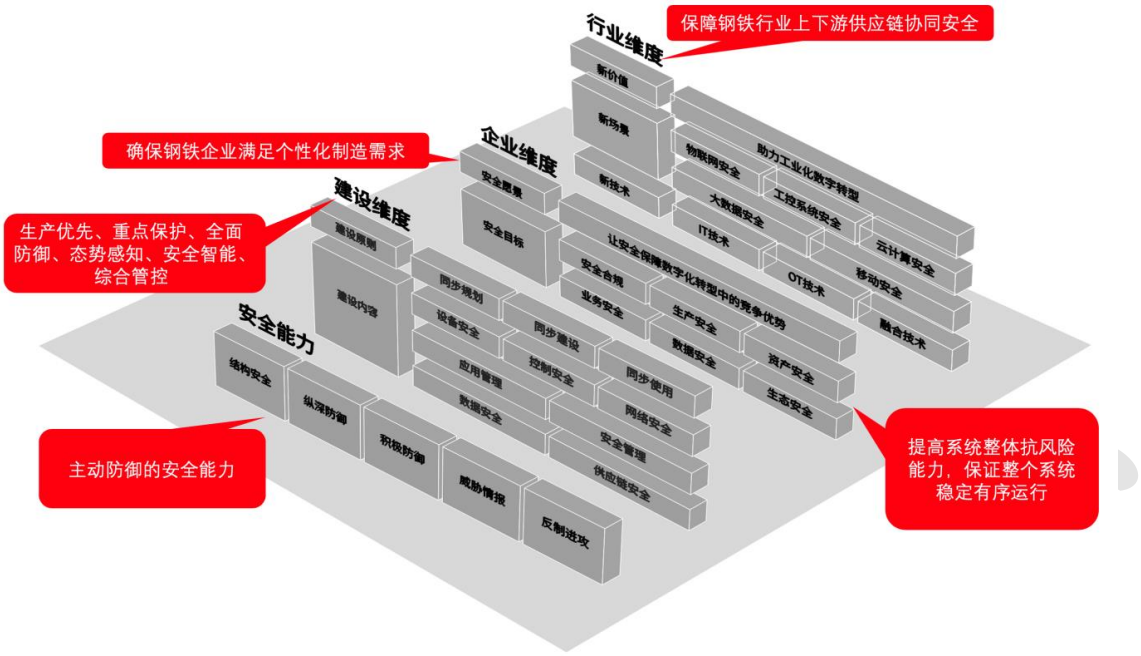

图 10-1 钢铁行业工业互联网方案

（1） 全局安全目标

在行业维度，钢铁企业以智慧制造的理念和方法推进供应链协同，研究以用户为中心，基于全程供应链协同模式，实施“按需求拉动组织生产”，提高交付精度、缩短交货周期、降低供应链库存，实现低库存成本、低资金占用、高效率响应、稳定可靠的供货保障协同解决方案，巩固并不断提升在供应链安全性和保障性方面的竞争优势，确保供应链协同基础设施安全，包括企业间数据实时的、高效的、在线交互的安全以及以敏捷制造、虚拟制造、网络数据交换为基础的协同制造平台的安全。

（2） 企业安全目标

在企业维度，工业控制系统负责完成生产控制、执行，网络安全性要求高，一旦受到恶性攻击、病毒感染，可能造成不同程度的经济损失和社会影响，严重的可能导致工控系统的控制组件或整个生产线被迫停止运转。工业控制系统具有很高的集成度，与其他信息网络的互联程度也随之提高。因此，各系统间的协同作业与信息交互，需构建一套完整的安全防护体系，从网络层、主机层、系统层、应用层等多方面进行主动式威胁管理，实现主动防护、审计监管、集中展示和分析溯源等功能，提高系统整体抗风险能力，保证整个系统稳定有序运行。

（3） **安全建设目标**

在建设维度，钢铁企业要遵循“三同步”建设原则，安全防护措施不能影响生产正常进行为优先原则，对工控网络、工控设备、企业云平台实施重点保护；并采用全流量分析与监测技术，既能够及时检测出勒索、挖矿、蠕虫等高级威胁，也要能够高效检测出诸如 0day 利用、高级逃逸等未知入侵威胁，实现全面防御；借助数据采集、分析技术，实现安全状态的全面了解与可视，安全风险与趋势的科学预测与预警，并能够综合各种因素，自动做出安全响应处置决策；建立统一的安全运维管理中心，实时监测上下游供应链交互信息、从下向上的生产数据以及从上向下的生产控制指令，及时发现入侵攻击并采取相应处置措施，实现统一安全运维管控。

（4） **安全能力目标**

在能力维度，钢铁企业通过安全建设，具备生产控制系统安全可控、安全运维可查可审计、个性化制造的业务系统与平台安全可信、符合等保 2.0 技术要求、高级与未知威胁及时发现与防范、攻击威胁事件证据留存可溯、全企业全供应链的安全态势可见、外部威胁情报能够为我所用，内部威胁事件经过处理后可对外共享等八大安全能力，核心能力是主动检测、主动预警、主动保护、主动响应的主动防御能力。

功能架构

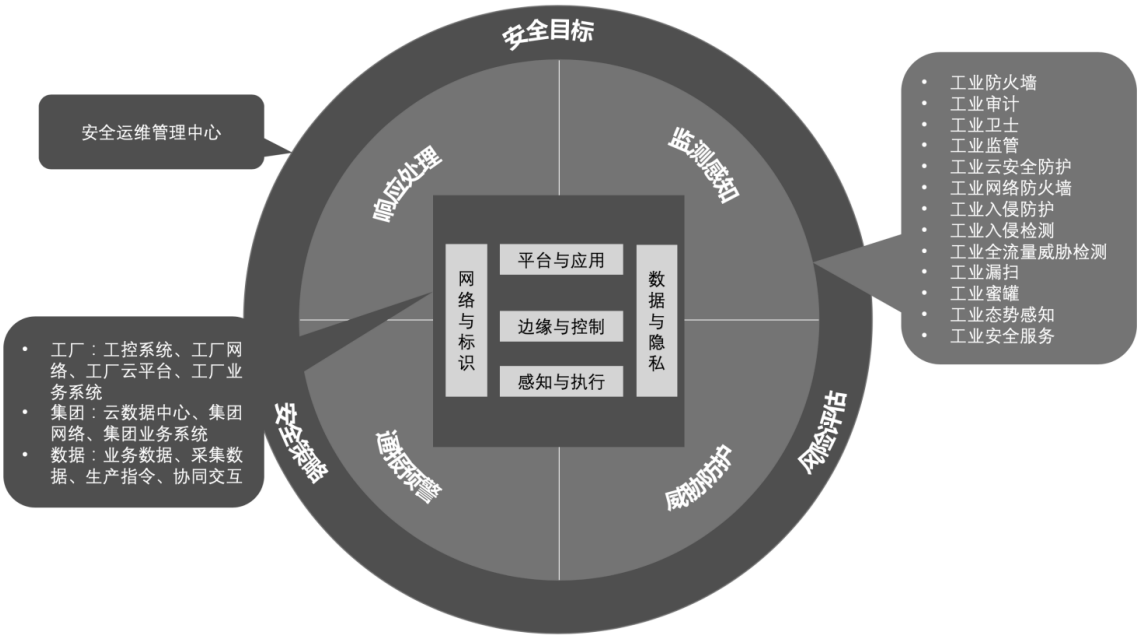

图 10-2 钢铁企业安全防护功能架构视图

钢铁企业的一般网络结构如下：

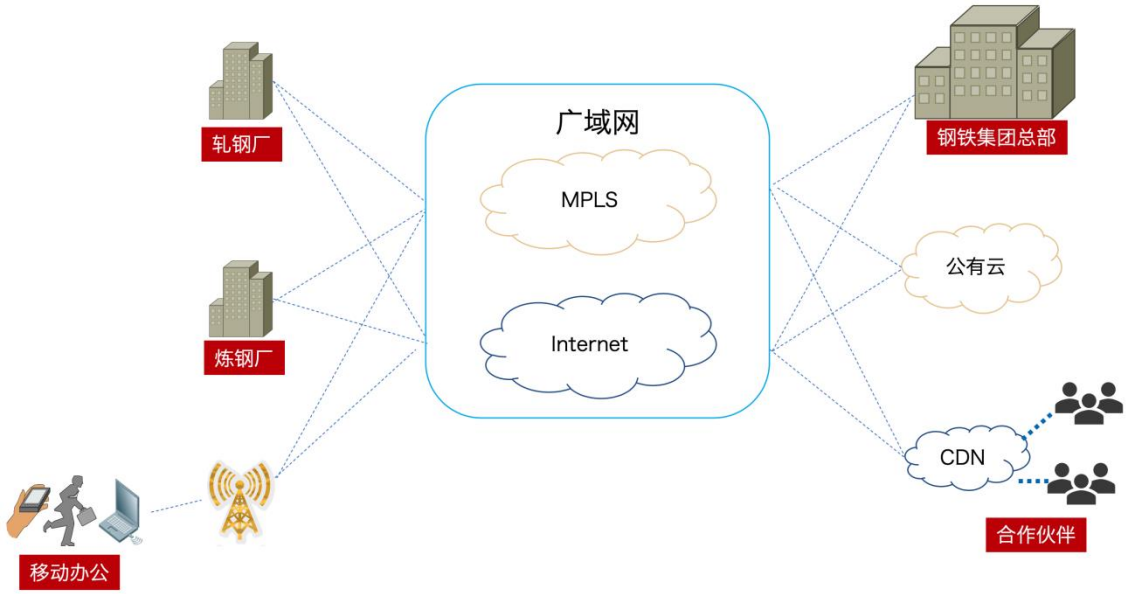

图 10-3 钢铁企业网络结构

（1） **防护对象**

从防护对象角度，可以从工厂、集团总部和数据三个对象来设计安全防护方案。

钢铁行业生产工厂的网络逻辑结构如下：

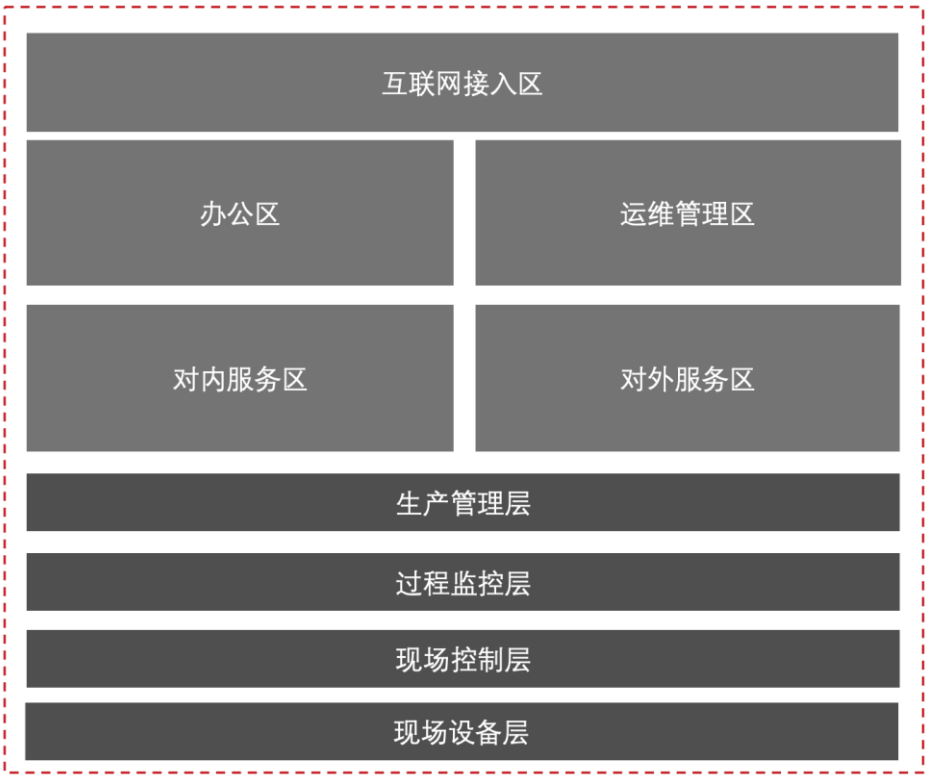

图 10-4 钢铁行业生产工厂的网络逻辑结构

比如轧钢厂的网络结构一般如下：

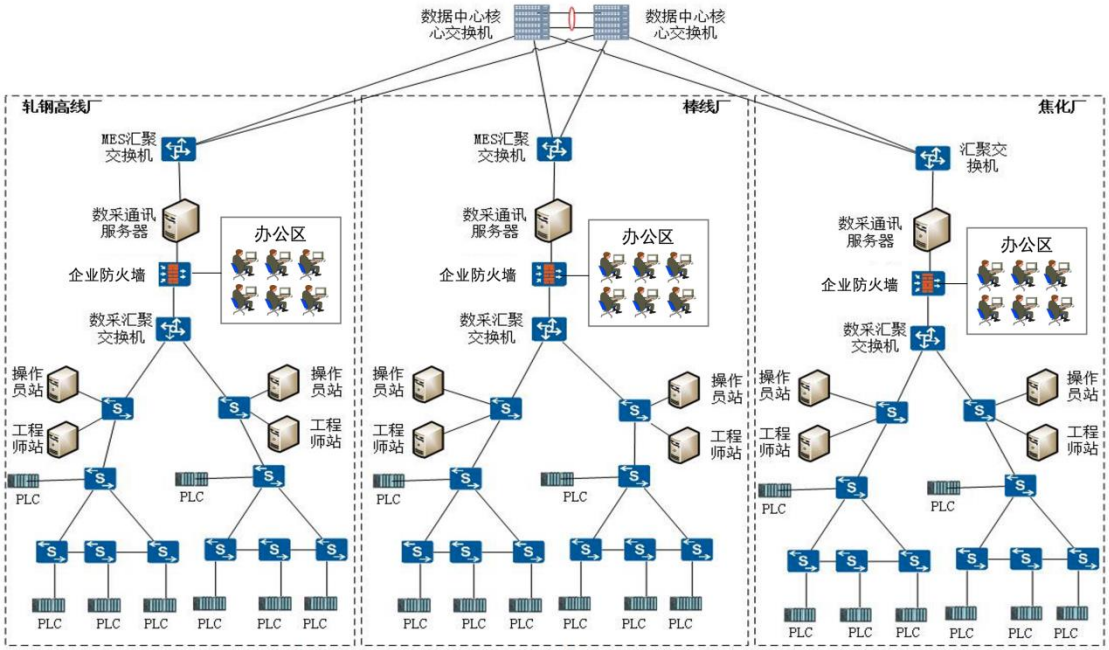

图 10-5 轧钢厂的网络结构

在工厂级而言，防护对象通常会包括生产工控系统、工厂网络、工厂业务系统、工厂虚拟化平台（规模较大的工厂可能会建设私有云）。

① 工控设备漏洞

在钢厂里面，工控设备漏洞基本上没有得到及时升级修补。以目前在钢铁行业普遍使用的 Simens S7-300 PLC 为例，作为市场占有率极高的一款工业控制设备，其漏洞数量多，影响大，且在现场普遍未被修复，具体漏洞列表如下（摘自工业态势感知系统漏洞信息库）：

表 10-1 Simens S7-300 PLC 漏洞列表

序号	漏洞等级	漏洞编号	漏洞名称
1	中危	CVE-2014-4685	Siemens SIMATIC WinCC 安全漏洞
2	高危	CVE-2017-12741	多款 Siemens 产品安全漏洞
3	高危	CVE-2016-3949	Siemens SIMATIC S7-300 CPU 拒绝服务漏洞
4	高危	CVE-2015-2177	Siemens SIMATIC S7-300 CPU 设备输入验证漏洞
5	高危	CVE-2016-9158	SIMATIC S7-300 和 S7-400 CPU 安全漏洞
6	中危	CVE-2018-4843	多款 Siemens 产品安全漏洞
7	中危	CVE-2013-0675	Siemens WinCC CCEServer 缓冲区溢出漏洞

序号	漏洞等级	漏洞编号	漏洞名称
8	中危	CVE-2017-6865	多款 Siemens 产品输入验证漏洞
9	中危	CVE-2017-2681	多款 Siemens 产品安全漏洞
10	中危	CVE-2013-0674	Siemens WinCC RegReader ActiveX 控件缓冲区溢出漏洞
11	中危	CVE-2016-8673	多款 Siemens 产品跨站请求伪造漏洞
12	中危	CVE-2014-4686	Siemens SIMATIC WinCC 安全漏洞
13	中危	CVE-2012-3028	Siemens SIMATIC WinCC 跨站请求伪造漏洞
14	高危	CVE-2014-8551	多款 Siemens 产品 WinCC 服务器代码注入漏洞
15	高危	CVE-2016-5743	多款 Siemens 产品安全漏洞
16	中危	CVE-2017-12069	多款 Siemens 产品 OPC Foundation UA .NET Sample Code 和 Local Discovery Server 安全漏洞
17	中危	CVE-2014-4684	Siemens SIMATIC WinCC 提权漏洞
18	中危	CVE-2013-0677	Siemens WinCC web 服务器拒绝服务漏洞
19	中危	CVE-2016-9160	SIMATIC WinCC 和 SIMATIC PCS 7 安全漏洞
20	中危	CVE-2013-3959	SIMATIC PCS7 Siemens WinCC Web Navigator 安全漏洞
21	中危	CVE-2014-4683	Siemens SIMATIC WinCC 提权漏洞
22	中危	CVE-2010-2772	Siemens Simatic WinCC 和 PCS 7 SCADA 系统硬编码密码权限许可和访问控制漏洞
23	中危	CVE-2016-7165	多款 Siemens 产品非引用 Windows 搜索路径漏洞
24	中危	CVE-2012-3015	Siemens SIMATIC STEP/ PCS 不安全库加载漏洞
25	中危	CVE-2015-1594	多款 Siemens 产品不可信搜索路径漏洞
26	高危	CVE-2013-3958	SIMATIC PCS7 Siemens WinCC Web Navigator 登录实现安全漏洞
27	高危	CVE-2013-3957	SIMATIC PCS7 Siemens WinCC Web Navigator 登录界面 SQL 注入漏洞
28	高危	CVE-2012-3032	Siemens SIMATIC WinCC SQL 注入漏洞
29	中危	CVE-2018-4832	多款 Siemens 产品输入验证漏洞
30	中危	CVE-2014-4682	Siemens SIMATIC WinCC 信息泄露漏洞
31	中危	CVE-2014-8552	多款 Siemens 产品 WinCC 服务器信息泄露漏洞

序号	漏洞等级	漏洞编号	漏洞名称
32	中危	CVE-2012-3030	Siemens SIMATIC WinCC 权限许可和访问控制漏洞
33	中危	CVE-2016-8672	多款 Siemens 产品安全漏洞
34	中危	CVE-2013-0676	Siemens WinCC 敏感信息漏洞
35	中危	CVE-2013-0678	Siemens WinCC 敏感信息漏洞
36	中危	CVE-2013-0679	Siemens WinCC web 服务器目录遍历漏洞
37	中危	CVE-2016-9159	SIMATIC S7-300 和 S7-400 CPU 信息泄露漏洞
38	中危	CVE-2012-3031	Siemens SIMATIC WinCC 多个跨站脚本漏洞
39	中危	CVE-2012-3034	Siemens SIMATIC WinCC 信息泄露漏洞
40	中危	CVE-2017-14023	Siemens SIMATIC PCS 安全漏洞
41	中危	CVE-2017-2680	多款 Siemens 产品安全漏洞

② 工控协议漏洞

工业控制协议主要传输的各类协议的指令码，使用之初尚未采用 TCP/IP，在工业网络的以太网化过程中，协议也基于 TCP/IP 协议族做了重新设计，而这一过程，仅仅将工业控制指令作为 TCP/IP 的数据载荷在进行传输封装，缺乏安全性考量，导致存在大量的漏洞可被利用。

例如，在数据监控与采集中经常应用的 OPC Classic 协议（OPC DA，OPC HAD 和 OPC A&E）基于微软的 DCOM 协议，而 DCOM 协议是在网络安全问题被广泛认识之前设计的，极易受到攻击；并且，OPC 通讯采用不固定的端口号，导致目前几乎无法使用传统的安全设备来确保其安全性。

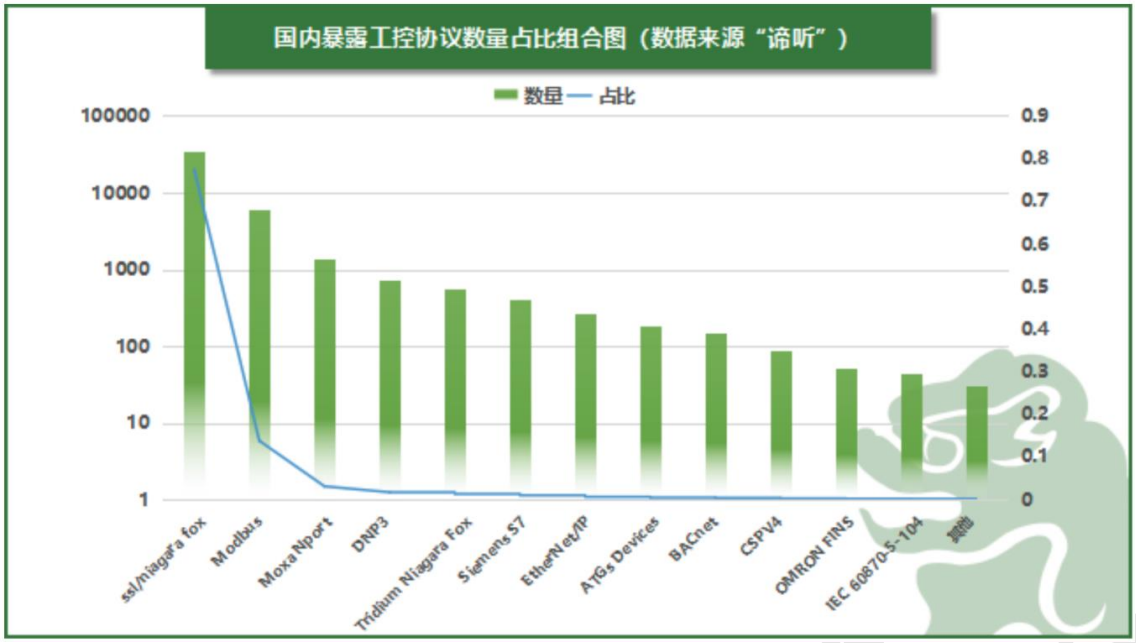

图 10-6 国内工控协议暴露数量和占比（2019）

③ 工业应用软件漏洞

由于工业应用软件多种多样，很难形成统一的防护规范以应对安全问题；另外当应用软件面向网络应用时，就必须开放其应用端口。因此常规的 IT 安全设备很难保障其安全性。

以常见的工业应用 GE IFIXv5.0 及三维力控为例，GE IFIX 公开披露漏洞 8 个，其中包含高危漏洞 1 个（CNVD-2013-14823，远程缓冲区溢出漏洞。成功利用后可使攻击者在受影响应用上下文中执行任意代码），三维力控存在公开披露的中危漏洞 2 个，可造成拒绝服务及任意代码利用的严重影响。

④ 操作系统漏洞

目前企业的工程师站/操作站/HMI 都是基于 Windows 平台的 Windows XP 及 Windows7 操作系统。由于传统上一般认为工业控制主机是在隔离的“安全环境”中，又要保证上位机上各类工控软件的稳定运行，通常现场工程师在系统开始运行后便不会对 Windows 平台安装任何补丁。不安装补丁系统就存在更多被攻击的可能，从而埋下安全隐患。目前工控系统经常出现的误中勒索病毒及“矿机病毒”的事件，利用的多数都是已经提供补丁的漏洞，其影响之大可见一斑。

钢铁集团一般都会管理多个工厂，信息化建设比较好的钢铁集团还会建设内部的行业云，对炼钢生产过程中各个环节的生产厂以云服务的方式提供 IT 基础实施比如虚机，对上下游合作伙伴提供专属的云服务以便于供应链协同。钢铁集团的网络结构一般如下：

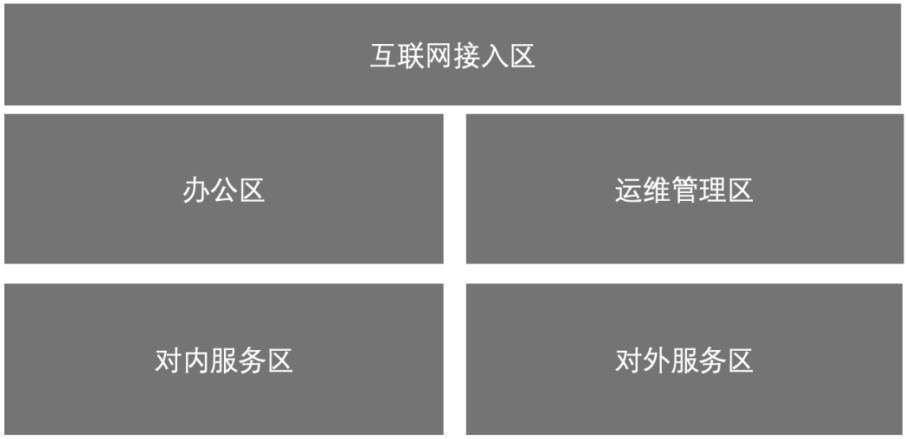

图 10-7 钢铁集团的网络结构

在集团级而言，防护对象通常包括集团对内和对外提供服务的云数据中心、集团办公网络、集团运维管理区以及互联网接入区。

钢铁行业的数据防护，包括从下而上的采集数据、从上而下的控制指令、上下游协同数据。

① 工业现场采集的数据

- 各类 PLC 系统中时序数据采集通过工业网关 ICG 连接进行协议转换，适用于特殊的协议，如：电力 104 协议，MODBUS 协议，再通过 ICG 提供的 OPC 传送到边缘服务器的实时数据库；
- 采用数据库抽取方式从 L2 数据库获取数据，传送到边缘服务器的关系数据库；
- I/O Server、PDA&FDAA 的数据通过 OPC 接入数据到实时数据库；
- 对于某些需要高速实时采集或难以通过配置实现数据采集的场合，编写 tcp/ip 通信接口电文程序实现；
- 特殊仪表的数据采集，需要编写 tcp/ip 通信接口电文程序；
- 图像、声音、视频以 ftp 文件方式传输。

② 从上而下的生产控制指令

生产控制指令随业务不同不同，比如钢铁行业经常会需要对轧机震动进行监测和控制，通过生产工艺参数调整、乳化液参数调整、设备间隙调整、轧制负荷分配调整等手段来消除轧机振动。

从防护角度，诸如生产控制指令需要确保不被阻断、窃取、篡改等入侵威胁。

③ 上下游协同数据

钢铁企业为了实现个性化制造，需要实现企业间数据实时的、高效的、安全的在线交互，建立以敏捷制造、虚拟制造、网络数据交换为基础的协同制造平台，使供应 链上下游的企业和合作伙伴共享客户、设计、生产经营信息。

- 重点客户实行全程周期管理，分段标准周期精细化，覆盖对订货、制造、发货、在途、仓储及加工配送全过程；
- 对供应链库存动态监控和多级预警响应，通过移动互联将供应链库存变化和多级预警及应对建议智能推送至相关方；
- 打破传统客户按月订交货模式，按客户需求进行拉动式订货管理；
- 通过提前了解客户连续生产计划及后续用钢需求，结合厂内生产组织优化限制，合理安排订单集批节奏；
- 在厂内按周交货精度保障、全程库存/周期管控的前提下，实现供应链全程低库存、短周期、高效率的滚动供货和快速响应，保证用户供料。

从防护角度，需要确保交互安全和交互数据的安全，包括数据隐私侵犯、数据被非法访问与使用、数据被窃取、被篡改、被破坏等。

（2） **防护措施**

从防护措施角度，构建事前防范、事中控制和事后审计的完整闭环防护。

① 事前防范：

- 加入工业审计，实时监测，及时告警；
- 加入工业防火墙，合理分区与访问隔离（防止病毒扩散），入侵防御（及时将网络病毒入侵阻止）；
- 加入工业卫士，防止工业主机中毒，防止非法终端接入工控网络；
- 加入工业蜜罐，诱捕入侵攻击；
- 加入工业漏扫或专用安全检查工具，实施合规检查与测评；
- 工业信息安全服务（工业信息安全制度与培训，定期查毒，定期报表，应急响应，漏洞挖掘、安全意识培训等）。

② 事中控制：

- 通过工业防火墙，调整分区，访问控制策略，阻止病毒进一步扩散；调整应用控制策略，阻止病毒从外面继续进入和木马（勒索病毒属于木马），蠕虫（通过网络

传播）等非法外联；

- 通过防恶意代码 U 盘查杀工业主机病毒。

③ 事后审计：

- 查看工业审计安全事件日志，分析病毒行为，来源；
- 查看工业卫士 sever 的安全事件日志，分析工业主机中毒情况，非法外联，非法接入等行为；
- 分析总结，输出后续整改与预防措施。

（3） **安全管理**

从安全运维管理角度，按照如下思路进行工业信息安全管理制度与规范建设：

① 工业信息安全领导小组

公司成立信息安全领导小组是信息安全的最高决策机构，下设分厂信息安全办公室，负责信息安全领导小组的日常事务。

信息安全领导小组负责对公司人员进行培训安全知识，保障公司信息安全，研究重大事件，落实方针政策和制定总体策略等。职责主要包括：

- 根据国家和行业有关信息安全的政策、法律和法规，制定公司信息安全总体策略规划、管理规范和技术标准；
- 公司人员进行定期自检；
- 公司人员进行信息安全培训，加强安全意识；
- 确定公司信息安全各有关部门工作职责，指导、监督信息安全工作。

② 日常管理制度与规范

主要包括工业现场设备检查和使用培训、工业安全设备检查与使用培训等。

③ 工业现场设备管理制度与规范

主要包括工业主机管理、工业网络管理、工业软件管理、工业设备管理、机房管理等制度与规范。

④ 工业安全设备管理规范

主要包括常见工控安全、网络安全、云安全、态势感知等安全设备与系统管理规范。

⑤ 安全事件应急响应流程与规范

主要包括预防预警、应急响应、后期处置、保障措施、监督管理等方面的流程与规范。

实施部署

（1） **实施框架**

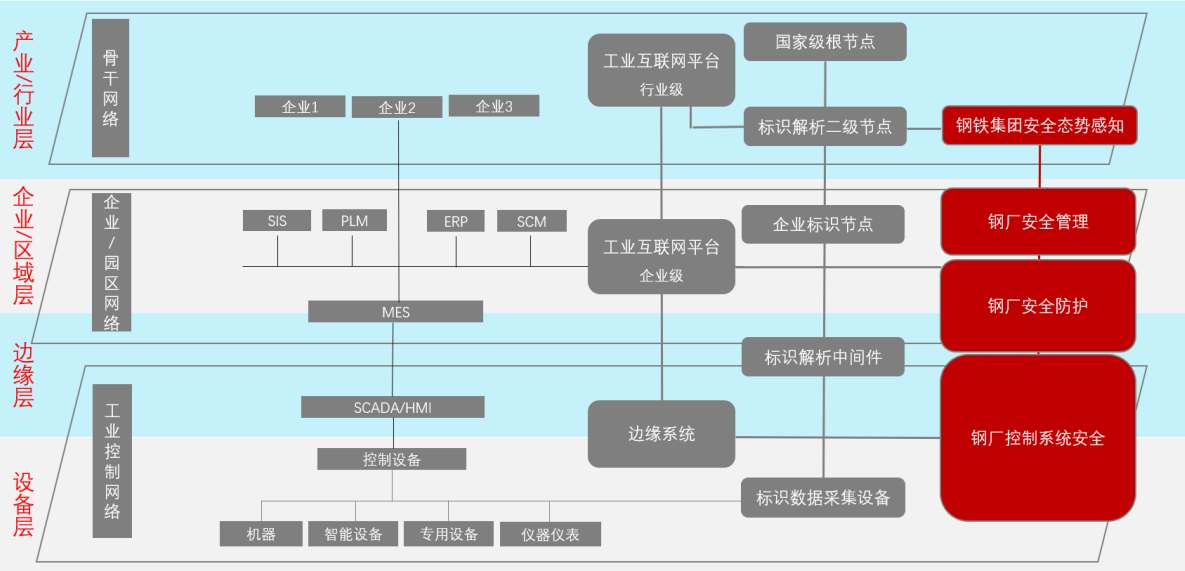

图 10-8 钢厂企业安全防护实施框架

整体实施上，与工业互联网安全实施架构保持一致，从钢厂工控系统安全、钢厂网络安全、钢厂安全管理和钢铁集团安全态势感知四个层次进行安全建设与实施。

（2） **实施要素与关键技术描述**

根据钢铁行业工业控制系统信息安全现状与特点，按照事前预防，事中防护，事后审计的方针，整体提高企业工业控制网络的安全保障能力。

① 安全管理

人是工业控制系统信息安全中最关键的因素。不管是技术的实施和维护，标准的制定与修订、流程的遵从、改善和管理，都离不开经过培训、有专业素质的人的参与。

- 企业对员工实行从业全周期的信息安全培训，使从业人员接受信息安全系统、机制化的教育培训，增强员工信息安全意识，减少误操作，并使之具备预防和发现隐患的能力；
- 培养一批了解生产实际情况，熟悉国内外信息安全标准和信息安全管理的专业人才，将工业控制系统信息安全工作专人化、专业化。除了人员培训和培养外，还需要从组织上保障：

- 明确领导责任，制定明确的、可操作的工控系统信息安全管理方针，完善流程、标准及各项制度，建立信息安全管理风险评估机制；
- 以硬件设备为核心建立工控信息安全台账，梳理设备接口，使得整个物理网络稳定、可控、可查；
- 工业控制系统服务商需签订安全服务保密协议，防范企业信息外泄；
- 督导员工之信息作业安全，防范不法及不当行为，并定期对工控系统进行巡检；
- 根据审计系统中收集的各类安全事件的相关数据材料，综合分析，制定工控安全事件的应急响应预案，并定期进行应急演练。

② 预防监测

- 搭建工业控制系统在线监测平台，对包括 MES、PCS、DCS、HMI、PLC、SCADA 等工控系统，以及服务器、数据库、工程师站、操作站、智能仪器仪表、嵌入式设备、视频监控设备、路由器、工业防火墙、工业网关等进行监控预警；
- 在工控系统网络交换机上部署流量审计设备，重点监测工控网络内部异常的流量、访问、操作以及非法入侵等行为；
- 在进行停机检修或系统上线、维护时进行漏洞扫描，并对漏洞修复及补丁进行评审后再进行修补；
- 对钢铁企业工控系统信息安全现状进行周期性风险评估，通过风险评估，确定风险管理计划、需要采取的控制措施以及企业信息安全管理的现状。检查内容包括系统配置检查、病毒检查、系统日志检查等，尤其是对一些开发放行服务协议、账号密码策略、加密方式等问题进行重点关注，并对存在的风险进行持续性改进。

③ 安全防护

- 边界防护，区域隔离，单向传输。在工控系统网络与企业网络边界部署工控防火墙类安全设备，阻止从工控系统外部发起的网络攻击行为。在各一二级区域间部署工业网关、网闸类安全设备，禁止未经授权通讯传入或传出工控系统从而实现对 IP、端口、访问、流量等内容的实时控制；
- 对服务器实行主机加固，对操作站、工程师站以及其他工控类计算机部署集杀毒、系统管理、应用程序管理、进程管控以及接口管理于一身的工控机安全管理系统，实现移动存储介质使用的管理、软件黑白名单管理，起到防病毒和恶意代码的作

用；

- 对关键主机设备、网络设备、控制组件等进行冗余配置，冷、热备机，异地灾备；
- 工业控制系统网络准入机制。防火墙遵循安全最大化的原则，所有与工业控制网络有接入的网络必须进行配置后方可接入，必须是其所隔离的网络之间的唯一信息通道，在进行远程访问时，需指定访问对象，对通讯流量进行审计，记录并保存访问日志，并定期进行备份、审计、追踪非授权访问行为；
- 纵深防御。严格遵循 ANSI/ISA-99 标准，采用 ANSI/ISA-99.02.01 和 IEC-63443 标准的区级防护，将网络划分为不同的安全区，在安全区之间按照一定规则安装防火墙或可信网关。这样即使在某一点发生网络安全事故，也能保证其他区域的正常安全稳定运行。

具体产品配置如下：

表 10-2 钢厂企业安全防护产品配置

组件	防护维度	防护产品	关键功能	关键技术
钢厂工控系统安全	设备安全	工业卫士/工业防火墙	设备身份鉴别与访问控制	
			固件安全增强	
			漏洞修复	
	控制安全		控制协议安全机制	身份认证
				基于角色访问控制
				加密
			控制软件安全加固	
		工业审计	指令安全审计	协议深度解析
				攻击异常检测
				无流量异常检测
				重要操作行为审计

				告警日志审计
		全流量威胁检测系统	故障保护	合理可预见误操作
				恶意攻击操作
				智能设备对环境的抵抗或切断
				异常扰动或中断的检测与处理
	网络安全	工业防火墙/工业网闸	通信与传输保护	
			边界隔离	
			接入认证授权	
钢厂安全防护系统	网络安全	网络防火墙/网络入侵防护/网络入侵检测/WAF/网闸	通信和传输保护	
			边界隔离	
			网络攻击防护	访问网络设备和标识解析节点做身份认证
				源地址限制
				访问失败审计
	应用安全	云安全防护类（微隔离、云监测与审计）	用户授权与管理	租户资产隔离
				租户数据资产共享保护
			虚拟化安全	不同层次隔离
				不同用户隔离
				虚拟化加固
		代码审计类	代码安全（源代码审计）	
	数据安全	边缘计算安全网关/云安全防护系统	数据防泄漏	工业设备与工业互联网平台之间网络传输数据防泄漏
				工业互联网平台中虚机之间交互数据
				虚机与存储之间交互数据防泄漏

				主机或虚机与网络设备交互数据的防泄漏
				维护通道加密
		云平台加密模块/独立加密软件	数据加密	分级加密存储数据
				按国家密码管理规定生成、使用和管理秘钥
				工业互联网平台不能解密客户数据
			数据备份	发生个人信息泄露，及时采取补救措施和告知用户并向主管部门报告
				签订数据备份策略服务协议
钢厂安全管理	保障企业内部安全管理有序进行	工业监管/厂站级工业态势感知系统/工业全流量威胁检测系统/工业蜜罐	安全信息采集	
			资产识别管理	通过流量探针针对企业内网扫描，发现并对资产集中管理
			安全审计	通过记录和分析历史操作事件及数据，发现能够改进系统性能和系统安全的地方，防止有意或无意的人为错误，防范和发现网络犯罪活动
			安全告警	及时发现资产中的安全威胁、实时掌握资产的安全态势
			安全处置跟踪	根据安全事件或安全资产溯源到相关责任人
			数据治理	对收集到的相关数据进行分析统计，为企业做出相关研判提供依据
	与省/行业级安全 平台实现有效协同			
钢铁	保障本省/行业平台的安	行业级安全态势感知系统	工业资产探测	
			流量分析	

集团安全态势感知	全运行		风险识别	
			态势分析	
			预警通报	
			应急处置	
	与国家级安全平台和企业安全综合管理平台实现对接		企业基础数据管理功能	
			策略/指令下发	
			情报库共享	
			信息推送	

应用成效

（1） 无需改造升级正在运行的工控系统组件，通过补偿式安全方案让工业控制系统中存在多种漏洞无法轻易被恶意利用；

（2） 钢铁企业网络区域划分合理，有效隔离，并实现安全网络通信；

① 钢厂级

- 实现生产控制网络与办公网络有效隔离与访问控制；
- 通过工业 NAT 实现对生产控制网络的隐藏，缩小被攻击面。

② 集团级

- 各钢厂之间网络隔离与访问控制；
- 各钢厂通过诸如 IPSec VPN 访问集团总部实现加密网络通信；
- 企业合作伙伴互访实现身份授权管理与审计。

（3） 钢铁企业云数据中心及云服务得到深度保护

一般上规模的钢铁企业在集团总部，甚至在工厂一级建设云数据中心，以面向内部和合作伙伴提供云服务。

云数据中心涉及云边界安全、云网络安全、云主机安全以及云监测与审计。

（4） 实现从工厂到集团到合作伙伴的全网监测与未知威胁防范

在应对各类针对已知问题和现有网络设计缺陷带来的风险的同时，还必须充分应对各类基于 0 day 漏洞的 APT 攻击。

工业安全领域存在极为严重的信息的不对称，工控系统中的问题往往难以被察觉，且普遍存在攻击事件未被披露的情况，导致大量的安全防护知识未能被利用。

这一背景，也导致了在工业环境中有更多可被轻易利用的 0 day 漏洞，未知威胁攻击在工业互联网越来越多打通工业工业控制系统与互联网络边界的未来，将成为企业工控系统安全防护的重点课题之一，而企业目前针对工控系统未知威胁的防护还是空白。

（5） 贴合钢铁行业的工业现场管理制度与规范

追求可用性而不注重安全性，是目前工业控制系统中存在的普遍现象，缺乏完整有效的安全策略与管理流程也给工业控制系统信息安全带来了一定的威胁。例如在多个网络事件中，事由都源于对多个网络端口进入点疏于防护，包括 USB 钥匙、维修连接、笔记本电脑等。

人是工业控制系统信息安全中最关键的因素。不管是技术的实施和维护，标准的制定与修订、流程的遵从、改善和管理，都离不开经过培训、有专业素质的人的参与。因此通过安全建设，对员工实行从业全周期的信息安全培训，培养一批了解生产实际情况，熟悉国内外信息安全标准和信息安全管理的专业人才，将工业控制系统信息安全工作专人化、专业化。

10.2 能源行业让数字化采油更安全

背景与目标

对于石油化工企业来说，油气是一种同质产品，产业竞争的核心是成本竞争。物联网技术催生出的生产环节“无人化”，大数据、云计算、人工智能带来的数据挖掘、利用与辅助决策，无疑都会带来生产成本的大幅降低，勘探成功率的上升与安全管理效能提升。根据 IEA 的预测：数字技术的大规模应用，能够让油气生产成本减少 10%~20%，让全球油气技术可采储量提高 5%。

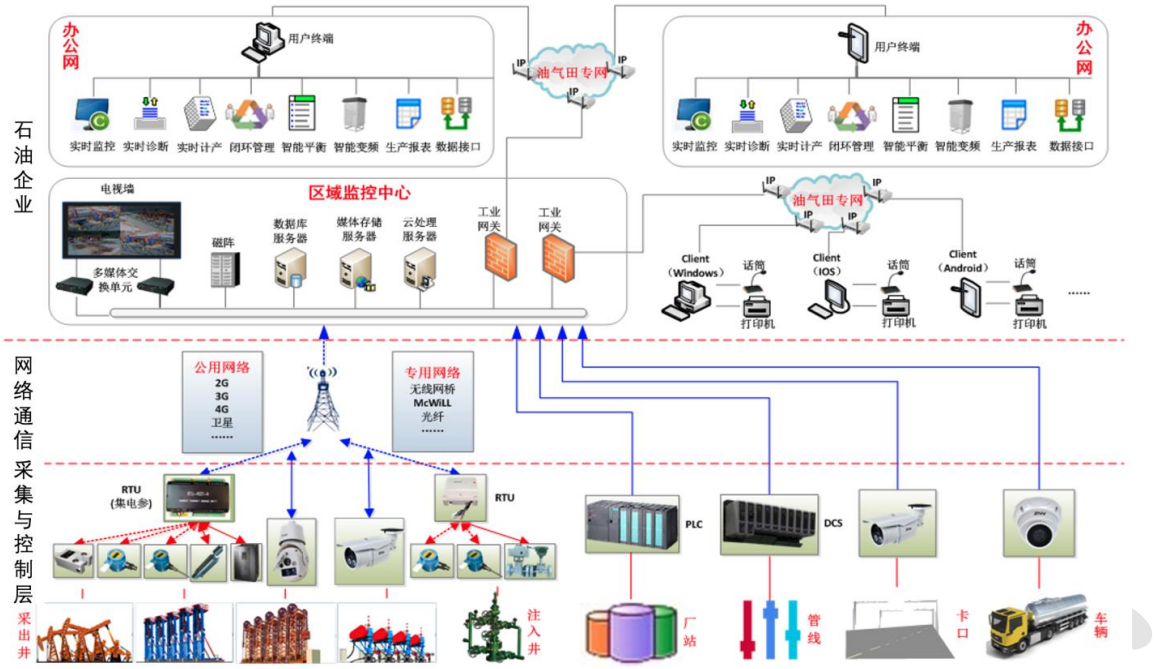

图 10-9 数字化采油场景

在油田中，数字化采油技术是以井、站、管线等基本生产单元为对象，融合自动化数据采集、集中数据共享、自动生产过程监控、自动风险识别的复杂系统工程。

第一，在井场增压站和抽油机中的生产设备上进行自动化仪表的安装，如载荷位移传感器、压力传感器等，他们带有数据远传功能，能够实现对各种生产数据的采集，并以有线或无线网络送到增压站中。

第二，在联合站和增压站中进行生产监控系统的安装，以处理所采集的数据，自动报警实现的同时，能够有效监控集输站点和采油井场的生产流程。

第三，运用一定存储策略，将采集的生产数据存储到共享数据库（实时数据库和关系数据库）。

第四，全部井场和增压站中引入网络生产管理平台，来实现对原油厂油储和采油生产的精细管理与集中管理。

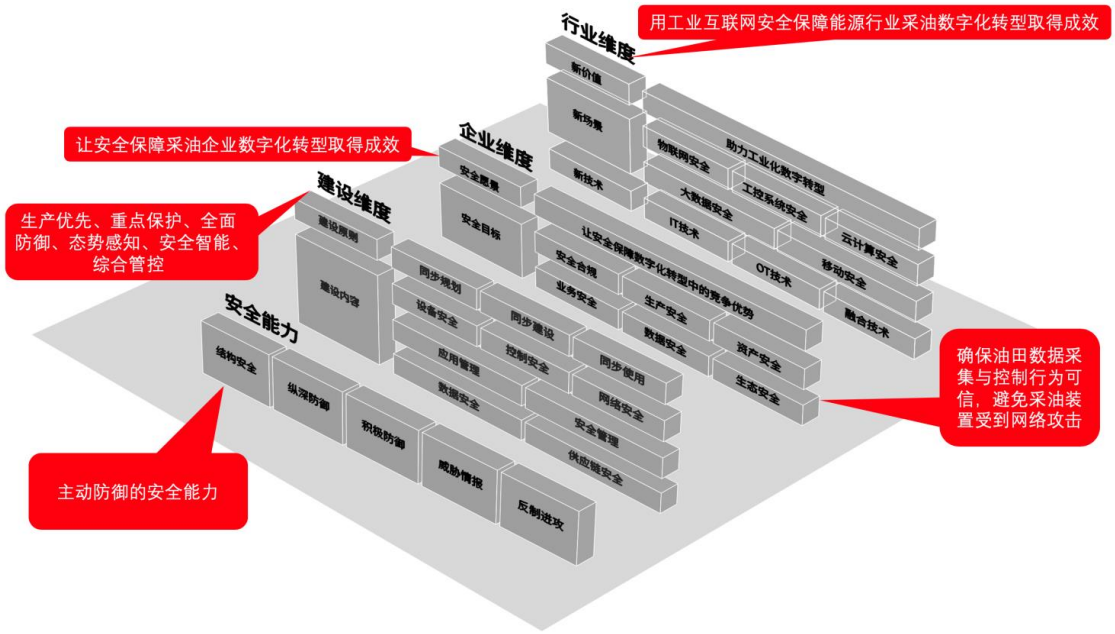

图 10-10 能源行业工业互联网方案

能源行业工业互联网方案目标：

（1） 全局安全目标

数字化采油成为当前精益采油，提质增效的必然选择。数字化采油主要涉及到采油现场生产数据采集、传输、存储、分析与决策等环节，数据与控制安全成为采油企业数字化转型是否成功的关键因素之一。

数字化采油大量采用物联网技术，同时会采用工控、云计算、大数据等技术，因此采用诸如物联网安全、工控安全、云计算安全、大数据安全等工业互联网安全技术和手段来确保采油数字化转型免受网络入侵攻击，从而取得数字化转型成功，从能源采油行业的高度来看，是必然的选择。

（2） 企业安全目标

油田使用 RTU 采集采油井设备的工艺状态，部分 RTU 还有控制设备启停的功能。RTU 的数据经过 4G/5G 网络设备传输到采油控制中心，随着针对关键基础设施的攻击事件增加，需要一款安全设备来保证油田数据采集与控制行为可信，避免采油装置受到网络攻击。

此安全设备至少要满足如下基本要求：

① 适应油田采油井的环境温度，即工作温度在-40~75℃；

② 外形尺寸尽可能小，安装方式为 DIN35mm 导轨安装；

③ 电源功耗要低，采用冗电设计，电源输入为 24VDC；

④ 接口提供 RS-232、RS485、RJ45 接口；

⑤ 协议支持：ModBus-RTU、ModBus-TCP、自定义串口协议；

⑥ 数据加密 VPN 功能；

⑦ 安全防护功能。

（3） 建设安全目标

在建设维度，采油企业要遵循“三同步”建设原则，安全防护措施不能影响生产正常进行为优先原则，对工控网络、工控设备、云平台实施重点保护；并采用全流量分析与监测技术，既能够及时检测出勒索、挖矿、蠕虫等高级威胁，也要能够高效检测出诸如 0 day 利用、高级逃逸等未知入侵威胁，实现全面防御；借助数据采集、分析技术，实现安全状态的全面了解与可视，安全风险与趋势的科学预测与预警，并能够综合各种因素，自动做出安全响应处置决策；建立统一的安全运维管理中心，实时监测上下游供应链交互信息、从下向上的生产数据以及从上向下的生产控制指令，及时发现入侵攻击并采取相应处置措施，实现统一安全运维管控。

（4） 安全能力目标

在能力维度，采油企业通过安全建设，具备生产控制系统安全可控、安全运维可查可审计、个性化制造的业务系统与平台安全可信、符合等保 2.0 技术要求、高级与未知威胁及时发现与防范、攻击威胁事件证据留存可溯、全企业全供应链的安全态势可见、外部威胁情报能够为我所用，内部威胁事件经过处理后可对外共享等八大安全能力，核心能力是主动检测、主动预警、主动保护、主动响应的主动防御能力。

功能架构

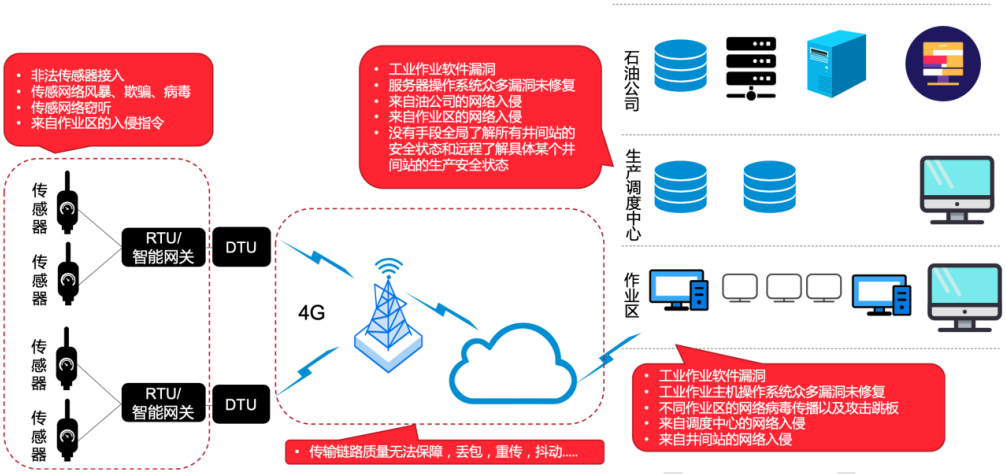

图 10-11 能源企业安全防护功能架构视图

表 10-3 能源企业安全防护功能架构分析

防护对象	安全风险	防护措施	安全管理
传感网络	·非法传感器接入 ·传感网络风暴、欺骗、病毒 ·传感网络窃听 ·来自作业区的入侵指令	·设备接入认证 ·抗 DDoS 攻击 ·通信加密 ·指令审计	1）安全目标 ·确保采油装置不被网络入侵破坏； ·生产数据不被泄漏； ·生产控制指令不被阻断或篡改； 2）风险评估 ·实时监测，及时预警，远程运维 3）安全策略 ·纵深防御：纵向分层、横向分区 ·高度融合：将安全思想和安全措施有机融合到工业设备中，包括物理层面和操作系统层面 ·生产优先：所有安全措施或设备都具有硬件 bypass 功能，一旦
数据远程传输	·传输链路质量无法保障，丢包，重传，抖动 ·数据被窃听、篡改、阻断等	·网络通信加密	
作业区	·工业作业软件漏洞 ·工业作业主机操作系统众多漏洞未修复 ·不同作业区的网络病毒传播以及攻击跳板 ·来自调度中心的网络入侵 ·来自井间站的网络入侵	·软件白名单防护 ·网络区域隔离 ·网络入侵防护/检测	
生产调度中心	·工业作业软件漏洞 ·服务器操作系统众多漏洞未修复	·软件白名单防护 ·网络区域隔离	

	· 来自油公司的网络入侵 · 来自作业区的网络入侵 · 没有手段全局了解所有井间站的安全状态和远程了解具体某个井间站的生产安全状态	· 网络入侵防护/检测 · 全局安全态势感知	出现故障，立即将安全措施或安全设备旁路，不影响正常生产作业

实施部署

（1） 整体实施框架方案理念与原则如下：

① 纵深防御：纵向分层、横向分区；

② 高度融合：将安全思想和安全措施有机融合到工业设备中，包括物理层面和操作系统层面；

③ Safety 优先：所有安全措施或设备都具有硬件 bypass 功能，一旦出现故障，立即将安全措施或安全设备旁路，不影响正常生产作业。

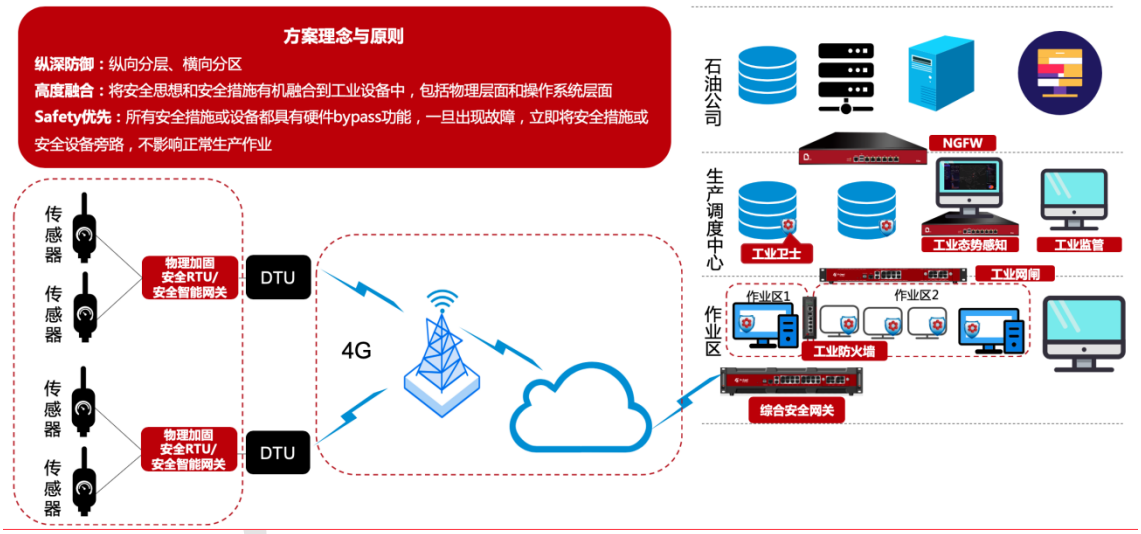

图 10-12 能源企业安全防护方案理念与原则

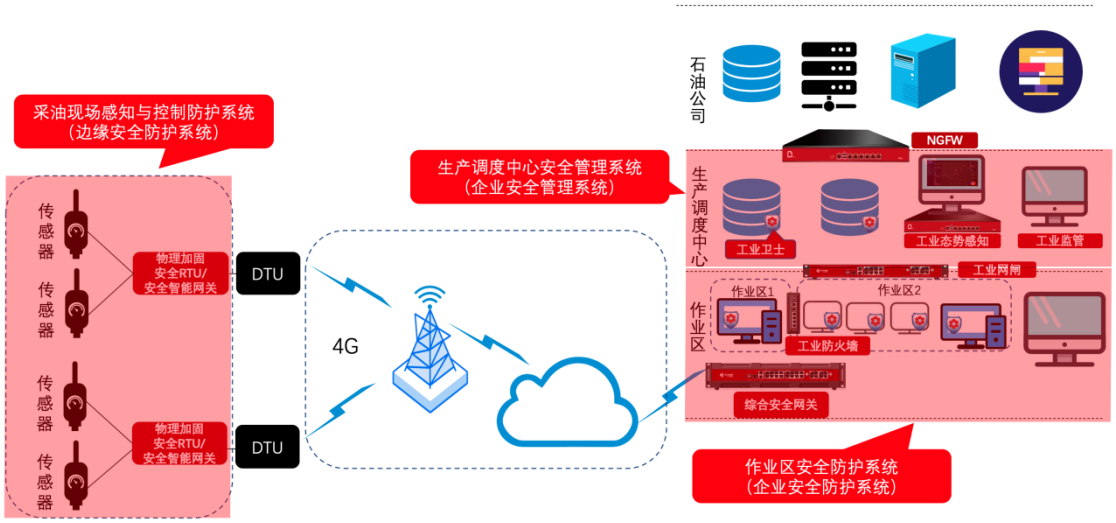

图 10-13 能源企业安全防护实施框架

（2） 构建边缘层工控安全防护系统

构建采油现场感知与控制防护系统的方式有两种，一种改造加固 RTU，一种是在 RTU 和 DTU 之间接入独立的智能安全网关设备。

改造加固 RTU 优点是采集与安全防护一体化设计，实现采集、计数、控制、存储、报警、传感器接入认证、传感网络安全防护等综合功能。与在 RTU 和 DTU 之间接入独立的智能安全网关设备相比，性价比高，有效节约项目投资。

安全加固 RTU 或智能安全网关的基本要求：

① 安全防护模块可以在故障或紧急情况下被旁路，以不影响正常生产；

② 安全防护支持标准 Modbus RTU 协议，可针对协议实施白名单和黑名单防护措施，不需再投入人力物力单独开发安全防护功能，加快项目开发进度；

③ 存储容量大，可在本机循环存储监测数据和安全事件日志，掉电不丢失；

④ 工业级硬件设计：-30~+75℃宽温设计，宽电源输入（DC5-35V），耐高低温，耐风沙尘，耐强电磁干扰。适用于各种恶劣的工业现场。采用完备的系统保护机制和防掉线机制，保证数据终端永远在线；

⑤ 集中分布式管理，维护方便；

⑥ 不仅数据采集支持远程配置（短信和数据），管理及软件升级，而且安全防护模块支持远程安全策略配置和设备调试，同时在生产调度中心提供工业监管系统，方便设备

集中管理和安全策略集中制定与分发。

（3） **构建企业层安全防护系统**

作业区的安全防护系统构建类似工控系统的 L1～L2 层，重点是区域隔离、上位机病毒防护。

为了防护采集数据和控制指令在互联网传输过程的安全，需要采油现场侧与作业区之间的通信加密，通常采用 IPSec VPN 方式，因此在作业区的边界需要部署 IPSec VPN 网关设备。

（4） **构建企业层综合防护系统**

① 在生产调度中心部署工业监管，至少需要具备如下功能：

- 资产拓扑画像：可以让终端主动注册上报，实时监控资产的状态，如果脱机或遇到有安全事件则告警；
- 可以对资产进行分组管理；
- 可以针对某个具体的或某组终端设备进行：远程固件升级、重启、安全策略制定与下发；
- 来自终端的安全事件和设备状态日志存储和展示；
- 可调用 RTU 的 API 将 RTU 的维护界面集成进来。

② 在生产调度中心部署厂站级态势感知系统，其主要功能如下：

- 在地图上实时展示所有 RTU 的安全状态和事件；
- 可查看具体某个 RTU 的安全事件；
- 提供调度中心管辖的所有井间站的整体安全态势；
- 可在应急响应中心向 RTU 下发紧急安全措施。

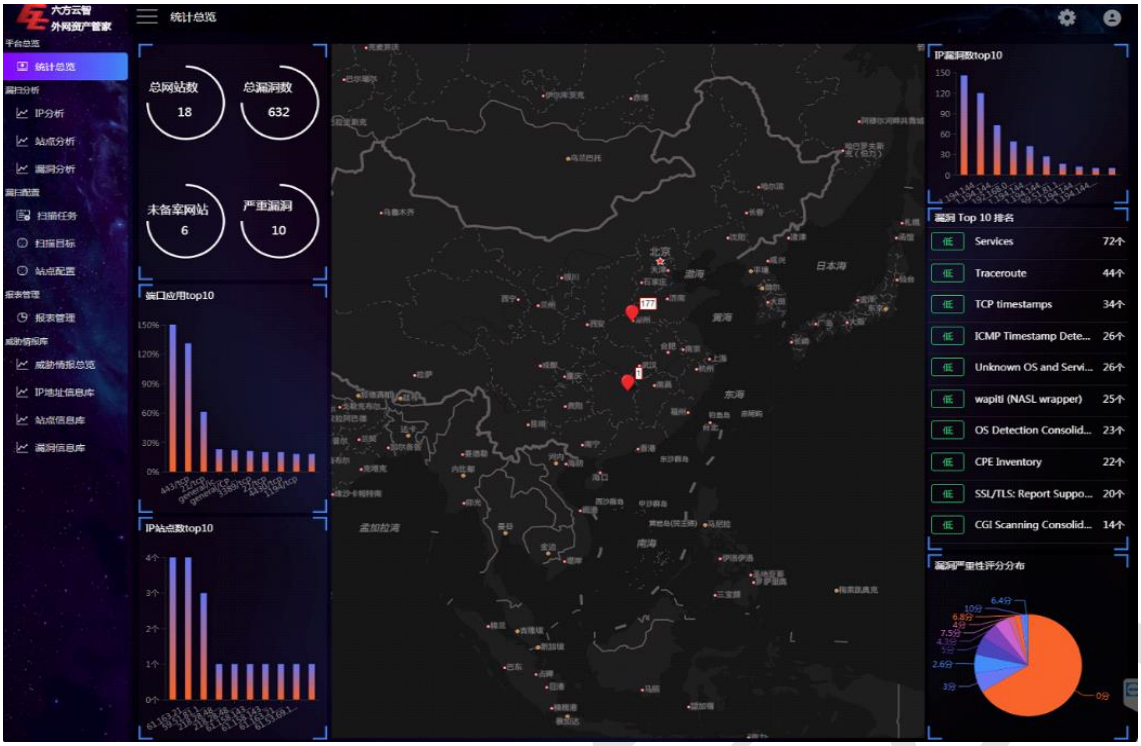

图 10-14 企业综合防护系统

应用成效

（1） 实施简单，后期维护成本大大降低；

（2） 将安全措施有机集成到 RTU 或智能网关中，安装实施只需要一台设备即可，同时针对户外恶劣环境在机箱、主板、器件等方面进行物理加固，大大降低了物理损坏的概率；

（3） 提供安全态势监测，使得决策和应急响应措施更及时与科学；

（4） 从 IT 和 OT 安全视角，以地理位置的展示方式来监测各个井间站的安全状态和趋势；

（5） 有效防范已知威胁和未知威胁；

（6） 有效防范传感网络自身安全威胁和来自传感网络的网络入侵；

（7） 有效防范来自互联网的网络入侵；

（8） 有效提升跨广域网传输的链路质量，提高作业操作和调度中心监控数据的实时性；

（9） 有效杜绝通过外设介质感染和传播恶意代码入侵。

第十一章 工业互联网安全发展展望

工业互联网显示出巨大的希望，可以大大提高设备在各种应用中的能力，包括工厂自动化、医疗系统和各种各样的其他系统。通过连接设备以实现彼此和云之间的通信，它打开了使设备 “智能化”的可能性，潜在地提供前所未有的能力。

工业互联网大量采用诸如云计算、边缘计算、大数据、人工智能、区块链、5G 等新技术，使新一代设备比前代设备更智能、效率更高。与之同时，工业互联网安全风险也随之增加和变得越来越复杂。

新技术采用是一把双刃剑，新技术能让工业互联网建设更高效和更有价值，但同时新技术会引入新的安全风险，包括新技术本身容易被攻击破坏和被恶意利用。比如网络黑客采用人工智能技术发起恶意攻击已经很广泛。

工业互联网安全也可以借用工业互联网所采用的技术来更好的防护工业互联网系统。比如安全监测可以采用边缘计算来很好的解决数据隐私、数据安全问题。比如可以采用软件定义网络（SDN）技术可以高效灵活的实现网络和数据隔离，从而提高工业互联网网络的安全性。它们还允许动态更改 IP 地址，使攻击者更难了解网络。比如物理不可克隆功能（Physical Uncloclable Function, PUF）等技术允许端点设备在不存储密钥的情况下表现为拥有私钥，从而降低与攻击硬件以检索存储密钥相关的安全风险。比如区块链技术可以很好的解决工业互联网数据共享安全、安全操作日志被篡改等安全问题。

工业互联网虽然不能说像 19 世纪的工业革命那样具有变革性，但它必将加速工业数字化、网络化、智能化的进程。在世界各国都在加速建设工业互联网的同时，我们也必须高度重视并强烈建议工业互联网安全与网络、平台同步规划、同步建设和同步运行，以确保技术进步最终不会使我们付出昂贵的代价。

第十二章 关于六方云

六方云是一家在人工智能、云计算、大数据等新技术被广泛应用的“新时代”背景下应运而生的技术领先的“新安全”公司。

“新时代”要求“新安全”公司能够适应时代发展、能够解决好万物互联场景下的信息安全问题；能够采用最先进技术如人工智能使得安全能力更智能，不仅能够防范已知威胁，而且要能够精准防范各种未知威胁和变种威胁，从而推动网络安全行业的安全理念由被动防御向主动防御转变。

六方云借助人工智能技术仿生人体免疫机制，针对工业互联网和物联网，创造性地提出了“AI 基因、威胁免疫”的“新时代、新安全”安全理念，将人工智能技术应用于全系列产品，构建安全威胁免疫系统。在国家新基建战略下，致力于提供关键信息基础设施保护、工业互联网安全的产品和解决方案。

六方云董事长任增强表示：工业互联网安全、云安全、人工智能安全是“新安全”，是未来，而未来世界发展的主要推动力来自于技术。六方云坚持以吸引和团结有共同价值观的人才为核心，持续不断地耕耘攻坚，实现“以技术保障技术”，用最先进的技术解决国家与行业在高速发展中的安全问题，保障国家工业互联网战略、国家网络空间安全战略以及新基建安全的实现，让万物安全互联。

12.1 六方云新一代工业互联网安全体系

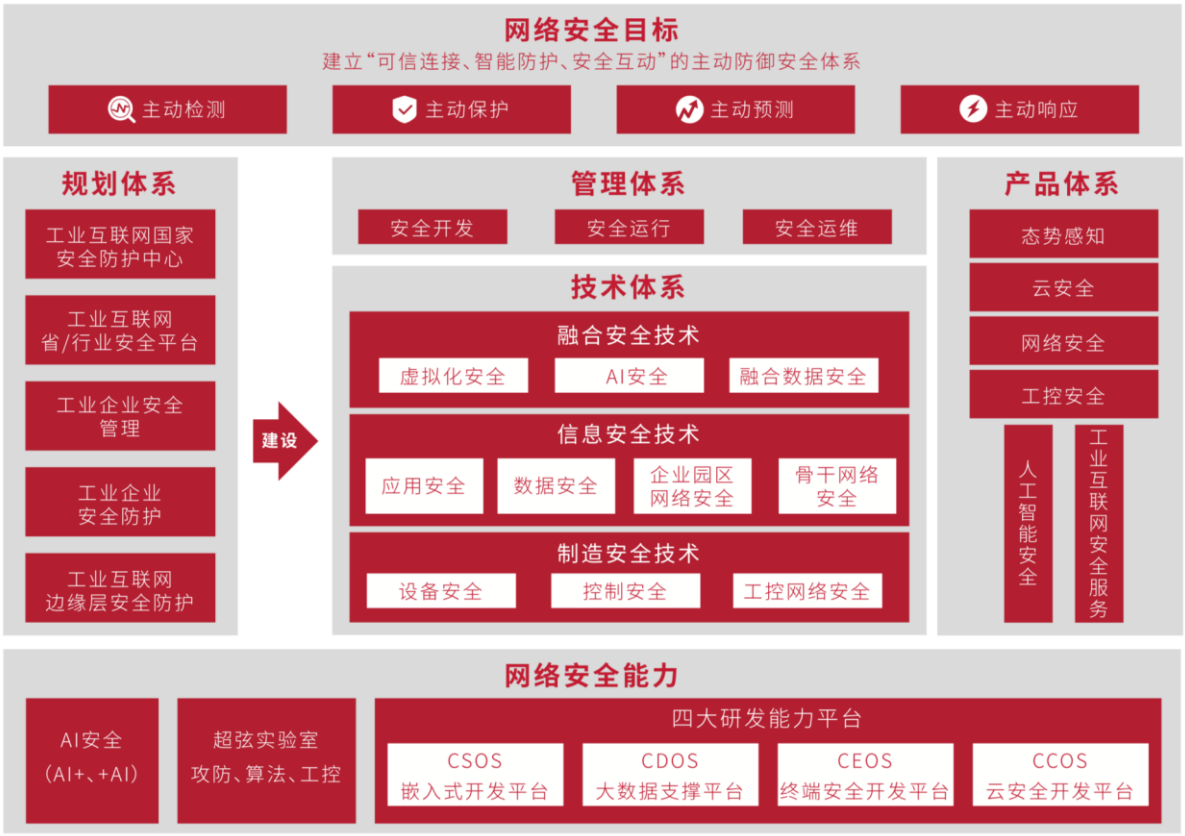

图 12-1 六方云“新一代工业互联网安全体系”

1 个安全理念：AI 基因，威胁免疫。

1 个总体目标：建立“可信连接、智能防护、安全互动”的主动防御安全体系。

4 层安全规划体系：设备层、边缘层、企业层、产业层。

5+1 产品体系：工控安全、网络安全、云安全、安全态势感知、AI 安全、安全服务。

3 大技术体系：OT 安全技术、IT 安全技术、融合安全技术。

3 大管理体系：安全开发、安全运维、安全运行。

3 大网络安全能力：AI 安全、超弦实验室、4 大研发能力平台。

12.2 六方云 5+1 工业互联网安全产品体系

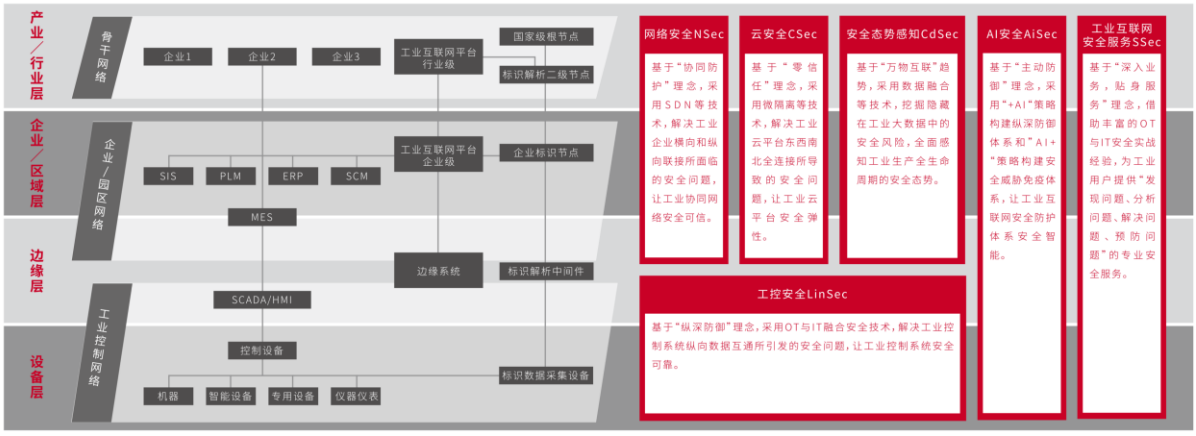

图 12-2 六方云产品体系

六方云工业互联网安全解决方案以“中国制造 2025”为主旨，提供 5+1 产品线：工控安全 LinSec、网络安全 NSec、云安全 CSec、安全态势感知 CdSec、AI 安全 AiSec 及工业互联网安全服务 SSec。为工业业务应用提供具有更多主动性、适应性和智能化的信息安全解决方案。

AI 安全 AiSec 产品线基于“主动防御”理念，采用“+AI”策略构建纵深防御体系和“AI+”策略构建安全威胁免疫体系，让工业互联网安全防护体系安全智能。

工控安全 LinSec 产品线基于“纵深防御”理念，采用 OT 与 IT 融合安全技术，解决工业控制系统纵向数据互通所引发的安全问题，让工业控制系统安全可靠。

网络安全 NSec 产品线基于“协同防护”理念，采用 SDN 等技术，解决工业企业横向和纵向联接所面临的安全问题，让工业互联网安全可信。

云安全 CSec 产品线基于“零信任”理念，采用微隔离等技术，解决工业云平台东西南北全连接所导致的安全问题，让工业云平台安全弹性。

安全态势感知 CdSec 产品线基于“万物互联”趋势，采用数据融合等技术，挖掘隐藏在工业大数据中的安全风险，全面感知工业生产全生命周期的安全态势。

工业互联网安全服务 SSec 基于“深入业务，贴身服务”理念，借助丰富的 OT 与 IT 安全实战经验，为工业用户提供“发现问题、分析问题、解决问题、预防问题”的专业安全服务。

参考资料

[1] 中国工业互联网产业联盟，《工业互联网安全框架》，2018 年 11 月

[2] 中国工业互联网产业联盟，《工业互联网体系架构（版本 2.0）》，2020 年 4 月

[3] 中国工业互联网产业联盟，《中国工业互联网安全态势报告（2018 年）》，2019 年 3 月

[4] 东北大学“谛听”网络安全团队，《2019 年工业控制网络安全态势白皮书》，2020 年 4 月，https://mp.weixin.qq.com/s/phcpafQnNBnyQ1OFOcSriQ

[5] 美国工业互联网产业联盟，《Industrial Internet of Things Volume G4: Security Framework》，2016 年 9 月

[6] 美国工业互联网产业联盟，《The Industrial Internet of Things Volume G1: Reference Architecture》，2017 年 1 月

[7] 中国工业互联网产业联盟，工业互联网垂直行业应用报告（2019 版），2019 年 2 月

6cloud 六方云

微信公众号

电话：400-6060-270

邮箱：mkt@6cloudtech.com

地址：北京市海淀区信息路 12 号中关村发展大厦 C 座 201

官网：www.6cloudtech.com