# 工业互联网安全体系理论与方法

闫怀志 著

科学出版社

国家重点研发计划资助出版著作

# 工业互联网安全体系理论与方法

闫怀志 著

科学出版社

北京

## 内 容 简 介

本书以体系思想为指导，系统研究并深入论述了工业互联网及工控网络的安全体系，涵盖了工业设备与控制、网络、应用及数据等安全领域，特别强调工业、互联与安全的融合，以及理论思想和技术方法的融合。全书主要内容包括：工业互联网平台形态、架构与安全框架；IT、OT 与 CT 安全融合与安全体系；信息安全与功能安全的融合；工业芯片、嵌入式、SCADA、DCS、PLC 等安全；安全域与隔离、访问控制、工业防火墙及网络传输安全；工业应用软件、工业 APP 与工业微服务架构安全；工业大数据安全等。作者长期对工业网络安全进行深入思考并在工控安全领域持续实践迭代，本书是对该过程成果的高度凝练与系统总结，同时还参考了国内外最新理论和技术进展。

本书可作为工业互联网、网络空间安全、自动化、智能制造、工控系统、信息对抗、安全工程、物联网、计算机及软件等领域的科研人员及工程技术人员的参考书，也可作为高等院校相关专业高年级本科生和研究生的学习用书。

**图书在版编目（CIP）数据**

工业互联网安全体系理论与方法 / 闫怀志著. —北京：科学出版社，2019.5

ISBN 978-7-03-060488-0

Ⅰ. ①工… Ⅱ. ①闫… Ⅲ. ①互联网络－应用－工业发展－网络安全－研究 Ⅳ. ①F403-39②TP393.08

中国版本图书馆 CIP 数据核字(2018)第 019469 号

责任编辑：王 哲 / 责任校对：张凤琴

责任印制：吴兆东 / 封面设计：迷底书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 5 月第 一 版 开本：720×1000 1/16

2019 年 5 月第一次印刷 印张：15 3/4

字数：310 000

**定价：108.00 元**

（如有印装质量问题，我社负责调换）

# 前　言

工业互联网是在工业产业革命与互联网创新发展持续交汇的大背景下，工业体系与互联网体系深度融合的产物，是完成人、机与物等工业生产经营各要素全面互联的新型工业基础设施，不仅具有典型的工业特征，更是网络空间的重要信息系统形态和新一轮工业革命的关键支撑。随着“中国制造 2025”的推进，中国也适时成立了工业互联网产业联盟，在框架、标准、测试、安全等方面开展了有效工作。毫无疑问，工业互联网作为将工业领域人、机器、物体、网络等全面互联的新型网络基础设施，通过实现工业世界、信息世界和人类社会的互联互通形成了新生态体系，必将对工业领域产生全面、深刻和革命性的影响。

工业互联网安全，涉及工业与网络、工业与安全、网络与安全、工业安全与网络安全等多维度、多层次融合问题。然而，工业、互联与安全分属三个学科和行业领域，当前“三张皮”割裂的问题十分严重。如何把握开放发展和安全可靠的辩证关系，是工业互联网发展必须解决的核心问题。首先，工业和互联的融合是基础。而工业互联网本质是互联网络信息系统，存在网络信息系统的安全共性问题；另一方面，工业互联网的特色是工业应用，必须考虑区别于其他网络的特有安全问题。工业互联网及其安全问题的复杂性，为解决这个问题带来了严峻的挑战。目前，尚无一本系统论述工业互联网安全理论与方法问题的著作。如何弥合工业、互联及安全之间的鸿沟，如何建立工业互联网安全保障体系，是工业互联网健康发展不可回避的问题，也是本书要着力解决的基本理论和方法问题。

“不谋全局者，不足以谋一域”。工业互联网安全由网络信息安全及工控安全等领域融合发展而来，涉及工控系统、工业设备与控制器、因特网、云计算、嵌入式、工业 APP、工业微服务以及供应链等众多对象，包括设备与控制安全、网络安全、应用安全、数据安全以及安全管理等层面，物理安全、功能安全和信息安全融合需求强烈，具有跨时空、多层次、立体化、广渗透、深融合、工业化的新形态和鲜明的体系特征。

本书以体系思想为指导，系统研究并深入论述了工业互联网及工控网络的安全体系，涵盖了工业设备与控制、网络、应用及数据等安全领域，特别强调工业、互联与安全的融合，理论思想和技术方法的融合。全书共分 7 章。第 1 章概论包括：工业互联网的发展历程、主流平台形态及安全；通用架构与功能体系；工业互联网安全的内涵、外延与基本框架等。第 2 章研究工业互联网安全体系与体系能力构建，包括：体系思想与方法；IT、OT 与 CT 安全需求差异、冲突与统一；工业互联网安

全风险分析；工业互联网安全体系能力构建等。第3章讨论工业设备与控制安全，包括：工业现场设备与控制系统的功能与安全影响因素；物理安全、功能安全与信息安全及其融合设计；工业芯片、嵌入式操作系统、SCADA、DCS、PLC安全等。第4章研究工业互联网的网络安全，包括：网络防御体系构建；网络安全域、访问控制与工业防火墙；网络传输安全问题等。第5章研究工业互联网的应用安全，包括：工业应用软件、工业APP、工业微服务架构的设计及安全问题。第6章探讨工业互联网的数据安全，包括：工业数据分类分级；数据安全能力需求；工业数据采集、传输与交换、存储、处理以及销毁等方面的安全问题。第7章展望安全可信、自主可控等未来安全要求与发展趋势。

本书为国家重点研发计划(2016YFB0800700、2016YFC1000301)的研究成果之一。作者长期从事网络空间安全和工控系统研究，承担了大量的国家级、省部级和企业课题，对工业网络安全有系统深入思考并在工控安全领域持续实践迭代，本书是对该过程成果的高度凝练与系统总结，同时还参考了国内外最新理论和技术进展。

在研究和著述过程中，得到了清华大学、北京大学、国家卫生健康委科学技术研究所、上海交通大学、北京航空航天大学、北京理工大学、中国科学院信息工程研究所、解放军联合参谋部、解放军装备发展部、中国航天系统科学与工程研究院、中国航天科工集团公司第二研究院、公安部第一研究所、中国电子科学研究院等单位同行专家的许多支持和帮助，谨表谢意。科学出版社给予了大力支持，王哲编辑为本书付出了辛勤努力。同时，本书还参阅了大量的国内外专著、科研论文以及网络学术资源，篇幅所限未能尽录，在此一并致谢。

本书撰写历经数载，尤其是2018年春以来，进入作者最艰难的时刻。感谢家人和亲友的理解、宽容、忍耐、支持与提供的不竭动力，使本书得以完成。还要特别感谢江苏省运河中学各位校友在作者最困难的时刻给予的无私帮助。

本书付梓之际，特别感谢恩师：著名网络空间安全专家胡昌振教授、著名武器与机电系统专家谭惠民教授、著名自动化专家赵彤教授、著名工控系统专家于春阳博士。没有他们的教诲和指导，就没有本书的面世。

本领域涉及的理论技术复杂，加之作者水平有限，虽已力避不足，难免仍有疏漏之处。抛砖引玉，恳请读者将意见和建议发至：yhzhi@bit.edu.cn，作者不胜感激。

闫怀志

2019年春于北京中关村

# 目　录

# 第 1 章　工业互联网及其安全体系概论

作为工业互联网安全研究的基础背景分析，本章将重点介绍工业互联网的发展、形态及内涵、功能体系，典型工控系统形态及安全分析，工业互联网的功能体系，国内外典型平台及其安全性实例分析，工业互联网技术与平台发展途径，以及工业互联网安全的内涵和外延等内容，为进一步研究工业互联网安全体系奠定基础。

## 1.1　工业互联网的发展历程、主流平台形态及安全问题

工业互联网(Industrial Internet)是在国际科技变革与工业产业革命、互联网创新发展与工业 4.0 持续交汇的大背景下，工业体系与互联网体系深度融合的产物，是工业领域中完成人、机与物等生产经营各要素全面互联的新型工业基础设施，不仅具有典型的工业特征，更是网络空间的重要信息系统形态，是新一轮工业革命的关键支撑。本节将讨论工业互联网的发展历程与趋势、形态演变及内涵等基本内容。

### 1.1.1　工业互联网的发展历程与形态演变

当前，人类社会正向信息社会全面飞速转变。信息革命以互联网、物联网、云计算、大数据、人工智能等技术发展与广泛应用为核心标志，极大地促进了生产力水平提升。工业一直是信息技术(Information Technology，IT)进步的重要牵引力量，而 IT 的发展也对工业领域起到了巨大的推动作用。工业革命的技术驱动核心逐渐从物质、能量转移到信息及信息技术本身。

从 20 世纪 50 年代开始，IT 的发展就持续推动着工业技术的进步。从可编程逻辑控制器(Programmable Logic Controller，PLC)到集散控制系统(Distributed Control System，DCS)，从工业现场总线到工业以太网，从工控系统到工控网络，从传感器网络到工业物联网，IT 不断向工业领域渗透，实现了人-物通信和物-物通信，系统集成和互联互通互操作取得了丰硕成果，网络化、智能化与融合化雏形初现，也为进一步利用互联网为工业领域服务奠定了良好基础。目前，互联网创新发展与以“德国工业 4.0”、“中国制造 2025”为代表的工业革命正处于难得的历史交汇期，全球各主要工业强国纷纷对工业互联网的核心标准、关键技术与基础平台等方面成体系加速布局和大力推动，培育并发展数字驱动的工业新生态。

2011 年美国 GE 公司提出“工业互联网”概念，旋即引起了高度关注与重视。2015 年，GE 与 AT&T、Cisco、IBM 及 Intel 创立了工业互联网联盟(Industrial Internet

Consortium，IIC)。IIC 认为，工业互联网是“一种物品、机器、计算机与人的互联网，利用先进的数据分析方法，辅助提供智能工业操作，改变商业产出。它包括了全球工业生态系统、先进计算和制造、普适感知、泛在网络连接的融合。” 工业互联网平台正逐步向工业设计、研发、生产、制造、营销、运维、服务等全工业流程深度渗透。

GE 擅长于工业领域，拥有大量的工业设备产品，它推出的 Predix 平台，旨在“通过连接物理和数字世界推动工业转型”，曾被期冀成为工业互联网的标准平台。

AT&T 长期关注信息通信和物联网的工业应用，尤其是 M2M(Machine to Machine)在工业互联网领域中的应用。2013 年，AT&T 与 GE 签署了全球联盟协议：GE 生产的机器设备可与 AT&T 网络及云端连接，操作人员可通过高安全性无线通信与 M2M 通信系统，实现在全球任何地点对 GE 机器的远程跟踪、监控、记录和操作，合作开发 Predix 的 M2M 解决方案，实现对 GE 工业产品的远程控制和主动维护。

Cisco 更注重网络连接性方面的优势，形成了雾计算(Fog Computing)、应用平台、物理与网络安全、网络连接性、数据分析与应用、管理与自动化等六大核心。Cisco 与 GE 协作提供了支持 Predix 的工业路由器，可胜任石化和燃气设施等恶劣环境。2016 年，Cisco 或考虑到工业互联网的未来战略价值，放弃了 IIC 创始成员身份，旨在扶持、加强开放雾计算联盟(OpenFog Consortium)的 OpenFog 在工业互联网领域的基础地位。无独有偶，AT&T 也退出了 IIC 创始成员。

IBM 作为智慧地球的提出者，从 2008 年起一直致力于“智慧地球”战略，期望找到驱动智慧地球的新动力，这也是其加入 IIC 的主要动机之一。

Intel 试图通过对工业互联网领域的参与，重新进行战略布局，以期形成其在传统 PC 领域的类似影响力。Intel 联合 GE，推出了边缘设备参考架构，实现了 Intel 处理器与 GE Predix 软件的综合集成，可将智能联网接口内嵌到任何设备当中。

2011 年，Cisco 正式推出“雾计算”概念。2015 年，ARM、Cisco、Dell、Intel、Microsoft 与普林斯顿大学边缘(Edge)实验室共同创建了 OpenFog 联盟，将发展工业物联网的希望寄予雾计算之上。雾计算作为分布式计算框架模型之一，位于物联网现场设备与云数据中心的中间层。雾计算理论认为，仅仅依靠云计算，无法解决物联网设备和传感器部署所面临的高延迟、网络阻塞、系统过载、系统可靠性差、安全性低、服务质量差等问题。雾计算架构在云设备-终端之间、设备-网关之间，将计算、控制、通信与存储资源及服务，分配给用户或用户端系统。雾计算架构更为分散、更加接近网络边缘，所以更适合处理分布于工业网络边缘的设备信息。

德国提出了工业 4.0 概念，构建了“工业 4.0 统一参考架构模型”，以“信息物理系统(Cyber Physical System，CPS)”为核心，令生产设备获得智能，并将智能化制造能力向涵盖全生命周期的价值链条和各层级的工业系统映射，力图实现以数据为驱动的工业智能化。

国际上公认，工业互联网必将成为工业和经济发展的关键信息系统。当前，中国是当之无愧的制造大国，但距离制造强国尚有相当的差距。中国还处于世界制造业的中低端水平，劳动密集、低附加值、高污染、高消耗的制造业态大量存在，随着人口红利日渐式微、人力成本持续走高、资源环境承载能力不堪重负的形势日益严峻，传统的工业发展模式已难以适应，在工业 4.0 时代，更难以为继。在云计算、物联网、大数据、人工智能等先进 IT 持续发展、工业应用日益广泛深入的大趋势下，中国的两化融合逐步深入、“中国制造 2025”持续推进，并及时成立了工业互联网产业联盟(Alliance of Industrial Internet，AII)，迅速在工业互联网框架、标准、测试、安全等方面开展工作，并积极与国际各主流工业互联网参与方合作，取得了长足进展。

目前，全球共有多家供应商宣称能够提供工业互联网平台及相关服务，其中有 1/5 的供应商具有较高的知名度和影响力。不过，目前国内外能够完全满足工业数据广泛采集、海量工业数据即时处理、工业数据综合分析及知识复用、工业 APP 研发至运行全流程服务四层功能的工业互联网平台并不多见。大部分工业互联网平台，因其行业影响与技术水平欠缺，仅能实现工业数据采集与部分分析功能，离实现基于 PaaS(Platform as a Service)平台的工业 APP 研发设计与生态体系尚有较大差距。下面以国内外部分典型工业互联网平台为例来研究和分析其平台架构与功能、安全性。

## 1.1.2　Predix 平台及其安全分析

### 1.1.2.1　Predix 平台架构与功能分析

Predix 平台是 GE 基于 VMware 的开源 PaaS 云平台 Cloud Foundry(CF)而设计的，其中，CF 为 Predix 平台提供全生命周期支持。国际上各工业互联网平台 PaaS 多以 CF 和 Docker 等作为核心基础架构。CF 的优势有：①强力支持持续交付(Continuous Delivery，CD)软件战略，实现工业应用全生命周期的集中管理且易于运维；②支持对 Spring for Java、.NET、Python、PHP 等框架的灵活选择；③实现了工业应用与其所依赖服务的分离，二者可使用绑定策略，使得工业应用在 PaaS 平台的部署更加方便快捷；④可灵活部署于 vSphere/vCloud、OpenStack 等工业公有云、私有云、社区云或混合云之上。

Predix 平台利用分布式计算模型、工业大数据处理与 M2M 通信等手段，实现了工业现场设备、工业数据、企业运管数据、人员与企业其他资产的相互连接，目的是将设备端到云端顺利互通，并通过大量的工业 APP，将工业云平台云端储存的海量工业数据的分析结果呈现给各类用户。Predix 平台的体系结构由边缘连接层、基础设施层以及应用服务层组成。Predix 平台的系列服务相互贯通，特色鲜明。

Predix 平台的工业数据管理服务是为研发人员提供 Predix 平台数据并应用到具体 APP 上。工业数据应用过程涉及：工业数据源、工业数据采集、工业数据湖泊、工业数据分析与使用。

Predix 平台拥有众多 OT(Operational Technology)，能够完成 IT/OT 的有机结合。Predix 平台的设备资产管理服务功能包括组织结构和业务逻辑。表 1.1 为 Predix 平台的设备资产管理服务功能分析。

表 1.1　Predix 平台的设备资产管理服务功能分析

| 类型 | 子类 | 主要功能 |
| --- | --- | --- |
| 组织结构 | 资产与成组分类 | 实现资产分类与成组分类功能 |
| | 资产结构模板 | 与工业产品的物料清单结构类似 |
| 业务逻辑 | 业务规则框架 | 快速横切资产模型，提供数据反馈；修改相关资产，执行相关规则 |
| | 目录服务 | 制定资产组织与管理的相关原则，为资产共享服务 |
| | 配置管理与审计 | 实现资产的配置管理及相关审计工作 |

Predix 平台还能够提供时间序列服务。生产制造车间的工业生产设备生成的数据实时性强，时间序列服务采用列式存储格式，查询效率较高。也可以采用外部数据模型来获取(摄入)海量数据，实现大数据高效存储，借助快速检索数据索引，实现 ms 级数据处理精度。Predix 平台分析功能采用了适用于工业场景的百余种算法，还允许接入外部分析程序与 Predix 平台的分析服务实现互补。而且，用户还能够将基于 Matlab 自行研发的算法发布至 Predix 平台。

#### 1.1.2.2　Predix 平台安全性分析

Predix 平台安全措施较为完备，安全机制包括了安全工业应用、平台硬化、可视化持续监控以及 PaaS 安全责任等主要方面。为了提供工业数据的整体安全性，Predix 平台将云端部署于安全的工业数据中心。云层的客户生产数据存储于相对独立的云空间中，不对其他云服务提供共享功能。此外，Predix 平台还能实时扫描与监测各种层次的云栈脆弱性。

Predix 平台硬化的主要目标是“用所必需”，将非必需的服务、应用、网络协议、配置操作系统 OS(Operating System)用户认证以及配置资源控制，从 Predix 平台及其底层基础设施中删除，对系统漏洞等脆弱性进行自动化或人工识别和修复，特别是增强了在用户、工业设备、应用软件以及工业数据等层次的协同识别，以保障工业互联运行环境的统一性和安全性。

在工业应用方面，Predix 平台注重对 APP 能力的验证和信任，实现安全静态、动态分析测试、研发过程生成物集成与自动化，完成代码仓库和审查交付，并对平台基础代码进行 DevOps 安全评估。可视化持续监控方面，Predix 的 PaaS 平台为保障信任关系的建立，以及端到端平台和基础设施的可见，对安全事件实施监测和自

动隔离，并对工业应用程序的行为进行安全评价。安全职责方面，Predix 的 PaaS 平台重点保障硬件基础设施的物理安全，将客户环境隔离，客户业务环境和数据对外不可见。操作系统安全方面，Predix PaaS 进行了 VM 硬化，并维护相关基础操作系统镜像。存储方面，Predix PaaS 提供了加密块存储、对象存储及相应的服务。同时，通过 IPSec(Internet Protocol Security)与 SSL(Secure Sockets Layer)/TLS(Transport Layer Security)来保障该平台上工业数据的安全传输。通过身份识别商店，完成联邦身份识别的管控，并提供安全的单点登录(Single Sign On，SSO)服务。在安全监控与日志分析领域，重点关注云平台的网络入侵攻击、恶意行为以及不合规活动的主动检测。风险管理方面，Predix PaaS 完善了工业云环境安全风险评估流程，不仅有渗透测试和合规扫描，还有安全控制及其过程评估。

### 1.1.3　MindSphere 平台及其安全分析

2016 年，SIEMENS 结合工业 4.0 理念，推出了开放式工业云平台 MindSphere，并联合设备制造商、最终用户、数据采集工具研发者、工业系统集成商以及工业应用研发人员等，力图打造完整的工业物联网(Internet of Things，IoT)产业生态链，以“全面掌控数字化转型”。

#### 1.1.3.1　MindSphere 平台架构与功能分析

MindSphere 平台也采用了 CF 作为基础架构。该平台采用 PaaS 模式，专为物联网设计，定位于 IoT 操作系统，具有生产数据采集、记录、分析、连接等功能，向下处理包括 I/O 在内的各类硬件，向上支持各类 MindApp，既能在公有云上实现部署，也可以在工业企业的私有云上实现部署。

MindSphere 架构分为边缘连接层、开发运营层以及应用服务层，关键要素有 MindConnect、MindClound 与 MindApp 等。MindConnect 负责工业现场的数据采集，并将其上传给工业云平台；MindClound 负责进行工业数据统计分析，并向需求方提供 APP 研发环境与相关工具等；MindApp 负责向需求方提供工业 APP，这些 APP 实现了工业知识与工业数据统计分析结果的综合集成。

MindSphere 使用 MindConnect Nano 来实现 SIEMENS 产品及第三方设备的海量工业数据采集。Nano 还能够构建工业现场到云端的加密通信链路，可在 MindSphere 最底层通过 MindConnect 实现各工业设备的网络连接。Nano 可与支持 S7 或 OPC(Object Linking and Embedding for Process Control)架构的工业设备实现联网，并与 MES(Manufacturing Execution System)集成，也可以与内嵌以太网通信功能的工业设备相集成。不支持 S7 系列协议或 OPC UA(Unified Architecture)协议的工业设备，可采用 MindConnect 定制通信协议来联网采集数据。工业数据分析使用 MindSphere 内含的 Sinalytics 分析工具。MindSphere 平台还提供边缘计算能力，在

接近工业装置或工业数据源一侧进行本地化计算，将网络连接、数据计算、数据存储、数据应用等关键功能融为一体。

#### 1.1.3.2　MindSphere 平台安全性分析

保障工业数据安全、增强工业设备可用性是 MindSphere 的核心主张之一。MindSphere 明确了工业数据的拥有者是客户本身，客户可以通过 API(Application Programming Interface)自行开发或交由第三方开发 APP，这对于降低安全风险、增强设备可用性等都是一种保障。

MindSphere 的数据传输采用 HTTPS(Hypertext Transfer Protocol Secure)。MindConnect 只可与 MindSphere 平台连接，通过 TLS 1.2 进行数据通信。SIEMENS 重视云数据中心的安全，特别是端到端的工业数据传输与存储安全。SIEMENS 工业 APP 平台提供了“KeepSecure!”，可用于安全漏洞扫描、潜在威胁识别和异常检测，并提供漏洞补丁等解决方案。在可用性与可靠性保障方面，MindSphere 能适应 –40～85°C 的宽温范围，还能够适应电力和石油天然气等行业的恶劣现场环境。

此外，为保证安全，Mindsphere 仅提供实时分析功能，不具备现场设备控制能力。其出发点是，一方面，工业现场已有本地 PLC、DCS 等系统，现场设备控制由其中的控制器来执行。另一方面，如果采用 Mindsphere 来进行工业设备控制，则必然会导致现场 PLC 设备中的控制程序指令重写，否则会造成不可靠、不合规的多处赋值情况。

### 1.1.4　COSMOPlat 平台及其安全分析

2017 年，海尔发布了工业互联网云平台 COSMOPlat。该平台摒弃了国外工业互联网平台聚焦工业现场生产、设备运维来改造升级的模式，而是强调让用户定义制造需求，实现了专属个性化定制与通用大规模生产的平衡与融合。作为中国自主创新的工业互联网平台之一，COSMOPlat 平台是推行“中国制造 2025”的应用典范，海尔也成为当时唯一获得“2017 年度 Gartner 高科技制造创新者奖”的工业生产制造类企业。

#### 1.1.4.1　COSMOPlat 平台架构与功能分析

COSMOPlat 平台的突出特点是用户“赋能”，将用户需求精准传递给制造方，双方实时交互和反馈，为用户提供最佳体验，实现了工业企业与最终用户连接、企业与生产经营资源连接、最终用户与生产经营资源连接的工业智能制造云平台。

COSMOPlat 平台架构自底至上分为资源层、平台层、应用层与模式层四层。最下面的资源层实现对软件、硬件、物流、服务资源的聚合，涵盖了完全开放的国内外数百万家资源，目标是全球资源的最优匹配和分布调度。平台层主要是基于物联网的

分布式、开放型云平台，提供模块化微服务架构，实现公有云、私有云、混合云的部署、开发和实施。应用层则基于 SaaS(Software as a Service)应用来构建，其目标是实现工业 Know-how 的软件化，从而为生产制造企业提供具体的互联工厂应用服务，对工业 APP 的快速敏捷研发设计、部署实施与运行等提供基础支持。模式层体现了 COSMOPlat 平台的特色精华，是海尔自身制造模式、工业互联模式、产品定制模式、资源共享模式的积淀与创新应用。

COSMOPlat 平台不仅可以实现交互定制、开放研发、智能生产、迭代升级等生产制造环节的贯通，同时还将数字营销、物料采购、智慧物流等服务环节涵盖了进来。该平台通过为用户赋能提供支撑，使用户持续深度参与到产品的各个环节当中，实现个性化定制需求服务。

#### 1.1.4.2　COSMOPlat 平台安全性分析

COSMOPlat 平台采用了海尔“海安盾”进行安全监控与防护。海安盾平台基于现有网络安全保障体系架构，注重工业物联网在网络基础架构、应用、数据保护和加密、身份和权限等方面的保障，更加强调全流程纵深防护，覆盖所有业务流程特别是用户数据的安全保护。基于海安盾建立安全体系的核心是建立安全运营中心(Security Operations Center，SOC)，实现相关安全技术和产品的集中管控与协同，对所有安全资源进行统一监管、同步策略管控、智能日志分析与审计，并通过安全手段之间的智能联动，获取所有安全相关数据，对安全事件进行智能关联与统计分析，及时反映平台的安全基线遵循情况，实现其中安全事件及风险的实时监控、定位与预警，并提供相应的安全解决方案。

物理安全方面，COSMOPlat 平台侧重于数据中心、办公区域、视频监控的安全。数据安全方面，其侧重于数据分类保护、用户隐私保护、数据加密以及数据防泄露等。基础架构安全方面，其侧重于网络主机、工控设备以及互联网终端的安全等。账号权限和访问方面，其侧重于认证和访问、账号生命周期、证书管理体系等。应用安全方面，其侧重于 Web/APP 安全、安全开发周期、业务流程安全等。安全实践管理方面，其侧重于日志收集和存储、日志关联、威胁分析和建模等。

海尔还与合作伙伴联合推出了嵌入式虚拟智能安全平台 COSMOPlat-FOX，利用 AI 来兼顾智能制造效率与平台安全，保护上云的生产制造与经营数据的安全。

### 1.1.5　INDICS 平台及其安全分析

2017 年，中国航天科工集团旗下的航天云网公司发布了工业互联网平台 INDICS(Industrial Intelligent Cloud System)。INDICS 与 Predix、MindSphere 一道，成为国际上定位于工业级操作系统的主流工业互联网平台。INDICS 结合了中国具体国情