

网络空间安全丛书

# 安全物联网系统设计

苏米特·阿罗拉(Sumeet Arora)

[美] 拉马钱德拉·甘菲尔(Ramachandra Gambheer) 著

米纳克希·沃赫拉(Meenakshi Vohra)

姚凯 曾大宁 栾浩

译

清华大学出版社

北 京

北京市版权局著作权合同登记号 图字：01-2021-6888

Sumeet Arora, Ramachandra Gambheer, Meenakshi Vohra

Design of Secure IoT Systems: A Practical Approach Across Industries

978-1-260-46309-5

Copyright © 2022 by McGraw-Hill Education.

All Rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation edition is published by Tsinghua University Press Limited in arrangement with McGraw-Hill Education(Singapore)Pte. Ltd. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Translation Copyright © 2023 by McGraw-Hill Education(Singapore) Pte. Ltd and Tsinghua University Press Limited.

版权所有。未经出版人事先书面许可，对本出版物的任何部分不得以任何方式或途径复制传播，包括但不限于复印、录制、录音，或通过任何数据库、信息或可检索的系统。

此中文简体翻译版本经授权仅限在中华人民共和国境内(不包括中国香港特别行政区、澳门特别行政区和台湾地区)销售。

翻译版权©2023 由麦格劳-希尔教育(新加坡)有限公司与清华大学出版社有限公司所有。

本书封面贴有 McGraw-Hill Education 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。举报：010-62782989, beiqinquan@tup.tsinghua.edu.cn。

#### 图书在版编目(CIP)数据

安全物联网系统设计 / (美) 苏米特·阿罗拉 (Sumeet Arora), (美) 拉马钱德拉·甘菲尔 (Ramachandra Gambheer), (美) 米纳克希·沃赫拉 (Meenakshi Vohra) 著; 姚凯, 曾大宇, 栾浩译. —北京: 清华大学出版社, 2023.4

(网络空间安全丛书)

书名原文: Design of Secure IoT Systems: A Practical Approach Across Industries

ISBN 978-7-302-63152-1

I. ①安… II. ①苏… ②拉… ③米… ④姚… ⑤曾… ⑥栾… III. ①物联网—系统设计 IV. ①TP393.409 ②TP18

中国国家版本馆 CIP 数据核字(2023)第 053392 号

责任编辑: 王 军

装帧设计: 孔祥峰

责任校对: 成凤进

责任印制:

出版发行: 清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址: 北京清华大学学研大厦 A 座 邮 编: 100084

社 总 机: 010-83470000 邮 购: 010-62786544

投稿与读者服务: 010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质 量 反 馈: 010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印 刷 者:

装 订 者:

经 销: 全国新华书店

开 本: 170mm×240mm 印 张: 12.25 字 数: 283 千字

版 次: 2023 年 6 月第 1 版 印 次: 2023 年 6 月第 1 次印刷

定 价: 68.00 元

产品编号: 094832-01

谨以本书献给挚爱的亲友们：

**Krishan先生和Raj Arora–Sumeet夫人**

**Vittal Rao Gambheer先生和已故的Raghothama Vittal–Ramachandra夫人**

**Jagdish 先生和 Usha Vohra–Meenakshi 夫人**





# 作者简介

---

Sumeet Arora 担任数据分析公司 ThoughtSpot 的首席研发官。ThoughtSpot 公司的使命是利用搜索和人工智能技术，为知识工作者增加分析能力和洞察能力，帮助知识工作者创建一个更趋向于以事实为驱动的世界。在加入 ThoughtSpot 公司之前，Sumeet 曾担任 Cisco System 公司的高级副总裁并兼任服务提供商网络部总经理。在总经理岗位上，Sumeet 领导了面向全球服务提供商的网络/路由产品的工程、研发和产品管理团队。

Ramachandra Gambheer 担任 Cisco System 公司的高级技术和业务运营经理。Ramachandra 在硬件系统设计、物联网和海量硬件测试自动化领域拥有 30 年的全面经验，并在美国境内期刊和国际期刊上发表了多篇论文。Ramachandra 曾经为包括机器视觉在内的各个行业设计了多个基于 FPGA 的嵌入式系统。Ramachandra 也是 Surathkal NITK (KREC)的校友和前教员。

Meenakshi Vohra 作为安全专家，曾在 Uber、VMware、洛克希德马丁和赛门铁克等大型公司和初创公司工作。Meenakshi 实现了嵌入式平台和云计算软件系统的安全协议，以及出租汽车、无人机、出租飞机、自行车和滑板车等自主车辆的边缘系统。Meenakshi 拥有二十多年的网络和软件产品研发经验。Meenakshi 具有计算机科学学士学位和网络与安全硕士学位。



# 译者序

---

全球物联网正在高速增长。GSMA 发布的《2020 年移动经济 (The mobile economy 2020)》报告显示, 2019 年全球物联网总连接数达到 120 亿, 预计到 2025 年, 全球物联网总连接数规模将达到 246 亿, 年复合增长率高达 13%。2019 年我国的物联网连接数 36.3 亿, 全球占比高达 30%。而根据 2021 年 9 月世界物联网大会的数据, 2020 年末, 我国物联网的连接数已经达到 45.3 亿, 预计 2025 年将超过 80 亿。

2021 年初发布的《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》划定了 7 大数字经济重点产业, 包括云计算、大数据、物联网、工业互联网、区块链、人工智能、虚拟现实和增强现实, 这 7 大产业也将承担起数字经济核心产业增加值占 GDP 超过 10% 目标的重任。该纲要明确在“十四五”期间, 让 5G 用户普及率提高到 56%, 并且 5 次提到关于物联网的规划发展。国家在“新基建”方面的建设进一步发展, 5G 基站、工业互联网、数据中心等领域加快建设。物联网作为新型基础设施的重要组成部分, 同样将得到快速发展。截止 2021 年底, 我国物联网产业规模已超 2.6 万亿元, 三家基础电信企业的蜂窝物联网用户达 13.99 亿户。

然而, 人们在享受万物互联带来的便利同时, 物联网终端的安全问题却逐渐暴露出来, 甚至成为最薄弱环节。大量物联网设备在部署时, 几乎没有同步配置防护能力, 影响了物联网的整体安全可靠。而由于物联网设备本身的局限性, 传统的安全防护措施在部署时面临着极大的挑战。但是, 随着物联网与业务的融合日益加深, 其漏洞给各组织的整体信息安全带来巨大的隐患。不断增长的物联网互联设备为攻击方提供了广泛的网络攻击入口, 导致物联网面临着大量的问题和挑战。国家互联网应急中心(以下简称 CNCERT)发布的《2020 年我国互联网网络安全态势综述》显示, 联网智能设备恶意程序样本数量持续上升, 采用 P2P 传播方式的联网智能设备恶意程序异常活跃。2020 年, CNCERT 运营的国家信息安全漏洞共享平台(CNVD 漏洞平台)新增收录的通用联网智能设备漏洞数量同比增长 28%, 境内联网智能设备被控端 2929.73 万个, 通过控制联网智能设备发起的 DDoS 攻击日均 3000 余起。累计控制规模大于 10 万的僵尸网络共 53 个, 控制规模为 1 万至 10 万的僵尸网络共 471 个, 涉及的设备类型主要有家用路由器、网络摄像头、会议系统等。

分析认为, 很多厂商和组织缺乏安全意识和安全能力, 在研发和部署物联网智能设备时, 没有做好安全考虑, 导致出现软硬件安全漏洞。而且, 很多设备也缺乏软件安全更新机制或机制不安全, 导致从根本上无法修复漏洞, 从而产生了恶劣的后果。有鉴于此, 清华大学出版社引进并主持翻译了《安全物联网系统设计》一书, 希望通过本书,

让广大物联网从业人员和安全从业人员理解物联网面临的独特安全挑战，物联网的不同应用场景，物联网的网络架构和数据架构，将信任和安全融入物联网设计的方法，以及物联网的生命周期管理。本书领衔作者 Sumeet Arora 是数据分析公司 ThoughtSpot 的首席研发官，利用搜索和人工智能为每位知识工作者带来见解和分析，帮助创建一个更现实的世界。第 2 位作者 Ramachandra Gambheer 是 Cisco System 公司的高级技术和业务运营经理。Gambheer 在硬件系统设计、物联网和大容量硬件测试自动化领域拥有 30 年的经验，并在美国和国际期刊上发表了多篇论文。Gambheer 为包括机器视觉在内的各个行业设计了多个基于 FPGA 的嵌入式系统。第 3 位作者 Meenakshi Vohra 是一名安全专家，曾在 Uber、VMware、洛克希德马丁和赛门铁克等大型公司以及各种初创公司工作。Vohra 已在嵌入式平台和云软件系统以及边缘系统中实施了安全协议，并且在网络和软件产品研发方面拥有 20 多年的经验。本书以网联汽车为案例，贯穿全书的讨论，同时，在第 9 章深入探讨了在第 2~8 章中学习的设计和构建物联网基础设施所支持的案例。

翻译过程中，译者力求忠于原著，希望尽可能传达作者的原意。全书的翻译工作历时一年有余，有近十名译者参与翻译和校对工作，有他们的辛勤付出，才有本书的出版。感谢参与本书校对的信息系统和网络安全专家，保证本书稿件内容表达的一致性和文字的流畅，同时要感谢栾浩、姚凯和曾大宇先生对组稿、校对和统稿等工作所投入的大量时间和精力，保证了全书在技术和内容表达上的准确、一致和连贯。

同时，还要感谢本书的审校单位北京金联融科技有限公司(以下简称“金联融”)。金联融是集数字化软件技术与数字安全于一体的专业服务机构，凭借现代化的企业管理手段与优秀高效的团队，不断发挥自身优势和整合行业资源，利用丰富的技术经验，专注于数字化软件技术与数字安全领域的研究与实践，为党和政府、大型国有企业、银行保险、大型民营企业等客户群体提供数字经济建设、数字安全规划与建设、网络安全技术、数据安全治理、软件造价和信息系统审计等项目，以帮助客群实现管理目标和数字资产价值交付为核心的全方位、定制化的专业服务。在本书的译校过程中，金联融的数字化专家、安全专家和研发团队结合行业特点与前沿技术信息，投入了多名人员和大量时间支持本书的译校工作，保证了全书的质量。

最后，再次感谢清华大学出版社编辑的严格把关、悉心指导，正是有了他们的辛勤努力和付出，才有了本书中文译稿的出版发行。

物联网技术和物联网安全类书籍涉及多个纵向专业领域，内容涉猎广泛，术语体系复杂且难于辨析。译者能力所限，在翻译中难免有错误或不妥之处，恳请广大读者朋友不吝指正。

# 译者介绍

---

栾浩，具有美国天普大学 IT 审计与网络安全专业理学硕士学位，持有 CISSP、CISA、CISP、CISP-A 和 TOGAF 9 等认证。负责金融科技研发、数据安全、云计算安全和信息化审计和内部风险控制等工作。担任中国计算机行业协会数据安全产业专家委员会专家、(ISC)<sup>2</sup> 上海分会理事。栾浩先生担任本书翻译工作的总技术负责人，并负责全书的校对和定稿工作。

姚凯，具有中欧国际工商学院工商管理硕士学位，持有 CISSP、CCSP、CEH 和 CISA 等认证。负责 IT 战略规划、策略程序制定、IT 架构设计及应用部署、系统取证和应急响应、数据安全、灾难恢复演练及复盘等工作。姚凯先生负责本书第 1 章的翻译，以及全书的校对、定稿工作，并为本书撰写了译者序。

曾大宁，具有南京航空航天大学飞行器工程专业工学学士学位，持有 CISSP 和 PMP 等认证。现任信息技术经理职务，负责芯片行业的数据中心建设与运营、高性能计算环境、网络通信、云计算安全与信息安全等工作。曾大宁先生负责本书第 5 章的翻译，以及全书的校对、定稿和项目管理工作。

王向宇，具有安徽科技学院网络工程专业工学学士学位，持有 CISP、CISP-A、软件工程造价师和软件研发安全师等认证。现任高级安全工程师职务，负责安全事件处置与应急、数据安全治理、安全监测平台研发与运营、云平台安全和软件研发安全等工作。王向宇先生负责全书的校对、定稿工作。

齐力群，具有北京联合大学机械工程学院机械设计与制造专业工学学士学位，持有 CISA、CIA 和 CISP-A 等认证。现任技术负责人职务，负责数据安全治理、信息系统审计、信息安全技术等工作。齐力群先生负责本书的校对、通稿工作。

李浩轩，具有河北科技大学理工学院网络工程专业工学学士学位，持有 CISP、CISP-A 等认证。现任安全技术经理职务，负责 IT 审计、网络安全、平台研发、安全教培和企业安全攻防等工作。李浩轩先生负责本书前言的翻译，以及全书的校对工作。

徐坦，具有河北科技大学理工学院网络工程专业工学学士学位，持有 CISP、CISP-A 等认证。现任安全技术经理职务，负责数据安全技术、渗透测试、安全工具研发、代码审计、安全教育培训、IT 审计和企业安全攻防等工作。徐坦先生负责本书的校对工作。

刘竞雄，具有长春工业大学计算机工程硕士学位，持有 PMP、CISP 等认证。现任安全咨询顾问职务，负责政府行业智慧城市安全建设及数据安全、云计算安全和信息化安全咨询评估等工作。刘竞雄先生负责本书第 2 章的翻译工作。

陈皓，具有上海交通大学软件工程专业工学硕士学位，持有 CISSP、CGEIT、CISM、

CRISC、CISA 和 TOGAF 等认证。现任雅培中国大中华区域网络安全总监职务，负责企业内部网络安全、数据保护、隐私技术合规等工作。陈皓先生负责第 3 章的翻译工作。

张伟，具有天津财经大学国际贸易专业本科学历，持有 CISSP、CISA 等认证。现任高级安全咨询顾问职务，负责向客户提供信息安全咨询、信息安全实施、应急响应等服务。张伟先生负责本书第 4、6 章的翻译工作。

刘宇馨，具有郑州大学计算机科学与技术专业工学学士学位，持有零信任专家等认证。现任网络安全企业技术总监等职务，负责网络安全技术研究与架构规划设计等工作。刘宇馨先生承担第 7 章的翻译工作。

刘建平，具有华东师范大学计算机专业工学学士学位，持有 CISP 等认证。现任信息技术运营经理，负责信息技术基础架构、信息技术运维、安全技术实施、安全合规等工作。刘建平先生负责第 8 章的翻译工作。

王厚奎，具有南宁师范大学教育技术专业网络信息安全方向理学硕士学位，持有 CISI、CISP 和 CISP-PTE 等认证。现任南宁职业技术学院教师/广西网络信息安全服务研究院副院长职务。担任南宁市信息技术学会会长。负责信息安全专业教学、网络安全项目咨询、安全服务等工作。王厚奎先生负责第 9 章的翻译工作。

汤国洪，具有电子科技大学电子材料与元器件专业工学学士学位，持有 CISSP、CISA 和 ISO/IEC27001 等认证。现任 IT 经理与信息安全负责人职务，负责 IT 运维、基础架构安全、网络安全和隐私合规等工作。汤国洪先生负责第 10 章的翻译工作。

梁龙亭，具有北京理工大学计算机科学与技术专业工学学士学位，持有 CISSP 和 ISO/IEC27001 等认证。现任信息安全与合规经理职务，负责安全技术架构设计、安全攻防、安全技术实施、安全合规等工作。梁龙亭先生负责本书第 2 章的校对工作。

张帆，具有上海交通大学工商管理硕士学位，持有 CISA 和 CISSP 等认证。负责 IT 安全策略和制度制定、IT 安全架构及应用部署、跨境数据传输安全、灾难恢复演练等工作。张帆先生负责本书第 4 章的校对工作。

陈欣炜，具有同济大学工程管理专业本科学历，持有 ISO27001LA 等认证。现任云安全合规职务，负责金融云安全和合规管理等工作。陈欣炜先生负责本书第 5 章的校对工作。

周爱玲，具有长春邮电学院通信工程无线通信专业工科学士学位，持有 CISA 认证，现任企业数字化高级行业经理，负责企业互联网、5G 2B 物联网、云计算、安全管理等数字化建设运营方面的工作。周爱玲女士负责本书部分章节的校对工作。

孙立志，具有石家庄工商职业学院软件技术专业专科学历，持有 CISP-A 等认证。现任安全技术工程师职务，负责信息系统审计、安全咨询、安全服务、渗透测试和教育培训等工作。孙立志先生负责本书部分章节的校对工作。

# 前 言

---

人们在教育和职业生涯中，曾一直痴迷于获取所学和所做一切事物背后的知识。

对于 Sumeet Arora 来说，无论是在印度理工学院获得的科学和工程专业知识，还是在沃顿商学院学习管理，这种广泛阅读某一学科并将跨多个学科的知识点联系起来的好奇心一直都激励着他。长达 22 年的 Cisco System 公司工作经历促成了 Sumeet 帮助建立和扩展互联网的使命。在建立尖端科技以支持互联网发展的同时，作为商业领袖，Sumeet 还看到了网络对于公司以及国家的影响。最近，Sumeet 开始涉足数据和分析领域，这一领域是数字化转型的关键环节。Meenakshi 在其职业生涯中曾从事多项安全技术的开发，涉及本地部署、云计算、边缘基础架构、软件应用程序和企业以及政府机构信息安全，曾通过在自动驾驶车辆方面的工作涉足物联网安全。Ramachandra 对教学抱有热情并将这一核心能力带入本书。此外，Ramachandra 在硬件设计方面、网络和制造业价值链方面具有深厚的知识和经验。

本书的编撰团队借助在网络、数据及其分析、软硬件、安全、物联网和商业方面的多年经验，构建了更广泛的物联网跨域视图。物联网发展势头强劲，从网络技术的角度看待物联网也成为关键和核心。然而，网络和其他技术只是达成最终目标的途径，这就是从数字化转型以及价值链转型的角度编写本书的原因。编撰团队相信这些正是物联网所推动的结果。编撰团队结合对于商业、网络技术、安全和数据分析几个方面的思索，描述通过连接、自动化、分析和改进的活动如何共同改变不同行业的价值链。编撰团队通过使用数字科技来连接、自动化、分析和改进价值链上的每个环节。

数字化转型对世界的影响极其深远。几乎每个行业甚至公共部门都在以很快的速度发生变化。本书的目标是帮助专家们建立起广泛且跨技术的数字化转型知识，从而实现公司和公共部门通过规划物联网的落地达成关键绩效目标，以便更好地适应这个快速变化的世界。所有这些活动都必须安全地完成并以可信安全的平台作为基础。这就是本书广泛讨论安全主题并在物联网系统设计中强调“安全”的原因。

编撰团队也希望通过本书建立起一个学习团队，大家能够相互交流并收获彼此的见解。本书不仅汇集了编撰团队的知识 and 思想，也诚邀专家们提出宝贵意见，进而编撰团队能够更好地在本领域改进并提升。数字化转型和物联网是横跨多项技术的独立领域。编撰团队真诚希望物联网专家们能从此书获益并提供富有建设性的意见，以便不断完善本书。

书中包含的参考网址可通过扫描本书封底的二维码获取。

在此，编撰团队感谢所有家人和同事们对此书出版的大力支持，还要特别感谢为此书内容提供建议和指导的专家们。

Sumeet 和 Meenakshi 还要感谢他们的孩子 Saanvi 和 Krish Arora，感谢他们的父母 Krishan 和 Raj Arora，以及 Jagish 和 Usha Vohra。

Ramachandra 感谢他妻子 Bhagya 在本书写作过程中的无条件支持，也万分感激他的父母和老师。

编撰团队要感谢 McGraw Hill 公司对出版本书的帮助，尤其感谢 Lara Zoble 在撰写本书过程中给予的巨大支持、耐心和激励。2020 年，全世界因为疫情都在封控中。在最坏的这段时期，按时交稿是件很不容易的事。Lara 一直给予编撰团队大力支持，帮助本书顺利完成。编撰团队还想向项目经理 Parag Mittal，编辑主管 Stephen M. Smith，生产主管 Pamela A. Pelton，以及所有其他 McGraw Hill 和 KnowledgeWorks 环球公司的支持人员们致以最诚挚的谢意。没有上述人员的支持，本书就无法出版。

Sumeet Arora  
Ramachandra Gambheer  
Meenakshi Vohra



# 目 录

|                     |    |
|---------------------|----|
| 第 1 章 物联网的演进        | 1  |
| 1.1 数字化转型简介         | 1  |
| 1.1.1 共享汽车          | 3  |
| 1.1.2 语音辅助导航系统      | 4  |
| 1.1.3 使用机器学习的数字购物体验 | 4  |
| 1.1.4 智能医疗健康系统      | 5  |
| 1.1.5 数码即时摄影应用场景    | 7  |
| 1.1.6 制造自动化         | 8  |
| 1.1.7 网联汽车          | 8  |
| 1.2 连接的价值链          | 9  |
| 1.3 什么是数字化转型        | 10 |
| 1.4 物联网简介           | 10 |
| 1.5 物联网系统的基本构建块     | 11 |
| 1.6 物联网的发展          | 13 |
| 1.7 网联汽车案例          | 14 |
| 1.8 总结              | 16 |
| 第 2 章 物联网架构和技术要点    | 19 |
| 2.1 简介              | 19 |
| 2.2 物联网系统架构         | 19 |
| 2.2.1 基础架构平面        | 20 |
| 2.2.2 应用程序平面        | 27 |
| 2.3 物联网技术和协议        | 27 |
| 2.4 将学到的知识运用到网联汽车案例 | 39 |
| 2.5 总结              | 41 |
| 第 3 章 联网机器          | 43 |
| 3.1 简介              | 43 |
| 3.2 机器对机器           | 44 |

|                      |    |
|----------------------|----|
| 3.3 M2M 通信           | 44 |
| 3.4 M2M 的应用场景        | 45 |
| 3.5 M2M 的主要特点        | 46 |
| 3.6 M2M 的架构和组件       | 46 |
| 3.7 M2M 应用通信原则       | 47 |
| 3.8 M2M 的注意事项和相关的问题  | 49 |
| 3.9 M2M 的标准化努力       | 49 |
| 3.10 总结              | 50 |
| 第 4 章 物联网网络架构        | 51 |
| 4.1 简介               | 51 |
| 4.2 网络术语             | 51 |
| 4.3 ISO-OSI 参考模型     | 55 |
| 4.4 网络协议             | 58 |
| 4.5 广域网架构            | 59 |
| 4.5.1 广域网技术类型        | 59 |
| 4.5.2 IP 网络          | 60 |
| 4.5.3 Ethernet 上的 IP | 62 |
| 4.6 MAC 源地址          | 63 |
| 4.7 数据接收             | 66 |
| 4.8 多协议标签交换          | 67 |
| 4.9 数据中心             | 70 |
| 4.10 数据中心网络          | 71 |
| 4.11 物联网网关           | 72 |
| 4.12 总结              | 75 |
| 第 5 章 物联网硬件设计基础      | 77 |
| 5.1 简介               | 77 |
| 5.2 硬件系统需求           | 77 |
| 5.3 硬件功能规范           | 79 |

|              |                      |            |
|--------------|----------------------|------------|
| 5.4          | 软件功能规范               | 80         |
| 5.5          | 硬件组件选择               | 80         |
| 5.6          | 可制造性设计               | 85         |
| 5.7          | 可测试性设计               | 86         |
| 5.8          | 原理图、布局和 Gerber       | 88         |
| 5.9          | PCB 制造和组装            | 90         |
| 5.10         | 硬件设计流程总结             | 91         |
| 5.11         | 将学习内容应用于互联车辆使用案例     | 91         |
| 5.11.1       | 系统规范                 | 92         |
| 5.11.2       | 硬件功能规范               | 92         |
| 5.11.3       | 软件功能规范               | 92         |
| 5.11.4       | 组件选择                 | 94         |
| 5.11.5       | 物联网视觉系统              | 94         |
| 5.12         | 商用物联网设备示例            | 95         |
| 5.12.1       | 家庭自动化应用              | 95         |
| 5.12.2       | 监测装置                 | 97         |
| 5.13         | 硬件组件配置使用的标准          | 99         |
| 5.14         | 物联网应用场景的网络硬件选择       | 103        |
| 5.15         | 物联网硬件安全              | 104        |
| 5.16         | 总结                   | 105        |
| <b>第 6 章</b> | <b>物联网数据系统设计</b>     | <b>107</b> |
| 6.1          | 简介                   | 107        |
| 6.2          | 物联网数据系统              | 107        |
| 6.3          | 价值链活动产生数据            | 108        |
| 6.4          | 运营数据：传感器和设备          | 109        |
| 6.4.1        | 传感器用途和传感器数据          | 109        |
| 6.4.2        | 传感器数据特性              | 110        |
| 6.5          | 业务和消费者/用户数据          | 110        |
| 6.6          | 运营数据与业务数据的交集         | 111        |
| 6.7          | 结构化与非结构化数据           | 111        |
| 6.8          | 数据系统设计               | 112        |
| 6.9          | 数据传输                 | 112        |
| 6.10         | 数据收集                 | 112        |
| 6.11         | 数据存储                 | 113        |
| 6.12         | 数据准备                 | 114        |
| 6.13         | 为分析整理数据              | 114        |
| 6.14         | 数据湖、数据仓库和数据的高效访问     | 115        |
| 6.15         | 分析和商业智能              | 115        |
| 6.16         | 数据科学与物联网             | 116        |
| 6.16.1       | 不同的物联网数据科学           | 116        |
| 6.16.2       | 数据科学成功因素             | 117        |
| 6.17         | 机器学习                 | 118        |
| 6.18         | 建立物联网数据系统            | 118        |
| 6.19         | 学以致用：网联汽车案例          | 119        |
| 6.20         | 总结                   | 121        |
| <b>第 7 章</b> | <b>物联网：可信与安全的设计</b>  | <b>123</b> |
| 7.1          | 简介                   | 123        |
| 7.2          | 为什么需要安全的物联网系统        | 123        |
| 7.3          | 安全的物联网系统需求           | 124        |
| 7.4          | 物联网设备安全              | 125        |
| 7.5          | 可信物联网设备              | 126        |
| 7.6          | 可信的设备身份              | 127        |
| 7.7          | 物联网设备安全存储            | 127        |
| 7.8          | 安全启动与可信执行环境          | 127        |
| 7.9          | 信任根                  | 128        |
| 7.10         | 可信的固件与软件             | 128        |
| 7.11         | 公钥基础架构               | 128        |
| 7.12         | 可信供应链                | 129        |
| 7.13         | 安全随机数生成器             | 129        |
| 7.14         | 物联网 D2X 通信安全         | 129        |
| 7.15         | 互相验证的端点              | 130        |
| 7.16         | 安全信道与端到端消息完整性        | 130        |
| 7.17         | 安全持续监测系统             | 131        |
| 7.18         | 物联网设备到云端的安全          | 131        |
| 7.19         | 物联网数据安全策略与法律法规监管合规要求 | 131        |
| 7.19.1       | 物联网数据安全              | 131        |
| 7.19.2       | 物联网设备数据防护            | 132        |

|                               |            |                                 |            |
|-------------------------------|------------|---------------------------------|------------|
| 7.19.3 物联网用户隐私 .....          | 132        | 8.9.6 可观察性 .....                | 148        |
| 7.19.4 物联网云端数据保护 .....        | 132        | 8.9.7 应用程序安全 .....              | 148        |
| 7.20 物联网可信平台 .....            | 133        | 8.10 价值链工作流的自动化 .....           | 149        |
| 7.21 安全身份验证 .....             | 134        | 8.11 边缘计算和云计算 .....             | 149        |
| 7.21.1 密钥的安全配置 .....          | 134        | 8.12 学以致用：网联汽车<br>案例 .....      | 150        |
| 7.21.2 安全 Web 接口 .....        | 134        | 8.13 总结 .....                   | 151        |
| 7.21.3 安全移动应用程序 .....         | 134        |                                 |            |
| 7.21.4 安全 API 网关 .....        | 134        | <b>第 9 章 跨行业物联网应用案例 .....</b>   | <b>153</b> |
| 7.22 端到端安全(含第三方) .....        | 134        | 9.1 简介 .....                    | 153        |
| 7.23 学以致用：网联车辆<br>案例 .....    | 134        | 9.2 制造业 .....                   | 155        |
| 7.24 总结 .....                 | 136        | 9.2.1 汽车制造业 .....               | 155        |
| 附录 物联网网络安全威胁与<br>风险审查案例 ..... | 136        | 9.2.2 电子制造服务 .....              | 158        |
|                               |            | 9.3 网联汽车 .....                  | 160        |
| <b>第 8 章 自动化 .....</b>        | <b>141</b> | 9.4 智能海港 .....                  | 162        |
| 8.1 简介 .....                  | 141        | 9.4.1 智能海港管理 .....              | 162        |
| 8.2 物联网设备的生命周期<br>管理 .....    | 142        | 9.4.2 用物联网管理集装箱 .....           | 163        |
| 8.2.1 预置和配置 .....             | 142        | 9.5 智能机场 .....                  | 165        |
| 8.2.2 运营 .....                | 142        | 9.5.1 旅客追踪 .....                | 166        |
| 8.2.3 维护 .....                | 143        | 9.5.2 行李追踪 .....                | 167        |
| 8.2.4 退役 .....                | 143        | 9.5.3 机场安全保障 .....              | 167        |
| 8.3 零接触物联网设备 .....            | 143        | 9.6 医疗健康系统无人机 .....             | 167        |
| 8.4 即插即用物联网设备 .....           | 144        | 9.7 物联网在石油天然气行业<br>的应用案例 .....  | 172        |
| 8.5 物联网 SIM 卡和管理 .....        | 144        | 9.8 总结 .....                    | 174        |
| 8.6 商用物联网控制软件 .....           | 144        |                                 |            |
| 8.7 物联网网络架构的安全<br>自动化 .....   | 144        | <b>第 10 章 物联网案例集锦 .....</b>     | <b>175</b> |
| 8.8 物联网应用软件设计原则 .....         | 145        | 10.1 银行物联网 .....                | 175        |
| 8.9 云原生软件 .....               | 146        | 10.2 农业物联网 .....                | 177        |
| 8.9.1 Linux .....             | 147        | 10.3 增强型智能家居(家居<br>自动化) .....   | 178        |
| 8.9.2 虚拟机 .....               | 147        | 10.4 智能制造 .....                 | 179        |
| 8.9.3 容器 .....                | 147        | 10.5 医疗物联网 .....                | 180        |
| 8.9.4 Kubernetes .....        | 147        | 10.6 配备智能汽车和智能家居的<br>智慧城市 ..... | 181        |
| 8.9.5 持续集成和持续交付 .....         | 148        | 10.7 智能电网 .....                 | 181        |

# 第1章

## 物联网的演进

本章首先通过简单的现实世界示例讨论数字化转型的概念。通过学习这些真实案例，安全专家们能够了解什么是物联网(Internet of Things, IoT)以及其所连接的价值链。接下来，还将探讨物联网的基本构建块(Building Block)。本章重点介绍基本的物联网单元，这些单元将在本书中作为物联网结构中的核心单元。本书所有章节都使用相同的案例，以便将本书所有的知识都运用到真实案例中。

### 1.1 数字化转型简介

标准普尔 500 指数(S&P 500, 又称 S&P)是衡量在美国证券交易所上市的 500 家大型公司股票表现的股票市场指数。标准普尔 500 指数是最受关注的股票指数之一，业内认为，标准普尔 500 指数不仅是美国股市的最佳代表之一，能否入选标准普尔 500 指数也是衡量一家企业是否成功的标准。

计算标准普尔 500 指数值的公式为

$$\text{指数水平} = \frac{\sum P_i \cdot Q_i}{\text{除数}}$$

其中， $P$  是指数中每只股票的价格， $Q$  是每只股票的公开可用股票数量。除数在股票发行、分拆或发生类似结构变化的情况下有所调整，以确保此类事件本身不会改变指数值。图 1.1 是 1950—2016 年的标准普尔 500 指数。有关标准普尔 500 指数的更多信息，请访问网址 1.1。

在标准普尔 500 指数中，公司平均寿命已经从 1950 年的 60 年下降到现在的不到 20 年。技术的快速革新以及技术自身的快速迭代是各行业公司变革步伐加快的主要原因。预计随着数字化转型的深入发展，变化的速度只会进一步加快。

数字化转型(Digital Transformation, DT)正在席卷各行各业的价值链，甚至改变了政府为民众服务的方式。在所有行业或者政府部门中，“价值链”(Value Chain)都是指投入价值用于创造产品或服务，进而通过产品或服务交付更高价值的一系列活动。产品价值

链示例如图 1.2 所示。运营为入库的产品或服务增加价值，最终通过营销和销售渠道将产品交付给客户。

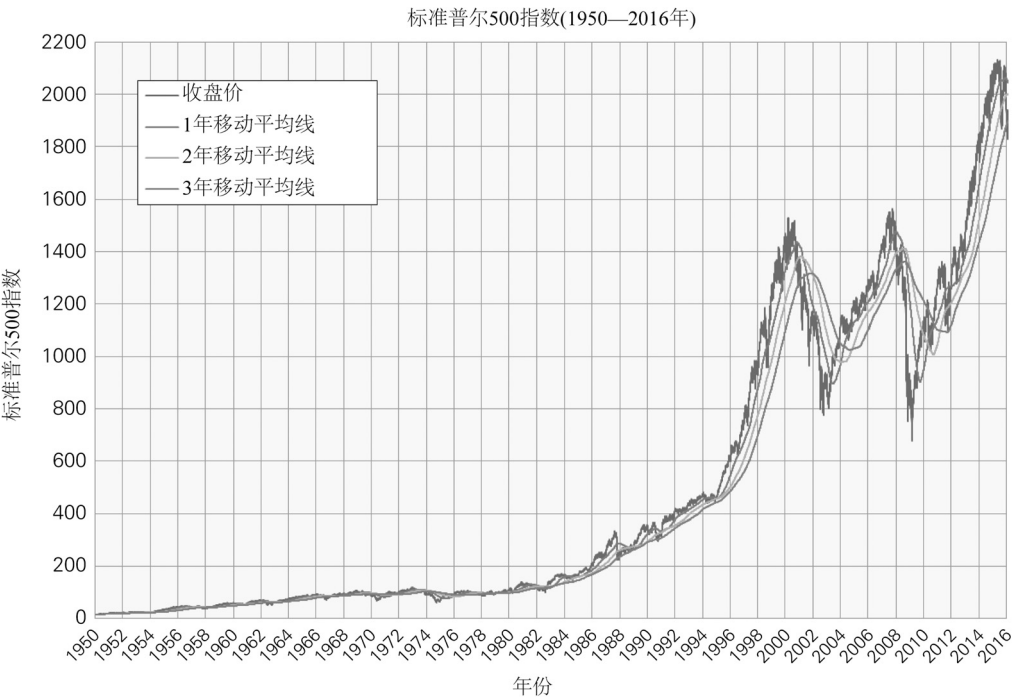


图 1.1 标准普尔 500 指数收盘价(1950—2016 年)以及 1 年、2 年和 3 年的移动平均线  
(由 Overjive-Own 提供, CC BY-SA 4.0)



图 1.2 产品价值链示例

数字化转型是通过数字技术实现的，这些数字技术有助于将整个价值链延伸到消费端，帮助完成价值的交付和反馈自动化、价值链的数据分析工作，帮助改善价值链内和行业的生产效率、成本以及价值交付。互联网、移动通信、传感器和运营技术、物联网、云平台基础架构、自动化和分析正在随集成化的趋势逐渐结合，以实现跨行业和政府的价值链的连接、自动化、分析和改进。

1.1.1 共享汽车

物联网能够帮助实体进行连接，实现自动化和分析，并不断提高其为最终客户提供的价值。要研究数字化转型的影响，需要了解各行各业的示例。先来看看共享汽车是如何改变交通部门的。几年前，人们乘坐出租车需要拨打运营公司的电话预订时间。出租车的可用性和定价由持有执照的出租车行业和可用车辆的数量决定。过去的运营模式存在司机与乘客的联系有限，乘客对自身体验的反馈也很有限的问题。同时，用于需求、供应、体验、乘车时间、交通状况、价格敏感度和安全等因素的数据很难收集和分析，且成本高昂。随着共享汽车(Uber、Lyft 等)的出现，乘客可与服务提供方(司机)实时按需地连接起来——掌握需求(乘客需求，即乘客想去的地方)、寻找供应(可让乘客到达目的地的司机)、匹配合适的司机(基于优化算法)、实时持续监测行程的工作流程、付款和收集乘客及司机的体验数据都是自动处理的。图 1.3 显示了共享汽车应用程序的示例。整个工作流程可达成收集数据，持续分析，并提升乘客体验、司机体验、收入水平以及平台规模和盈利能力等。因此，交通行业受到了前所未有的颠覆，这就是物联网和相关技术所展示出的颠覆性力量。

物联网所使用的资产包括云计算平台(平台托管的物理位置)、移动通信(司机和乘客的智能手机)、定位服务(定位司机和乘客的位置)和在线支付服务。平台、汽车、司机和乘客都可被视为组成网络的连接实体。

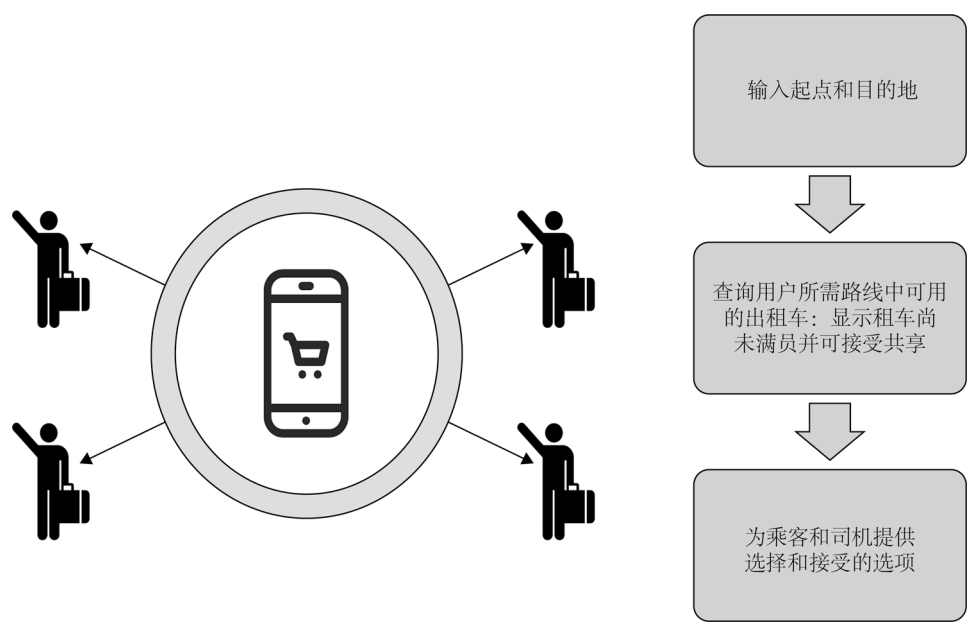


图 1.3 共享汽车应用场景

1.1.2 语音辅助导航系统

再来看看其他示例。20 世纪 90 年代初，人们出行常带着纸质、雅虎或美国汽车联合会(AAA)的地图。但现在是什么情形呢？无论是智能手机或车载信息娱乐系统都有基于 GPS 的地图，如谷歌地图，可显示从起点到目的地的驾驶路线，导航可显示随着移动而动态变化的实时交通状况，并提供语音指导。地图服务数字化转型的价值不仅已从离线纸质地图大幅提升到在线实时导航，还可优化实时交通状况。图 1.4 是谷歌地图导航的示例，可根据当前的实时交通状况为车主提出更佳的路线建议。

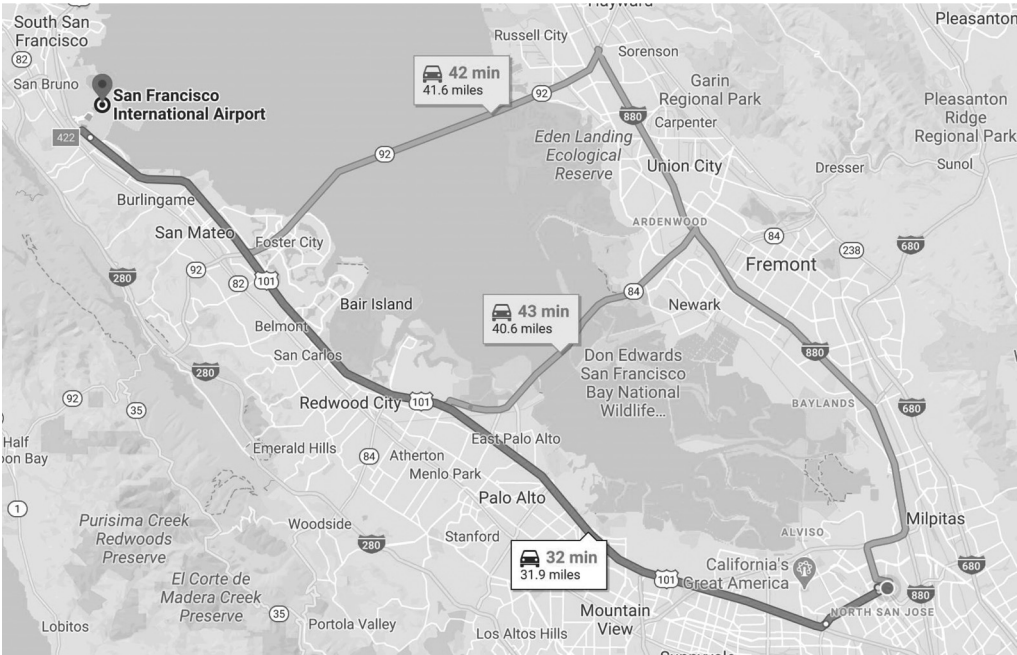


图 1.4 谷歌语音辅助地图(图片来源：网址 1.2)

1.1.3 使用机器学习的数字购物体验

现在，在线购物完全改变了客户的购物体验。许多在线购物门户网站允许用户全天候购买商品，甚至会根据用户的需求提供建议。通过移动购物应用程序，用户可通过上传自己的图片实现虚拟试衣功能。图 1.5 是智能手机的虚拟试衣类应用程序屏幕截图。



图 1.5 智能设备的在线购物应用程序

这些技术和应用程序可提升用户的在线购物体验，令体验过程更加生动，更贴近真实的线下商店购物体验。当用户在搜索引擎中查找商品时，商品的数字广告就开始出现在用户浏览的其他网站中。用户相关性和个性化算法(机器学习算法)完成了这一功能。一旦用户在线确认订单，就可在智能手机上轻松获得所有跟踪信息，直到商品送到用户的家门口。从挑选商品到交付给用户的整个价值链都实现了数字化的跟踪和改进，以帮助获得更好的用户体验。几乎所有运输提供方(航空、公路或铁路)都有自己的用户界面应用程序，用户可在智能手机上自由选择应用程序提供的所有服务，从预订旅行到跟踪旅程直至抵达最终目的地。图 1.6 选取了几个示例，用户通过使用手机应用程序将获得无感知的在线交易和体验。

#### 1.1.4 智能医疗健康系统

接下来探讨医疗健康系统。以前，患者预约医生，需要提前打电话到医生办公室，先了解医生是否有时间，再预约医生的时间。如今，患者只要拥有一部智能手机，就能通过医疗机构的应用程序预约甚至自动付款。有些医疗健康应用程序在启用后，会自动检测患者是否到达医生办公室，并为患者办理登记手续，并将用户列入候诊患者名单。检测结果也可通过应用程序获悉且可随时查看。有些医疗健康应用程序还提供提醒服务，以免用户错过预约。还有一个加强医患价值链的示例，药房的处方药品预配自动化改变了整个医疗健康系统的应用场景，旨在帮助患者在预约、等待时间和获取医疗信息方面获得更好的体验。图 1.7 是医院或者医疗机构办公室中的患者候诊监视屏的示例。图 1.8 是智能手机上医疗健康应用程序的屏幕截图示例。



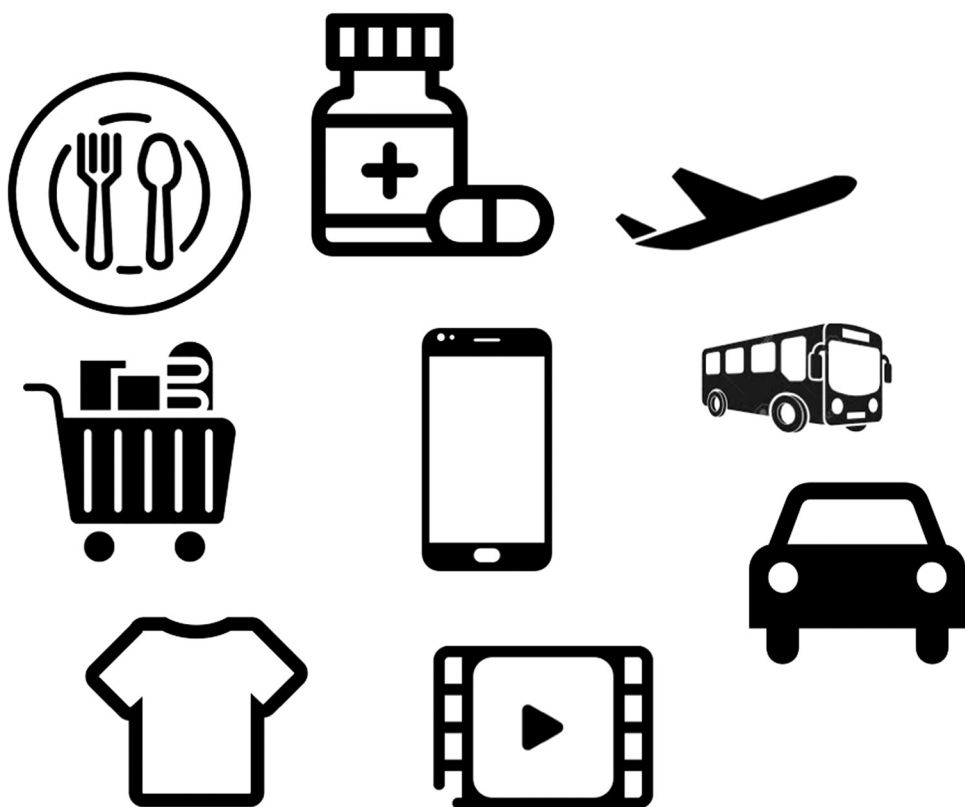


图 1.6 在线购物应用程序



图 1.7 患者候诊监视屏



图 1.8 智能手机中的医疗健康应用程序

1.1.5 数码即时摄影应用场景

摄影师们应该还记得在 20 世纪 90 年代的经历。那时，使用配备胶卷的手动单反 (Single Lens Reflector, SLR) 相机拍摄照片是一项大工程。从购买胶卷到冲洗底片和打印照片的费用相当昂贵，与家人和朋友即时分享照片更只是一个梦想。此外，图片质量只有在胶片显影和冲印后才能知道，有时，当拿到照片时，人们才会发现：由于某个失误，重要照片的拍摄效果很差。现今的人们无法体验到这个场景。如今的情况是，通过用自己的智能设备，可以随时随地拍摄绝对高质量的照片，并在几秒钟内分享到全球各地。这之所以成为可能，是因为在摄影中使用了数字技术以及在云端存储和共享照片，如图 1.9 所示。

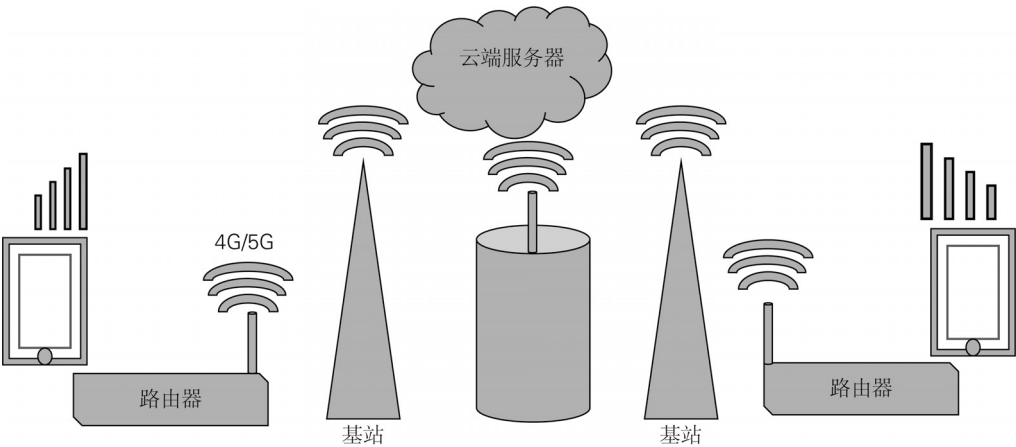


图 1.9 使用智能手机拍照并共享/保存到云端

### 1.1.6 制造自动化

对于任一行业，如汽车、制药或电子制造服务(Electronic Manufacturing Service, EMS)的制造部门，自动化能够提高生产效率和产品质量，这也是数字化转型的另一个示例。

如图 1.10 所示，在制造过程中，机器人拾取并放置部件，完成装配过程，同时，机器人由相互连接的各个加工机器所控制。在全自动流水线中，第二台机器的加工过程取决于第一台机器的加工结果。



图 1.10 制造自动化实例(图片来源：网址 1.3)

### 1.1.7 网联汽车

网联汽车解决了交通和道路安全方面的许多现实问题。如今，大多数汽车都有数百个传感器连接到发动机控制单元(Engine Control Unit, ECU)和车身控制单元(Body Control

Unit, BCU)。数传感器都支持 IP 网络，允许互联交互并与外部设备通信。支持 IP 的传感器与道路上的其他车辆通信并发出警报以规避碰撞。这种通信不仅提供了道路安全，而且还有助于交通管控。图 1.11 阐述了网联汽车的概念。

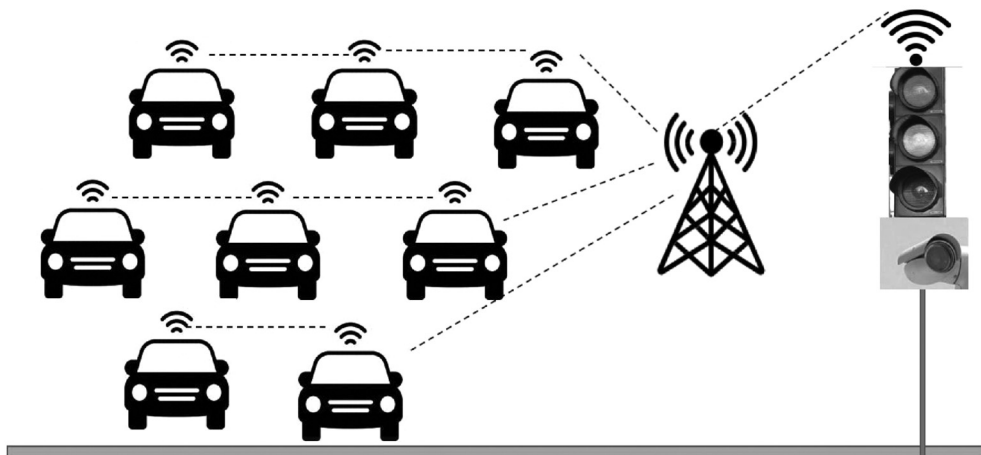


图 1.11 网联汽车

数字化转型能够颠覆的领域十分广泛，凡能想到的应用场景都可考虑实现数字化。数字化转型已经彻底改变了人类的生活方式乃至世界的方方面面。

在行业整体考虑中，公司需要专注于运用数字技术连接运营资产，在包括客户在内的整个价值链中实现工作流的自动化，并投资数据分析以提高价值链的生产效率和用户体验。

## 1.2 连接的价值链

请回顾价值链的概念。例如，咖啡店使用咖啡豆和多种食材，通过咖啡机以及咖啡师的专业知识为客户制作饮料。这杯咖啡所赚取的价格要高于制作过程中所有投入的成本。当获得的价格超过所有投入的总成本时，价值就创造出来了。价值链中的创新通常通过改变创造的价值(如显著提高赚取的价格)和/或产生的成本(如大幅降低投入成本)以创造价值。图 1.12 展示了从获取咖啡豆到制备咖啡的价值链创造示例。

需要记住的一个关键点是，企业必须将产品的客户和用户纳入价值链背后的数据链之中。了解谁是实际消费者非常重要，必须尽一切努力连接和收集来自实际最终消费者的数据。



图 1.12 价值链的创建

## 1.3 什么是数字化转型

数字化转型是运用数字技术来连接、自动化、分析和改进价值链的各个方面。在产品领域，数字化转型涵盖了从产品研发到产品部署，以及客户和用户消费的整个产品生命周期。商业中的数字化转型正将数字技术应用于商业的每个方面和每个阶段，包括分析和处理来自商业(产品或服务)生命周期各部分的数据。

## 1.4 物联网简介

物联网指的是连接智能事物的网络系统，物联网能够帮助实体发送和接收数据以及指令。“物”(Thing)包括从烤面包机到汽车、打印机、闹钟、温度计、电话和各种机器的所有事物，当然，列表还不止于此。物联网期望将任何有价值的“物”连接到互联网，以便能够创建更好的价值链和更好的体验。“物”的概念甚至包括人类！

例如，当人们早上醒来时，闹钟将通知用户实时交通情况，同时将交通情况同步至用户的汽车，然后将导航汽车行驶到路况较好的道路，并且，汽车还会收到可用停车位的数据，当然，这一切都无须人工干预和输入信息。或者，打印机在工作时收到提示彩色墨盒电量不足的警报并自行订购墨盒。这只是物联网工作的几个示例，但目前，物联网技术提供的潜力仅处于应用场景的初始阶段。心脏等器官的医疗传感器已经与互联网连接，传感器帮助医生获得有关患者健康的实时告警信息，告警信息可用于挽救人们的生命。另一方面，物联网信息也引发了大众对个人隐私、数据安全、信息安全和人身安全

全的担忧，人类社会需要一套可信的物联网平台。

## 1.5 物联网系统的基本构建块

物联网系统的基本构建块已经使用了一段时间，而作为控制系统的互联系统则在工业自动化方面运行了更长时间，甚至人类的身体也是一套运行良好的控制系统。尝试理解这样一套闭环系统，假设人们在工作时感到饥饿，大脑从人体的消化系统中得到信号，即饥肠辘辘并期待进食。因此，大脑现在要决定进食方式以及在哪里找到食物。假设可在自助餐厅买到食物，大脑就会向身体提供必要的指令以做出决定。首先，身体会停止当前正在做的工作，大脑发布指令，命令迈开腿步行到自助餐厅。在行走过程中，如果有障碍物，眼睛向大脑提供必要的信号，大脑根据眼睛提供的反馈，指示腿走向正确的路径。整个过程其实是一套闭环反馈控制系统。一旦到达自助餐厅，大脑就会向手提供必要的指令，命令手购买食物和吃饭。手向嘴里喂食时，舌头会感觉到味道。这些动作会一直持续到胃发出“饱”的信号。如果把人体看成一个系统，那么，大脑就是中央处理单元(Central Processing Unit, CPU)，手和腿就是执行器，眼睛和耳朵是传感器，所有这些部分都与 CPU 互连。整个系统在带有闭环反馈系统的命令/响应协议下展开工作。图 1.13 展示了人体的闭环反馈系统。人体是连接系统的一个典型示例，为更好地理解物联网系统打下了基础。

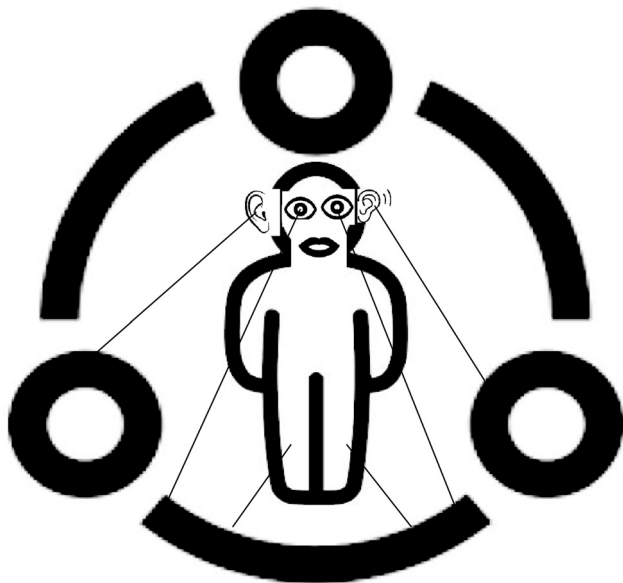


图 1.13 人体的闭环反馈系统

物联网系统可被看作一组连接到 CPU 的传感器和执行器，其中，CPU 接收来自传感器(Sensor)的输入信号，同时向执行器(Actuator)发出指令以执行任务。或许添加一个内存元素将有助于记住指令和数据。在物联网系统中，上述一组基本构建块分布在整个网络中，且规模可以扩展到海量规模和大型网络。

首先定义“物联网单元”(IoT Cell)。物联网单元由作为输入单元的传感器、通过可选存储器确定作为处理/决策的处理单元和作为输出单元的执行器组成。图 1.14 显示了基本物联网单元的结构。本书使用物联网单元描述各种物联网概念。后续章节将详细介绍如何为任何特定的应用程序构建物联网单元的硬件。

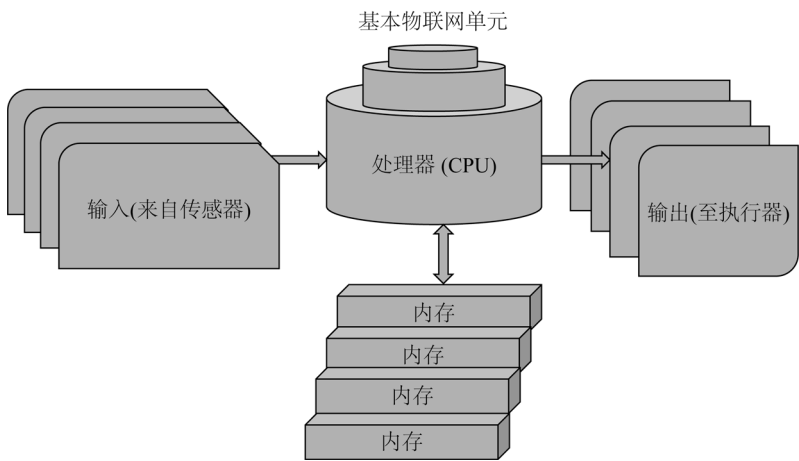


图 1.14 基本物联网单元

通用的物联网系统基本架构如图 1.15 所示。

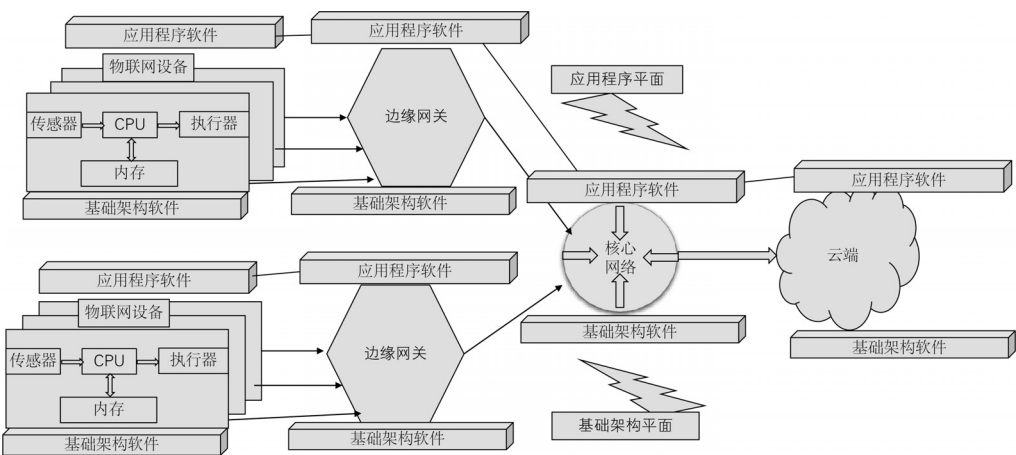


图 1.15 物联网系统的基本架构

传感器和执行器是一种转换器，用于将一种形式的能量转换为另一种形式的能量。传感器将不同类型的输入(如温度和压力)转换为电信号。而执行器将电信号转换为不同类

型的输出,如控制机器的旋转运动。与其他的计算设备一样,CPU 是物联网系统的核心,根据不同的应用场景,可选择合适的 CPU。内存用来存储指令、数据和结果。

第2章将介绍常见物联网应用程序中使用的各种传感器和执行器,以及 CPU 和内存元器件的选择。

## 1.6 物联网的发展

物联网系统可被视为由基础架构平面(Infrastructure Plane)和应用程序平面(Application Plane)组成。基础架构平面由物联网设备(依次包含传感器、CPU、内存和执行器)、网络以及跨边缘和云端的计算资源组成。应用程序平面通常是通过软件实现的逻辑,软件用于处理来自传感器的数据,运用算法和策略来推动和改进,以提高支持物联网的系统创造的价值。

人们致力改善跨行业和政府部门的价值链时,真正追求的目标就是改善所创造的价值和体验,令世界变得更美好。物联网是实现这一目标的手段之一。为了实现这一目标,作为物联网的一部分,人们希望将所有必须在互联网上相互交互且通信的实体连接起来,在价值链中提供安全性,价格更便宜,价值更高。

随着互联网的高速扩张以及越来越多的实体上线,物联网应用场景在过去十年间逐步渗透到各行各业。互联网并不是唯一的推动者,移动通信、云计算、开源软件和分析能力正在共同创造条件,使物联网成为价值的赋能方。如今,在物联网中,计算机程序会处理来自传感器的数据,做出决策并运用决策改进系统功能。

最近的研究表明,到2020年已有超过200亿台设备连接到互联网。物联网创造的价值如此强大,几乎没有任何行业或政府部门免受物联网的影响。根据 Mordor Intelligence (2019)发布的报告,互联可穿戴设备将从2020年的8.35亿台增长到2022年的11.05亿台,如图1.16所示。未来,物联网设备会有更大的规模,而现在才刚刚开始。



图1.16 互联可穿戴设备增长趋势



## 1.7 网联汽车案例

本书将涵盖多个物联网案例，每个主题讲解一个对应的案例，这样可更容易地理解每个主题并加快学习过程。

本书将在所有章节中都使用“网联汽车”这个案例。网联汽车是指能够与外部世界双向通信的车辆。通常，这是用车辆中的互联网连接来完成的，这样数据就可与车辆外部的其他系统共享。从一个点自动(不需要驾驶员)驾驶到另一个预定点的车辆称为自动驾驶车辆(Autonomous Vehicle)。自动驾驶汽车使用各种传感器和执行器以自动驾驶模式运行，无须人工干预。自动驾驶汽车通常也是网联汽车。

根据美国交通部(United States Department of Transportation, USDOT)的研究，仅部署美国交通部正在研发的众多网联汽车安全应用程序中的两个，就可挽救约 1083 条生命。网联汽车使用无线电信号与另一辆网联汽车通信，驾驶员将收到正在接近的交通信号或盲点中存在另一辆车或车辆偏离车道的通知。连接的车辆在与另一辆车通信时会共享移动信息，从而提高道路交通安全。根据美国国家公路交通安全管理局(National Highway Traffic Safety Administration, NHTSA)的研究，网联汽车可能减少 80% 的碰撞事故，从而挽救数百万人的生命并保护数百万人免受伤害。

提供信息的车载娱乐系统称为信息娱乐系统。一般来说，信息娱乐系统将以下(但不限于)功能集成到系统中：

- 收音机(AM 和 FM)
- 带声音控制的音乐播放器(从 CD/USB 驱动器或蓝牙播放音乐)
- 各种车内控制器(如内外温、湿度)
- 连接到手机的蓝牙
- 导航
- 监测来自所连接车辆摄像头的流视频
- 自定义应用程序

信息娱乐面板示例如图 1.17 所示。



图 1.17 车载信息娱乐面板示例

网联汽车将执行以下任务：

- 通过与其他网联汽车和交通控制单元通信以持续监测车辆安全
- 通过持续监测发动机温度、发动机油液位及黏度、冷却液液位(如果使用冷却液)等重要参数，检查发动机的健康状况
- 通过持续监测胎压检查轮胎的健康状况
- 检查车轮平衡
- 监测 ECU 和 BCU 的性能
- 控制器将车辆参数传送给维修代理商并持续获得维修提示

通过网联汽车中必要的物联网单元，可执行上述所有任务以及更多类似任务。后续章节将介绍各种传感器。此刻，可先了解在网联汽车中所使用的一些传感器。假设所有传感器都是数字传感器，即传感器的输出是数字信号。

传感器是将一种形式的能量转换为另一种形式的能量的转换器。例如，温度传感器感测温度并提供与感测温度成比例的数字信号作为输出。控制器读取数字信号，并存储或显示等效温度值。

油压传感器由一个弹簧式开关组成，弹簧式开关与直接暴露于油箱中油压下的膜片相连。油压传感器输出的是一个与油压成正比的数字信号，这个数字信号连接到控制器，控制器将解释信号并存储或显示油压。

距离传感器无须任何物理接触即可检测附近区域中是否有物体存在，这是通过发射电磁波或者在传感器周围形成电磁场实现的。通过拦截磁场或接收信号变化，距离传感器可感知到物体的存在，然后转换为等效的数字信号并将之传送到控制器。控制器使用信号存储和显示对象。安装在车身上的距离传感器可检测物体距离的远近。

图 1.18 展示了安装在汽车中的各种传感器。这些传感器连接到控制器，而控制器通常连接到车辆的 ECU。控制器通过编程感应来自各种传感器的数据并维护车辆的安全和健康。控制器通常使用无线局域网实现双向通信。控制器单元还包括用于存储和处理数据的必要存储器。温度传感器提供温度信息，胎压传感器提供胎压数据。距离传感器可识别附近的任何物体，所提供的数据可用于保障安全以避免碰撞。

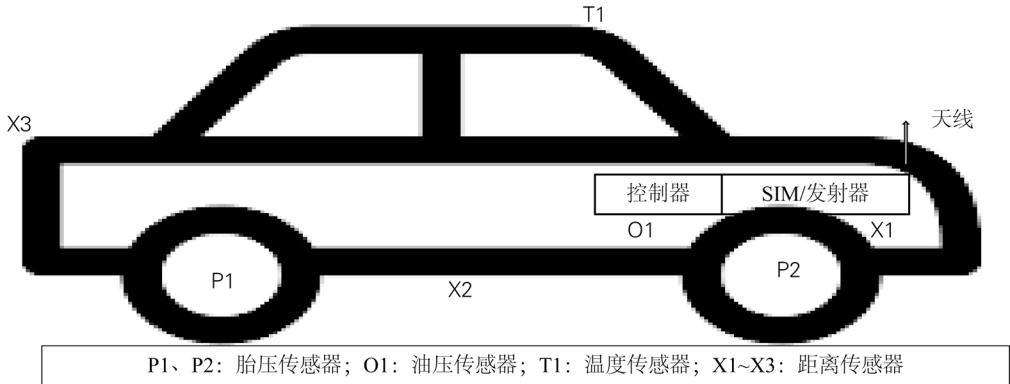


图 1.18 安装在汽车中的各种传感器

遥测(Telemetry)是指从各个远程位置到中央数据收集点(如云服务器)的自动数据采集和无线传输。控制器将车辆数据传输到云服务器以供车辆服务站点使用。网联汽车与当地的交通控制系统通信以确保道路安全,并防止与其他车辆发生碰撞。当车辆检测到附近有其它车辆时,控制器会向驾驶员发出必要的警告信号,并显示在信息娱乐系统屏幕上。图 1.19 展示了网联汽车的遥测和云端处理。

- 网联汽车具有以下关键特征:
- (1) 物联网单元具有必要、合适的传感器,可对车辆执行诊断、启用导航、检测碰撞、辅助安全以及生成用于分析和改进的数据。
  - (2) 车载计算和存储能力帮助软件处理来自传感器的数据并采取行动。

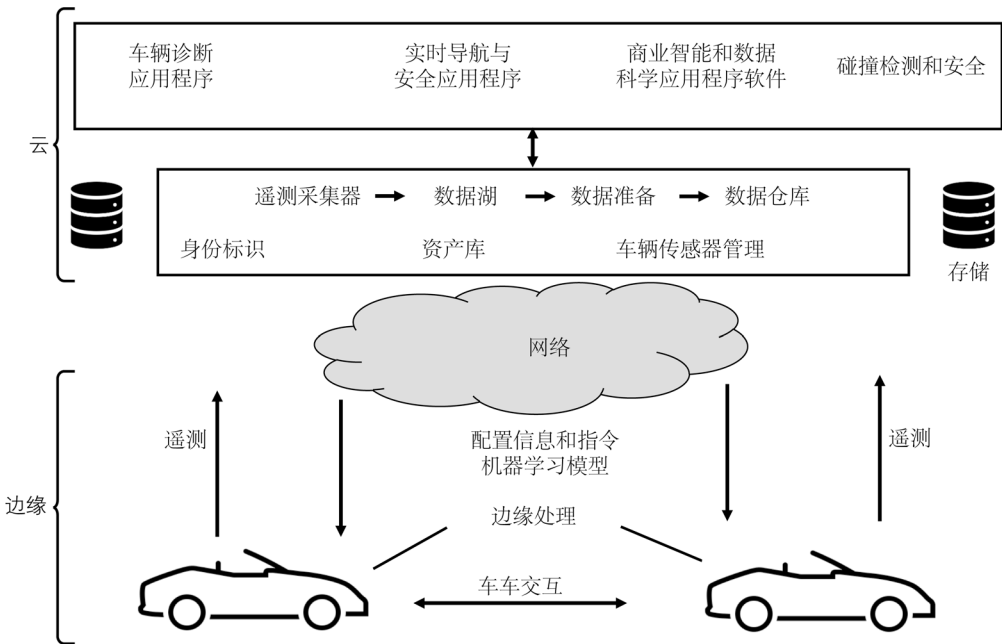


图 1.19 网联汽车

- (3) 与基于云平台的软件系统、其他车辆以及交通系统连接。
  - (4) 分布在边缘和云端的分析系统。
- 车联网是当今时代重要的物联网应用场景,将通过提高车辆安全水平和驾驶员体验改变整个交通运输行业。在阅读本书时,这个价值数十亿美元的市场正在进行数字化转型。

## 1.8 总结

希望安全专家们能够对所介绍的数字化转型、价值链和物联网感到兴奋。接下来的

章节将深入探讨如何构建支持物联网的价值链。第2章介绍物联网架构、基本构建块和所涉及的各种协议。第3章详细介绍联网机器。第4章涵盖网络和网络通信协议。网络是物联网的核心，掌握网络的作用至关重要。第5章讲解与构建物联网单元和物联网系统相关的硬件设计和硬件设计周期的基础知识。第6章介绍数据系统设计。安全、隐私和信任是当今世界关注的重中之重。随着传感器在物联网中生成数据，需要数据系统能够安全、可扩展且经济实惠地处理和存储数据。第7章介绍设计可信与安全的物联网系统。由于物联网涉及跨地域和数量的规模化，因此必须实现自动化。第8章涉及基础架构自动化，包括网络自动化。最后介绍特定于案例的应用程序平面。第9章深入探讨在第2~8章中学习的设计和构建物联网基础设施所支持的案例。第10章通过列举一些真实案例，供安全专家们作为练习尝试。读完本书，安全专家们将获得理解、设计和构建物联网系统所必需的关键知识，这些系统反过来又在很大程度上实现了数字化转型。期待安全专家们多多提出宝贵意见和建议，以逐步迭代的方式完善本书。