第 4 章 工业互联网安全体系

4.1 工业信息安全概述

4.1.1 工业信息安全的再认识

工业是国民经济的主体和建设现代化经济体系的主要着力点，工业竞争力是国家竞争力的重要体现。随着德国“工业 4.0”、美国“再工业化、先进制造”和我国“制造强国、网络强国”等国家战略的推出，以及云计算、大数据、物联网等新一代信息技术的大规模应用，工业体系由自动化向数字化、网络化和智能化方向发展。新一轮产业变革为经济转型带来新机遇的同时，也加速了网络安全风险向工业领域的全面渗透，工业信息安全问题日益凸显。

从内容来看，工业信息安全泛指工业生产运行过程中的信息安全，涉及工业领域各个环节，其核心任务就是要确保工业自动化、信息化、网络化和智能化等基础设施的安全。

从保障对象上看，工业信息安全要保障工业系统和设备（如工业控制系统）、工业互联网平台（包括承载平台运行的工业云以及应用服务）、工业网络基础设施（包括基础电信网络、解析网络和其他网络）及工业数据等的安全。

因此，工业信息安全不仅涉及传统计算机网络和信息系统安全，还涉及工业软硬件设备、控制系统和工业协议等的安全。

从工业信息安全的发展路径来看，早期的工业领域处于自动化阶段，生产环境相对封闭，工业信息安全作为网络安全的细分应用方向，主要集中在工业企业信息管理层的安全。近年来，工业企业逐渐进入数字化转型时期，工业控制系统（以下简称“工控系统”）和生产设备的网络安全风险激增，工业信息安全的重点在于工控安全。当前，两化融合进程加速了由数字化向网络化过渡，互联网快速渗透到工业领域的各个环节，工业实体逐步趋向泛在互联，工业互联网安全逐渐成为工业信息安全的焦点和核心。工业信息安全从面向企业端的

传统信息安全、工控安全逐步延伸至工控网络安全、工业主机安全、工业设备安全、工业应用安全、工业漏洞扫描以及工业漏洞挖掘等领域。

4.1.2 工业信息安全产业的界定

习近平总书记在2018年4月召开的全国网络安全和信息化工作会议上明确指出：“加强网络安全时间应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。”在工业互联网快速发展的大背景下，新一代信息技术在工业生产领域广泛渗透和深度融合，不断升级的安全挑战对新时期的工业信息安全产业发展提出了更高、更新的要求。

工业信息安全产业发展的初期阶段以工控安全为核心，以纵深防御的技术理念为基础，涌现出大量围绕工控系统的“外建”安全防护产品和解决方案。随着工业互联网的加速推进，传统工业现场相对封闭可信的制造环境和强调高可靠性的格局逐渐被打破，工控系统、工业互联网智能设备、工业互联网平台等自身的安全问题不容小觑，内嵌信息安全功能的产品和服务市场需求激增。因此，工业信息安全产业发展应以提升企业工业信息安全综合防护水平为目标，统筹考虑内嵌安全和外建安全的市场需求。市场需求和时间的对应关系如图4-1所示。

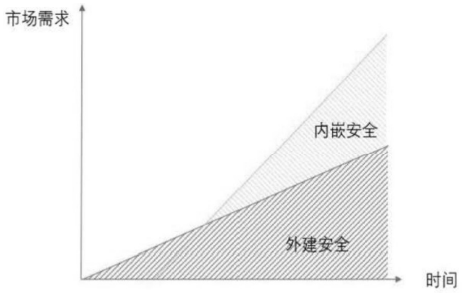

图4-1 市场需求和时间的对应关系

当前，国内外缺乏对工业信息安全产业的公认界定，产业相关数据的统计口径也尚未建立。结合工业信息安全的内涵，工业信息安全产业可以定义为从事工业生产、运行、管理过程中的安全技术研究开发、产品生产经营和提供相关服务的经济活动。

4.2 工业互联网安全概述

4.2.1 工业互联网安全内涵与范畴

当前，以移动互联网、云计算、大数据、物联网和人工智能等为代表的新一代信息技术与制造技术加速融合，推动着制造业向数字化、网络化、智能化和服务化方向发展，成为推动经济转型升级、新旧发展动能接续转换的强劲引擎。

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、网络化和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部分。

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、工业云安全和工业电子商务安全等内容。

根据普渡参考模型，工业企业信息系统架构可以分为企业网络层、信息管理层、生产管理层、过程监控层、现场控制层和现场仪表/设备层，如图 4-2 所示。从安全防御技术成熟度来看，工业领域各行业在信息管理层的信息安全防护发展较早，技术和产品都相对成熟。

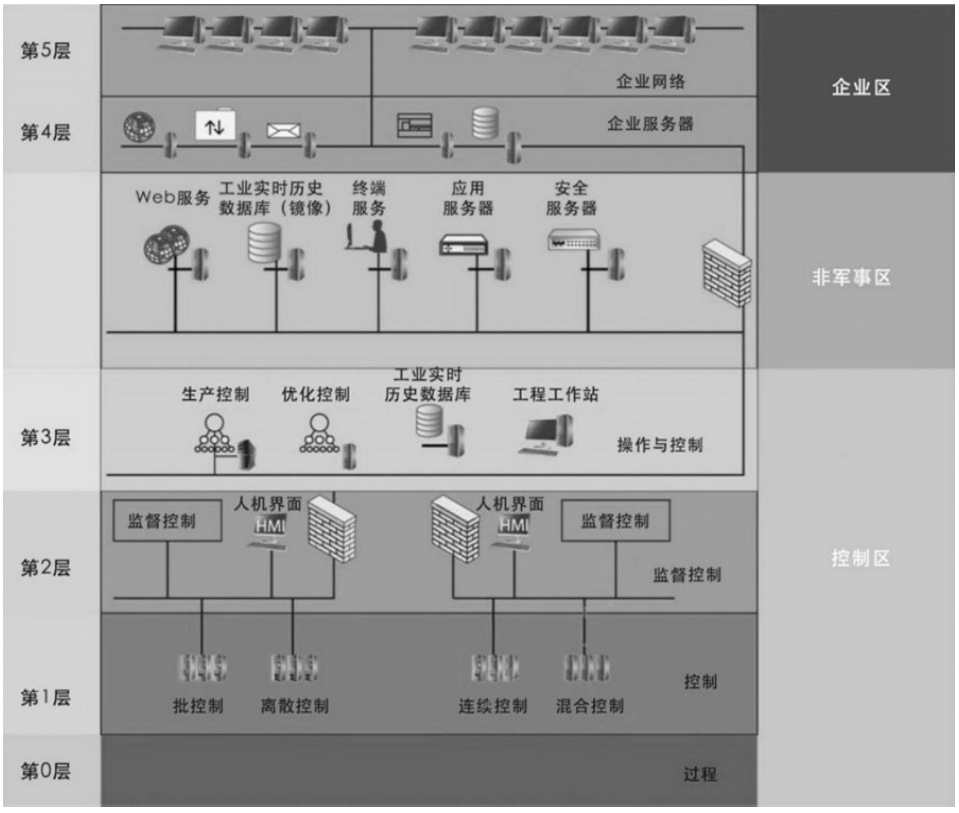

图 4-2　工业企业普渡参考模型（Purdue Model）

工控安全或以资产为中心的操作技术（Operational Technology，OT）安全主要指生产管理层、工业控制层及现场设备层所涉及的信息安全防护。Gartner

在 2017 年的《OT 安全市场指南》中，指出工业信息安全市场重点关注的操作运行系统包括数据采集与监控系统（SCADA）、过程控制网络（PCN）、离散控制系统（DCS）、制造执行系统（MES）、远程信息处理、机器人、设施管理、建筑自动化系统（BAS）以及交通运输管理系统等。

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。

4.2.2 工业互联网安全产业结构分类

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，可以将工业信息安全产业结构分为产品和服务两大类。具体的工业互联网安全产业结构如图 4-3 所示。

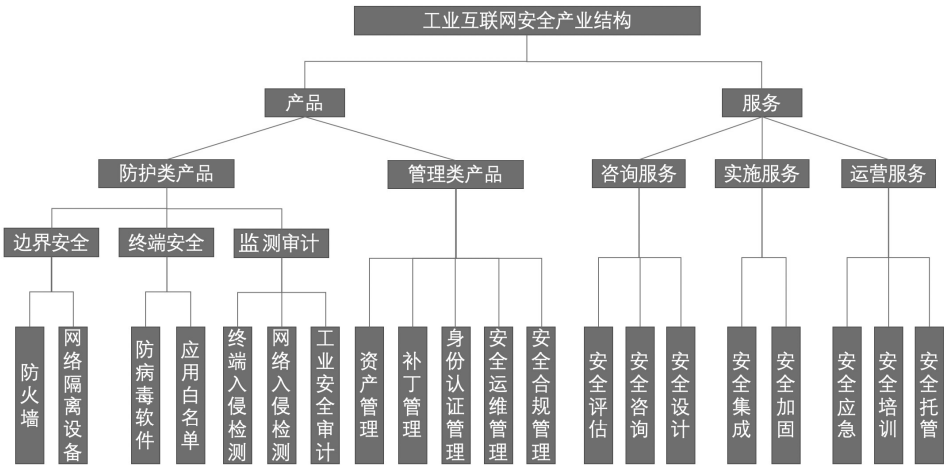

图 4-3 工业互联网安全产业结构

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防护类产品与管理类产品两类。